50TH ESREDA SEMINAR ON 25 YEARS OF ESREDA SEMINARS

European Safety, Reliability & Data Association

PROCEEDINGS

SAFETY AND RELIABILITY ENHANCEMENT THROUGHOUT EUROPE: LOOKING BACK, LOOKING AHEAD

EDITORS OF THE PROCEEDINGS OF THE 50TH ESREDA SEMINAR

ANTONIO SOLA ROSIQUE
ADOLFO CRESPO MÁRQUEZ

Escuela Técnica Superior de INGENIERÍA DE SEVILLA

UNIVERSIDAD DE SEVILLA

ingeman ASOCIACIÓN PARA EL DESARROLLO DE LA INGENIERÍA DE MANTENIMIENTO

Proceedings Safety And Reliability Enhancement Throughout Europe: Looking Back, Looking Ahead
50th Esreda Seminar

EDITORS: Crespo, Adolfo; Sola, Antonio
Address: Escuela Superior de Ingenieros Camino de los Descubrimientos s/n. 41092 Seville. E-mail: adolfo@us.es

ISBN 978-84-608-9444-5. INGEMAN

Foreword

In recent years there is an enormous progress made by industry and public authorities in reliability and security of systems, new methodologies for risk assessment, advanced research methods to ensure a more stable and safe systems operation, precise methods for predicting assets remaining useful life, better safety and security, innovative procurement processes and improved data management, etc. All these efforts represented a real challenge due to a growing complexity in dynamic market conditions, with continuous relocation of industries to places that would facilitate more competitive production processes. Modern society is much more demanding of energy and raw materials, but at the same time more vulnerable to the impact of emerging products and services.

Over the past 25 years, dependability management frameworks and the corresponding supporting systems have gone through a process of adaptation to these new challenges and opportunities. New products and services are designed, manufactured and tested to meet the needs of their final users within this very exigent society. This is possible thanks to the development of technology, but also thanks to the observation of products behaviour and performance, data analysis and organizational learning.
ESReDA has been a reflection of this very dynamic environment, over the last 25 years, 50 seminars were developed by the association with a wide variety of topics, which were covered with great depth by different experts attending to these international meetings.

This 50th ESReDA seminar has tried to collect some of these experiences accumulated in these 25 years, but also future expectations, including two panels of experts who were discussing these issues. Moreover, the items presented are an approximation to the generated concerns in the field of safety, reliability and data, structured in several areas as follows:

1. Development of practical applications in industry today
a. Criticality analysis in a regasification plant
b. Risks in the early design phase
c. Assessment of seismic risk in NPP
d. NPP operation experience
e. Security impact arising from the conditions of the tramway systems
f. MTTF increases in offshore equipment

2. Methodological Developments
a. Prediction Systems air accident
b. Best practices in maintenance departments
c. Vulnerability and resilience in the supply chain
d. PSA software failures
e. Risk assessment in early design phase
f. Empirical studies of risk
g. Criticality analysis for development of maintenance plans
h. Optimization in building maintenance
i. Dynamic depending on the criticality risk conditions defendant

3. Other issues
a. Risk management, safety and reliability. Past and future

All these perspectives represent wide range of work, and a tremendous effort carried out to improve the effectiveness and efficiency of processes, systems and methodologies, with the intention of improving sustainability of production systems by lowering both, operational and organizational risks, reducing at the same time uncertainty in the decision-making processes.
We do hope that, by reading these papers, young researchers are encouraged to delve into these techniques, to deal properly with existing uncertainty in our industrial practice and society.

Antonio Sola Rosique
Adolfo Crespo Márquez

Editors of the Proceedings of the 50th ESReDA Seminar
Escuela Técnica Superior de Ingenieros de la Universidad de Sevilla
Isla de la Cartuja. Sevilla

Content

1 Transformational Phenomena as Predictors of Aircraft Accidents: What Goes Around Comes Around
Brian E. Smith, NASA Ames Research Center;
Rudi den Hertog, Netherlands Aircraft Company;
Alfred Roelen, Netherlands Aerospace Centre NLR

2 Methodology for continuous best practice application in maintenance departments
María del Carmen Carnero. University of Castilla-La Mancha and University of Lisbon;
Antonio Sola. University of Seville

3 Seismic risk assessment of nuclear power plants: a combination of engineering judgment, legacy design calculations and state-of-the-art numerical simulation
Manuel Pellissetti. AREVA Gmbh – Erlangen, Germany

4 Practical application of criticality analysis in a regasification plant
Javier Serra. ENAGAS, Spain,
Adolfo Crespo. University of Seville, Spain

5 Supply chain vulnerability and resilience – case study of footwear retail distribution network
Tomasz Nowakowski,
Agnieszka Tubis,
Sylwia Werbińska-Wojciechowska
Wroclaw University of Technology, Wroclaw, Poland

6 Modelling Software Failures of Digital I&C in Probabilistic Safety Analyses
Mariana Jockenhövel-Barttfeld,
Andre Taurines,
Yousef Abusharkh
AREVA gmbh – Erlangen, Germany

7 Assessment of risks and uncertainties for concepts during early-phase design of public investment-projects – Outlining the concept of Reversed LCC as a basis for a generalized framework for infrastructure assets
Erling Salicath University of Stavanger, Norway
Vicente González-Prida University of Seville, Spain,
Antonio Guillén University of Seville, Spain
Jayakumar Shambhu, University of Stavanger, Norway.
Adolfo Crespo University of Seville, Spain

8 The impact of system conditions on tramway safety
F.J. Restel,
L. Wolniewicz
Wroclaw University of Technology, Faculty of Mechanical Engineering

9 Change Point Technique Application for a Wind Turbine Malfunction Detection System

Miguel A. Rodríguez, Iberdrola Ingeniería y Construcción, SAU
Luis M. López, Universidad de La Rioja
Nuria López, Iberdrola Ingeniería y Construcción, SAU
Ángel Marín Iberdrola Ingeniería y Construcción, SAU
Antonio J. Fernández Iberdrola Ingeniería y Construcción, SAU

10 Complex Engineering Assets Criticality Analysis for Maintenance Purposes

Khairy Kobbacy . University of Taibah, Madinah. Saudi Arabia. MM BinLadin Chair of Operations and Maintenance
Adolfo Crespo. University of Seville. Department of Industrial Management, School of Engineering
Antonio Sola. University of Seville. Department of Industrial Management, School of Engineering
Pedro Moreu University of Seville. Department of Industrial Management, School of Engineering
Samir Shariff. University of Taibah, Madinah. Saudi Arabia. MM BinLadin Chair of Operations and Maintenance
Juan Gomez. University of Seville. Department of Industrial Management, School of Engineering

11 Do experts agree when assessing risks? An empirical study

Nektarios Karanikas
Steffen Kaspers
Amsterdam University of Applied Sciences / Aviation Academy. The Netherlands

12 ZEDB - A Data Base of Nuclear Power Plant Operating Experience of German Design

G. Becker, RISA
Y. Abusharkh, AREVA

13 Building Maintenance Optimización: Current Gaps and future opportunities Survivability Framework in Network Utilities: A background and practical view

Samir Shariff
Khairy Kobbacy.
MM BinLadin Chair in Operations and Maintenance Technology.Taibah University, Madinah, Saudi Arabia

14 PSA driven Safety Improvements of Nuclear Power Plants

Jörg Blombach, Herzogenaurach, Germany
Hermann Fabian, Erlangen, Germany

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

André Lannoy. Institut pour la Maîtrise des Risques.France

16 Notion of a Dynamic Criticality Concept Adapted to Risk Demanded Conditions

Joel Adams. University of Cambridge, UK
Vicente González-Prida. University of Seville, Spain
Jayakumar Shambhu. University of Stavanger, Norway
Adolfo Crespo. University of Seville, Spain

Annex 1

1 Increase MTBF Indicator of Offshore Equipment by applying new technologies in order to increase Availability and Reliability

Mr. Abbas Ahmad Zadeh , PMO
Mr. Mohammad Ali Rahbari, PMO
Mr. Dezhangah. Consulting Engineers Group

Transformational Phenomena as Predictors of Aircraft Accidents: What Goes Around Comes Around

Brian E. Smith
NASA Ames Research Center
Mail Stop 262-11
94035, Moffett Field, CA, USA

Rudi den Hertog
Netherlands Aircraft Company
Hendrik Walaardt Sacréstraat 433
1117 BM, Schiphol Oost, The Netherlands

Alfred L.C. Roelen
Netherlands Aerospace Centre
Anthony Fokkerweg 2
1059 CM, Amsterdam, The Netherlands

Amsterdam University of Applied Sciences
Weesperzijde 190
1097 DZ, Amsterdam, The Netherlands

Abstract

The Future Aviation Safety Team (FAST) is a multidisciplinary international group of aviation professionals that was established to identify possible future aviation safety hazards. The principle was adopted that future hazards are undesirable consequences of changes, and a primary activity of FAST became identification and prioritization of possible future changes affecting aviation. In 2004, the team finalized a list of 'Areas of Change' (AoC), presenting nearly 150 specific changes that could potentially influence aviation safety. To verify if the AoCs identified in 2004 have indeed become relevant for aviation safety, the FAST analysed worldwide fatal accidents that occurred between 2004 and 2014. The results of the analysis demonstrate that changes catalogued many years previous were directly implicated in the majority of fatal aviation accidents over the past ten years.

Keywords: aviation safety, prognostics.

1. Backgroud

In the 1990s, the Joint Aviation Authorities, Europe (JAA) and the Federal Aviation Administration, USA (FAA) sponsored a number of groups to develop interventions aimed at improving safety of the global aviation system. To further this effort, in early 1998 the JAA launched the JAA Safety Strategy Initiative JSSI (JSSI, 2000). The JSSI mission was the continuous improvement of aviation safety in Europe in particular and worldwide in general, leading to further reductions in the annual number of aviation accidents and thus fatalities, irrespective of the fact that air traffic

will continue to grow. Safety improvements are first achieved through identification of causal factors, or hazards, and then taking the necessary steps to eliminate, avoid, or mitigate these hazards. Hazards are defined as events and/or conditions that may lead to a dangerous situation or events and/or conditions that may delay or impede the resolution of such situations. Three complementary approaches are currently used to identify hazards that affect safety of the global aviation system:

- The "Historic" approach is based on accident and incident investigation and analysis. It uses proven investigative techniques to discover all facts pertinent to a past aviation incident or accident, and thus identify opportunities for improvements meant to avoid future, similar accidents.

- The "Diagnostic" approach is targeted at identifying accident pre-cursors within the larger collections of information in various aviation safety reporting systems. There are many diagnostic processes in use within the global aviation system.

- A "Prognostic" or "Predictive" approach is aimed at discovering future hazards that could result as a consequence of future changes inside or outside the global aviation system and then initiating mitigating action before the hazard is introduced.

In 1999, the JSSI Steering Group established a dedicated working group to develop and implement methods and processes to support the systematic identification of these latter future hazards. That group was called the Future Aviation Safety Team (FAST) and continues to operate today. The FAST core team includes about ten aviation professionals with various backgrounds and expertise from Europe, the U.S. and Canada. Over the years of its existence, the composition of the FAST has changed but several members (including the authors) have been part of FAST since the beginning. In 2004, Bob Kelly-Wickemeyer, Chief Engineer, Safety & Certification, Performance & Propulsion (Boeing retired) credited the FAST with the originating the forensic-diagnostic-prognostic safety triad described above (Kelley-Wickemeyer, 2004). This paradigm has since been embraced by the International Civil Aviation Organization (ICAO, 2013).

2. Areas of change

At the start of FAST, the principle was adopted that future hazards are undesirable consequences of future changes, and the primary objective of FAST became identification and prioritization of possible futures. The team finalized a list of 'Areas of Change' (AoC), presenting nearly 150 specific changes that could potentially influence aviation safety (JSSI, 2000). In this context, changes must be understood as broadly as possible. An AoC is a description of the change, not an identification of the hazards that result from the change. AoCs were subsequently prioritized on numerous criteria, i.e., nature and scope of the change, any trends or profiles present or anticipated timing of the considered change and interactions with other areas.. Prioritization was done using the AHP process (Saaty, 2006) in a series of workshops with approximately 90 aviation professionals. The AoC that came out of this process

as the future change with the highest priority was 'Reliance on automation supporting a complex air transportation system' (FAST, 2001).

The FAST AoC list is re-audited on a regular basis by the FAST core team. In addition, the FAST core team continuously monitors the aviation system and the external environment for new AoCs that may arise – so-called "horizon scanning." The FAST AoC list is publicly available on a website hosted by the Netherlands Aerospace Centre NLR (http://www.nlr-atsi.nl/fast/aoc/) and currently includes 120 AoCs.

Transformations affecting the future aviation system come in two distinct categories.

- Progressive or rapid-onset physical, functional, and procedural changes that stakeholders plan for the aviation system with the deliberate intention of improving throughput, safety and/or efficiency/economics.

- Unintentional technological innovation, shifting operational tasks, subtle changes in organizations or actors in the system, and contextual factors external to aviation itself that can nonetheless influence the robustness of the support systems upon which operational safety depends.

Areas of Change are not strictly limited to the future. They may have begun in the past and actually cease at some point in the future. They also may have begun now and continue into the future, or be not yet in place but begin at some near, mid- or far-term timeframe.

Changes affecting future aviation safety can come from either within the system or from events and circumstances outside aviation – the contextual environment in which aviation operates. Therefore, aviation stakeholders know some transformations, but not others. Those not recognized within the aviation community may nevertheless be known to organizations outside aviation.

Areas of Change are not hazards per se, but may when combined with other technologies, operational concepts or related AoCs be the catalysts for new hazards or modify the probability or severity associated with existing hazards.

3. Verification of Areas of Change relevance

To verify if the AoCs identified in 2004 have indeed become relevant for aviation safety, the FAST analysed worldwide fatal accidents that occurred between 2004 and 2014. The Aviation Safety Network database (https://aviation-safety.net/database/) was used as the initial source of accident information. All fatal accidents involving commercial operations with fixed wing aircraft with a maximum take-off weight heavier than 5,700 kg were included in the analysis. Military, ferry/positioning, air ambulance and agricultural operations were excluded. For each accident, the team determined it if one or more AoCs (with a maximum of three) could be associated with the occurrence. An association does not necessarily mean that the change caused or contributed to the accident. It merely indicates that the AoC was relevant in the sequence of events that ended-up as an aircraft accident. In addition to the Aviation

Safety Network, the team consulted public and non-public sources such as aircraft accident investigation reports, articles in professional magazines (Flight, Aviation Week & Space Technology, etc.) to obtain information relevant for each accident.

The total set included 247 fatal accidents. AoCs were assigned to 178 accidents (72%). For the remaining 69 accidents, none of the AoCs was considered relevant, or a link could not be made because of lack of detailed information about the accident. Of the 120 AoCs that are currently on the list, 43 (36%) could be associated with one or more accidents.

The nine most frequently assigned AoCs are listed in Table I. Note: the automation-related AoC that was given the highest priority in 2004 ended up in this top-eight.

Table I: Area of Change frequency across accident set (FAST AoC number).

Area of change	**Accident count**
Socio-economic and political crises affecting aviation (AoC-265)	48
Operation of low-cost airlines (AoC-125)	44
Smaller organisations and owners operating aging aircraft (AoC-252)	42
Reliance on automation supporting a complex air transportation system (AoC-013)	40
Increasing operations of cargo aircraft (AoC-114)	39
Increasing reliance on procedural solutions for operational safety (AoC-282)	19
Operational tempo and economic considerations affecting flight crew alertness (AoC-205)	16
Accelerated transition of pilots from simple to complex aircraft (AoC-122)	10
Decreasing availability of qualified maintenance staff at stations other than home base of operations (AoC-256)	8

4. Discussion on most frequent Areas of Change

In the following sections, each of the Areas of Change listed in Table I is briefly discussed.

4.1 Socio economic and political crises affecting aviation

The vast majority of the 48 accident aircraft linked to this top scoring AoC come from African operators. The high accident rate in ‘failed states’ such as Sudan and the Democratic Republic of Congo is unacceptable and should be given highest priority by the international aviation community. The strength of the economy of the country of the operator is a dominant influence factor, explaining for most of the differences in accident rates across geographical region (Visser, 1997). This finding indicates that addressing the traditional 'human factor' will not succeed in bringing down accident

rates worldwide if the economic environment in which individual airlines operate (the 'prosperity factor') is left untouched.

Excluding hijackings and external attacks, a mere one in 16 million passengers has been killed on the airlines of the world's 30 wealthiest states and territories during the past 15 years (Economist, 2015). Significant changes in aviation technologies, functions and procedures even if well-intended need to be introduced with great care to avoid destabilizing this safety record. The Aviation Team Looking Ahead at Safety (ATLAS) operating under the aegis of the U.S. Commercial Aviation Safety Team (CAST) meets regularly to assess potential safety impacts of nearer-term changed proposed for introduction in the U.S. In contrast, for carriers of the 30 poorest jurisdictions, the rate was 57 times higher, at one in 283,000 passengers.

4.2 Operation of low cost airlines

This group is about small, low cost airlines that operate anywhere between 3 and 15 aircraft, not the well-established large low cost carriers such as Southwest, easyJet or RyanAir. The regional spread of accidents associated with this group is more diverse than the previous group and includes two accidents in the US and one in Europe.

Analysis of the 42 cases also showed that at least half of the airlines had one or more prior accidents. This suggests that continued airline oversight by the authorities appears to be a difficult issue.

4.3 Smaller organisations and owners operating aging aircraft

Aircraft airworthiness is defined by the remaining service life, measured in years, flight hours and quantity of take-offs and landings; each assessed independently. This is why some aircraft age relatively quickly, due to frequent flights on shorter routes. In theory, there is no concept of an 'old aircraft' in terms of aviation: it is either operable or inoperable. If it is authorized to operate, it should be as safe as an absolutely new airplane. Nevertheless, critical knowledge to carry out operations, maintenance and inspection of older aircraft types, in terms of know-how and know-why, appears to be fading with time.

4.4 Reliance on automation supporting a complex air transportation system

In 2004 the FAST conducted a study of the topic, "Increasing reliance on flight deck automation" at the behest of the JSSI (FAST, 2004a). This study resulted in 21 prioritized (out of 286) hazards that were divided in 4 themes:

- Theme I: Global Air-Ground-Space System Issues
- Theme II: Flight Crew-automation Interactions Issues
- Theme III: General Threats
- Theme IV: Absence of Human Agent (On Board).

The results of further FAST work confirmed these findings, and also the existence of "weak signals", defined as information which could anticipate an event but remains difficult to understand and interpret because of their ambiguous, uncertain and fragmentary characteristics (Guillaume, 2011). Examples of weak signals identified

by FAST are a) that there will be problems with maintaining "hands-on" currency due to future advances in flight deck automation and b) that stress and fatigue will increase rapidly when the flight crew does not understand what flight deck automation is asking the aircraft to do. This information came from a pilot survey among more than 190 respondents, with a mean of 10,000 flying hours and 20 years in the business (FAST, 2004b).

Although the increasing reliance on flight deck automation has been a major factor in the current favourable safety record of western commercial aviation, the misuse/misunderstanding of automation has been implicated in certain high-profile accidents, see Table II.

Table II: Overview of automation surprise in high-profile accidents

	Colgan Air Q400 Feb 12, 2009 (NTSB, 2010)	**Turkish Airlines B737-800 Feb 25, 2009 (DSB, 2010)**	**Air France A330 June 1, 2009 (BEA, 2012)**	**Asiana B777 July 6, 2013 (NTSB, 2014)**	**Air Asia A320 Dec 28, 2014 (KNKT, 2015)**
Automation surprise	Crew surprised by stickpusher operation and responded inappropriately.	Crew unaware that auto-thrust reduction was triggered by faulty radio altimeter.	Aircraft response to control input when in alternate law at high altitude not understood by crew.	Crew failed to recognise that selection of the autopilot mode cancelled the auto-thrust speed protection.	Crew failed to recognise that pulling the circuit breakers in-flight keeps the aircraft in alternate law.

In each of the accidents listed in Table II automation surprises led the crews away from appropriate action. It is yet unclear whether revised training - e.g., upset recovery training-, new procedures or design changes can prevent the occurrence of such cases in the future, because we do not fully understand human decision making in unusual situations (Lamme, 2010). The FAST position has been that better understanding and research into human behaviour and decision making in normal and off-nominal conditions will help to reduce these types of accidents. Such knowledge is relevant for improving flight training and flight deck design.

For many aircraft and ground ATC and space systems now in use, there is a lost appreciation for the fact that these technology systems will be in production and operation far longer than ever conceived by their designers. This in-service 'inertia' acts as a moderator/constraint to automation evolution. Largely due to airline economic factors, the life span of commercial aircraft and their flight decks is known to be much longer than commonly imagined. The projected future fleet of more than 22,000 Boeing 737 and Airbus 320 single-aisle aircraft by 2025 is an example (Airbus, 2015; Boeing, 2015). Thus manufacturers may have reduced incentives to produce aircraft that push technology/automation envelopes. The same constraints will be true for the ground and space "nodes" of the future AGS system under development within the Single European Sky Air traffic management Research (SESAR) and U.S. NextGen air traffic control modernization programs – both highly dependent on automated systems. Increasing heterogeneity will remain a significant factor/disruption to be recognized and appreciated. It will also require preventive

action. Designers, researchers, regulators, and operators may have left the aviation industry long before the last derivative enters service and hence essential information on the subtleties of automation design, related training, and operational lessons learned may be lost.

4.5 Increasing operations of cargo aircraft

Cargo aircraft are disproportionately represented in accident statistics. Nearly all of the fatal cargo accidents in the last decade have involved feeder and ad hoc carriers (GAO, 2009). A study conducted by the Netherlands Aerospace Centre (NLR) and the U.K. Civil Aviation Authority (CAA) in 2000 (Roelen et al, 2001) indicated that there were 2.5 accidents per million large cargo airplane flights in North America, which is nearly five times higher than the accident rate for passenger flights in North America and more than twice as high as the accident rate for cargo flights in Europe.

Cargo flights are not required to meet the same regulations as those for passenger flights. For instance, cargo airline pilots are excluded from the more stringent flight and duty time regulations imposed in the US in 2014.

4.6 Increasing reliance on procedural solutions for operational safety

There is a belief construct that says “we are safe because we followed the rules”, but it's not that simple. For example, except for very few aircraft that have special protections, safety of flight under winter operations is entirely procedure based. A simple instruction (e.g., perform "a tactile check" on the wings) when in ground icing conditions is not enough to prevent accidents. A deeper study is required why certain lessons learned – not just winter operations, but also in other aspects of operation and maintenance - apparently fade away, and the authorities need to investigate if current regulations are indeed adequate. How decisions are made and in what context are of paramount importance. We must better understand the interactions among humans, technical systems and the overall socio-technical context in which the two operate together. This is also where Safety Management Systems (SMS) and mature safety cultures come into play (Fox, 2012).

4.7 Operational tempo and economic considerations affecting flight crew alertness

Flight crew fatigue is traditionally managed by pilot rest and duty limits. FAR Part 117, enacted January 2014, was the first major revision to pilot rest and duty limits in the US in more than 60 years. The regulations are based on scientific knowledge of the effects of fatigue, sleep and circadian rhythms on the human body. ICAO and IATA promote fatigue risk management as a means of ensuring that relevant personnel are performing at adequate levels of alertness. In an FRMS an operator continues to have flight and duty time limitations but these are identified through their own FRMS processes, specific to a defined operational context, and are continually evaluated and updated in response to their own risk assessments and the data the operator is collecting (ICAO, 2011). It is therefore of paramount importance that pilots are free to report instances of fatigue. However, an FAA Office of Inspector General report (FAA, 2011) found that pilots might not be reporting all

instances of fatigue. The report noted that, of 33 air carrier pilots interviewed by OIG researchers, 26 (79 percent) said that, at some time, they had been fatigued while on duty; nevertheless, only eight pilots notified their air carrier of their condition. Among the reasons cited for not reporting fatigue was the fear of punitive action from their employers.

4.8 Accelerated transition from pilots from simple to complex aircraft

Worldwide economic pressures to recruit needed pilots for Part 121 operations will likely result in more rapid transition of trainees from simple to complex aircraft. Current certification standards may need to be revisited in light of this phenomenon. Training curricula must provide the skills needed for command of complex, advanced aircraft. This phenomenon is evident in proposals for Multi-Crew Pilot License (MCPL). Potential concerns are the following (ECA, 2013):

- There is no relevant Air Traffic Control (ATC) simulated environment available to date,
- The currently approved MPL syllabi meet the minimum requirement of 12 real landings and even less in some cases,
- Some currently approved MPL syllabi do not include real Instrument Flight Rules (IFR) flight,
- Some currently approved MPL syllabi do not include asymmetric flight in real aircraft,
- MPL syllabi introduce a global training syllabus timescale reduction, including little to no consolidation time (i.e. time to allow for reinforcing the just acquired skills,
- There is a limited sample of MPL graduates flying the line today,
- There is no proof of capability for a MPL license holder to upgrade to captaincy (no MPL trainee has graduated to Captain yet, and no requirement for Pilot in Command (PIC) task analysis),
- There is scarce/limited data feedback on the performance of MPL cadets and pilots.

4.9 Decreasing availability of qualified maintenance staff at stations other than home base of operation

It is known that technical defects are more often documented in the aircraft technical logbook during flights to a home base than during flights away from home base (Hakkeling-Mesland et al, 2005). The non-availability of qualified maintenance staff at outstations is one of the possible explanations for this phenomenon; pressure to complete flights maybe another.

5. Conclusion

The results of the analysis presented in this paper demonstrate that changes catalogued many years previous were directly implicated in the majority of fatal aviation accidents over the past ten years. Areas of Change as utilized in this paper form a predictive approach that combines the following dimensions (Cagnin and Scapola, 2007):

- Look forward, e.g. through forecasting, trend analysis, gaming and scenarios, futurist writing, etc.

- Look across, e.g. through systemic thinking across multiple domains that reflect technology convergence.

- Look backwards, through historical analogy, previous future-oriented studies, trend, analysis, etc. History is important, although it shouldn't be the sole basis for the identification and analysis of future risks.

- Finally, there also needs to be a) a concerted effort "to prepare" the recipient of the prognostic message(s) and b) continued processing of signalled problems in a follow on team. This is an essential strategy for success.

One major difficulty with the assessment of future risks is to predict the future system with enough certainty and provide a good, complete and trustable description of the future. Although the future can never be entirely predicted, certain changes are likely to happen, such as the introduction of 4D trajectory management and System Wide Information Management (SWIM) into Air Traffic Management. These 'solid' elements can then be combined with less certain elements (e.g. demographics, fuel price changes, socio-technical-cultural factors, etc.) to form various scenarios from collections of future changes.

Collections of changes affecting aviation such as maintained by the FAST can be important catalysts for assessment of the following predictive safety questions:

1. How do the Areas of Change, in isolation or in combination, introduce or affect the hazards and risks from traditional system safety assessments?

2. Are there novel emergent hazards generated by interactions between and among AoCs that could adversely impact the safety characteristics of the future system being assessed? Interactions among these future changes –may weaken critical functions that must be maintained to ensure safe operations. Critical functions are defined as potential pathways leading to successful management of emerging risk rather than simply preventing failure. Assessments that do not appreciate or reflect the consequences of interaction complexity will not be fully informative and can lead to inappropriate trade-offs and increases in other risks (IRGC, 2010).

3. How do the Areas of Change, in isolation or in combination, affect the robustness or resilience of the risk controls (barriers) being considered?

4. The use of AoCs provides a different view on accidents as they happen worldwide since it triggers questions like a) how does the industry ensure information availability for operations, maintenance & overhaul, b) if human factors work will not bring down world-wide accident rates in view of the economic environment, we should review and consider change to the current safety efforts addressing e.g. 'loss of control' accidents.

5. Are there weak signals that should be acted upon?

Areas of Change help an analyst adopt a prospective mind-set: an ability to project oneself into the future; i.e. reflect within a framework that is unknown or uncertain. Many FAST Areas of Change that were identified in 2004 are correlated with the examined set of fatal accidents over the past ten years. The "Prognostic" or "Predictive" approach so in vogue these days aims to uncover such correlations, and the present analysis demonstrates the value of such a look-ahead. Examining future changes enables discovery of future hazards by using collections of change inside or outside the global aviation system. Once such hazards have been identified, mitigating actions can be initiated before the hazard appears. Prognostic hazard identification informs design processes so that the hazards can be eliminated from the future, avoided in the future, or mitigated in the future. The FAST Areas of Change inventory will be a great help in this endeavour.

References

Airbus. (2015). *Flying by numbers 2015 2034*, Global Market Forecast, Airbus S.A.S., Blagnac Cedex, France.

BEA. (2012). *Accident of an Airbus A330-203 registered F-GZCP and operated by Air France crashed into the Atlantic Ocean*, BEA f-cp090601, Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile, Paris, France.

Boeing. (2015). *Current Market Outlook 2015–2034*, Boeing Commercial Airplanes, Seattle, WA, USA.

Cagnin, C., Scapola, F. (2007). *Technical Report on a Foresight Training Course*, EUR 22737 EN, Institute for Prospective Technological Studies, Joint Research Centre, Seville, Spain.

DSB. (2010). *Crashed during approach, Boeing 737-800, near Amsterdam Schiphol Airport, 25 February 2009*. Dutch Safety Board, The Hague, Netherlands.

ECA. (2013). *ECA Position Paper on Multi-Crew Pilot License (MPL)*, European Cockpit Association, Brussels, Belgium.

Economist. (2015). *Par for the course*, 19 Aug 2015. Retrieved on 11 February 2016 from http://www.economist.com/blogs/graphicdetail/2015/08/aviation-safety

FAA. (2011). *FAA and industry are taking action to address pilot fatigue, but more information on pilot commuting is needed*, Audit Report AV-2011-176, Office of Inspector General, Federal Aviation Administration, Washington D.C.

FAST. (2001). *FAST second phase final report*. Retrieved on 20 January 2016 from http://www.nlr-atsi.nl/fast/downloads/

FAST (2004a). *Report on the phase 3 of the work of the Future Aviation Safety Team*, Increased reliance on flight deck automation. Retrieved on 20 January 2016 from http://www.nlr-atsi.nl/fast/downloads/

FAST (2004b). *Airline Industry Survey of Hazards Associated with Reliance on Flight Deck Automation*, Retrieved on 20 January 2016 from http://www.nlr-atsi.nl/fast/downloads/

Fox, K. (2012). The Relationship between SMS and Good Corporate Governance, presented at the *Aviation Human Factors and SMS Wings Seminar 2012*, Pensacola, Florida, September 13-14, 2012.

GAO. (2009). *Better Data and Targeted FAA Efforts Needed to Identify and Address Safety Issues of Small Air Cargo Carriers*. GAO-09-614. United States Government Accountability Office, Washington, D.C., USA.

Guillaume, E.M.E. (2011). *Identifying and Responding to Weak Signals to Improve Learning from Experiences in High-Risk Industry*, PhD thesis, Delft University of Technology.

Halleling-Mesland, M.Y., Bos, T.J.J., Roelen, A.L.C. (2005). *Onderzoek inzake niet-vastleggen technische klachten door vliegers*, NLR-CR-2005-164, NLR Amsterdam. (in Dutch)

IRGC. (2010). *Risk governance deficits: analysis, illustration and recommendations : policy brief*. International Risk Governance Council, Geneva, Switzerland.

JSSI (2000). *Future hazards working group report*, retrieved on 20 January 2016 from http://www.nlr-atsi.nl/fast/downloads/

ICAO. (2011). *Fatigue Risk Management Systems Manual for Regulators*, Doc 9966. International Civil Aviation Organization, Montreal, Canada.

ICAO. (2013). *Safety Management Manual*, Doc 9859, third edition. International Civil Aviation Organization, Montreal, Canada.

Kelley-Wickemeyer, Bob. (2004). *A Large Commercial Jet Transportation Perspective*, presentation to the FAST, 2 March 2004.

KNKT(2015). *Aircraft Accident Investigation Report*. Indonesia Air Asia, Airbus A320-216; PK-AXC, Karimata Strait, Coordinate 3°37'19"S - 109°42'41"E, Republic of Indonesia, 28 December 2014. Komite Nasional Keselamatan Transportasi, Jakarta, Republic of Indonesia.

Lamme, V. (2010). *De vrije wil bestaat niet*. Bert Bakker. (in Dutch)

NTSB. (2010). *Loss of Control on Approach*, Colgan Air, Inc., Operating as Continental Connection Flight 3407, Bombardier DHC-8-400, N200WQ, Clarence Center, New York, February 12, 2009. AAR-10/01. National Transportation Safety Board, Washington, D,C., USA.

NTSB. (2014). *Descent Below Visual Glidepath and Impact With Seawall*, Asiana Airlines Flight 214, Boeing 777-200ER, HL7742, San Francisco, California, July 6, 2013. AAR-14/01 National Transportation Safety Board, Washington, D,C., USA.

Roelen, A.L.C., Pikaar, A.J., Ovaa, W. (2001). An analysis of the safety performance of air cargo operators, *Flight Safety Digest*, Vol. 20, pp. 1-16.

Saaty, T.L. (2006). *Fundamentals of Decision Making; the Analytic Hierarchy Process*. RWS 3 Publications, Pittsburgh, PA, USA.

Visser, H.C. (2013). If I were a rich man…my accident record wouldn't be so bad! In Soekkha, H.M. (ed.), *Aviation Safety*, VPS, pp. 365-389.

Methodology for Continuous Best Practice Application in Maintenance Departments

María Carmen Carnero,
University of Castilla-La Mancha
Technical School of Industrial Engineering, Avda. Camilo José Cela s/n,
13071 Ciudad Real, Spain
University of Lisbon
Instituto Superior Técnico, Avenida Rovisco Pais, 1
1049-001 Lisbon, Portugal

Abstract

This article presents a methodology for choosing best practice or improvement projects in maintenance departments involved in continuous improvement processes. To this end, given that what is not measured cannot be improved, it firstly sets out an audit designed by the Measuring Attractiveness by a Categorical Based Evaluation Technique (MACBETH). The worst-behaved areas are determined from the results. To choose the best combination of projects, an additive multicriteria model has been designed, using two types of benefit (internal and external) and the cost of introducing each project. The multicriteria audit thus created, and the Taguchi loss function, are used in estimating the benefits of each project. From the efficient frontier resulting from all combinations of project packages that might be introduced, and the specifics of the maintenance department, the first project package to be introduced is chosen, and the improvements it would bring to the organization are shown. Through this methodology any organization can become aware of the state of the Maintenance Department, assess where its weaknesses are, plan projects to overcome these deficiencies and control the state of the department once the projects are introduced. This methodology has been applied to the Maintenance Department of a Health Care Organization.

Keywords: Best practice selection. Maintenance audit. MACBETH. Efficient frontier, Taguchi loss function. Health care organization.

1. Introduction

Maintenance departments are currently considered a key element in achieving improvements in availability, quality, safety, environment implications and cost reduction. While this has been known for decades in manufacturing companies, it is not given the same importance in Health Care Organizations.

Nonetheless, hospitals have specific characteristics which require high quality maintenance:

- Technologically highly advanced equipment.
- Large numbers of machines, medical devices and facilities.
- A requirement for very high availability. This guarantees swiftness in carrying out diagnostic tests, reduction in waiting times, etc.)
- A requirement for much greater safety and quality in the operation of systems than in other organizations because of the possible consequences of deficiencies in the working of medical devices on patients and care workers (for example malfunctioning x-ray machines).

Maintenance departments therefore need control tools to detect deficiencies, to assist in solving them, and to propose practical improvements to maintenance efficiency, all within a process of continuous improvement.

Although there are contributions in the literature which analyse project selection using a variety of multicriteria techniques (see Forman and Forman (1987), Forman and Selly (2001), Halouani et al. (2009), Larson and Forman (2007), Liesio et al. (2007), Mavrotas et al. (2006), Mohanty et al. (2005) and Nowak (2005)), and also contributions which apply the efficient frontier to project selection (see Bana e Costa et al. (2005), Birch and Donaldson (1987), Lorenço et al. (2008), Phillips (2004) and Phillips and Bana e Costa (2007)); it should be observed that the choice of practical improvements by multicriteria techniques in not traditionally applied in maintenance departments, and it is particularly unusual in Health Care Organizations.

This article describes a methodology for continuous improvement through the selection of the most efficient practices and projects to be applied in the maintenance department of a Health Care Organization. The benefits of each practice (project) are assessed in two ways: internal benefits, related to process quality, organizational matters, technical questions, etc. and external benefits; these latter are those which directly influence the satisfaction of users (patients) and care staff. To quantify the internal and external benefits for each practice or project a multicriteria audit was constructed using the Measuring Attractiveness by a Categorical Based Evaluation Technique (MACBETH) (Bana e Costa and Vansnick, 1997). Also, in quantifying external benefits, the Taguchi loss function was used. The cost/benefit ratio in practice sets was then used to find the efficient frontier. The analysis of the efficient frontier allows the most efficient set of practices to be chosen.

This paper, therefore, describes an original way of quantifying the improvements achieved by applying maintenance practices, looking at different types of benefits. It also includes an innovative use of the Taguchi loss function in this process. A multicriteria model taking into account costs and benefits gained from the audit is recommended, to obtain, from the benefit/cost ration, the most efficient set of practices.

The layout of the article is as follows: Section 2 shows the characteristics of the audit designed via MACBETH. Section 3 describes the criteria used to choose the most efficient set of maintenance practices (projects). Section 4 describes the possible improvements to be applied in a maintenance department and the resulting efficient frontier. Finally, Section 5 sets out the conclusions.

2. Multicriteria Maintenance Audit

The construction of the audit relies on work from the literature such as Bana e Costa et al. (2012), Carnero (2006), Dixon (1995), Kelly (2006), Mobley (2001) and Wireman (2005).

Maintenance audits are structured according to different criteria: maintenance strategy, attitude of maintenance and other staff, resources and facilities, registers, planning, programming, work orders, purchasing, storage, Maintenance Documentation, calibration, technical issues, effectiveness and control. Each criterion includes a number of subcriteria. Table I shows the number of subcriteria within each criterion. This audit is especially prepared for a Health Care Organization, but could be applied to any kind of business, with some modification. The full list of criteria and their definitions may be seen in Carnero (2015).

Each subcriterion has an associated descriptor. A descriptor is an ordered set of impact levels which can measure, quantitatively or qualitatively, the degree of fulfilment of a subcriterion by an alternative (Bana e Costa and Carvalho, 2002). For example, Table II shows the scale levels of the indicator associated to the criterion Storage space. The descriptors used in this audit are constructed, and are generally qualitative, although in some cases they may be quantitative. In each descriptor there are usually different scale levels, from which the levels good and neutral are identified, and are considered to be reference levels.

Table I: Criteria and number of subcriteria of the audit.

Criteria	**Number of subcriteria**
Attitude	4
Calibration	7
Control	11
Efficiency	9
Human resources	8
Purchases	3
Maintenance documentation	9
Planning	6
Registers	7
Programming	4
Storage	8
Strategy	3
Technical issues	10
Resources	6
Work orders	4

Each subcriterion requires a MACBETH judgement matrix with pairwise comparison of the scale levels of the descriptor. This is done using the MACBETH semantic categories which, in increasing level of attractiveness are: no, very weak, weak, moderate, strong, very strong and extreme. An intermediate value between two semantic categories can also be assigned. Firstly, the most attractive and the least

attractive levels are compared, followed by the second most attractive level with the least attractive, and so on. Then the most attractive level is compared with the remaining levels in order of increasing attractiveness. Then the most attractive level is compared with the second most attractive option, the second most attractive with the third, and so on (Bana e Costa and Chagas, 2004). M-MACBETH software, used to apply MACBETH technique, can detect inconsistencies and suggest modifications. Next, a numerical scale is constructed based on the qualitative judgements with value scores of 100 assigned to the good reference level and zero to the neutral level. Figure 1 shows the numerical scale and the value function corresponding to the subcriterion Storage space.

Table II: Descriptor of subcriterion Storage space

Level	Definition of scale level
The best level of performance (good) L_1	There is more than enough space. There are several storerooms or a central storeroom and secondary storerooms in areas of easy access and which connect quickly with any area of the Hospital. There is sufficient space to use different storage systems (normal shelves, dynamic shelves, moving shelves, rotating storage racks, etc.). There are special stores with a given temperature and pressure, etc., for special supplies. There are hallways with clearance allowing for the use of automatic trolleys and order preparation trolleys. The loading and unloading area of the storeroom is oversized with regard to present needs, allowing several suppliers to be attended to simultaneously. There is office space to control the storeroom.
L_2	There is sufficient space. There are several storerooms or a central storeroom and secondary storerooms in areas of easy access and which connect quickly with any area of the Hospital. There is sufficient space to use different storage systems (normal shelves, dynamic shelves, moving shelves, rotating storage racks, etc.). There are special stores with a given temperature and pressure, etc., for special supplies. There are hallways with clearance allowing for the use of automatic trolleys and order preparation trolleys. The loading and unloading area of the storeroom is suited to present needs, and allows several suppliers to be attended to simultaneously.
Neutral L_3	There is sufficient space. There are several storerooms or a central storeroom and secondary storerooms in areas of easy access and which connect quickly with almost all areas of the Hospital. There is room to use the most appropriate storage system, although it is not possible to introduce different types of shelves. There are special stores with a given temperature and pressure, etc., for special supplies. There are hallways for the use of automatic trolleys and order preparation trolleys. The loading and unloading area of the storeroom is suited to present needs, and only two suppliers may be attended to simultaneously.
L_4	There are some problems of space at specific moments. There is a single storeroom with easy access although it is not possible to reach all areas of the Hospital quickly. Only conventional shelves can be used. There are no special stores with a given temperature or pressure, etc. The hallways allow the passage of people but not of automatic handling systems or the transit of machines and supplies. The loading and unloading area of the storeroom is suited to present needs, and only two suppliers may be attended to simultaneously.
L_5	There are permanent problems of space. There is a single storeroom with normal access and it is not possible to reach all areas of the Hospital rapidly. Only conventional shelving may be used. There are no special stores with a given temperature or pressure, etc. The hallways allow the passage of people but not of automatic handling systems or the transit of machines and supplies. The loading and unloading area of the storeroom is small with regard to present needs, and only one supplier may be attended to at a time.
The worst level of performance L_6	There is no storeroom.

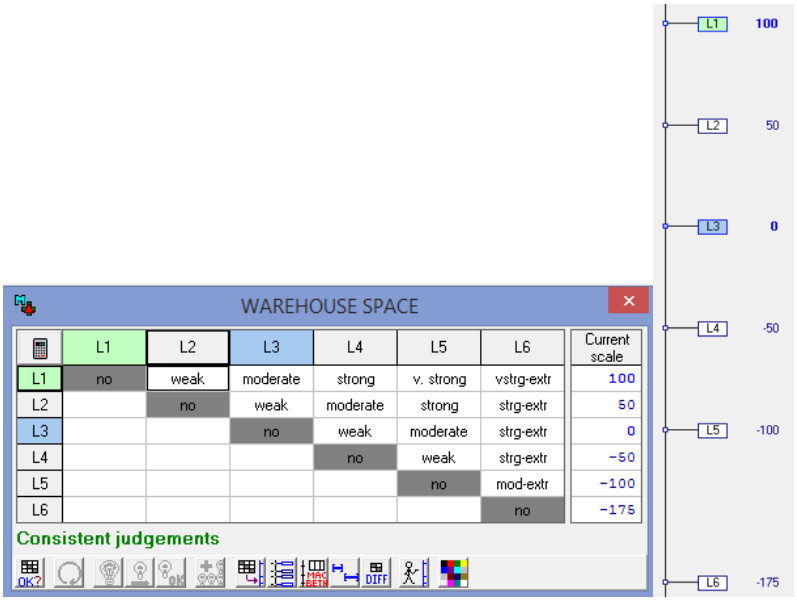


Figure 1. Judgement matrix and value function for Storage space.

The weightings of the different criteria and subcriteria can now be obtained using the MACBETH semantic categories. The MACBETH judgement matrix between the subcriteria of the criterion Storage are shown in Figure 2. The corresponding relative weights adopted for the subcriteria of Storage are shown in the last column in Figure 2.

	[POLICY]	[DATABASE]	[ORGANIZATION]	[CONTROL]	[CRITICITY]	[SPACE]	[ACCESS]	[AUTOMATIZATION]	[all low]	Current scale
[POLICY]	no	no	no	no	no	vweak-weak	weak-mod	mod-strg	positive	15.38
[DATABASE]	no	no	no	no	no	vweak-weak	weak-mod	mod-strg	positive	15.38
[ORGANIZATION]	no	no	no	no	no	vweak-weak	weak-mod	mod-strg	positive	15.38
[CONTROL]	no	no	no	no	no	vweak-weak	weak-mod	mod-strg	positive	15.38
[CRITICITY]	no	no	no	no	no	vweak-weak	weak-mod	mod-strg	positive	15.38
[SPACE]						no	very weak	weak-mod	positive	11.55
[ACCESS]							no	vweak-weak	positive	7.70
[AUTOMATIZATION]								no	positive	3.85
[all low]									no	0.00

Figure 2. Judgement Matrix and weightings of the subcriteria of Storage.

The possible states in which each criterion can be found in a maintenance department are: excellent, satisfactory, acceptable, alarm and catastrophic. Also, the best and worst possible states for each criterion are defined as totally excellent and totally catastrophic, respectively. The limits between each pair of states by area are defined as: limit excellent/satisfactory, limit satisfactory/acceptable, limit acceptable/alarm and limit alarm/catastrophic (see Carnero (2015) for an extension of this idea). The current state of the maintenance department is called "current state".

To quantify the limits between states by criteria, bottom-up and top-down procedures have been used as described in Bana e Costa and Carvalho (2002) and, a variation of them to each criterion (see Carnero 2015 for an extension of the procedures applied). The final limit values obtained by criteria are shown in Figure 3.

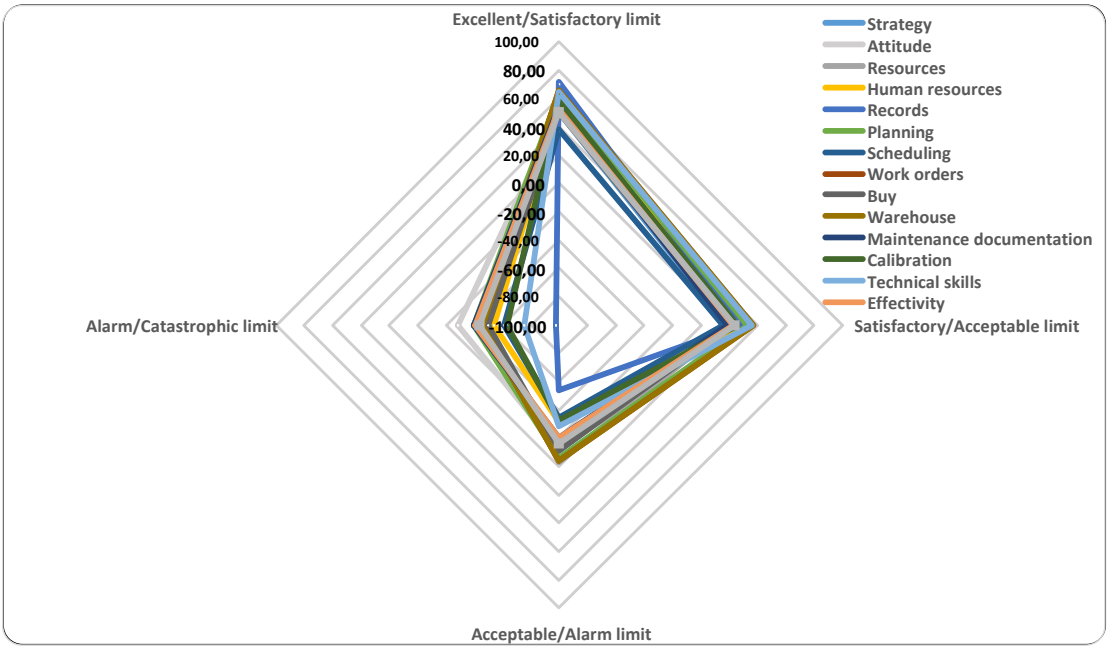


Figure 3. Limit values between states for each criterion.

3. Methodology for the selection of best Maintenance practices

The aim is to obtain an efficient frontier with the best practices or maintenance projects which provide the highest cost/benefit ratio. An additive multicriteria model has been created as shown in Eq. (1).

$$V_i = \sum_j w_j v_{ij} \tag{1}$$

Where v_{ij} is the value associated to alternative i in criterion j and w_j is the weighting assigned to criterion j. In fact, a double weighting is used, following the procedure set out by Goodwin and Wright (1991); in this way the scale amplitudes are equalized between the criteria. Thus, the practices or projects can be compared as they are homogenized to the same scale:

This model uses the criteria Cost and Benefit. Within the criterion Benefit the subcriteria External and Internal benefits were considered.

The external benefits are related to the quality of care provided. This increase in satisfaction of patients and care staff is due to the improvement produced by the maintenance project in matters that directly or indirectly influence quality of care. External quality is related to modifications in opportunity costs, defined as the losses caused by the medical apparatus or devices not fulfilling their function. The Taguchi loss function was used to assess the external quality of the maintenance department. This is done by using Eq. (2) (Taguchi, 1989).

$$L(y) = l * (y - \tau)^2 \tag{2}$$

where $L(y)$ is the loss associated with a value y, l is a loss coefficient, and τ is a target value. In this paper, $L(y)$ is the benefit in quality expected from the implementation of a project, l the effect on the quality of the improvements in the maintenance department subject, y the current value obtained from the maintenance audit in the subject, and τ the target value in the subject desired in a project.

Internal benefits are related to the different subcriteria analysed in the previously described multicriteria audit. In each case of best practice of maintenance project to be introduced, the benefit that may be obtained is quantified when the results of the audit are improved. The estimated values provided by the projects in each criterion are obtained by using Eq. (3).

Internal benefit of a project = (estimated value of the criterion to be applied to a project-current state of criterion) (3)

The cost/benefit ratio r_{ik} is defined by dividing the difference of benefit B_{ik} between one level and the next $B_{(i-1)k}$ into the cost difference, as shown in Eq. (4).

$$r_{ik} = \frac{B_{ik} - B_{(i-1)k}}{C_{ik} - C_{(i-1)k}} \tag{4}$$

The efficient frontier is the curve of the best set of investments or most beneficial package of projects for each level of total cost. The shaded elliptical area of the graph represents all the possible combinations of packages (each comprising three maintenance projects)

4. Selection of improvement projects for the Maintenance Department

The values associated with each descriptor on the Health Care Organization are obtained via a questionnaire with the different levels of the descriptor. Depending on the values obtained from the questionnaire, and considering the weightings of each subcriterion, the current value of the Maintenance Department of the Hospital was found, within the limits between states shown in Figure 3. These current values are shown in Table III.

4.1 Definition of best practices

From the results of the multicriteria audit performed, the worst performing criteria and/or subcriteria can be found. Fourteen good practices or improvement projects are proposed. These have been classified into the following areas:

- Internal projects. Carried out by the staff of the Health Care Organization as they require high levels of skill and broad knowledge of hospital maintenance. The projects defined in this area are:
  - Design a control system for the benefits obtained by the maintenance department relative to availability, quality and safety offered by the Hospital (BC).
  - Design historical records with all the information about the calibrations of sensors and other electronic devices (CA).
  - Analyse the available information on maintenance to determine or update the most relevant parameters for machine and/or devices (DA).
  - Organize a pilot program of total productive maintenance (TPM) in care areas (PM).
  - Produce technical procedures for maintenance activities satisfying standard ISO 9001 (PR).
  - Produce maintenance stock and part lists (RE).
- University projects. Developed with the support of the University. These projects are:
  - Produce technical procedures for maintenance activities and to control them (TP).
  - Apply a multicriteria method to analyse the criticity of maintenance parts (SC).
  - Produce a maintenance manual adapted to the requirements established by the ISO standards (MM).
  - Produce an audit that allows faults and anomalies to be detected during the introduction of the Computerised Maintenance Management system (AI).
- Outsourcing. Projects carried out by specialized consultants. These are some of the projects included:
  - Provide continuous training to maintenance workers on innovative technical questions (TT).
  - Quantify the time necessary to perform maintenance activities (EM).
  - Introduce a predictive program based on vibration analysis (VA).
  - Introduce a program of predictive maintenance based on thermography (TH).

4.2 Selection of good practices

Each combination of maintenance improvement projects is called a package (Goodwin and Wright, 1991). In this article the package is constructed with one practice chosen per area; this is because of time constraints. Each package is thus made up of three improvement projects.

The internal benefits obtained by best practice or projects are estimated from the audit. Each best practice improved only one criterion and in some cases only a subcriterion. The external benefits are obtained by using Eq. (2). The internal and external costs and benefits obtained in each project are shown in Table III. To obtain the total benefits per project, the additive multicriteria model shown in Eq. (1) was

applied. The cost/benefit ratio of each best practice is shown in Table III together with the criterion that each best practice would improve.

Table III: Cost/benefit ratio of the best practices.

CODE (Best practice)	**Cost (€)**	**Internal benefit**	**External benefit**	**Benefit/Cost ratio**	**Associated criterion**
BC	20,000	28.12	15814.69	0.00590	Control
CA	12,000	18.6	3459.60	0.00367	Calibration
DA	12,000	10.26	3459.60	0.00008	Registers
PM	60,000	19.52	19051.52	0.00132	Human resources
PR	20,000	16.65	27722.25	0.00400	Maintenance documentation
RE	12,000	15.38	4730.89	0.00250	Storage
TP	7,200	28.85	39125.03	0.02153	Maintenance documentation
SC	7,200	46.14	191600.96	0.07431	Storage
MM	7,200	16.65	8316.68	0.00444	Maintenance documentation
AI	2,700	12.5	3906.25	0.00000	Control
TT	60,000	9.73	5715.46	0.00000	Human resources
EM	12,000	20.52	21053.52	0.00717	Registers
VA	60,000	33.33	111088.89	0.00540	Resources
TH	50,000	33.33	111088.89	0.00648	Resources

Figure 4 displays the efficient frontier that links the packages with the greatest benefits for a given cost. They define the efficient frontier and will always be on the upper surface of the envelope. The elliptically shaped area of the graph represents the plot of all the possible project packages. Equity software was used to calculate the efficient frontier.

The projects with the highest cost/benefit ratio make up package A; it would be made up of the projects codified as TH, SC and BC. These projects would improve the criteria Resources, Storage and Control. The first two criteria are in a state of alarm and would move to the acceptable and alarm state respectively, while the criterion Control would move to a satisfactory state. The total cost of this package is €77,200 and the benefit is 977.43. A project package B is defined, made up of projects TT, SC and PR. Each of these projects would, on introduction, improve the state of the criteria Human Resources, Storage and Maintenance documentation respectively. These areas are found to be in a state of alarm and with the introduction of these projects would move to an acceptable state. The total cost of this package is €87,200 and the benefit is 614.86. Package C is made up of projects EM, SC and BC. The cost is €39,200 and the benefit is 739. A cheaper package than that proposed (D) would be one made up of the projects EM, SC and CA. The cost would be €31,200 and the benefit 665.30. Packages C and D would both improve two criteria from the alarm state to acceptable.

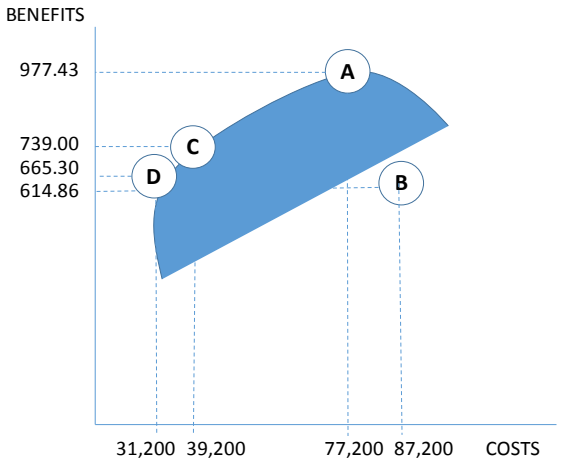


Figure 4. Efficient frontier: the best package (A), preference package (B), a cheaper package (D) and package (C).

Finally package A is chosen to be introduced as it gives an increase in benefit of +58.97 with respect to the project proposed with a decrease in the cost of -11.47 with respect to project P. The increase in benefit provided by this project is held to be more satisfactory that the possible reduction in cost of packages C and D.

The project Store control was developed during 2005 and 2006, and was introduced in the summer of 2006. This is a key project because of the closure of two hospitals which offered health care in the area and the moving of activity to a new hospital in 2004. The project Thermography was introduced in 2008. It detected 102 anomalies in the electro-medical and electrical facilities and the lighting of the hospital. The project Benefit control has been under development since 2006.

Acknowledgements

This research is supported by the Junta de Comunidades de Castilla-La Mancha and the European Regional Development Fund (ERDF) within the project PPII-2014-013-P.

References

Bana e Costa, C.A. and Carvalho, R. (2002) Assigning priorities for maintenance, repair and refurbishment in managing a municipal housing stock. *European Journal of Operational Research*, vol. 138, pp. 380-391.

Bana e Costa, C.A. and Vansnick, J.C. (1997) Applications of the MACBETH approach in the framework of an additive aggregation model. *Journal of Multicriteria Decision Analysis*, vol. 6, no. 2, pp. 107-114.

Bana e Costa, C.A. Carnero, M.C. and Duarte Oliveira M. (2012) A multi-criteria model for auditing a Predictive Maintenance Programme, *European Journal of Operational Research*. vol. 217, pp. 381-393.

Bana e Costa, C.A. and Chagas, M. P. (2004) A career choice problem: An example of how to use MACBETH to build a qualitative value model based on qualitative value judgments. *European Journal of Operations Research*, vol. 15, pp. 323-331.

Bana e Costa, C.A., Fernandez, T.G. and Correia, P.V.D. (2005) Prioritisation of public investments in social infra-structures using multicriteria value analysis and decision conferencing: a case-study, Operational Research working papers, LSEOR 05.78, London School of Economics and Political Science, London.

Birch, S. and Donaldson, C. (1987) Applications of cost-benefit analysis to health care. *Journal of Health Economics*, vol. 6, pp. 211-225.

Carnero, M. C. (2006) Predictive Maintenance Programme Audit with MACBETH. *Safety and Reliability for Managing Risk Conference*, Lisbon, Portugal.

Carnero, M.C. (2015) Methodology for selection of optimal portfolio in maintenance departments. *International Journal of Industrial Engineering: Theory, Applications and Practice*, vol. 22, no. 5, pp. 549-574.

Dixon, J. (1995) *Uptime*. Productivity Press Inc., Portland (Oregon).

Forman, E. and Selly, M. A. (2001) *Decision by Objectives*. World Scientific Press, New Jersey.

Forman, E.H. and Forman, E.A., (1987) Limitations and Extensions of Benefit Cost Analysis, *Proceedings of NATO ASI Conference on Decision Support Systems*, Val d'Isere, France.

Goodwin, P. and Wright, G. (1991) *Decision Analysis for Management Judgement*. Wiley, Chichester.

Halouani, N., Chabchoub, H. and Martel, J.M. (2009) PROMETHEE-MD-2T method for project selection. *European Journal of Operational Research*, vol. 195, no. 3, pp. 841-895.

Kelly, A. (2006) *Maintenance Management Auditing*. Industrial Press, New York.

Larson, C.D. and Forman, E. H. (2007) Application of analytic hierarchy process to select project scope for videologging and pavement condition data collection. *Transportation Research Record: Journal of the Transportation Research Board*, 1990, pp. 40-47.

Liesio, J. Mild, P. and Salo, A. (2007) Preference programming for robust portfolio modelling and project selection. *European Journal of Operational Research*, vol. 181, pp. 1488-1505.

Lorenço, J., Bana e Costa, C. A. and Morton, A. (2008), Software Packages for Multi-Criteria Resource Allocation. *International Engineering Management Conference - Europe*, Estoril, Portugal.

Mavrotas, G., Diakoulaki, D. and Caloghirou, Y. (2006) Project prioritization under policy restrictions. A combination of MCDA with 0–1 programming. *European Journal of Operational Research*, vol. 171, pp. 296-308.

Mobley, K. (2001) *Plant Engineer's Handbook*. Butterworth-Heinemann, Woburn, MA, US.

Mohanty, R. P., Agarwal, R., Choudhury, A. K. and Tiwari, M. K. (2005) A fuzzy ANP-based approach to R&D project selection: a case study. *International Journal of Production Research*, vol. 43, no. 24, pp. 5199-5216.

Nowak, M. (2005) Investment projects evaluation by simulation and multiple criteria decision aiding procedure, *Journal of Civil Engineering and Management*, vol. 11, no. 3, pp. 193-202.

Phillips, L.D. (2004) The Mathematics of Hiview and Equity, 2004. Available from http://www.catalyze.co.uk. [14 May 2004].

Phillips, L.D. and Bana e Costa, C.A. (2007) Transparent prioritisation, budgeting and resource allocation with multi-criteria decision analysis and decision conferencing, *Annals of operations research*, vol. 154, no. 1, pp. 51-68.

Souris, J.P. (1992) *El mantenimiento: fuente de beneficios*. Díaz de Santos, Madrid.

Taguchi. G., Elsaytd. E.A. and Hsiang, T., (1989) *Quality Engineering in Production Systems*. McGraw-Hill, Singapore.

Wireman, T. (2005) *Developing performance indicator for managing maintenance*. Industrial Press Inc., New York.

Seismic risk assessment of nuclear power plants: a combination of engineering judgment, legacy design calculations and state-of-the-art numerical simulation

Manuel Pellissetti
AREVA NP GmbH, PEPS-G
Paul-Gossen-Str. 100
91052 Erlangen, Germany

Abstract

The risk of seismic-induced severe accidents at nuclear power plants (NPP) - possibly leading to a large radioactive release – is typically estimated using PSA (probabilistic safety analysis) models consisting of event trees and fault trees.

A key concept in the PSA modeling of seismic events is the fragility curves of systems, structures and components (SSC). These curves quantify the probability of seismic-induced failure of SSC, as a function of the intensity of seismic ground motion, typically expressed in terms of the peak ground acceleration.

Given the large amount of safety relevant SSC in PSA models of NPP – of the order of 10^3 - a detailed, individual evaluation of the fragility curves of all components is not feasible under realistic resource constraints. Instead, a pragmatic and widely adopted approach is to combine fragility estimation methods with very different levels of sophistication. These methods range from experience-based engineering judgment (lowest level) to non-parametric fragility curves using state-of-the-art methods for structural mechanics and probabilistic modeling (highest level). An intermediate, frequently used level of sophistication consists in developing fragility curves by scaling the input data / results of existing design calculations.

The present contribution explains the rationale behind the various levels of modeling resolution in the fragility analysis of SSC and illustrates their combination in plant-level seismic risk assessment, making reference to case studies from recent seismic risk analyses.

Keywords: PSA, Seismic risk, Fragility

1. Introduction

Seismic PSA[1] is the preferred method for performing seismic risk assessment of NPP[2].

The chronological structure of a seismic PSA is typically as follows:

1. Development of the Seismic Equipment List (SEL)
2. Walkdown[3]
3. PSA modeling[4]
4. Fragility analysis
5. Risk quantification, i.e. the evaluation of the seismic induced core damage frequency (level 1 PSA) and large-early-release frequency (level 2 PSA, if applicable)

The methodological guidance observed by Seismic PSA practitioners is represented by various standards and guidance documents, with different levels of detail and diffusion [1]-[4].

The present paper focusses on the fragility analysis, i.e. the evaluation of the probability of seismic-induced failure of systems, structures and components (SSC), as a function of the intensity of seismic ground motion, typically expressed in terms of the peak ground acceleration (PGA).

In principle, the fragility of all components which play a role in the mitigation of a seismic induced transient or accident is of interest. Thus, the number of equipment items potentially relevant for seismic PSA is initially very large. Partially, this is due to the fact that the seismic induced loads on the SSC not only may lead to a failure of active equipment (e.g. pumps) but also damage components with passive functions (e.g. piping, tanks, heat exchangers). This is an important difference to the level 1 PSA for initiating events other than seismic induced ones, where the considered failure modes are mostly related to the active function of components.

Engineering judgment is thus an indispensable ingredient of the process of screening of equipment, with the objective to reduce the list of those SEL items which receive individual attention, to a manageable size. On the other hand, well established and quite sophisticated methods exist for the quantitative estimation of the fragility, based on dynamic analysis of buildings and equipment.

The purpose of the present paper is to present the fundamental ideas behind the alternative approaches to estimate the fragility of SSC.

---

[1] Probabilistic Safety Analysis

[2] Nuclear Power Plants

[3] If Seismic PSA is applied in the context of licensing of new plants, then the walkdown is likely to shifted towards the end of the Seismic PSA process, with the objective to confirm assumptions made along the way.

[4] In this context, PSA modeling refers to the incorporation of seismic induced failures in the PSA model.

2. Review of fragility curves

2.1. General remarks

Seismic fragility is defined as a conditional failure probability, where the condition is represented by a seismic event with a given value of the characteristic ground motion parameter, denoted by a. The characteristic ground motion parameter most widely used in seismic PSA is the peak ground acceleration (PGA).

$$Fr(a) = P\left[\text{failure} \middle| PGA = a\right] \tag{1}$$

By definition, the fragility is thus a monotonously increasing function of a. It is useful to express the fragility in terms of a random variable representing the capacity, denoted by A and defined in terms of the same ground motion parameter used for the fragility definition. Obviously, failure occurs if the capacity is lower than the peak ground acceleration a of the assumed seismic event. The definition of the fragility can then be extended as follows,

$$Fr(a) = P\left[\text{failure} \middle| PGA = a\right] = P\left[A < a\right] = F_A(a) \tag{2}$$

The right portion of the above equation emphasizes that the fragility is equivalent to the cumulative density function of the capacity A.

The most widely used guidance document on fragility analysis is [6]. More recent guidance – mostly updating the guidance ref. [6] – is given in [8] and [13].

2.2. Log-normal fragility curves

Due to its mathematical tractability, a fragility model based on the log-normal distribution has been the standard choice of seismic PSA practitioners in the past. The model is based on the following definition of the seismic capacity[5],

$$A = \breve{A}\varepsilon_R\varepsilon_U \tag{3}$$

where $\breve{A}$ is the median of the capacity, while ε_R and ε_U are log-normally distributed with unit median and logarithmic standard deviations of β_R and β_U, respectively. The random variables ε_R and ε_U model the variability due to randomness and due to uncertainty, respectively. Thus, the log-normal fragility model in equation (3) contains –

[5] The capacity is defined as the level of the ground motion at which onset of failure occurs.

in the form of ε_U - a parameter that permits to account for engineering judgment in a quantitative way.

An exemplary set of fragility curves resulting from this model is shown in Figure 1 for the arbitrary parameter values $\breve{A} = 0.5g, \beta_R = 0.3, \beta_U = 0.4$. Due to the separate modeling of randomness and uncertainty, the model leads to an ensemble of fragility curves, each one corresponding to a different value of the random variable ε_U.

In Figure 1 the bounding curves associated with this ensemble of fragility curves are shown for 5%, 50% and 95% non-exceedance probability of ε_U. In addition, the mean of the ensemble is also shown.

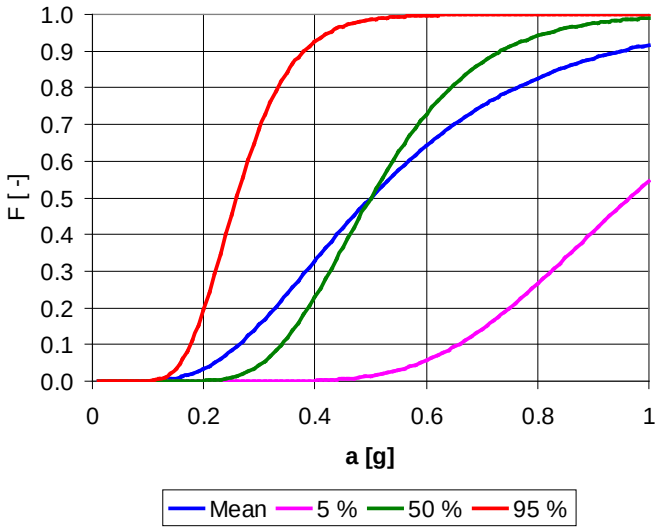


Figure 1. Exemplary set of fragility curves

2.3. HCLPF capacity

The HCLPF capacity is a characteristic parameter of the fragility curves. It is defined – implicitly - as the value of the PGA for which there is a high confidence (95 %) that the probability of failure does not exceed 5 % (i.e. it is low). Based on this, the HCLPF capacity can be related to the median capacity and the variability parameters as follows,

$$HCLPF = \breve{A}\exp\left(-1.65\left(\beta_R + \beta_U\right)\right) \tag{4}$$

A good approximation of the HCLPF capacity is the following,

$$HCLPF = \breve{A}\exp\left(-2.33\beta_C\right) \tag{5}$$

where $\beta_C = \sqrt{\beta_R{}^2 + \beta_U{}^2}$ is called the composite variability.

3. Different qualities of fragility curves

In the present section different qualities of fragility curves are distinguished. The qualities range from generic fragilities based on experience data and walkdown (section 3.1) to plant specific fragilities based either on design calculations (section 3.2) or on dedicated dynamic analyses (section 3.3).

3.1. Generic fragilities based on earthquake experience and engineering judgment

The number of components in the initial SEL of a seismic PSA (in the order of magnitude of 10^3) prevents a consistent degree of detail to be applied in the analysis of all of them. The initial SEL of the seismic PSA has thus to undergo a more or less extensive screening process in order to reduce the number of equipment items on the list. The main purpose of doing so is to enable the analysts to focus the majority of their subsequent efforts on equipment with relatively low capacity and consequently with the highest risk relevance.
The screening process takes part of its legitimacy from vast earthquake experience accumulated over the years, in particular in the United States, where field observations regarding seismic damage in industrial facilities during actual earthquakes have been extensively gathered and documented (see [7] and references therein). In addition, the screening process draws on fragility evaluations in past seismic PSA studies, as discussed in ref. [9].

Within the screening process a key task is to judge whether the equipment in the experience database is representative of the components encountered in the plant under investigation. This judgment is informed by a seismic walkdown conducted by suitably qualified specialists. With the aid of standardized checklists, as presented in [5], these specialists look out for configurations or features which have caused SSC to perform poorly during past earthquakes[6].
If the criteria in the checklists[7] are satisfied for a given SSC, then the experts involved in the preparation and release of ref. [5], and its predecessor ref. [9], support the judgment that the HCLPF of this SSC is at least 0.3 g PGA[8]. If some additional criteria hold[9], then they support the judgment that the HCLPF capacity is at least 0.5 g PGA.
Given the nature of the checklists, the judgment whether an SSC can be assigned to one of the two screening levels, is strongly based on qualitative criteria. To give an example, one of the criteria included in the checklists of all classes of SSC, is whether the SSC is "of good seismic design". It is therefore reasonable to associate significant uncertainty

[6] In addition, the walkdown also ensures that risk factors due to local conditions – e.g. unfastened, non safety-relevant equipment threatening safety-relevant SSC - are identified, so that proper countermeasures can be taken.
[7] These criteria are referred to as "caveats".
[8] This level of the PGA is - with some conservatism - in the range of PGA values recorded at the sites where the above mentioned field observations were gathered.
[9] Refer to Table 2-4 in [5].

with this judgment. As will be discussed in section 4.1, current guidance is not necessarily reflecting this, the reason being the objective to err on the safe side.

The result of the screening based on ref. [5] is actually not a full fragility curve, but only a HCLPF capacity. In order to obtain a fragility curve, the current guidance literature provides ranges for the generic composite variability parameter β_C (see also sections 3.4 and 4.1). This method is referred to as hybrid method in the guidance literature[10].

3.2. Plant specific fragilities based on scaling the seismic loads quantified during design

The most widely used approach for deriving fragility curves is based on the log-normal model introduced in section 2.2 and is described in detail in references [6] and [10]. The approach is applicable both to equipment qualified by analysis and by testing.

The basic concept underlying this approach is the following expression for the capacity A as a product of the (deterministic) value of the PGA, a_{design}, adopted in the seismic design of the SSC under consideration, and the scaling factor F,

$$A = a_{\text{design}} \cdot F \tag{6}$$

The scaling factor F may hence be viewed as the maximum scalar, by which the design ground motion can be multiplied ("scaled") without producing failure[11]. Alternatively, the factor F may however also be viewed as a safety factor, considering that it is the ratio between the actual capacity A and the acceleration used in the design, a_{design},

$$F = A \big/ a_{\text{design}} \tag{7}$$

In order to facilitate the evaluation of the scaling (safety) factor F, it is convenient to break it down into a product of "partial" safety factors. This permits the systematic evaluation of conservatism and variability in each step of the "analysis chain", typically starting with the dynamic analysis of the seismic induced motion of safety relevant buildings[12], continuing with the dynamic analysis of the equipment response and finally leading to the stress analysis of relevant equipment parts (e.g. supports, anchorage).

In the practical application of this method, it is typically assumed that seismic loads of the components – and the resulting stresses - are a linear function of the characteristic ground motion parameter (PGA). In this way, the results of the design calculation can be

[10] Refer to section 2.2.6 in ref. [8].
[11] This state is often referred to as "onset of failure". A straightforward, conservative approach is to assume that this state is reached when the stress induced by the seismic ground motion - in combination with permanent non-seismic loads – is equal to the allowable stress.
[12] This results in the design floor response spectra of each building.

reused, thus avoiding the additional effort to recompute the seismic loads experienced by the component for higher levels of ground motion than the design ground motion. The key steps of the formulation underlying fragility analysis by scaling of design seismic loads, including the assumption of linearity of the failure relevant parameter ("end-item-of-interest"), are summarized in the following Table I.

Table I: Fragility estimation by scaling of design seismic loads

Scaled ground motion (PGA):	$A(F) = F \cdot A_{\text{design}}$ (*scaling factor*)
Original ground motion:	$A_{\text{design}} = A(1)$
Realistic end-item-of-interest (e.g. stress):	$\sigma(F) = f(F)$ (*non-linear function*)
Standard assumption (linearity):	$\sigma(F) \approx F \cdot \sigma(1)$

The assumption of linearity of the end-item-of-interest, with respect to the characteristic ground motion parameter, entails that linearity is implicitly assumed for all the steps in the analysis chain. This is detailed in the following Table II, where the flow of data from the building ("B") to the equipment ("E") is explictly indicated. In this representation, the functions x and r denote the excitation (input) and response (output), respectively, of each link of the analysis chain.

Table II: Seismic analysis chain - dependence of the quantities of interest on the scaling factor

Actual dependence of quantities of interest on F:	
Excitation (building) → $x_B(F,t) \longrightarrow r_B(F,t)$ (*Response*)	(*End-item-of-interest*)
Excitation (equipment) → $x_E(F,t) \longrightarrow r_E(F,t) \longrightarrow \sigma(F)$	
Assumed dependence (standard assumption):	
End-item-of-interest (approximately) linear function of F	$\sigma(F) \approx F \cdot \sigma(1)$
implies	$\Rightarrow$
Linear equipment response	$r_E(F,t) \approx F \cdot r_E(1,t)$
implies	$\Rightarrow$
Linear building response	$r_B(F,t) \approx F \cdot r_B(1,t)$

Examples of fragilities based on scaling design seismic loads are presented in [11].

3.3. Plant specific fragilities based on re-evaluation of the seismic loads with scaled input excitation

In particular cases, the additional effort of a re-evaluation of the seismic loads induced by higher ground motion than the one assumed for the design, might be warranted. This can be the case for components with particular safety relevance, if the actual conservatism in the design calculations is difficult to quantify (e.g. for test-qualified equipment) or if it is expected that the conservatism is larger than one can quantify by scaling design seismic loads. In case of a re-evaluation, the assumption of a linear dependence of the quantities of interest on the scaling factor is not necessary any longer.

A fragility analysis based on a full reevaluation of the entire analysis chain has been presented in detail in [12]. The goal of that study is the fragility analysis of those sub-components of the reactor pressure vessel of a PWR[13], which are critical for the success of the reactor trip by insertion of the control rods, during or after a strong seismic event.

The seismic ground motion used as input excitation for the dynamic building analysis is significantly higher than the original design seismic ground motion. In addition, for one of the relevant failure modes, namely the excessive deformation of the fuel assemblies[14], the assumption of a linear dependence of the failure relevant quantity of interest[15] on the scaling factor is dropped for the last step in the analysis chain, i.e. the non-linear dynamic analysis of the fuel assemblies. In other words, for this part of the analysis chain the *input* excitation is iteratively scaled and the permanent deformation re-evaluated, until it reaches the maximum acceptable value, i.e. until the onset of failure. The results presented in [12] indicate that this "scale-to-fail" approach leads to significantly lower variability in the resulting fragility curve and thus a more precise estimate of the seismic ground motion level at which failure must be expected to occur.

3.4. Median centered fragilities versus HCLPF based fragilities

There is a basic difference between the generic fragility curves obtained with the method described in section 3.1, and the ones obtained with the methods described in section 3.2 and 3.3.

The generic fragilities are HCLPF based, i.e. the HCLPF is obtained *first*, whereas the median capacity is calculated *after*, using an estimate of the composite variability parameter β_C [16] and rearranging equation (5).

In contrast, the fragility methods described in section 3.2 and 3.3 revolve around the explicit quantification of the median capacity and of the variability parameters, whereas the HCLPF value is only a by-product of the analysis.

---

[13] Pressurized water reactor

[14] This would disturb and hence slow down the gravity-driven insertion of the control rods into the core in case of reactor trip.

[15] For this failure mode the quantity of interest is the permanent deformation of the spacer grids of the fuel assemblies.

[16] This approach is referred to as „hybrid method", as mentioned in section 3.1.

An alternative approach for obtaining HCLPF based fragility curves consists in applying the so-called CDFM[17] method, described in [13][18]. In this method, the HCLPF capacity is estimated directly, by calculating the seismic loads and the resulting stresses for an earthquake larger than the design earthquake, namely for the so-called review level earthquake (RLE). The calculation is based on conservative assumptions. If the resulting failure margin factor[19] is greater than one, then the HCLPF capacity is at least as high as the RLE. Fragility curves can then be obtained by making an assumption for the composite variability.
Analogously to the different options for deriving median-based fragilities (see sections 3.2 and 3.3), the calculation or estimation of the loads and stresses due to RLE can be performed either by scaling existing design seismic calculations or by re-evaluating the dynamic responses explicitly for the ground motion corresponding to the RLE.

4. Discussion of specific aspects regarding generic fragilities

4.1. Uncertainty associated with generic fragilities

As mentioned in section 3.1, the estimation of generic fragilities requires a particularly significant portion of engineering judgment. One would expect that for generic fragilities the parameter measuring uncertainty, i.e. β_U, should be larger than for fragilities based on plant specific calculations. On the contrary, according to the current guidance on the hybrid method[20] it is recommended to use a small value for β_C - and hence implicitly for β_U - "when in doubt".
This apparent contradiction is rooted in the intention to obtain a conservative risk estimate. Indeed, the seismic induced risk has been observed to be more sensitive to the median capacity than to the low-probability tail. For a fixed HCLPF capacity[21], a smaller β_C implies a smaller median capacity; this is exemplified in the following Figure 2. Consistent with the above mentioned observation, case 1 (smaller value of β_C) implies a larger risk and is thus conservative.

[17] Conservative deterministic failure margin
[18] Refer to Appendix A.
[19] This factor is defined as the ratio of the strength over the stress. Clearly, if the strength is larger than the stress, then there is margin with respect to failure. At the same time, the margin factor is then larger than one.
[20] Refer to section 2.2.6 in ref. [8].
[21] Recall that generic fragilities are HCLPF based fragilities, rather than median centered fragilities.

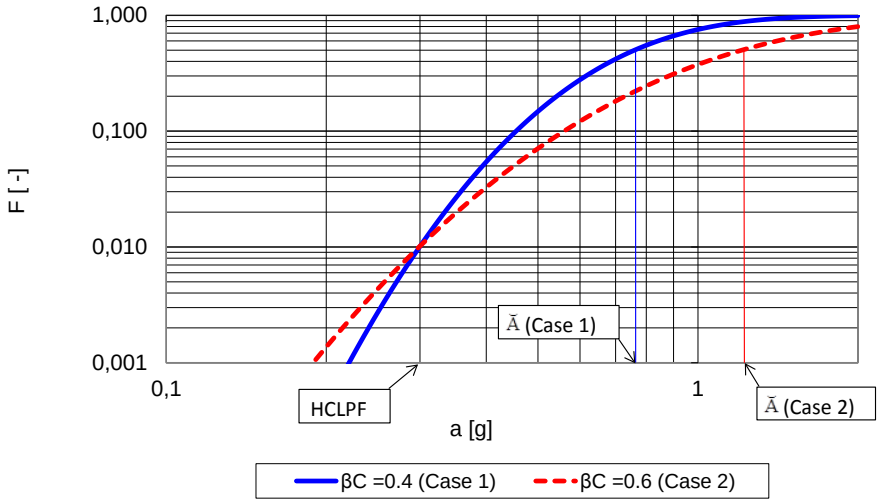


Figure 2. Two fragility curves with the same HCLPF value

4.2. Limitations for sites with high seismicity

An important limitation in the use of generic fragilities is associated with the screening levels mentioned in section 3.1: for sites with a high seismic hazard, applying seismic capacities in the order of 0.3 g or 0.5 g (HCLPF values, PGA) to a large number of components might not be acceptable. In this case, a much larger number of plant specific fragilities (as described in sections 3.2 and 3.3) have to be developed or alternative screening approaches have to be adopted.

Conversely, for sites with a very low seismic hazard (e.g. below 0.1 g PGA), generic capacities in the order of 0.3 g or 0.5 g can appear to be relatively high. In particular, the generic capacities might be higher than some of the capacities based on plant specific fragility analyses according to sections 3.2 and 3.3.

5. References

[1] IAEA (1993), Probabilistic safety assessment for seismic events.
IAEA-TECDOC-724.

[2] ASME (2009), Addenda to ASME/ANS RA-S-2008, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications.
ASME/ANS RA-Sa-2009

[3] Electric Power Research Institute (2003)
Seismic Probabilistic Risk Assessment Implementation Guide.
EPRI report 1002989

[4] Bundesamt für Strahlenschutz (German Office of Radiation Protection, 2005), Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke (Methods for probabilistic safety analysis for NPP, in German)
BfS-SCHR-37/05

[5] Electric Power Research Institute (1991)
A Methodology for Assessment of Nuclear Power Plant Seismic Margin.
EPRI NP-6041-SL

[6] Electric Power Research Institute (1994)
Methodology for Developing Seismic Fragilities
EPRI TR-103959

[7] Sandia National Laboratories (1992)
Part I: Use of Seismic Experience and Test Data to Show Ruggedness of Equipment in Nuclear Power Plants
Part II: Review Procedure to Assess Seismic Ruggedness of Cantilever Bracket Cable Tray Supports
SAND92 – 0140 – UC-523

[8] Electric Power Research Institute (2002)
Seismic Fragility Application Guide
EPRI report 1002988

[9] Lawrence Livermore National Laboratory (1985)
An Approach to the Quantification of Seismic Margins in Nuclear Power Plants.
NUREG/CR-4334

[10] Kennedy, R.P., and Ravindra, M.K. (1984)
Seismic Fragilities for Nuclear Power Plant Risk Studies
Nuclear Engineering and Design
Vol. 79, pg. 47-68

[11] Pellissetti, M., and Dirksen, G. (2012)
PSA-based seismic margin assessment of a NPP with advanced passive safety features
15th World Conference on Earthquake Engineering, Lisbon, Portugal, September 24-28, 2012

[12] Pellissetti, M., et.al. (2015)
Seismic robustness of reactor trip via control rod insertion at increased seismic hazard estimates
23rd Conference on Structural Mechanics in Reactor Technology (SMIRT23), Manchester, United Kingdom, August 10-14, 2015

[13] Electric Power Research Institute (2009)
Seismic Fragility Applications Guide Update
EPRI report 1019200

ESReDA
European Safety, Reliability & Data Association
Safety and reliability enhancement throughout Europe
50th ESReDA Seminar, May 18th 2016, University of Sevilla, Spain

Practical application of criticality analysis in the Spanish Natural Gas Transport Network

Javier Serra Parajes
Asset Management Technician, Enagas
Paseo de los Omos 19
28005, Madrid, Spain

Adolfo Crespo Márquez
University of Seville, Spain

Abstract

Risk management is emerging as one of the fundamental pillars for asset management in modern industry. The appearance of ISO 55001 as well as the recent revision of ISO 9001 introduced this concept as the best basis to make decisions in operation and maintenance.
These regulations do not require the application of a specific technique, so companies are responsible for searching the methodology that best meets their needs. In this case, companies do not only pursue that results provide a clear and relevant information about the risk of equipment, but obtaining these results within a reasonable time and of a large amount of equipment, because in some facilities it could be analysed thousands of items.
The aim of the exhibition is to expose the real case of the application of a specific methodology, criticality analysis, in a particular installation of OIL & GAS industry, a gas transport network. It is not only about reviewing the theoretical concepts that sustain the methodology and the benefits for mass analysis in an optimum time, but to discover those aspects that occur when an real analysis is developed and how may influence the result in a significant way.

Keywords: Maintenance Strategies, Asset and Maintenance Management, Decision Support, Criticality Analysis, Risk management

1. Introduction

In this paper, it is shown a real development of a criticality analysis for maintenance purposes as a base for different working lines of operation and maintenance. The main target of the methodology is to prioritize the equipment depending on the consequences of a hypothetical failure. The adaptation of the theoretical methodology to make it confluence with the company strategy provides to the user an analysis of the relative importance of the equipment.

The study of the consequences of a functional loss and the frequency of these failures let get us closer to the concept of what equipment is more valuable for the company. The main

advantage of the methodology is to allow the analysis of a big amount of items into a limited time. That is the reason why is so powerful as a base for developing a maintenance management model in a company with a big number of assets.

2. Theoretical model adaptation

The target of the paper is not to show the theoretical model adaptation. In order to simplify the reading, it is just going to be described the result of the adaptation. Just to remark that this phase must be done as closer to the strategy of the company as possible. This methodology must be a tool that allows to understand the relative importance of one item for the company. Probably it is more usual to make partial assessments and analyse the importance of an item for a specific area of the plant; safety area, maintenance area, operational area…

If the analysis criteria are defined close to the global company strategy, the result will be a global and common assessment of a specific item for all the areas of the company. The target of criticality analysis is to prioritize assets evaluating its relative importance. The criticality concept is defined as the product of the failure frequency of an item multiplies by the possible consequence of a functional loss:

Criticality = Frequency failure * Consequence

(CTR = FF *C)

a. Criteria definitions

To define criteria to assess functional loss, most of theoretical models propose two main concepts; criteria related with cost and criteria related with safety. That's the reason why it has been used the Asset Management Policy of the company as a base for criteria definition. This policy is sustained in two main concepts that involve every working line that the company is developing about operation and maintenance. The first base is "integrity". In this concept are included definitions as personal safety, industrial security and environmental care. The second base is "Efficiency and Improvement" and involves concepts as availability, quality service and maintenance costs.

To connect the criteria proposed by the methodology with the asset management policy of the company, five analysis criteria are defined based in these two bases. Two of them are related to the integrity and the other three are related to the efficiency. It is important to remark that criteria related with costs don't directly imply "spend money", even "profit lost" or "production lost". They can be related to reputational lost, stakeholders repercussion or even hypothetical penalties for service loss.

The criteria defined for consequence analysis are:

Safety Criteria:

- Industrial safety: The industrial safety factor assesses the consequences of the functional loss of an element related to:
    - Injuries to internal or third party personnel in the facility, and/or any other person who could be involved in.
    - Damage to of industrial assets, products and materials used in production or in end products, either in its own or third party facilities

- Environmental: The environmental factor assesses the environmental consequences of the functional loss of an element, including recovery costs, penalties, compensation, etc.

Cost criteria:

- Quality service: The quality service factor assesses the impact of the functional loss of an element on the gas reception, delivery service conditions, and any other services that Enagas offers to its clients.
- Availability: The availability factor assesses the impact on the installation's nominal capacity of the functional loss of an element It matches with the design capacity (emergency or reserve equipment not included).
- Maintenance costs: The maintenance cost factor assesses the impact of the functional loss of an element on the corrective maintenance costs, including costs associated with the recovery of the equipment and other equipment that may have been damaged.

Every criterion has a specific weigh in order to change subjective opinions of technicians into a numeric mark. When a consequence is analysed for each criterion, four severity levels are defined, also with its weigh depending of the theoretical consequence.

The value table defined for the assessment is shown in table 1.

Industrial Safety (35%)		Environmental (15%)		Quality Service (25%)		Availability (20%)		Maintenance Costs (5%)	
Catastrophic	100	High	100	High	25	Very High	20	Very High	5
Critical	35	Medium	15	Medium	15	High	10	High	4
Moderate	20	Low	5	Low	5	Medium	5	Medium	3
Slight	0	No Impact	0	No Impact	0	Low	0	Low	1

Table 1: Criterion and severity weighs

b. Frequency failure definitions

Most extended models define four levels (low, medium, high and very high) for frequency failure definition. In this case, it has been defined assuring that this definition follows the real management developed in the company.

Specialist of the company agrees that they use these four definitions to classify failures because of its frequency:

- **Possible failures;** an average value lower than one failure every two years
- **Acceptable failures;** an average value of one failure between two years and one year
- **Repetitive failures;** an average value between one and two failures per year
- **Non acceptable failures;** an average value higher than two failures per year

3. Methodology application scheme

To reach a correct development of the methodology is important to be organized and follow the right steps of the technique as strictly as possible. For this reason, it is going to be explained a practical example of a criticality analysis in an item of a gas facility.

It has been defined a diagram with the main steps of the technique in order to simplify the methodology application. In the diagram are described key rules to develop a properly analysis. It is very important to analyze the item into its physical and operational context. The scheme proposed is:

a) **To define the facility and its functionality:** the aim is to get a whole vision of the facility in which the item analysed is working. Therefore, some analysis criteria are related to the whole plant. For example availability or quality service are not analysed for each item, but for the whole facility. It is very important to have defined the plant properly to make a correct assessment of the criticality.
b) **To define the system function:** Focussing in the system, it must be analysed the concrete function of the item into the facility (emergency system, control system…). It is important to know the real importance of the item for the correct operation of the plant.
c) **To define the item function and its operational context:** The final target for developing the criticality analysis is to analyse the consequence of a functional loss. That is the reason why this function must be defined: to pump, to close, to compress…
d) **To define functional loss:** Having the item function defined is easy to suppose the functional loss. The key point in this step is to differentiate a fault to a functional loss. Every item has multiple possible faults, but just a single functional loss for every function of the item. If the function of an item is "to pump", its functional loss will be "pumping absence".
e) **To analise failure consequence:** The consequences of a hypothetical functional loss will be assessed in this step. Using the table defined in the previous chapter, it must be selected the consequences of a hypothetical failure in every consequence criteria.
f) **To get the severity of a functional loss:** Every criteria consequence has a numeric value that reflects the importance of the consequences for the company. In this step, these numeric values are collected in order to get a final severity value.
g) **To calculate the frequency failure:** Depending on the definition made in the previous chapter, the frequency failure of every item must be calculated in order to get the second parameter needed for the severity.
h) **To get the criticality level:** We can obtain the criticality level using the frequency failure and the severity level calculated in the previous steps.

4. Practice application in a gas facility

It is going to be described a simple example of the methodology application. The previous application scheme is going to be followed step by step trying to highlight the key aspects of the analysis.

a) To define the facility and its functionality

The facility that is going to be analyzed is a valve point that provides gas to a "Measurement and Regulation Station". In the natural gas transport network, the NG is transported at high pressure (72 bars) across the country, but in order to deliver NG to clients, the pressure of the gas is reduced to 16 bars in MRS.

The functions of the valve point are:

- To section the pipeline in case of leaking gas
- To deliver NG from high pressure network to the MRS.

In this analyzed system, items related to the process are mostly valves. There are other functions made by other items of the facility related mostly with safety or control, but they are going to be omitted in order to simplify the example.

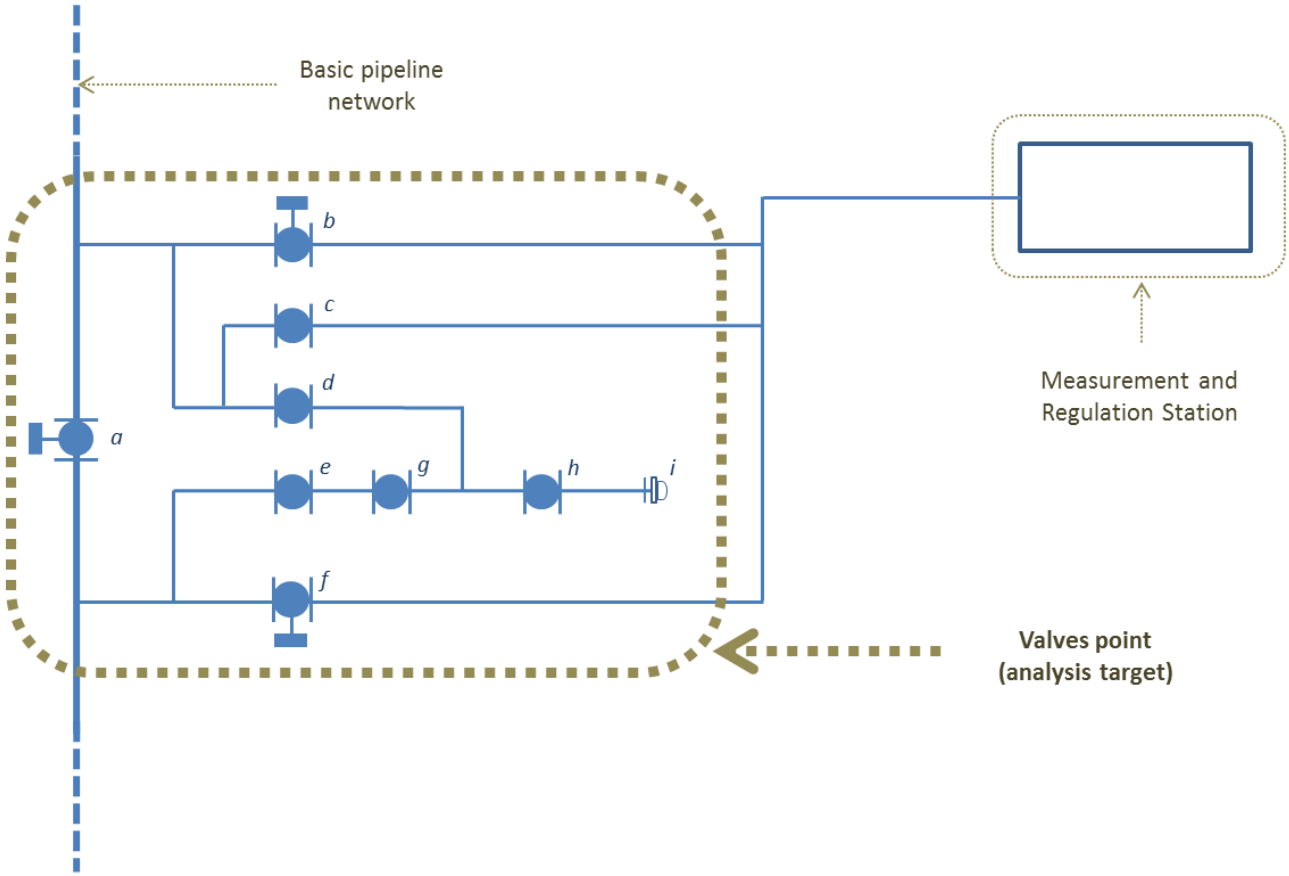


Fig. 1 : scheme of the facility

We can show the facility scheme in the figure 1. The example will be focused on valve "a".

b) **To define the system function:**

As it has been exposed previously, in the example we have focused the analysis in the valves system, so in this case, the system function is the same that the facility function. It is going to be described de valve function:

- Valve "a" is a "sectioning valve" and its function is to cut the NG flow through the pipeline in case of leaking.

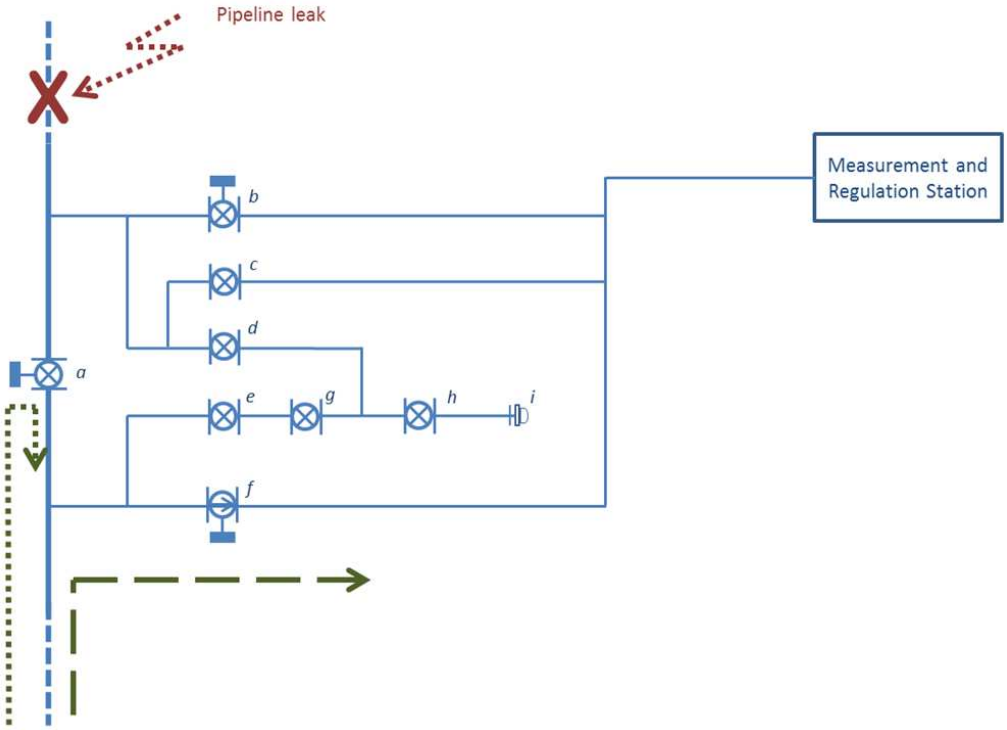


Fig. 2 : System function

c) To define the item function and its operational context

The valve is motorized. In case of valve "a" the function is usually opened to let the flow of NG through the pipeline. So the valve has two functions, to be opened in normal operation and to be closed and to cut the NG flow if a leak is detected. With the second function we can section the pipeline and to limit the damage derived from a possible incident.

d) To define functional loss

Criticality analysis is a methodology that doesn't analyze the hypothetical failure mode (breakdown, misalignment…) otherwise it assesses the consequence of a functional loss independently of the cause of the failure.

That is the reason why is so important to define properly the functional loss of every maintainable item. Moreover, each item has a main function (to pump, to compress…) but have also secondary functions (proper pressure, efficiency point…). In order to simplify the analysis, it is important to define just the main functions. It could be studied the functional loss over all the main and secondary functions, but one of the key points of the methodology is to analyze a big amount of items in a short period of time. If every function is included into the analysis, it could delay the development of the project.

So in this case, there will be only analyzed the main functions: "failed to open", "failed to close".

e) To analise failure consequence:

To develop this step properly, is important to be strict with the hypothetical situation and the correct question that let us to assess the consequences of a functional loss. The correct question that must be done is "What would be the consequence of a valve "a" failure, in case it would be needed?

It is important to remark that the functional loss must be assessed in the moment that its operation is required, so the consequences are negative for the facility. For example, the

analysis of a gas detector failure doesn't have any sense if it is not supposed a gas leak. Without gas presence, a gas detector failure never would have consequences. The right question for this example would be: "What would be the consequence of a gas detector failure, in case of a gas leak?

It is also interesting to note that concatenated failures are not analyzed in criticality analysis. It means that in order to assess a consequence failure, it must be only supposed the failure of the analyzed item and not hypothetical failures of other related equipment. In the end, criticality analysis assesses the consequence of an item functional loss for every criterion defined previously. It implies to adapt the question that must be done for every criterion:

-"What would be **the industrial safety consequence** of a gas detector failure, in case of a gas leak?
-"What would be **the environmental consequence** of a gas detector failure, in case of a gas leak?
- …

The hypothetical situation estimated for the analysis is a pipeline leak. There must be analyzed the possible consequences of a functional loss of the valve in the situation described. As it has been defined previously, the valve has two main functions: to open to allow the natural gas flow across the pipeline, and to close to cut this flowing. When two or more functions are analyzed, it must be taken the highest mark of every assessment. In this case the most critical function is a "close failure" so is the function that will be analyzed.

Industrial safety; the target of the valve is to cut the pipeline section that has benn damaged and in consequence, to limit the natural gas flow across the pipeline avoiding risks related with the leak. If the valve could not be closed, there will be a high risk becouse natural gas would being emitted to the atmosphere and in consequence there will be explosion risk. The consequence of a valve functional loss on industrial safety criterion will be "catastrophic".

Environmental; the assessment of this criterion is related with the natural gas emitted to the atmosphere. With the same reasons than the industrial safety analysis, if the valve could not be closed, natural gas would be flowing to the atmosphere. In this case the consequence is assessed as "Low" because the environment impact does not implies third parties.

Quality service; In this analysis, it must be assess the consequence of the valve function loss related to the clients. In this case, the function of the valve point is to allow the natural gas flow across the pipeline and to deliver natural gas to the Measurement and Regulation Station.This is a clear example that shows the importance of the operational context of the analysis. A valve failure would not cut the natural gas delivering. In fact, the real problem is that the natural flow could not be cutted. But the operational context define that if a valve can not be closed, it must be closed the nearest valve. In this case the natural gas flow would be cutted and the delivering to the MRS woud be interrupted. According to the severity levels definition, the consequence of this failure would be "high".

Availability; In this criterion, it must be analysed if the valve functional loss would imply a facility function loss. The facility has two main functions (defined previously). In this hypothetical situation, a valve functional loss would imply the loss of both functions; to cut

the natural gas flow across the pipeline and to deliver natural gas to MRS. According to the severity levels definitions, the consequence of the failure would be "very high".

Maintenance costs; this is probably the most objective criterion because it must be estimated the costs related to the hypothetical failure. The technicians agree the most common valve's failures and then estimate an average price for the reparation. In this case it has been estimated that the cost would be between 600€ and 5000€ what means that the consequence failure related to this criterion would be "medium".

f) To get the severity of a functional loss:

The next step is to obtain the mark of the consequences assessed in the previous chapter in function of the table defined by the technicians. The final table is the next:

Industrial Safety (35%)		Environmental (15%)		Service Quality (25%)		Availability (20%)		Maintenance Costs (5%)	
Catastrophical	100	High	100	High	25	Very Hihg	20	Very High	5
Critical	35	Medium	15	Medium	15	High	10	High	4
Moderate	20	Low	5	Low	5	Medium	5	Medium	3
No impact	0	No impact	0	No impact	0	Low	0	Low	1

Table 2 : Assessment example

g) To calculate the frequency failure:

This is probably the easiest step of the methodology. Just one requeriment is needed: a good failure register of the facility. With these records, the data can be obtained almost inmediatly. If the register does not exist there are alternative processes. It can be used the knowledge of the technicians or even public data bases as OREDA. In the example case, it estimated that this kind of valves do not fail usually, so the frequency failure is "low".

h) To get the criticality level:

In the end, the item must be located into the criticality matrix. It will be the graphic representation of the criticality analysis. The mark related to the severity of the functional loss is fixed in x-axys. In the example, the failure of the valve has the maximum puntuation (related to industrial safety criterion). So it is fixed at the right extreme of the matrix. The mark related with the frequency failure is fixed in y-axis. In the example the valve frequency failure is low, so the item is fixed at the bottom extreme of the matrix.

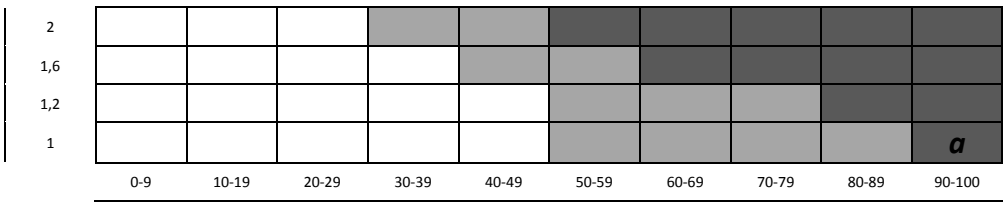


Table 3 : Criticality matrix example

5. Conclusions

To have a methodology that sustains the operation and maintenance strategies is an important requirement for the industry. Over the years, most of strategies have been focused on availability and costs, but risk management is more important every day. Many methodologies could be used to get a quality certification as ISO 9001, but not many methodologies are really useful for a real company development.

Criticality analysis allows allocating with a simple methodology your items assigning them a relative value in function of the strategy and target of the company.It is a very powerful tool and a solid starting point for an optimising policy of OPEX in the lifecycle.

6. Acknowledgements

The members of the University of Seville would like to acknowledge the collaboration of the MM Binladin Chair of Operations and Maintenance from the University of Taibah, in the development of this research.

7. References

[1] J. Adams and A. K. Parlikad, “Dynamic Maintenance Based on Criticality in Electricity Networks,” in *5th IET/IAM Asset Management Conference*, 2015.

[2] A. Kelly, *Maintenance strategy*. Elsevier, 1997.

[3] Assetivity - Asset Management Consultants, “Equipment Criticality Analysis – is it a Waste of Time?,” 2015. [Online]. Available: http://www.assetivity.com.au/article/reliability-improvement/equipment-criticality-analysis-a-streamlined-approach.html. [Accessed: 15-Oct-2015].

[4] A. Crespo Márquez, P. Moreu de León, A. Sola Rosique, and J. F. Gómez Fernández, “Criticality Analysis for Maintenance Purposes: A Study for Complex In-service Engineering Assets,” *Qual. Reliab. Eng. Int.*, p. n/a–n/a, 2015.

[5] A. C. Marquez, *The Maintenance Management Framework: Models and Methods for Complex Systems Maintenance*, 1st ed. Springer-verlag London, 2007.

[6] M. Braglia, M. Frosolini, and R. R. Montanari, “Fuzzy TOPSIS Approach for Failure Mode, Effects and Criticality Analysis,” *Qual. Reliab. Eng. Int.*, vol. 19, no. 5, pp. 425–443, Sep. 2003.

[7] W. Gilchrist, “Modelling Failure Modes and Effects Analysis,” *Int. J. Qual. Reliab. Manag.*, vol. 10, no. 5, 1993.

[8] J. Puente, R. Pino, P. Priore, D. de la Fuente, and D. D. La Fuente, “A decision support system for applying failure mode and effects analysis,” *Int. J. Qual. Reliab. Manag.*, vol. 19, no. 2, pp. 137–150, Mar. 2002.

[9] S. M. Seyed-Hosseini, N. Safaei, and M. J. Asgharpour, “Reprioritization of failures in a system failure mode and effects analysis by decision making trial and evaluation laboratory technique,” *Reliab. Eng. Syst. Saf.*, vol. 91, no. 8, pp. 872–881, Aug. 2006.

[10] M. Braglia, “MAFMA: multi-attribute failure mode analysis,” *Int. J. Qual. Reliab. Manag.*, vol. 17, no. 9, pp. 1017–1033, Dec. 2000.

[11] T. R. Moss and J. Woodhouse, "Criticality analysis revisited," *Qual. Reliab. Eng. Int.*, vol. 15, no. 2, pp. 117–121, Mar. 1999.

[12] M. Ben-Daya, A. Raouf, M. Ben-Daya, and A. Raouf, "A revised failure mode and effects analysis model," *Int. J. Qual. Reliab. Manag.*, vol. 13, no. 1, pp. 43–47, Feb. 1996.

[13] J. B. Bowles and C. E. Peláez, "Fuzzy logic prioritization of failures in a system failure mode, effects and criticality analysis," *Reliab. Eng. Syst. Saf.*, vol. 50, no. 2, pp. 203–213, Jan. 1995.

[14] C. E. Pelaez and J. B. Bowles, "Using fuzzy logic for system criticality analysis," in *Proceedings of Annual Reliability and Maintainability Symposium (RAMS)*, 1994, pp. 449–455.

[15] A. C. F. Guimarães and C. M. F. Lapa, "Fuzzy inference to risk assessment on nuclear engineering systems," *Appl. Soft Comput.*, vol. 7, no. 1, pp. 17–28, Jan. 2007.

[16] M. Braglia and M. Bevilacqua, "Fuzzy modelling and analytical hierarchy processing as a means of quantifying risk levels associated with failure modes in production systems," *Technol. Law Insur.*, vol. 5, no. 3–4, pp. 125–134, 2000.

[17] N. R. Sankar and B. S. Prabhu, "Modified approach for prioritization of failures in a system failure mode and effects analysis," *Int. J. Qual. Reliab. Manag.*, vol. 18, no. 3, pp. 324–336, 2001.

[18] C. L. Chang, P. H. Liu, and C. C. Wei, "Failure mode and effects analysis using grey theory," *Integr. Manuf. Syst.*, vol. 12, no. 3, pp. 211–216, 2001.

[19] C.-L. Chang, C.-C. Wei, Y.-H. Lee, C.-L. Chang, C.-C. Wei, and Y.-H. Lee, "Failure mode and effects analysis using fuzzy method and grey theory," *Kybernetes*, vol. 28, no. 9, pp. 1072–1080, 1999.

[20] M. Bevilacqua, M. Braglia, and R. Gabbrielli, "Monte Carlo simulation approach for a modified FMECA in a power plant," *Qual. Reliab. Eng. Int.*, vol. 16, no. 4, pp. 313–324, Jul. 2000.

[21] R. Smith, "Equipment Criticality Analysis," *Analysis*, no. 6, pp. 1–20.

[22] W. J. Moore and A. G. Starr, "An intelligent maintenance system for continuous cost-based prioritisation of maintenance activities," *Comput. Ind.*, vol. 57, no. 6, pp. 595–606, Aug. 2006.

[23] M. Cerrada, J. Cardillo, J. Aguilar, and R. Faneite, "Agents-based design for fault management systems in industrial processes," *Comput. Ind.*, vol. 58, no. 4, pp. 313–328, May 2007.

Supply chain vulnerability and resilience – case study of footwear retail distribution network

Tomasz Nowakowski, Agnieszka Tubis, Sylwia Werbińska-Wojciechowska
Wroclaw University of Technology, Faculty of Mechanical Engineering
27 Wybrzeze Wyspianskiego Str.
50-370, Wroclaw, Poland

Abstract

The aim of this article is to present and investigate the main concepts of supply chain vulnerability and resilience. Thus, the fundamental differences between vulnerability and resilience definitions are discussed. The main issues on vulnerability and resilience assessment are investigated, and the case study of footwear retail supply chain disruption problems is investigated.

Keywords: supply chain, vulnerability, resilience, assessment methods.

1. Introduction

Supply chain may be defined as *an integrated process wherein a number of various business entities (like suppliers, manufacturers, distributors, and retailers) work together in an effort to: (1) acquire raw materials, (2) convert these raw materials into specified final products, (3) deliver these final products to retailers and final customers* [4]. Such a logistic network is then characterized by a forward flow of materials and a backward flow of information. As a result, in today's uncertain environment, the reliability, resilience, and vulnerability of supply chain performance can be affected by many different factors. Moreover, based on the authors' previous research works (see e.g. [10, 25]) it may be stated that these concepts sometimes are used interchangeably or as polar opposites. There is also visible the diversity of their interpretations and reformulations across the area of supply chain performance. Thus, this research area still demands examination of real logistic systems performance and development of new complex framework for system vulnerability and resilience measurement.

Moreover, there exist many models in the literature which are concerned with material procurement, production, transportation, and storage or distribution activities and with information flows performance. However, lot of them treats each stage of supply chain as a separate system [12]. As a result, many of the supply chain interactions are ignored. This may led to improper identification of elements, which may influence the proper performance of a given chain also in the context of its resilience level (Figure 1).

Following this, in the presented paper, authors focus on the investigation of vulnerability and resilience assessment issues. As a result, in the article the main vulnerability and resilience definitions are discussed. Later, there is presented a comprehensive literature review connected with assessment methods used in the analysed research area. Based on this, the problem of supply chain vulnerability and resilience assessment is investigated on the simple example of supply chain of market leader in the Polish footwear retail. Authors focus on the disruption problems connected with distribution network organization in the case company. The vulnerability analysis encompasses the main disruption sources definition and possibilities of their estimation.
The research work is a preliminary step of authors research focused on new resilience assessment method development connected with new vulnerability index definition.

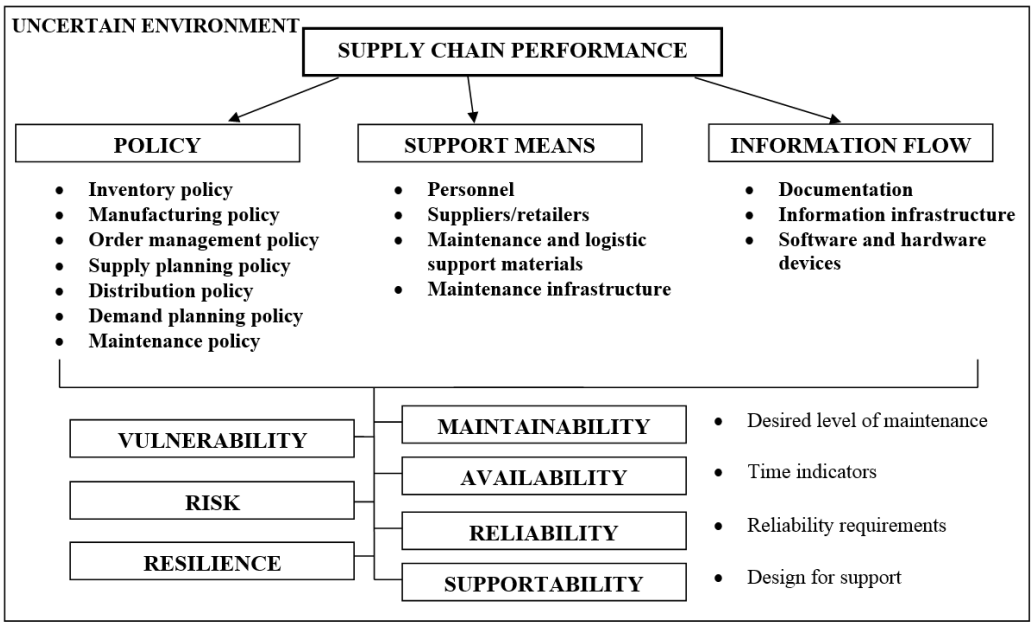


Fig. 1. The key characteristics in achieving supply chain performance
Based on: [6, 23, 26, 43]

2. Supply chain vulnerability and resilience assessment issues

Supply chain networks are vulnerable to disruptions and failure at any point in the supply chain may cause the entire network to fail. A key factor in the effective supply chain management is the ability to minimize the effects of such undesired events/disruptions occurrence. As a result, understanding what disruptions may occur in a supply chain, how they will affect a supply chain system, and how far reaching these effects will be, would be of considerable benefit [45].
Treating the supply chain disruptions as unexpected events occurrence, we can describe them as having uncertainty in supply chain operations [45]. Uncertainty in the supply chain can be seen from different aspects, such as [40]:

- time (in the sense of duration of activity/process, starting/ending moment of activity realization, frequency of activity/demand occurrence),
- quantity (of supply, demand or physical transfer of goods),
- location/place (where activity starts/ends),
- quality (of service/products),

- cost (fluctuation, occurrence).

For example, Landeghen and Vanmaele in their work [19] profiled sources of uncertainty in the supply chain. They highlighted 13 sources of uncertainty across three supply chain's planning horizons (operational/tactical/strategic) and categorized them as Low, Medium and High.

Taking the presented perspective of supply chain disruptions definition, *to prevent vulnerability, it is essential to manage risks in chains through creating more resilient supply chains that are able to respond to disruptions and adapt themselves to necessary changes* [11]. Thus, the issues on vulnerability and resilience of supply chains should be based on risk management perspective [39]. More information can be found e.g. in [33], where authors provide a comprehensive review and classification of supply chain risk management literature.

The term supply chain vulnerability is studied and defined by researchers in various ways. Some of the researchers studied supply chain vulnerability conceptually (see e.g. [27, 35, 36]), or mathematically (see e.g. [1, 2, 18]). Most of the known supply chain vulnerability definitions are consistent that this concept in a multidisciplinary approach determined by certain characteristics, supply chain design variables and the environmentally influenced [41]. The overview of some recent definitions on supply chain vulnerability is given by the authors in [10, 22, 25]. In their context, supply chain vulnerability can be defined as *an exposure to serious disturbance, arising from risks within the supply chain as well as risks external to the supply chain* [9].

Similarly, the number of research studies introduced the concept of supply chain resilience. Following the literature, supply chain resilience may be defined as the *ability of the supply chain to handle a disruption without significant impact on the ability to serve the supply chain mission* [5]. As reported e.g. in [14], the resilience definitions took into account the following supply chain aspects: its flexibility, agility, velocity, visibility and redundancy. A brief survey of resilience definitions from different disciplinary perspectives was given in [16]. The comprehensive literature review on supply chain resilience is presented e.g. in [7, 11, 20, 28, 31, 24].

To sum up, there can be presented the three main definitions of conceptions connected with effective performance of supply chains which are vulnerable to disruptions.

Reliability assessment is focused on the possibility of an unwanted event occurrence. Many researchers claim that the term supply chain reliability has been defined for the first time by Thomas in 2002 (see e.g. [21]). Author in his work [38], has been investigating the system reliability in terms of *a set of processes for providing the procurement, distribution, storage, and transportation of people, supplies, materials, and equipment*. The supply chain reliability is defined as *the probability of the chain meeting mission requirements to provide the required supplies to the critical transfer points within the system*.

Measures of the reliability should express uncertainty about the appearance of such an event, like failure, fault, error, etc. Thus, in this sense reliability (dependability) of a logistic system can be understood [8] as *the ability to deliver correct service under normal (ordinary) work conditions in a given time interval*. For more information see e.g. [37].

Safety means *absence of critical/dangerous events while security is focused on protecting the system environment against the effects of these damages*. Safety is measured generally by risk – two-dimensional combination of probability of an undesirable event and possibility of loss (consequences). Risk assessment consists on process of risk identification related to threat, includes its possibility (likelihood or

probability), impact, and consequences. More information can be found e.g. in [29], where the main definitions are investigated.

Resilience takes into consideration not only the discussed issues (reliability and safety) but also the possibilities of restoring the original properties of the system. Thus, resilience means [8] *readiness for secure and acceptable service under abnormal (uncommon) work conditions (e.g. disruptions, attacks, accidences, disaster).* And the measure of resilience can be understand as time to restore the capabilities of the system (worse than new, as good as new, better than new [22]). Following this, the resilience is about handling the consequences of a disruption, not about preventing a disruption from occurring. However, the effort to create a resilient system is made before a disruption occurs. For more information we recommend reading [25].

In the current literature, there can be found research works dedicated to vulnerability and resilience measurement issues. The vulnerability assessment issues are investigated in details by the authors in [10]. The examples of supply chain resilience measurement systems/methods are given e.g. in [3], where authors present two resilience-based component importance measures for networks, in [13], where authors investigate the assessment issues of passenger transportation system's resilience, in [15], where a method for measuring resilience based on fuzzy logic is proposed, and in [17], where authors develop generic metrics for quantifying system resilience. In work [16], authors introduce a resilience metric that incorporates the three resilience capabilities (absorptive capacity, adaptive capacity, recovery capacity) and the time to recovery. Following this, in the Figure 2, there is presented the resilience measurement framework.

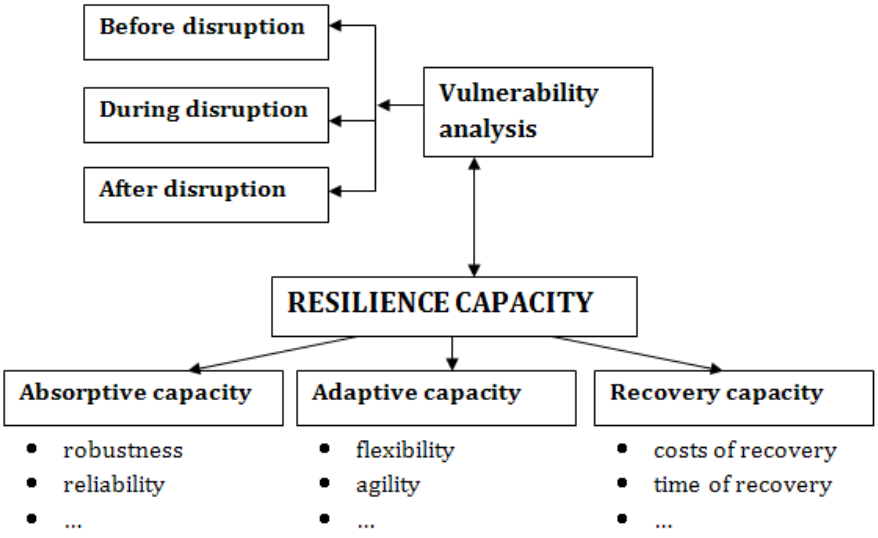


Fig. 2. Resilience framework
Based on [16, 30, 42]

Moreover, the complexity of the problem is connected with the necessity of taking into account some factors that might increase the level of risk, like [34, 44]:

- focusing on efficiency targets instead of effectiveness issues,
- supply chain globalisation,
- focussing on factories and centralised distribution,
- outsourcing,

- reduction of the supplier base,
- demand variability,
- lack of visibility and control procedures.

This factors are discussed in more depth e.g. in [33, 34].

3. Footwear retail supply chain – case study

The analysed company is a leader of the Polish retail footwear market. Products sale is carried out in over 700 stores located in modern galleries and shopping canters in 14 countries, where company sold 25 million pairs of shoes yearly. The company has its own leather shoes manufacturing factory. In one season there are offered collections containing almost three thousand models of shoes. The Group owns more than 67 brand names. The company's share in the retail footwear market in Poland is around 17-18%. The company's products are dedicated for customers of the middle segment of the market.

3.1 Supply chain structure

The current structure of the supply chain of final products for the consumer market is shown in Figure 3.

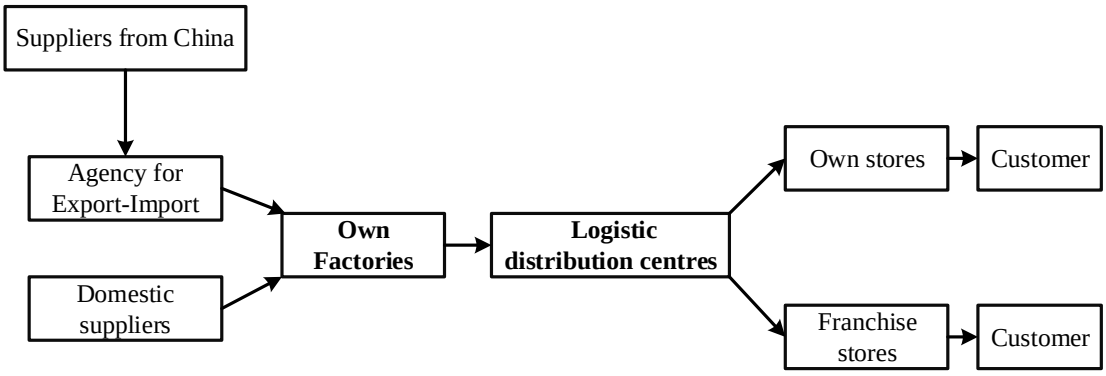


Fig. 3. Current structure of supply chain

The distribution supply chain includes domestic suppliers, company's own manufacturing facilities and foreign suppliers (mainly from China). Footwear imported from the territory of China comes from dozens of manufacturers, however the main delivery part is realized by a single unit acting as the export-import agency. The structure of the purchases in the first quarter of 2015 is shown in the Table I.

Table I: Purchasing structure in value 1Q2015

Foreign suppliers	Own manufacturing	Domestic suppliers
70,3%	21,6%	8,1%

Currently, the largest sales market is Poland, but there is noticed an increasing and significant impact on sales results of abroad distribution. The products are offered to

customers in company's own stores e.g. in Poland, Hungary, Slovakia, the Czech Republic, Austria, Slovenia, Croatia, Turkey and Germany. The franchise stores are operated in the Baltic countries, Russia, Romania, Ukraine and Kazakhstan. The sales structure is dominated by women's shoes sale in terms of both value and volume.

Table II: Sales structure 1Q2015

Sales structure	Women's shoes	Men's shoes	Children's shoes
In value	61%	25%	14%
In volume	56,2%	19,6%	24,2%

The company's logistics centre is now become an innovative complex of large objects. The most important building is a fully automated high-bay warehouse of mini-load type, with a total area of 23064 m2, which is able to accommodate a minimum of 500,000 cartons of various sizes, thus more than 5 million pairs of shoes. The new distribution centre, together with existing sorting facility, creates conditions to handle more than 100,000 cartons, what are about 1.1 million pairs of shoes, during the two working shifts. The process of mechanization guarantees the operation for future development and is fundamental for further development of logistics processes. Additionally, it enables optimization of storage space, the surface of which is currently about 82.3 thousand m2.

3.2 The process of goods delivery from the logistics centre to the points of sales

The authors' research is focused on the process of goods delivery from the logistics centre to the company-owned stores located on Polish territory. The logistics centre is located in Lower Silesia region. Its aim is to supply 406 stores (the number of stores in 03/31/2015) located in shopping malls throughout the country.
The process of footwear supply to points of sale is based on the VMI strategy (Fig. 4). The processes of inventory monitoring in stores, demand forecasting and orders delivery are managed by the central distribution. All the shops are incorporated in the computer system, which sends daily reports of daily sales and current inventory levels to a central distribution. On the basis of this information and inventory availability parameters for each brand and each shoe size, the system generates the demand for delivery to various points of sales. Orders for individual stores, after the approval of the responsible person, are sent to the logistics centre. In this centre, with the use of automated completion process there are prepared ordered goods and then they are directed to the dispatch zone. The physical delivery process from the distribution centre to the store is operated by external logistics operators. Currently, the company cooperates primarily with two logistics companies. Later, goods shipped to the point of sale are unpacked by employees and laid on the shelves. The location of goods is consistent with the accepted standard for individual brands and collections in the current season.

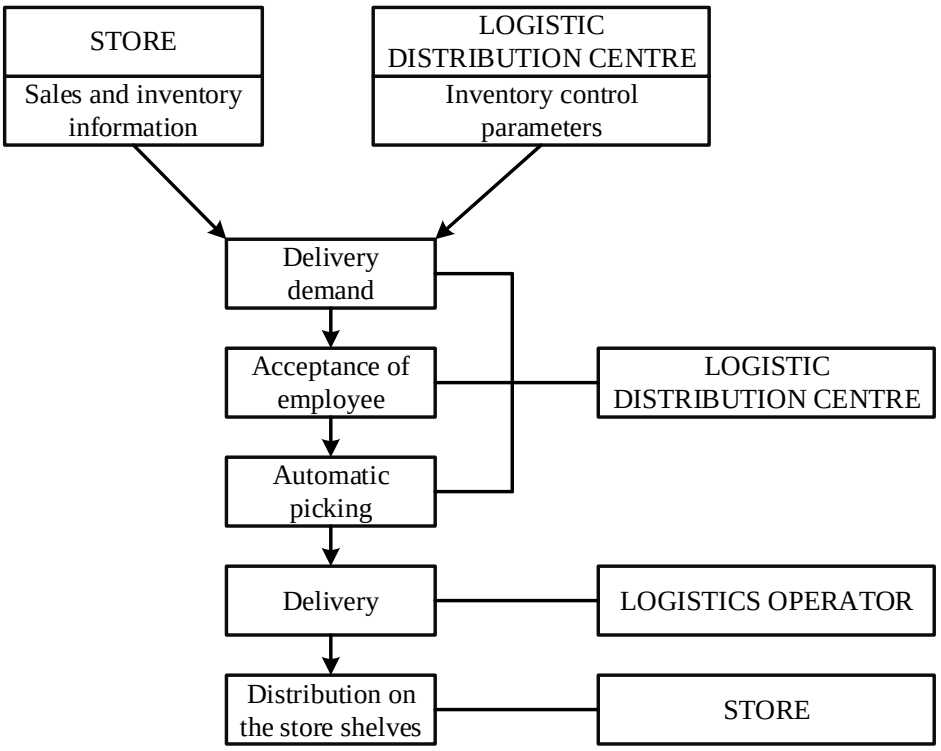


Fig. 4. The process of footwear supply to points of sale

4. Identification of groups of disruption events that may occurred in the analysed process

The concept of logistic processes continuous performance assumes four-element operational model [8]: (1) identification of potential sources of hazard event occurrence; (2) prediction of possible scenarios for the occurrence of these hazards; (3) monitoring, detection and recognition of occurred hazards; (4) prevention, i.e. prevention and protection against identified hazards. The current stage of authors' research is focused on the first step of the discussed performance model. The analysis regards to the process of planning and delivery of shoes from central distribution centre to stores located in Poland (the process described in the Section 3.2).

In the studies on supply chains management, there are identified 14 sources of hazards/uncertainties in their performance [32]. During the performance of chosen supply chain vulnerability analysis there are omitted two aspects - behavioural issues and parallel interaction. According to the authors, these elements are not the source of disruptions in the analysed supply network. For each source of disruptions defined in the model of supply-chain uncertainty there is assigned a hazard event/disruption being identified in the given footwear retail supply chain. Threats/hazards are defined on the basis of process and infrastructure analyses being conducted for the investigated supply chain and sectoral analysis implementation.

Table III: Identification of disruptions in the analysed supply chain of footwear retail

Sources of disruptions	**Risks in the defined supply chain**
Product characteristic	Shoes - product that is dependent on the weather conditions and fashion trends with short product life cycle
Manufacturing process	The production is based largely on the skills of employees
Uncertainty in control processes (control chaos)	Strong dependence of ordered values requested by shops on external factors being beyond the company's control Stores do not have control over the amount and type of ordered footwear
Decision-making process complexity	Footwear distributed to stores located in different regions, with its own specific sales characteristic, which should be included in the developed future sales and marketing plans
IT/IS systems complexity	The entire distribution system is strongly supported by IT systems. Failure of one of them stop the process of distribution and delivery to stores
End-consumer demand variability	Demand is seasonal, difficult to forecast due to the strong dependence on external factors
Demand amplification	Saturation of Polish market in footwear shops
Suppliers	About 70% of the products supplied to the shops come from foreign suppliers. In most cases these products are delivered by the sea from China
Order forecast horizon	Dependence on fashion and weather conditions makes long-term demand forecasts more vulnerable for estimation errors. It is possible to reliable forecast orders for the short time horizon.
Supply chain configuration, infrastructure, facilities	One central warehouse, which stores all products. Managing the flow of goods through the supply chain is implemented by a central processing unit
Environment	There operate several strong players at the footwear market. The main competitor is a company with foreign capital that has organized its supply chain in a similar way
Disasters and natural disasters	Location of headquarter in the intensive mining operation area - risks of tremors, failures of underground equipment. Flood risk – in the neighbourhood is located Odra river and Żelazny Most reservoir

These risks can be classified into three groups (Fig. 5):

1) **Internal organisation uncertainty.** This group can include product characteristics, manufacturing process, control chaos, decision complexity and IT/IS complexity. The responsibility for the management of this risk group rests primarily on the manufacturer. Most of these disruptions remain under its control, which allows for development of scenarios for preventive and limiting the likelihood of a particular threat occurrence.
2) **Internal supply-chain uncertainty.** Here should be introduced the following risks: end-customer demand, demand amplification, supplier, order forecast

horizon and chain configuration, infrastructure and facilities. Under the control of the supply chain participants, there are only a few sources of risk associated with creating demand, improving the quality of forecasts and creating chain configuration and infrastructure. For these components it is possible to prepare a strategy to prevent the occurrence of hazard. In the case of other disruption sources occurrence, the manufacturer is liable to develop scenarios that can only limit their negative effects.

3) **External uncertainties**, which include environment and disasters. These elements remain entirely outside the control of the supply chain participants. The only way to manage this type of risk is to prepare scenarios for reducing the effects of hazard event occurrence.

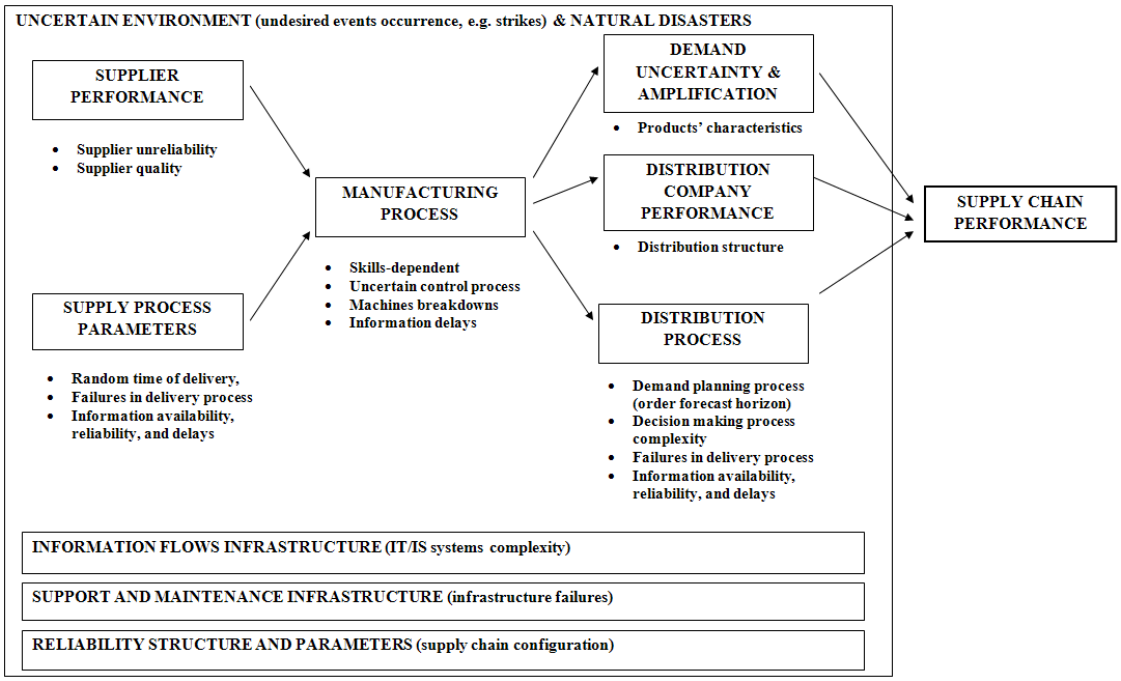


Fig. 5. Main disruptions that influence chosen supply chain performance

Analyzing the disruptions in manufacturer's logistics processes performance, it was found that the sources of risk are derived from all the three groups simultaneously. The example of conducted Ishikawa analysis for the defined disturbance - "low quality of created sales forecasts" are shown in Fig. 6.

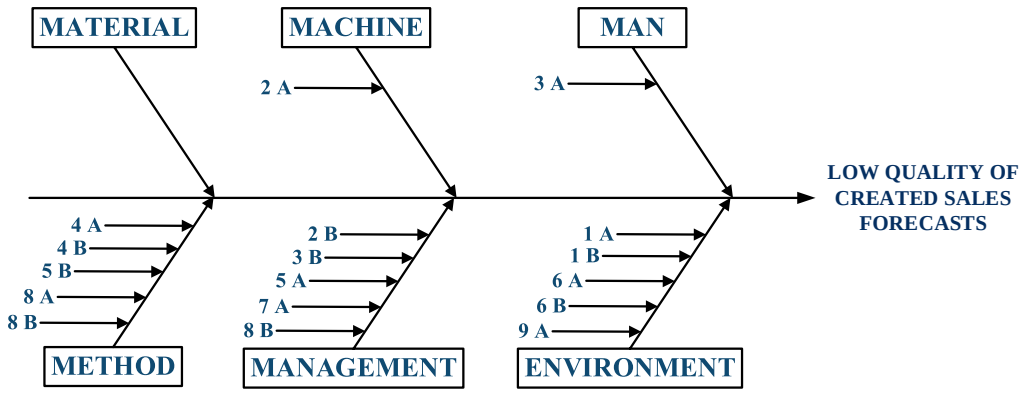


Fig. 6. Ishikawa diagram for low quality of created sales forecasts

In the Table IV, the causes highlighted in the Ishikawa diagram were classified as sources of risks defined in the Table III.

Table IV: The main causes of law quality of created sales forecasts consequence defined in the Ishikawa diagram

The causes' symbol	**The causes of disruptions**	**Source of disruption**
1A	The sale subject to weather conditions	Product characteristic
1B	Product dependent on fashion and current trends	
2A	Manufacturing constraints resulting from the machines and people efficiency	Manufacturing process
2B	Make to stock, (production surplus force company to organize the promotion that are not included in the forecasts)	
3A	Staff mistakes in recording of entry and release of goods in the shops	Uncertainty in control processes (control chaos)
3B	No measurement of the organized promotion influence	
4A	Forecasts created for many regions, each with different sales trends	Decision-making process complexity
4B	Forecasts created on the basis of historical data about the previous periods customers behaviour	
5A	Lack of important information about the external factors affecting the sale	IT/IS systems complexity
5B	The lack of various algorithms for determining the sale levels for different regions	
6A	Demand strongly dependent on external factors being difficult to predict	End-consumer demand variability
6B	Promotions strongly affecting consumer behaviour	
7A	Lack of changes in sales definition being a result of new stores opening	Demand amplification
8A	Only a short-term forecasting horizon can be optimized	Order forecast horizon
8B	Lack of determined methods and required information to make long-term sales forecasts	
9A	The strong impact of competition activities on the realized sale volume	Environment

The presented example clearly suggests that carrying out of risk analysis for logistics processes performance cannot be limited to only one group of the defined source of disruptions. Logistics systems, due to its complexity and interdisciplinary nature, have to be the subject of multi-criteria analysis, which are able to comprehensively investigate the existing problem.

The operations to prevent the occurrence of the defined risks can include the implementation of systems and procedures for securing the performance of IT tools (IT complexity) and the introduction of additional employee's training and

checkpoints on the production line (manufacturing process). Scenarios directed on reducing the effects of hazards occurrence can include strategies for the development of a distribution network in other markets (demand amplification) or can base on the development of special procedures in case of tremors or local flooding (disasters). The authors' further research studies are to be focus on the development of scenarios and strategies for preventing or reducing the effects of defined risks occurrence.

5. Summary

The high degree of coordination and the sales characteristic make described deliveries of footwear to retail chains are exposed to all kinds of disruptions. The company, in order to maintain a high competitive position must strive to reduce the impact of any occurred hazard events. Hence the high importance is given to properly carried out vulnerability analysis. The identification of hazards and determination of their nature will allow managers to better manage risk, both within the enterprise and across the supply chain. Because the manufacturer is a leader in the described supply chain and most of the associated chain units are his own or remains in a franchise, its ability to control and influence on individual units are much greater than in the classic supply chain performance. This fact should be used by him in order to reduce uncertainty of at least the first two classified groups (internal organization uncertainty and internal supply-chain uncertainty). Therefore, there should be taken steps regarding the appropriate procedures and the implementation of solutions based on planning scenario issues. In this way, managers will receive clear guidance on their actions performance in the event of the threat occurrence and, as a result, they shorten the time of their reaction.

The presented results provide an introduction to the initiated research on the use of vulnerability analysis as a tool for process controlling implementation in order to improve decision-making processes in the entire supply chain. The further research will be focused on the development of the tools to support risk management in supply chains and introduction of selection of analyses that support the controlling leader activities performance.

References

[1] Aleksic A., Stefanovic M., Tadic D., Arsovski S., A fuzzy model for assessment of organization vulnerability, Measurement, 2014, 51, pp. 214-223.

[2] Albino V., Garavelli A. C., A methodology for the vulnerability analysis of just-in-time production systems, International Journal of Production Economics, 1995, 41, pp. 71-80.

[3] Barker K., Ramirez-Marquez J. E., Rocco C. M., Resilience-based network component importance measures, Reliability Engineering and System Safety, 2013, vol. 117, pp. 89-97.

[4] Beamon, B. M., Supply Chain Design and Analysis: Models and Methods, International Journal of Production Economic, 1998, Vol. 55, No. 3, pp. 281-294.

[5] Berle O., Asbjornslett B. E., Rice J. B., Formal vulnerability assessment of a maritime transportation system, Reliability Engineering and System Safety, 2011, vol. 96, pp. 696-705.
[6] Blanchard, B. S., Logistics Engineering and Management (5th Ed), 2004, Upper Saddle River: Pearson Prentice Hall.
[7] Briano E., Caballini C. Revetria R., Literature review about supply chain vulnerability and resiliency, Proc. of the 8th WSEAS International Conference on SYSTEM SCIENCE and SIMULATION in ENGINEERING, 2009.
[8] Bukowski L., Feliks J, Evaluation of Technical Systems Dependability with the Use of Fuzzy Logic and Experts' Knowledge, Proceedings of the 15th World Multi-Conference on Systemics, Cybernetics and Informatics, Orlando (Florida), 07, 2011.
[9] Chapman P., Christopher M., Juttner U., Peck H., Wilding R., Identifying and managing Supply-Chain Vulnerability, Logistics & Transport Focus, 2002,Vol. 4, No. 4, pp. 59-70.
[10] Chlebus M., Nowakowski T., Werbińska-Wojciechowska S., Supply chain vulnerability assessment methods - possibilities and limitations, In: Safety and reliability of complex engineered systems: proceedings of the 25th European Safety and Reliability Conference, ESREL 2015, Zurich, Switzerland, 7-10 September 2015: CRC Press/Balkema, pp. 1667-1678.
[11] Christopher M., Peck H., Building the resilient supply chains, International Journal of Logistics Management, 2004, vol. 15, no. 2, pp. 1-14.
[12] Cohen, M. A., Lee, H. L., Strategic analysis of integrated production-distribution systems: models and methods, Operational Research, 1988, 36, 2, pp. 216-228.
[13] Cox A., Prager F., Rose A., Transportation security and the role of resilience: a foundation for operational metrics, Transport Policy, 2011, vol. 18, pp. 307-317.
[14] Creating a Resilient Supply Chains: A practical Guide. Cranfield School of Management, 2003, available at: *https://dspace.lib.cranfield.ac.uk/bitstream/1826/4374/1/Creating_resilient_supply_chains.pdf.*
[15] Fakoor A. M., Olfat L., Feizi K., Amiri M., A method for measuring supply chain resilience in the automobile industry, Journal of Basic and Applied Scientific Research, 2013, vol. 3, no. 2, pp. 537-544.
[16] Francis R., Bekera B., A metric and frameworks for resilience analysis of engineered and infrastructure systems, Reliability Engineering and System Safety, 2014, vol. 121, pp. 90-103.
[17] Henry D., Ramirez-Marquez J. E., Generic metrics and quantitative approaches for system resilience as a function of time, Reliability Engineering and System Safety, 2012, vol. 99, pp. 114-122.
[18] Huang Y-K., Vulnerability analysis of 18-hour retail delivery service using by Bayesian network, Electrical Review, 2012, 88(9b), pp. 9-12.
[19] Landeghem H. V., Vanmaele H., Robust planning: A New Paradigm for Demand Chain Planning, Journal of Operations Management, 2002, Vol. 20, No. 6, pp. 769-783.
[20] Longo F., Oren T., Supply chain vulnerability and resilience: a state of the art overview, Proceedings of The European Modeling & Simulation Symposium, Campora S. Giovanni (CS), Italy, 2008.

[21] Miao X., Xi B., Yu B., Triplex-network design for research of supply chain reliability, African Journal of Business Management, 2010, Vol. 4(1), pp. 31-38.
[22] Nowakowski T., Vulnerability vs. dependability of logistic systems, Proceedings of Carpathian Logistics Congress CLC 2013, 9-11 December 2013, Cracow, Poland.
[23] Nowakowski T., Analysis of possibilities of logistic system reliability assessment. In proc. symp.: ESREL 2006 Conference. Estoril, 18-22 September 2006, Estoril: Balkema.
[24] Nowakowski T., Tubis A., Werbińska-Wojciechowska S., Assessing the supply chain resilience – case study of footwear retail distribution network, Article prepared for European Safety and Reliability Conference ESREL 2016, 25-29 September, 2016, Glasgow.
[25] Nowakowski T., Werbińska-Wojciechowska S., Problems of logistic systems vulnerability and resilience assessment, In: P. Golinska (ed.), Logistics operations, supply chain management and sustainability, 2014, Springer, pp. 171-186.
[26] Nowakowski T., Werbińska S., Problem of logistic system availability assessment, In proc. symp.: X Total Logistic Management Conference. Zakopane, 7-9 December 2006.
[27] Peck H., Reconciling supply chain vulnerability, risk and supply chain management, International Journal of Logistics: Research and Applications, 2006, 9(2), pp. 127-142.
[28] Ponis S. T., Supply chain resilience: definition of concept and its formative elements, The Journal of Applied Business Research, 2012, vol. 28, no. 5, pp. 921-930.
[29] Rao S., Goldsby T.J., Supply chain risks: a review and typology, The International Journal of Logistics Management, 2009, vol. 20, No. 1, pp. 97-123.
[30] Sheffi Y., The Resilient Enterprise. Overcoming Vulnerability for Competitive Advantage, The MIT Press, 2007.
[31] Schoon M., A short historical overview of the concepts of resilience, vulnerability, and adaptation, Workshop in Political Theory and Policy Analysis Indiana University, Working Paper W05-4, 2005. *http://www.indiana.edu/~iupolsci/gradcv/schoon/historical_critique.pdf*
[32] Simangunsongy E., Hendry L.C., Stevenson M., Supply-chain uncertainty: a review and theoretical foundation for future research, International Journal of Production Research, 2012, pp. 4493–4523.
[33] Singhal P., Agarwal G., Lal Mittal M., Supply chain risk management: review, classification and future research directions, International Journal of Business Science and Applied Management, 2011, vol. 6, Issue 3, pp. 15-42.
[34] Supply chain vulnerability. Executive Report, Cranfield University School of Management, 2002. *http://www.som.cranfield.ac.uk/som/dinamic-content/research/lscm/downloads/Vulnerability_report.pdf*
[35] Svensson G., A conceptual framework of vulnerability in firms' inbound and outbound logistics flows, International Journal of Physical Distribution and Logistics Management, 2002, 32(2), pp. 110-134.

[36] Svensson G., A conceptual framework for the analysis of vulnerability in supply chains, International Journal of Physical Distribution and Logistics Management, 2000, 30(9), pp. 731-750.
[37] Szozda N., Werbińska-Wojciechowska S., Influence of the demand information quality on planning process accuracy in supply chain: case studies, LogForum, 2013, vol. 9, nr 2, pp. 73-90.
[38] Thomas M., U., Supply chain reliability for contingency operations. Proceedings of Annual Reliability and Maintainability Symposium, 2002, Available at: http://ieeexplore.ieee.org/iel5/7711/21135/00981621.pdf (29.11.2006).
[39] Thun J-H., Hoenig D., An empirical analysis of supply chain risk management in the German automotive industry, International Journal of Production Economics, 2001, 131, pp. 242-249.
[40] Vlajic J.V., van der Vorst J.G.A.J., Hendrix E.M.T., Food supply chain network robustness - A literature review and research agenda, Proceedings of the International Conference on Management in Agrifood Chains and Networks, 2008, Wageningen, the Netherlands, pp. 1 – 17.
[41] Wagner S. M., Neshat N., A comparison of supply chain vulnerability indices for different categories of firms, International Journal of Production Research, 2012, 50(11), pp. 2877-2891.
[42] Werbińska-Wojciechowska S., Time resource problem in logistic system dependability modelling, Eksploatacja i Niezawodnosc – Maintenance and Reliability, 2013, Vol. 15 (4), pp. 427-433.
[43] Werbińska S., Model of logistic support for exploitation system of means of transport, Ph.D. dissertation, 2008, Wroclaw University of Technology.
[44] Wicher P., Lenort R, Krausova E., Possible applications of resilience concept in metallurgical supply chains, Proc. of METAL Conference, 23-25.05.2012, Brno, Czech Republic, 2012.
[45] Wu T., Blackhurst J., O'Grady P., Methodology for supply chain disruption analysis, International Journal of Production Research, 2007, Vol. 45, No. 7, pp. 1665-1682.

Modelling Software Failures of Digital I&C in Probabilistic Safety Analyses

Mariana Jockenhövel-Barttfeld
Andre Taurines
Yousef Abusharkh
Christian Hessler
AREVA GmbH
Henri-Dunant-Strasse 50
91058 Erlangen, Germany

Hervé Brunelière
AREVA SAS
TOUR AREVA - 1 Place Jean Millier
92084, Paris La Défense cedex, France

Abstract

This paper focuses on the modelling of software failures of digital I&C systems in the PSA. Software faults, failures and effects are analyzed generally for digital platforms, which implement I&C safety systems of nuclear power plants. The safety platform TELEPERM® XS (TXS) developed at AREVA is used for illustration purposes. Based on this, a framework for modelling software failures using basic events in the PSA fault trees is presented.

Keywords: software reliability, failure modes, system software, application software, acquisition and processing unit, voting unit.

1. Introduction

Digital instrumentation and control (I&C) systems appear as upgrades in older nuclear power plants (NPP) and are standard in new plant designs. To assess the risk of the NPP operation and to determine the risk impact of digital system upgrades on NPPs, quantifiable reliability models are needed along with data for digital systems that are suitable for usage in existing probabilistic safety assessments (PSA). Due to the many unique attributes of digital I&C systems (e.g. complex dependencies, software), several challenges exist in systems analysis, modelling and in data collection.

Currently there is no common approach available in the nuclear field for assessing the reliability of digital I&C and meeting related regulatory requirements (for a literature review, see [1]). In addition, digital I&C systems can be probabilistically analyzed on several detail levels, which raises additional questions regarding the level of detail of

the fault tree modelling, relevant failure modes for hardware and software modules and dependencies between different I&C systems. Selection of plausible failure data, including common cause failure (CCF) data, for hardware and software failures is still an open issue for digital I&C systems.

This paper presents a framework for the consideration of software failures of I&C systems in a nuclear PSA context. The analysis covers the system software, i.e. operating system and runtime environment, and application software (AS), i.e. representation of I&C functions in the form of code. The aim is to define a simple yet sufficient framework for the software reliability analysis, which describes the software failure modes, mechanisms and effects.

The software analysis is carried out generically by considering common features of digital platforms, that can be qualified for the implementation of safety I&C systems in nuclear power plants. The safety I&C system platform TELEPERM® XS (TXS), developed at AREVA, is brought up in more detail with the purpose of illustrating the analysis.

Accordingly, a brief overview of the normal operation cycle of TXS is presented in the next chapter. In Chapter 2 a failure mode and effect analysis for software is presented. Chapter 3 outlines the framework to model software failures in the PSA, including insights regarding the modelling level. The main conclusions of this paper and future research activities are highlighted in Chapter 4.

The work presented in this paper has been developed within a corporate research and development program at AREVA in collaboration with the Nordic DIGREL Project (see references [1], [2]).

1.1 TXS Normal Operation Cycle

In Figure 1, the TXS application cycle during normal operation is shown. This cycle runs in every TXS processor.

Each processing cycle comprises eight phases, which are controlled by the runtime environment (static structure of code containing the calls to the individual pieces of code performing the activities of the individual phases).

The processing activities assigned to these phases comprise of(see Figure 1):

- Cyclic input (phase 1 to 3),
- Processing of the application software (phase 4; application functions A to E),
- Output of the application specific data (phase 5 to 7) and
- Self-tests and service tasks (phase 8).

The design of the processing cycle ensures a strictly cyclic operation of each processor of an I&C system independently of the status of the plant process. The self-test task covers tests of the hardware equipment (e.g. processor, memory) and is performed in a background process independently of the application processing cycle.

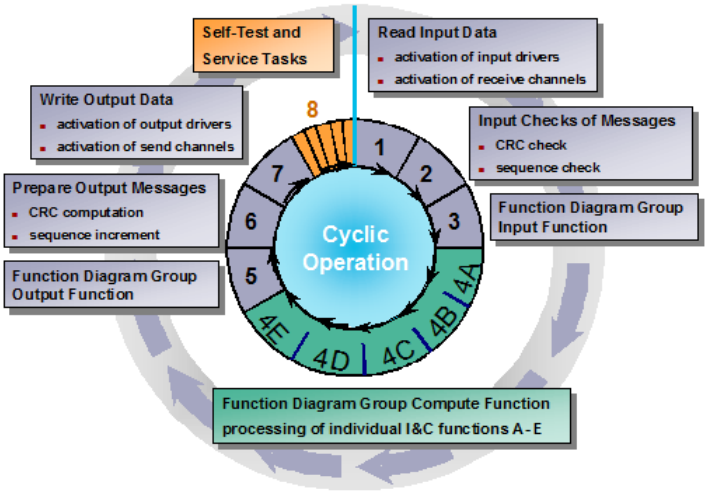


Figure 1. Normal TXS operation cycle.

In addition, self-monitoring activities are implemented as part of the processing unit application cycle task (e. g. input data validation, communication monitoring).

2. Software Failure Modes and Effect Analysis

The aim of this analysis is to derive failure modes and effects for probabilistic analyses of software (e.g. in the PSA). The main objective is to answer the questions associated to the failure of software, such as for example:

- Which are the relevant latent faults in the software that can be turned into failures?
- Which are the main triggers and mechanisms leading to software failures?
- Which are the covering failure modes and effects to be considered in reliability analyses?

The analysis of software failure modes and effects builds partly on the work on taxonomy of failure modes of digital components for the purposes of PSA conducted by the international OECD/NEA Working Group RISK [3].

The focus of this analysis lies on the reactor protection system (RPS) of a NPP, which is considered to be more relevant for the PSA than other I&C systems, such as the reactor limitation and control systems. In the next sections software fault, failures and effects will be analyzed.

2.1 Software Faults, Failures and Triggers

Software failures result as a combination of a latent fault with a trigger and are caused by systematic faults (i.e. due to errors when writing the design specification or implementing the design, or when performing modification). In the case of digital systems, software works incorrectly i.e. it does not perform its intended function, if (see [4])

- Its specification was inadequate, incomplete or incorrect,
- Its specification was interpreted incorrectly during implementation, and
- Testing did not include the specific signal trajectory that reveals the fault.

Since software cannot be proven to be 100% error free, software design faults are a credible source of software failures. As pointed out in [4], latent faults may be also related to maintenance or modification activities.

Software failures have a *common cause nature* given the fact that

- The same single piece (module) of software is processed in all divisions of a redundant I&C system,
- There are common triggers which can act upon all divisions of an I&C system, turning latent systematic faults of the software into coincidental failures.

Based on [4], the *triggers* that can activate latent software faults causing coincidental failures are

- Human actions (e.g. inadequate/faulty maintenance),
- Signal trajectory/internal states,
- External events,
- Temporal effects,
- Events associated to faulty communication between processors (e.g. faulty telegrams).

Note that external events as triggers (such as e.g. seismic event, flooding, extreme ambient conditions) are not relevant as they do not interact with the software. They may only act indirectly as triggers (through the plant response), which is only relevant if the probabilistic analysis includes the influence of such events, for example in the context of an external events PSA or seismic PSA.

Human actions can trigger latent software faults mainly in maintenance-related activities. Faulty maintenance can be both, a trigger of latent software faults and an introduction of latent faults into the software. Failures of maintenance can spread through the redundancies and can, at worst, have a similar effect as the one caused by the trigger “faulty telegram”.

2.2 Classification of Software Failures and Failure Modes

Software failures can be classified according to their *impact on the processor* into *fatal* and *non-fatal failures*. A fatal failure is characterized by the ceasing of the processor activity, i.e. the generation of outputs ceases (operation cycle stops, see Figure 2 (a) illustrating the TXS cycle) and an exception handler sets the output values into defined fail-safe (pre-defined) values.

A non-fatal failure is characterized by the correct execution of the code, but the code contains e.g. an algorithm which is inappropriate for certain values of the signals (e.g. a missing code branch in the code).

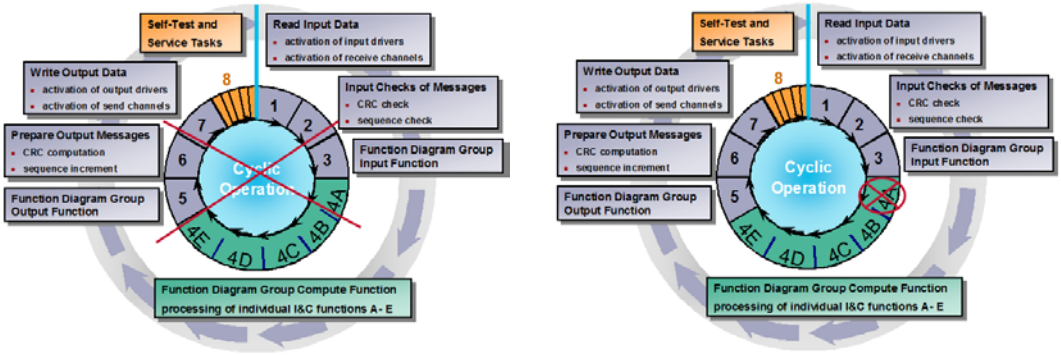


Figure 2. (a) Failure of one TXS processor. (b) Failure of one application function processed in TXS.

The effect is generally that the processing unit continues to operate cyclically (non-fatal consequences for the processor), but the requested application function (AF) is not executed (e.g. function A in Figure 2 (b), with consequences of a failure on demand), or a different response than expected is obtained (spurious actuation of the function).

Software failures can be further classified according to their *detectability* into self-announcing (SA) and not-self-announcing (NSA) failures. A SA failure is detected by the I&C system via the self-monitoring features, i.e. the failure is detected during plant operation independently from a plant demand. NSA software failures are those which cannot be detected by the I&C system and can only be revealed (and noticed by an observer) in case of a plant demand (i.e. a demand to the faulty safety function; the fault remains undetected until a demand occurs).

The operation of the TXS safety I&C system platform is independent from plant demand. Detected failures always lead to a ceasing of the processor activity with outputs set into defined fail-safe values (fatal failure). In addition to the design measures aiming at such a fail-safe behavior, various design features minimize fault propagation. These include separation between system and application software, separation between application functions and communication independence between processing units.

The *failure modes for software*, defined as the functional manifestation of the software failure, that can be derived for one processor of a safety digital platform can be defined as:

- Shutdown of the processor,
- Unavailability of one application function, and
- Spurious actuation of one application function allocated in the processor.

The extent of these failure modes to be considered in the PSA, i.e. how many processors/functions are involved in the coincidental failure, is analyzed in the next chapter.

2.3 Software Failure Effects

For the purpose of defining the effects and extent of software failures, the generic safety I&C architecture of the RPS shown in Figure 3 is assumed.

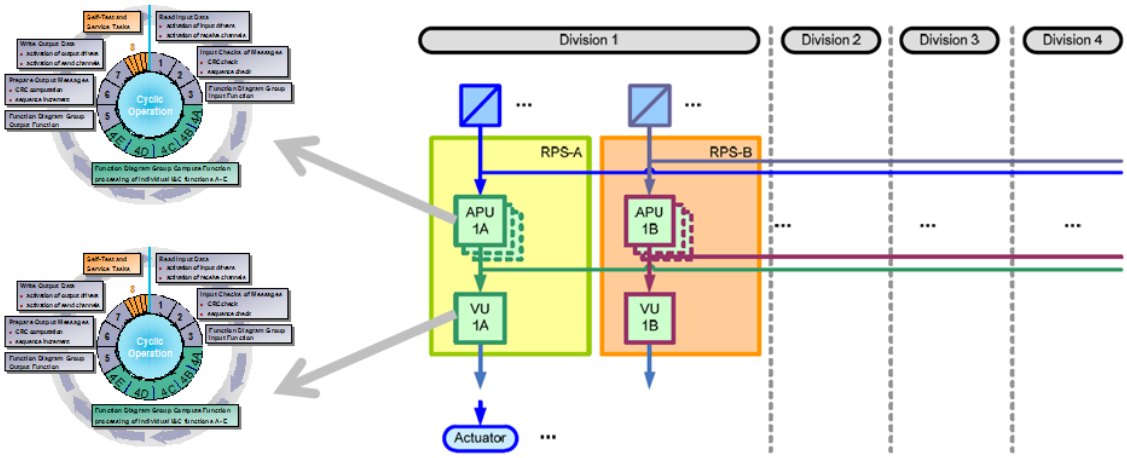


Figure 3. Generic RPS architecture, taken from [2]. Operating cycle of processors illustrated with the TXS cycle (see left hand side).

The example RPS consists of two diverse subsystems, called reactor protection system subsystem A (RPS-A) and subsystem B (RPS-B), both divided into four physically separated divisions. The following assumptions are considered to define the extent of diversity between RPS-A and RPS-B:

- The *platforms* of both subsystems, defined by the hardware modules, operating system and specific software, are assumed to be identical (an architecture found in several TXS applications - therefore the platform CCF has to be considered).
- Both subsystems, RPS-A and RPS-B, process different I&C functions (functional diversity between both subsystems is assumed).

The number of acquisition and processing units (APU) and voting units (VU) in each subsystem and division may vary. It is assumed that there can be more than one APU/VU per subsystem and division.

The qualitative software failure mode analysis focuses on

- Identification of safety-critical software modules in I&C units,
- Identification of possible effects of postulated faults in the safety-critical software modules and
- Identification of defensive measures against the software faults.

The failure mode and effects analysis for software is based on postulating successively a single software fault in each software module and determining the maximum possible extent of the failure.

The software modules defined in Table I are considered to be relevant for the PSA (for more details, see [2]). Depending on the location of the software fault, on the failure effect and on the system architecture, one or more units (APU/VU) in one or more subsystems can be affected.

Table I: Relevant software modules for the probabilistic analysis.

Software modules		**Abbreviation**
System software	Operating system and runtime environment (interaction between application and operating system).	SyS
Elementary functions	Reusable, closed, and classifiable piece of software, capable of processing signals, from which application software can be assembled using function diagrams.	EF
Application software	Functional requirements specifications (FRS) of I&C functions implemented in the APU/VU	APU-FRS VU-FRS
	Coding of I&C functions implemented in the APU/VU	APU-AS VU-AS
Proprietary software	Code that is embedded in specific hardware modules, different from the microprocessor module of APU, VU	-
Data communication software	Code that implements the data communication protocol. It is part of the system software.	DCS
Data link configuration	Specifies the data that constitute a given network and the data messages exchanged between the nodes of the network. This software module is specific to each subsystem (RPS-A resp. RPS-B).	DLC

As denoted in [1], the cases defined in Table II are considered to be relevant for modelling software failures in the PSA and implicitly cover the faults of other software modules (e.g. EF, proprietary software, DLC).

Next, the cases identified in Table II are briefly described. For more details, including failure mechanisms, refer to [1] and [2].

2.2.1 Unavailability of the Complete System

Case 1 of Table II considers a software failure causing the loss of both subsystems (SYSTEM, see Figure 4). This is a postulated failure for the PSA, which results from a latent fault in the system software combined with insufficient functional diversity in the subsystems RPS-A and RPS-B.

Failure mechanisms affecting computers within both subsystems can be triggered by the same internal states (latent fault in the system software) or by the same signal trajectories (latent fault in the application software). In both cases, the failure of the complete system results from an insufficient diversity of the application software in both subsystems. The cause of the system failure is an impermissible interference from the application software on the system software triggering an exception, which turns the processor into a “safe state” (fatal failure, output signals set into “fail-safe” values).

Table II: Screening of relevant software faults for the probabilistic analysis.

Failure effect	Definition of effects	Software fault location					
		SyS	APU-FRS	APU-AS	VU-FRS	VU-AS	DCS
SYSTEM	Loss of complete system (RPS-A and RPS-B)	case 1(1)					case 1(1)
1SS	Loss of one subsystem (e.g. RPS-A or RPS-B)	case 2a	case 2a		case 2a	case 2a	case 2b
1APU-1SS	Loss of one group of redundant APU in one subsystem		case 3a	case 3a			
1VU-1SS	Loss of one group of redundant voters in one subsystem				case 3b	case 3b	
1AF-1SS	Loss of one application function in all divisions of one subsystem		case 4a	case 4a	case 4b	case 4b	
1AF-1D-1SS	Loss of one application function in one division of one subsystem		case 4c	case 4c			

(1) Latent fault in the system software combined with insufficient functional diversity in both subsystems.

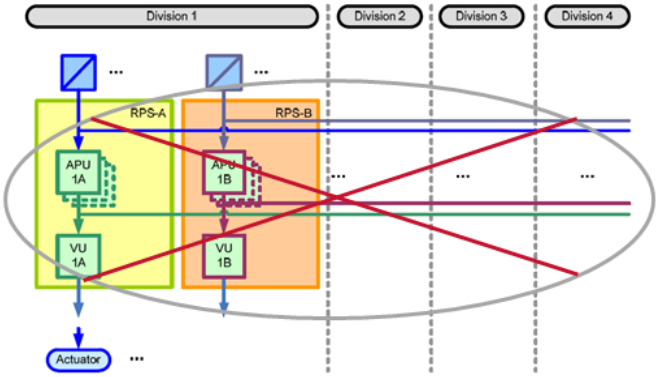


Figure 4. Postulated failure of the complete system caused by a latent fault in the system software in combination with insufficient diversity in the application software.

This failure can be considered in the PSA for all subsystems that have the same system software to evaluate the level of platform diversity involved in the I&C architecture. Note that in general I&C architectures for new plant designs involve back-up systems implemented in diverse platforms (not influenced by the loss of both RPS subsystems).

The probability associated to such an event is extremely low given the weak correlation between both RPS subsystems (RPS-A/B) if sufficient diversity has been considered for the application software. The correlation of both subsystems due to erroneous maintenance is very weak. This is prevented by a design that ensures clear separation of systems and networks and adequate access control. Correlation of both subsystems due to failure mechanisms triggered by faulty telegrams or by time-

related triggers can be neglected, if both subsystems do not communicate with each other and the processors of both subsystems are not started simultaneously to avoid time-dependent effects.

2.2.2 Unavailability of one Subsystem

Case 2 of Table II considers a software failure, which causes the loss of one subsystem (1SS) due to a fatal (fail-safe) failure (see Figure 5).

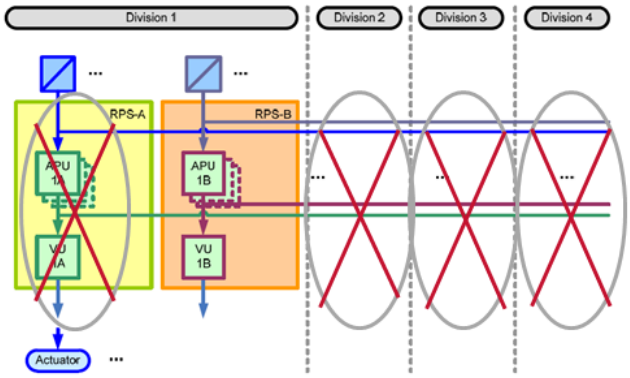


Figure 5. Failure of one subsystem.

This is the failure of one subsystem involving all divisions. The latent fault can be located in the system software (see case 2a in Table II) or in the communication software (case 2b).

2.2.3 Unavailability of one Group of Redundant Processors

Case 3 of Table II considers the failure of one group of redundant processors (APU/VU) in all divisions (see cases 3a – in Figure 6 - and 3b, respectively). In this case the latent fault is located in the application software (from design errors in the FRS or the coding of the FRS). The triggers are the input signals with the same trajectories that are processed in different divisions of an I&C system. The combination of latent AS faults with certain values (not-tested) of input signals has the potential of leading to a software failure affecting the group of redundant processors, in which the function is implemented.

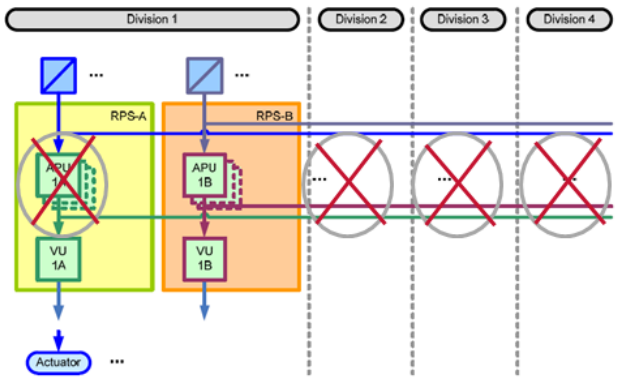


Figure 6. Failure of one group of redundant APU.

In this case, the failure causes an inadmissible interference with the system (e.g. as a consequence of inoperable values, such as a division by zero).

2.2.4 Failure of the one Application Function

Case 4 in Table II considers a latent fault in the application software causing the failure of one or more application functions (containing the faulty software module), but not leading to the loss of all application functions in the processor (cyclic processing is not interrupted).

The latent fault (either in the FRS or AS code, e.g. faulty specification of a threshold) can be located in the APU (see case 4a in Table II; see Figure 7), VU (4b) and have an effect in all (cases 4a and 4b) or in only one division (case 4c). The trigger is the same signal trajectory.

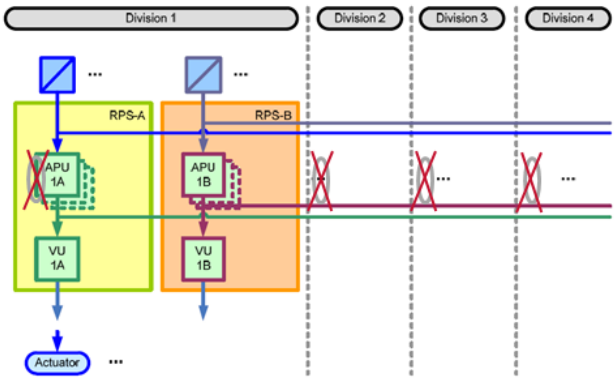


Figure 7. Failure of one application function processed in the APU.

This is a non-fatal failure and can result in the failure to actuate an application function (unavailability, e.g. threshold wrongly specified too high) or in the spurious actuation of an application function (e.g. threshold wrongly specified too low). These failures can only be revealed after a demand of the faulty function.

3. Modelling Software Failures in the PSA

The qualitative failure analysis outlined in the previous chapter builds the basis for modelling software failures in the PSA. The major challenge consists in defining a proper framework, which is compatible with existing PSA fault tree models.

In the next chapter, software failure modes to be considered in the PSA will be defined.

3.1 Definition of Software Failure Modes for the PSA

Table III summarizes the list of basic events for modelling relevant software failure modes for the PSA. As analyzed in Chapter 2, these basic events/failure modes cover all possible software fault sources, triggers and maximum extent of possible effects.

One basic event can be defined to model the (postulated) failure of the complete system. Even though the failure probability of this basic event, P(SYSTEM), is extremely low the consideration of this in the PSA allows evaluation of the level of platform diversity involved in the I&C architecture.

Table III: Basic events associated with relevant software failures for the PSA.

Basic event	Description	Failure mode	Reference group	Latent fault location			Triggering mechanism	Failure probability
				SyS	AS	DCS		
SYSTEM	Unavailability of the complete system(2)	Processor shuts down	All processors with the same system software	X(3)		-	Same internal states(3)	P(SYSTEM)
					X(4)		Same signal trajectory(4)	
1SS-i-SyS	Unavailability of one subsystem	Processor shuts down	All processors that are started-up simultaneously(5)	X			Temporal effect	P(1SS-SyS)
1SS-i-DCL	Unavailability of one subsystem	Processor shuts down	All processors that communicate with each other			X	Faulty telegrams/ maintenance	P(1SS-DCL)
1APUi-1SS	Unavailability of all APUi	Processor shuts down	All APUi that allocate the faulty software module(6)	X			Same signal trajectory	P(1APUi-1SS)
					X			
1VUi-1SS	Unavailability of all VUi	Processor shuts down	All VUi that allocate the faulty software module(6)	X			Same signal trajectory	P(1VUi-1SS)
					X			
ASi-UN	Unavailability of AS module i	Failure on demand of an AF	AS module i in all divisions		X		Same signal trajectory	P(ASi-UN)
ASi-SP	Spurious actuation of AS module i	Spurious actuation of an AF	AS module i in all divisions		X		Same signal trajectory	P(ASi-SP)

(2) Postulated failure for the PSA.
(3) Latent fault in SyS triggered by same internal states combined with insufficient functional diversity.
(4) Latent fault in AS triggered by same signal trajectory combined with insufficient functional diversity.
(5) Usually all processors within one subsystem are started-up simultaneously.
(6) The faulty module can be located in the application or in the system software.

One basic event for each subsystem can be defined to model the failure of one subsystem caused by failures of the system software (1SS-A-SyS, 1SS-B-SyS) and by communication-triggered failures (1SS-A-DCL, 1SS-B-DCL).

One basic event for each group of processors (APUi/VUi) models the unavailability of the group caused by latent failures in the system or application software triggered by the same signal trajectory.

Failures of one application function/module (see ASi-UN, ASi-SP in Table III) have to be modelled by application function and failure mode specific basic events. As recommended in [1], the modelling of application software failures in the PSA at a software module level is a convenient level to address dependencies between I&C functions. As various I&C functions may share common input signals, modelling the failure of input signals acquisition and processing with a specific software module allows the dependencies between functions using the same pieces of application software to be automatically addressed.

3.2 Assessment of the Probability of Software Failures

Failures of the system software can be directly assessed using the operating experience of the specific platform, if these failures can be detected during operation, independently of plant demands.

As discussed in [1], the probability assessment of the application software (see P(ASi-UN) and P(ASi-SP) in Table III) depends on the software complexity and level of verification and validation (V&V). The amount of application software faults introduced during the software design is considered to be correlated to the

- *Complexity of the application software*: the less complex the application, the lower is the likelihood of having latent faults in the software and
- *V&V* process: the higher the system classification, the higher the V&V requirements, the higher the likelihood to discover latent faults during the system design phase.

For the TXS platform, the operating experience is based on an assessment of the non-conformance reports database. The historical data includes the operating experience with the TXS platform installed in more than 60 nuclear-related plants worldwide for commercial plant operation. These I&C systems are permanently in operation, are broadly monitored, and have been working reliably and accumulating applicable operating experience, beginning with the first systems in 1998. Operating experience evaluated so far covers nearly 15 years. All observed failures of the TXS platform are single failures with no evidence of CCF.

For details on the estimation failure rates/probabilities for the failure modes listed in Table III, refer to [1]. For an outline of the methodology for the probabilities estimation, refer to [5].

4. Conclusions

This paper presented an analysis of software failures of digital I&C systems in nuclear context. Failure modes for modelling failures of system and application software in probabilistic safety assessments were defined. The effects of software failures were outlined for a generic RPS architecture. The analysis can however be extended to other I&C architecture/systems.

The following failures, which are caused by *system software* failures:

- Unavailability of the complete system (postulated failure),
- Unavailability of one subsystem caused by system software failures and
- Unavailability of a group of processors which communicate with each other (e.g. one RPS subsystem) caused by communication failures.

and by *application software failures*:

- Unavailability of one processor in all divisions (in which the faulty application function/module is processed),
- Failure on demand (unavailability) of one application function/module and
- Spurious actuation of one application function/module.

have been identified to be considered in probabilistic safety analyses.

Future work includes guidance on assessing the complexity level of the application software and dependency treatment among non-identical application software modules.

Acknowledgements

The authors are very thankful to Arnold Graf for the interesting discussions.

References

[1] Bäckstrom, O., Holmberg, J.-E., Jockenhövel-Barttfeld, M., Porthin, M., Taurines, A., Tyrväinen, T. (2015) Software reliability analysis for PSA: Failure Mode and Data Analysis - *Nordic nuclear safety research (NKS) Report, NKS-341* - ISBN 978-87-7893-423-9.

[2] Bäckstrom, O., Holmberg, J.-E., Jockenhövel-Barttfeld, M., Porthin, M., Taurines, A. (2014) Software reliability analysis for PSA - *Nordic nuclear safety research (NKS) Report, NKS-304* - ISBN 978-87-7893-381-2.

[3] OECD (2014) Failure modes taxonomy for reliability assessment of digital I&C systems for PRA, report prepared by a task group of OECD/NEA Working Group RISK, NEA/CSNI/R(2014)16, OECD/NEA/CSNI, Paris.

[4] IAEA (2009) Protecting against common cause failures in digital I&C systems of nuclear power plants - *Nuclear Energy Series No. NP-T-1.5*

[5] Jockenhövel-Barttfeld, M., Bäckstrom, O., Holmberg, J.-E., Porthin, M., Taurines, A., Tyrväinen, T. (2015) Modelling software failures of digital I&C in probabilistic safety analyses based on the TELEPERM® XS operating experience – *International Journal for Nuclear Power, atw Vol. 60 Issue 3*.

Assessment of risks and uncertainties for concepts during early-phase design of public investment-projects – Outlining the concept of Reversed LCC as a basis for infrastructure assets

Erling Salicath (*;***), Vicente González-Prida (**), Antonio Guillén (**), Jayakumar Shambhu (*), Adolfo Crespo (**)

(*) University of Stavanger, Norway
(**) University of Seville, Spain
(***) Utdanningsetaten, municipality of Oslo, Norway

Abstract

The purpose of this paper is to improve the decision-making process in the conceptual phase of public infrastructure-projects by identifying and managing risks, cost drivers and uncertainties based on uncertain conditions and lack of relevant data. Criticality analysis is introduced to clarify how to qualitatively identify risks and properly quantify costs associated with the most critical functions and business criteria in the conceptual phase. These phases can potentially be operationalized through a life-cycle design approach by comparing relative differences in risk-profiles, uncertainties, life-cycle costs and worst/-best case scenarios for different investment-alternatives; investment processes from the municipal sector in Norway is specified, with public schools as a basis to expand the practical knowledge on how to align conceptual life-cycle design-aspects with measurable project-goals and future cost drivers associated with the operations, safety, comfort, maintainability and functionality of assets. The life-cycle costing tool *Reversed LCC* [1] is presented, as a basis for generalized phases on infrastructure assets, aimed at both achieving the lowest possible life-cycle cost and meeting specific business objectives and needs.

Keywords: Asset Management, Criticality Analysis, Conceptual studies, Uncertainty, Risk, Life-cycle costing

[1] *Reversed LCC* is a cost-model developed by Erling Salicath in cooperation with the municipal agency Undervisningsbygg Oslo KF. The premise of this tool is to highlight how underfunded operating budgets for infrastructure affects the life-cycle economy.

1 Introduction

This paper presents a generalized research for infrastructure assets based on *Reversed LCC* (Salicath, 2015; Salicath & Liyanage 2015). The paper provides guidelines on how to optimize decision-making processes in the conceptual phase of public infrastructures, identifying- and highlighting relevant life-cycle cost drivers and manage future risks and uncertainties. Criticality analysis is introduced to this research, as a tool to quantify risks and costs associated with critical functions and business criteria. Infrastructure in this paper reflects both typical infrastructure such as roads and sewer assets, and social infrastructure which includes assets in the health, education, housing, utilities and transport sector.

Salicath et al. (2015) includes a case-study of public assets, which from a portfolio-perspective highlights how underfunded maintenance-budgets can potentially accelerate maintenance-backlog and increase the depreciation rate, due to reduced service-life and an earlier need for upgrading assets. The case-study highlighted that increased funds towards operational costs financed through activity-based rates in the rental contract, does release tied-up capital and reduces the life-cycle cost, including future development- and upgrading costs. The case-study supports the assumption that the implementation of an activity-based costing method sustains real value through the life-cycle of buildings, and lowers the total cost of ownership[2].

1.1 Asset management for building and infrastructure - ISO 55000 & PAS 1192

The optimization of building operational phase is increasingly complex. In addition to intrinsic complexity of such intricate facilities it has to consider legislated and sustainability demands, fit-up and space usage requirements (Zhang et al., 2009). This complexity scenario is completed with the trend to outsourcing services, and the introduction of procurement routes that include operation and maintenance in integrated supply contracts. FM (Facility Management) as discipline provides a holistic view of the building operation and maintenance, an overall management of the resource available towards the strategic objectives of facilities' users and owners. Here is located the potential of FM rather than the accumulation of maintenance task or new software applications. FM is a broad concept, covering everything from real estate and financial management to maintenance and cleaning (Atkin & Brooks, 2009). FM is defined by EN 15221-1 “integration of processes within an organization to maintain and develop the agreed services which support and improve the effectiveness of its primary activities.”

AM (Asset Management) and FM are overlapped disciplines. The terms AM and FM are often used interchangeably, though there are differences in approach between the asset management and facilities management disciplines. FM is focused on the infrastructure and building sectors while AM has a broader application field. Especially in the building sector, FM is considered a consolidated profession (IFMA, 2013). Both have generated their own standards or specifications and both have evolved their

[2] Based on qualitative assumptions, a buildings' life-cycle is assumed to be 15 years due to underfunded operating budgets, and 20 years due to activity-based operating budgets before upgrading is required. The correlation between capital costs, operating costs and investment in technical equipment does affect the assets' operational service life and upgrading costs. The life-cycle performance of the building in this example with a service-life of 20 years does potentially release a considerable amount of tied-up capital for the owner; the potential savings for the owner depends on how much funds are actually spent on activities that extends the life-cycle of critical assets, how much the activities cost in total, including upgrading- and development costs, and when these activities occur in time.

own language of preferred and defined terms. The ISO 55000 list FM as asset management activities. With this view FM can be considered as a part or tool of AM, since AM goes beyond FM providing a more comprehensive view and more potential benefits.

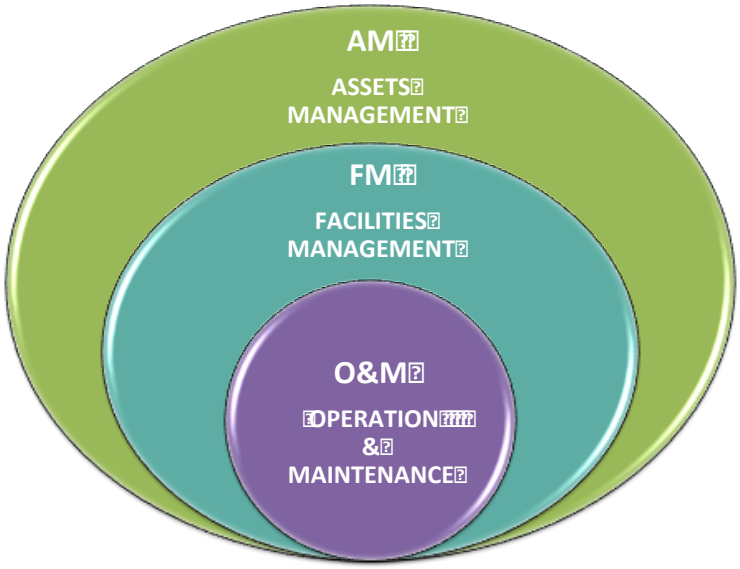


Figure 1: Integration of FM and AM in buildings

The benefits of AM are beginning to prove in many industries and business environments, improving the performance along the lifecycle and the contribution to the safety, health and the protection of the environment; while demonstrating organizational commitment to quality, performance or safety and helping to mitigate the legal, social and environmental risks associated with accidents industrial facilities. Asset Management, as discipline, allows organizations to optimize the whole life value of managing portfolios of assets. For a unique organization the list of assets, or portfolio, can contain varied assets in nature, distributed over extensive geographical areas and may be subjected to differing demand/utilization requirements. In concordance with the ISO 55000, AM can be applied to all type of assets, including physical assets (elements, inventory and properties) and intangibles assets (leases, brands, digital assets, use rights, licenses, intellectual property, etc.).

Asset management is not a new issue, because asset management activities have been ongoing since the use of capital goods, buildings, transportation systems, water systems, energy or any other type of asset production or service delivery. These physical assets have been controlled by business functions, such as maintenance, which manages the facility, as well as repair work and review to ensure the regular functioning and the good condition of production facilities, services and instrumentation for process control organizations. However, changes in our life and business environments make asset management "coordinated activity of an organization to realize value from its assets", which constitute an effective and efficient model to meet the challenges of the changing global market today.

The general principles of AM have been defined by the family of standards ISO 55000, ISO 55001 and ISO 55002. Among the aspects contained in this approach, those which can be described as more innovative, and representing a significant advance in the optimization of asset management may be included:

- Manage the value of the asset. AM supports the realization of value while balancing financial, environmental and social costs, risk, quality of service and performance related to assets.
- Risk based decision-making. Effective control and governance of assets by organizations is essential to realize value through managing risk and opportunity, in order to achieve the desired balance of cost, risk and performance.

- Integrating the longer term activity of asset management with the shorter term activity of asset acquisition
- Treatment of stakeholders. The stakeholders requirement but also the information exchange and the suitable access to the information (right information, to right person at the right moment)
- The information requirement and its treatment. AM is intensive in data/information management. Asset information system can be extremely large and complex; generating, controlling and documenting this information is a critical function of the asset management system.

This last point reinforces the importance of information management in AM. The Information System is one of the key elements of the asset management system (AMS) defined in ISO 55000-1 (figure 1). An asset management system is a set of interrelated and interacting elements of an organization, whose function is to establish the asset management policy and asset management objectives, and the processes, needed to achieve those objectives. In this context, the elements of the asset management system should be viewed as a set of tools, including the information systems, which are integrated to give assurance that the asset management activities will be delivered. For building asset management, this required information system could be implemented from the implementation of building information models (BIM).

The intention of BIM as a process is typically to reduce the time of construction. Managing the complexity of information for operating and maintaining assets might be a time-consuming factor, and can reduce the incentives behind implementing BIM for asset management systems. Implementation of BIM in asset management systems is useful though, particularly when the service life for physical assets have a long life-cycle span; aging assets does increase the risk for owners because the amount of necessary repairs, replacements etc. will at some point escalate over time regardless of the maintenance program. The implementation of BIM-models can therefore potentially provide useful information for asset managers through the life-cycle phases. An incentive within this context is that risks can be reduced through the assets' life-cycle because relevant information will be easily available through BIM.

1.2 PAS 1192-2 and PAS 1192-3

PAS 1192-2:2013 “Specification for information management for the capital/delivery phase of construction projects using building information modeling (BIM) Level 2” and PAS 1192-3:2014 “Specification for information management for the operational phase of assets using building information modeling”, are complementary documents that specified an information management process to support building information modelling (BIM) Level 2, referred previously in this chapter. These standards are associated with the following parts of the asset management process (based on figure 1):

- the capital/delivery phase of projects, PAS 1192-2, (PIM, project information model)
- the O&M phase PAS 1192-3. (AIM, Asset Information Model)

PAS 1192-2, PAS 1192-3 applies to both building and infrastructure assets, and the intended audience for these documents include organizations and individuals responsibilities for the procurement, design, construction, delivery, operation and maintenance of buildings and infrastructure assets. These standards cross-reference with other existing standards concerned with the management of assets, and is closely related to the ISO 55000 series of standards that provide one overarching framework for the adoption and implementation of PAS 1192-2 and PAS 1192-3.

PAS 1192-2 focuses specifically on project delivery, where the majority of graphical data, non-graphical data and documents, known collectively as the project information model (PIM), are accumulated from design and construction activities. PAS 1192-3 focuses on the operational phase of assets irrespective of whether these were commissioned through major works, acquired through

transfer of ownership or already existed in an asset portfolio. The operational phase of an asset is deemed to commence at handover, but the requirements within PAS 1192-3 may also be helpful during major works. Progressively working through the various stages of the information delivery cycle, the requirements within this PAS culminate with the delivery of the as-constructed asset information model (AIM). AIM is handed over to the employer by the supplier once the PIM has been verified against what has been constructed and it is used to support the portfolio management activity for the life of the asset, which include the maintenance management. Figure 2 illustrates the life-cycle delivery process and the interface between PIM and AIM.

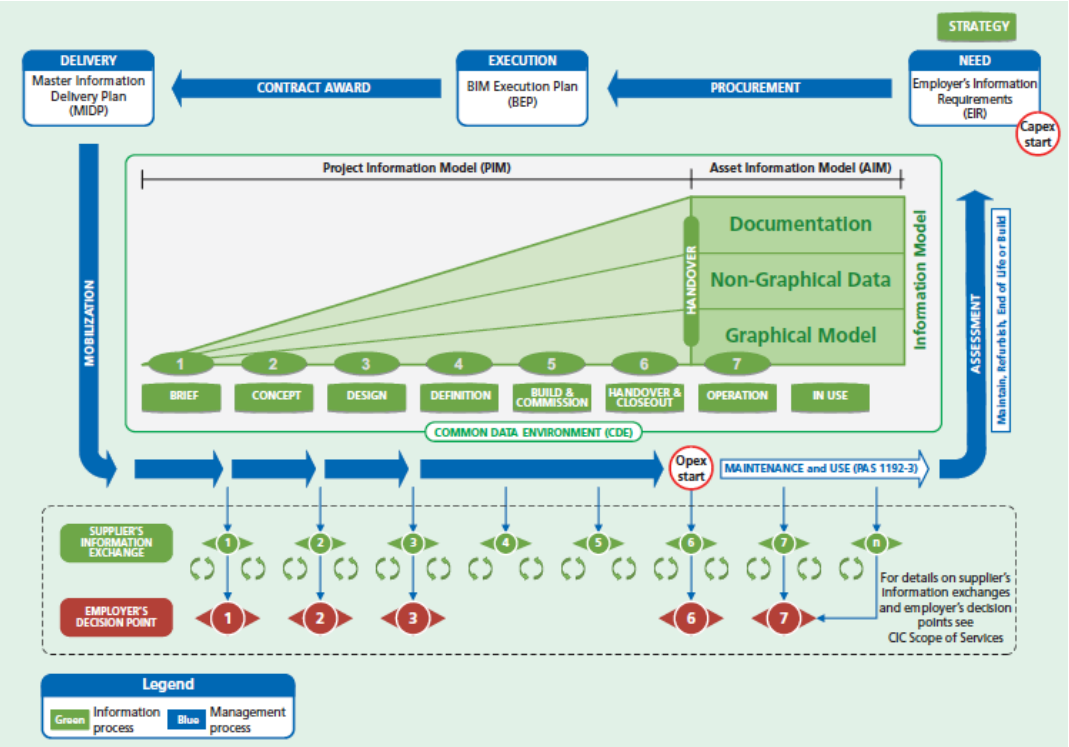


Figure 2 AIM and PIM. The information delivery cycle (PAS 1192-2:2013)

In any case, this family of standards and, in general terms the BIM-FM solution, has not been extensively applied yet. Kassem et al (2015) summarize the following challenges that are hindering the exploitation of BIM in FM:

- The lack of methodologies that demonstrate the tangible benefits of BIM in FM, which is reflected by limited demand for BIMs for FM by clients and operators; the need for rigorous BIM specifications for modelling requirements;
- The interoperability between BIM and FM technologies and the difference in their lifespan;
- Limited knowledge of requirements for the implementation of BIM in FM (e.g. what information is to be provided, when and by whom);
- The lack of open systems and standardised data libraries that can be utilised as a bridge between BIM and CAFM technologies;
- The current number of diverse operational systems, managing the same building;
- The lack of clear roles, responsibilities, contract and liability framework; the shortage of BIM skills in the FM industry; and
- The rigid industry cultural approach to adopting new processes and technologies.

2 A view on buildings Life-cycle costing phases

The generalized life-cycle phases are presented in table 1. These phases are process-based and should provide some insight for practitioners and academics on how infrastructure assets should be managed appropriately. These phases are generalized on a high level to compare conceptual options; rehabilitate versus new construction. Relevant cost drivers and uncertainties (cost, time, events, activities and technical performances) should be highlighted for both rehabilitation and new construction alternatives.

Table 1 – generalized phases for infrastructure assets (based on *Metodedokument V3.1*[3])

Phase	**Description**
Assess your operational needs	Traditionally the operational need for a company is to lower project-costs as much as possible, maximize yield from capital investments and provide a desired service-level. In order to reduce risks, this phase must be organized and viewed in perspective with design requirements, the stakeholders' expectations, measurable project goals and success criteria in alignment with the operational needs. The public sector's aim is typically to manage public fundings as effectively as possible, based on constrained budgets, and provide public services on a level that meet the citizens expectations. Cost effective management of public spending does add public value within its asset management context due to increased trust and accountability of their utilized services.
Develop different conceptual alternatives in accordance with your operational needs	Each concept must be developed as a solution aligned with the operational need. Each concept is developed through a creative and iterative process. The risks related to completing the construction phase and how the project goals are achieved, must be analyzed thoroughly.
Identify measurable project goals and business criteria	Project goals are specific goals relevant within its context, such as maximizing trust among citizens and customers measured through quantitative surveys, optimize utilization of utilities, reducing energy consumption etc. The quality of the result from this phase is achieved when the project goals can be measured based on concise quantitative data and qualitative fact-based driven reviews.
Identify stakeholders' expectations and needs	The interests and needs of stakeholders is necessary to identify, to analyze which stakeholders has the greatest effect on project goals, risks and uncertainties. Relevant regulatory issues should be identified as soon as possible. The design of the asset must be adjusted thereafter according to the regulatory risk. The stakeholders need and behaviors should be aligned with each concept. The stakeholder's viewpoint can then be taken into account to neglect developed concepts that does not satisfy the project goals.

[3] The phases in table 1 is based on *Metodedokument V3.1 15.06.2015* developed by Oslo municipality, Utdanningsetaten (public educational agency). *Metodedokument 3.1* defines a best-practice approach for practitioners in Oslo municipality on how to develop concepts and recommend investment-alternatives within its investment process for school buildings.

Analyze life-cycle costs of the conceptual design for the infrastructure asset	Recommended practice is to follow a cost-database, which is based on input from industry experts and relevant reference projects. Some life-cycle costs that are recommended as input in the cost-analysis are maintenance, operating, upgrading, energy, service and administrative costs. These life-cycle costs and future rehabilitation and replacement costs should be requested from decision-makers, before a decision is made. The total life-cycle cost for each concept should influence the strategy of the life-cycle program and provide a decision basis for whether the asset should be rehabilitated and upgraded, or replaced with a new construction.
Assess cost-drivers for each concept, and then compare life-cycle costs between each concept	Criticality-analysis is a tool that can be used to identify critical cost-drivers and risks. Schools as an example, have two important cost drivers, which are the physical area of the building and energy-costs. Criticality analysis highlights as such important functions that require higher maintenance-intensity to yield greater results on the comfort, safety and functionality for the system.
Compare the risk-profiles between different conceptual alternatives and scenarios.	Under uncertain conditions there are uncertain parameters without any further information on probability distributions, while in risk situations the uncertainty can be quantified with a probability distribution. Risks do arise from uncertainties, and is a threat to execution of the project (Ustinovičius et al., 2007). For certain infrastructure-projects, there might be a possibility to analyze more than one project and how they affect each other on an operative and strategic level. This phase involves comparison of concept-studies in different scenarios, which must include all life-cycle costs and qualitative parameters to show the differences of potential project goal realization between each concept. The conceptual alternatives with the lowest life-cycle cost might have a greater risk-profile and does necessarily not always give the best project-output in accordance with project goals and business criterias.
Define success criteria	The concepts must define the frame before detailed engineering design begins. Further, the physical constraints, such as location and physical volume of the asset, must be taken into account. Assets will perform differently with different volumes and architectural designs, which mean the operative consequences on costs and project-goals, should be discussed and highlighted. The systems reliability should be documented during this phase, to make sure a robust concept can developed into an infrastructure asset, and be managed effectively within its life-cycle program. In practice, this phase should provide some indications on operational performance measures (utilization of facilities for users, life-cycle costs, and design constraints) between new construction and rehabilitation options.
Decision-maker concludes on a concept	The decision-maker must conclude on a concept that becomes the investment. In its simplest terms, the choice for infrastructure assets is either to do nothing, rehabilitate, replace, upgrade or demolish (and develop the property for a different purpose). In case the process in practice proves that none of the conceptual alternatives yield value according to the operational need, revise if the investment-options is relevant for your company and consider selling or redo the process of this frame, to identify and develop infrastructure relevant to the companies' operative needs.

2.1 Strategies for infrastructure-assets & work breakdown-structure for life-cycle costs

Strategies for infrastructure assets can be divided into four broad items: utilization, decrease total cost, increase life-time value and enable best-practices. These items must be operationalized through relevant operative needs for the different type of infrastructure-assets. Particularly for schools, the strategic need is to guarantee the total capacity of schools for pupils, and that as many pupils as possible can complete their basic education within the public educational system. The operative need is fundamental and must be assessed properly before the business objectives and criteria can be fully developed; this first step does also have an impact on the life-cycle design.

An advanced estimation-technique during the preliminary phase is to adjust costs under uncertain conditions based on known and specific project design criterias (an example is that a known and specific project requirement could be to build a construction below ground-level, which requires cost driving ground work, and increases the investment cost). Table 2 shows an example of a LCC-cost breakdown structure for infrastructure assets. This table provides an idea on what type of costs are relevant in each life-cycle phase for infrastructure assets. Detailed work-breakdown structures and cost-elements must be designed specifically within the context of the infrastructure asset (tunnels, roads, schools, sewers etc.).

Table 2 simplified work-breakdown structure for LCC of infrastructure assets

Preliminary phase (high cost level)	**Construction phase**	**Operational phase**	**Upgrade/rehabilitation/demolish phase**
Acquisition costs, including capital costs based on a cost database Disposal costs for relevant investment options Upgrading costs for alternatives that requires rehabilitation	Professional fees (engineering/design costs, regulatory/planning etc.) Temporary works Construction of assets Initial adaption or refurbishment of asset Taxes Other	Administration costs Operating costs Maintenance costs Utilities (consumption costs) Cleaning costs Service costs User charges	Development costs Residual value (including estimated cost of disposing the asset)

2.2 Risks and uncertainty drivers for infrastructure-assets

A good practice is to quantify the uncertainty of the base-estimate within a cost-range measured with a optimistic, most likely and pessimistic point-estimate. Qualitative uncertainty drivers must be quantified as well, and its effect on the basic cost-estimate. Risk profiles must be based on an optimistic, pessimistic and most likely scenario. The deterministic value for the cost-estimate and uncertainty drivers, including uncertain events should theoretically not allow for uncertainties, which is difficult to achieve in practice. Available risk-analysis methods should therefore adjust the cost-uncertainty and highlight the confidence interval of the cost estimates, which in turn will provide decision-makers with valuable analytical data. Metier has made a report of practical use of uncertainty

analysis on a tunnel project (Torgersen & Eldor 2007). In this case, uncertainty drivers were multiplied with uncertainty of the base cost estimate.

The cost drivers do include uncertainty of cost-estimates and uncertain activities (i.e. sanitation work, demolition of specific structural elements, complexity of site conditions etc.) Uncertainties and risks are recommended to be dealt with in the cost estimate and the uncertainty drivers. The uncertainty driver does have an effect on the cost estimate uncertainty. The uncertainty drivers can be divided into five items (e.g. Stewart et al., 1995). Table 3 describes in more detail each uncertainty driver.

Table 3 – Uncertainty drivers, and its effect on costs and time

Event uncertainty	Uncertain events are complex project events that can occur. An example is an uncertain event were particular building designs are rejected because the performance of lighting conditions does not meet required technical requirements
Time uncertainty	The time uncertainty reflects the uncertainty in time distribution of an activity. Several risks are relevant, including stakeholders' influence on the project, organization and competence of the team, external dependencies (when is financial funding available, relation to ongoing construction projects etc.), regulatory requirements, political influence, market conditions (how many entrepreneurs will bid on the project etc.)
Activity uncertainty	Activity uncertainty is the risk related to an activity that is logically eliminated, failed to initiate or failed to complete
Technical performance	Identify risk and probability the technical performance will fail compared to the defined range for the technical criterion, i.e. required performances for heating and cooling
Cost uncertainty	Cost estimation relation, complexity factor analysis and statistical uncertainty analysis are risks that should be considered when analyzing the cost uncertainty

2.3 Criticality analysis – quantifying critical risks and uncertainties

Within the context of infrastructure assets, criticality analysis is a process providing a basis for which assets should have priority within a maintenance management program, and has become a clear business need in order to maximize availability during assets' operational phase. Most current quantitative techniques for asset criticality analysis uses a weighted scoring method defined as variation of the RPN method used in design (Ben-Daya et al., 2009). This approach can provide a basis for obtaining more effective maintenance operations.

Introduction of criticality analysis in the conceptual phase for infrastructure assets can improve the decision-basis, since both the relative differences in costs associated with the success-criteria, and the costs related to loss of functions for various conceptual alternatives becomes more evident. In this phase, frequency levels and frequency factors must be gathered from an asset management data system based on a higher level compared to the operational phase, but should still be able to provide good indicators on which investment-options has the best effect based on the relevant operating needs, project goals and success criteria.

Criticality of quantitative and qualitative parameters (uncertainties, risks, cost drivers, project goals) can be measured through the potential impact of a functional loss on an operative level with the scores N*o affection* (NA), *system stops for less than x minutes* (S <x), *stopping the system more than x* minutes (S>x) or *the system is left out of order* (00). Comfort can be evaluated with the grades *NA*,

affect a user (P), *affect an objective function* (F) or *affect the whole engineering system* (E). Based on these quantitative measures, the process for the criticality analysis is suggested as follows:

1) Define the frequency levels and frequency factors
2) Define the operative needs, success criteria and criteria effect levels to assess functional loss severity, criticality of risks and cost drivers
3) Identify none-admissible functional loss effects
4) Weight (contribution) of each criteria in each alternative aligned with the functional loss severity, criticality of risks and cost drivers
5) Define severity of categories, or levels per criteria effect for each alternative and in accordance with the measurable project goals
6) Retrieve data for actual functional loss frequencies for an element (r) and the quantitative criticality of risks and cost drivers
7) Retrieve data for maximum possible effects per criteria
8) Determine potential asset criticality at the current frequency
9) Retrieve data for the real effects per alternative aligned with measurable project goal
10) Evaluate the observed criticality at current frequency
11) Prepare results and guidelines on how to operationalize the maintenance strategy, and manage the most critical risks, cost drivers and life-cycle design of each alternative

In its current form, this process on criticality analysis should be used as a basis for further research and exploring new best practices within asset management practices in the conceptual phase.

3 Assessment of risks and uncertainties - Practical use of framework

The framework presented in this paper is a contribution on how to improve life-cycle planning from the earliest phase of an investment on infrastructures. Table 4 suggests a template on how the framework can be applied in practice. The quantitative data given in table 4 are arbitrary numbers, but is roughly based on real project cost data from public school projects, with the purpose to illustrate relative differences in each alternative.

Table 4 – practical use of generalized frame for investment of physical infrastructure

Operational need	**Investment-option/ conceptual alternative/ scenario**	**Base cost estimate**	**Effect of uncertainty driver and correlation of cost elements**	**Cost drivers through the projects life-cycle**	**Quantitative score on how project realization meet measurable project goals**	**Stakeholders influence on scheduled investment-process and costs**	**Success-criteria – *these criteria's must be based on the operative need, political incentives and activities that are time dependent***
Capacity need of 2500 pupil in the area	Rehabilitate three schools	600	30	Tender market conditions Maintenance & energy costs Upgrading costs	++	Supports the school administration's policies. Low risk property has to be regulated	Project must initiate latest 2017. Entrepreneur must have key-competence on school-buildings. Service-life before necessary upgrading must be least 15 years compared to a new investment project.
Capacity need of 2500 pupil in the area	Demolition of one school, increase capacity of two schools	500	30	Tender market conditions Maintenance & energy costs Upgrading costs	+	Most likely local resistance against change of school-structure. Low risk of regulatory failure based on project plans.	New structure of schools increases the effectiveness of school administration, and percentage of pupils who finishes upper secondary school. Project must be initiated latest 2018.

Capacity need of 2500 pupil in the area	Demolition of three schools, build one new school	550	40	Tender market conditions Maintenance & energy-costs Upgrading costs	--	High risk of regulatory failure, due to location of new building. Local resistance against the project. Public agencies have a strong influence on the regulatory process, such as the agency for cultural Heritage Management.	New school develops a solid educational profile, and improving educational learning. Project must be initiated latest 2019. New construction improves safety, comfort and basic functions compared to the existing situation and other similar schools. Final investment cost does not exceed expected investment costs.

Table 5 (continued from table 4) – Event uncertainty and time uncertainty

Investment-option/ conceptual alternative/ scenario	**Event uncertainty**	**Time Uncertainty**
Rehabilitate three schools	Complexity and organization & competence Complex design of existing buildings	Stakeholders' expectations have strong influence on scheduled process
Demolition of one school, increase capacity of two schools	Complexity of project (technical requirements are difficult to achieve due to shape and design of existing buildings) Tender market conditions	Dependency with other projects, due to when capacity is available in other schools
Demolition of three schools, build one new school	Uncertain drivers: Regulation, complexity, stakeholders' expectations, project maturity	Stakeholders interest and influence on time schedule, required regulation

The intention with table 4 and 5 is to show how the framework potentially can be applied in practice for infrastructure assets, based on a life-cycle cost design. The template in table 4 and 5 should be viewed as the first part of the life-cycle program. The project team should understand the concept of life-cycle planning, which for infrastructure assets is the initial design phase, construction phase, operational & maintenance phase, rehabilitation, upgrading and replacement. For this case, one of the most important political incentives within the educational sector is to provide enough capacity and a safe environment for children who attend these schools, which should be reflected in the success criteria. Measurable results for specific projects is recommended to be collected and analyzed through an iterative approach for each phase displayed in table 1, to meet the required quality and identify all relevant data before specific investment-decisions is made.

4 Discussion

The framed process presented in this paper is based on the principles of *Reversed LCC* and *Criticality analysis*. The phases are to some extent used in practice in the municipality of Oslo, though the strategic focus on life-cycle management for infrastructure assets can be improved in general. Advanced asset management with a combination of engineering, architecture and economy, and a holistic approach towards engineering systems is needed to appropriately decide whether an infrastructure asset should have extended its service life or replaced due to its age and technical limitations.

The life-cycle costing tool *Reversed LCC* was designed to highlight cost drivers through the life-cycle of public school buildings. This tool calculates the life-cycle drivers of buildings that already are constructed, based on the rate in rental contracts up to date. These rental rates and cost-drivers are compared with estimated activity-based life-cycle costing rates that need to cover all life-cycle costs, including the depreciation-rate and development costs for future upgrades. *Reversed LCC* highlights potential savings by changing the rates of rental contracts, based on an estimated activity-based cost-level. Criticality analysis can be used as a tool within this framework to quantify critical functions and the related risks, because it extends the analysis of typical uncertainty drivers, which does have an isolated effect on the investment cost. The difference in this case compared with typical uncertainty analysis-methods, is that the most critical cost drivers and risks is assessed quantitatively in aligned with the project goals. The real effect on measurable project goals is analyzed and can add value for the decision-makers.

The framework provides a basis for the project team and contractors to have a greater focus on life-cycle thinking with a greater strategic focus on the current availability of certain infrastructure assets and the life extension of aging assets. Since contractors tend to only focus on the acquisition costs, the owner of the project should explicitly define life-cycle costs as a measurable quantitative parameter in a competing environment to incentivize solutions that performs better in terms of operating costs through the life-cycle. In some cases the project owner might also require a minimum quality-level of the assets after the end of the contract. A particular success-criteria is to guarantee a reliable source of funding towards maintenance activities, but can be difficult to achieve in practice for various reasons, e.g. due to priority of the project is declining over time, and risks related to underfunded budget consumption behaviors such as unforeseen maintenance and upgrading needs. A possible solution in certain cases is perhaps to earmark funds for critical operational expenditures, which should include preventive maintenance routines.

5 Conclusion

The framework presented in table 1 requires a project team who understands the life-cycle concept for physical assets. Analytical skills among certain members of the team are required to work with the cost estimates and risk analysis under uncertain conditions in the conceptual phase. The confidence interval of cost-uncertainties and uncertainty drivers as described in table 3 should be highlighted because this is valuable information for decision-makers. Since the process of assessing uncertainty and risk is a complex task, a good method in practice is to estimate cost uncertainty and uncertainty drivers of concept-alternatives based on the best and worst outcomes in 1 of 10 projects[4]. Life-cycle planning is supported through the framed process in table 1; decision-makers are recommended to consider the most critical life-cycle cost drivers and whether the operating budgets are sufficient for their projects to be successful within the designed life-cycle period.

[4] The 1 out of 10 approach is based on a 10 % to 90 % uncertainty range. 2 outcomes exceeds the low or high estimates and 8 outcomes are within the 10 - 90 % uncertainty range.

References

Atkin B., Brooks, A., 2009. Total Facilities Management, Hoboken: Wiley.

Ben-Daya, M., Duffuaa, O., Raouf, A., Knezevic, J., Ait-Kadi, D., 2009. Handbook of Maintenance Management and Engineering. New York: Springer.

Kassem, M., Kelly G., Dawood, N., Serginson, M., Lockley, S., (2015). BIM in facilities management applications: a case study of a large university complex. *Built Environment Project and Asset Management Vol. 5 No. 3*, 261-277

Stewart, R. D., Wyskida, R. M., Johannes, J. D., 1995. Cost Estimator's Reference Manual, 2nd edition. New York: Wiley.

Salicath, E., Liyanage, J. P., Fladberg, D., 2015. Activity-Based Life-Cycle Costing of Public Assets: A Case Study of Schools in Norway LCC. *In: 10th WCEAM proceedings*, Tampere, Finland, 28-30 September.

Salicath, E., 2015. Life-cycle Costing analyser av skolebygg i Oslo kommune - Analysere krav, metodikk og praksis: Utvikling av kvantitativ LCC-modell Reversert LCC [Life-cycle Costing analysis of school buildings in Oslo municipality - Analyze requirements, methodology and practice: Development of Quantitative LCC-model Reversed LCC], Stavanger: University of Stavanger.

Salicath, E., Liyanage, J. P., 2015. Public Asset Management: Concept & Framework for Public schools with the life-cycle costing model Reversed LCC. *In: 10th WCEAM proceedings*, Tampere, Finland, 28-30 September.

Torgersen P., Eldor, J. E., 2007. High-speed Railway Lines in Norway, Concept Evaluation, Cost Estimate and Uncertainty Analysis, Report 1: Baisc assumptions and methodology, and calculations for the corridor Trondheim – Oslo. [Online].
http://www.jernbaneverket.no/globalassets/documents/prosjekter/hoyhastighet/report_1_-_cost_es_1720592a.pdf

Ustinovičius L., Migilinskas, D., Tamošaitienė, J., Zavadskas, E. K., 2007. Uncertainty analysis in construction project's appraisal phase. [Online].
http://leidykla.vgtu.lt/conferences/MBM_2007/2pdf/Ustinovicius_Migilinskas.pdf

Zhang, M., Savas, S., Batta, R., Nagi, R., 2009. Facility placement with sub-aisle design in an existing layout. European Journal of Operational Research, Issue: 1, Volume 197, pp. 154-165.

Standards:
EN 15221-1:2006, 2006. Facility Management - Part 1: Terms and definitions, rev. 1, 2007.

IFMA, 2013. BIM for Facility Managers, Hoboken: Wiley.

ISO 55000:2014, 2014. Asset management - Overview, principles and terminology, rev. 1, 2014.

ISO 55001:2014, 2014. Asset management - Management systems – Requirements, rev. 1, 2014.

ISO 55002:2014, 2014. Asset management -- Management systems -- Guidelines for the application of

PAS 1192-2:2013, 2013. Specification for information management for the capital/delivery phase of construction projects using building information modeling (BIM) Level 2, rev. 1.

PAS 1192-3:2014, 2014. Specification for information management for the operational phase of assets using building information modelling, rev. 1.

THE IMPACT OF SYSTEM CONDITIONS ON TRAMWAY SAFETY

Franciszek J. Restel, Lukasz Wolniewicz
Wroclaw University of Technology, Faculty of Mechanical Engineering
27 Wyspianskiego Street
50-370, Wroclaw, Poland

Abstract

The article presents the factors have influence on the operation process safety of tramway rolling stock, and in consequence will have influence on service intervals. The main goal is to collect a set of important factors, which will be helpful in planning of operation research.
After reviewing the state of knowledge, the article presents an general analysis of the tram rolling subsystem. Then sources of data on the operation process were described.
In later, processes occurring in the operation and maintenance of tram vehicles were identified. Also influencing factors due to each process phase were described. Then a concept of operation research for a new rolling profile of wheels was introduced. The paper ends with a summary and further research perspectives.

Keywords: Tramway, rolling stock, operation characteristics.

1. Introduction

Operation and maintenance of every technical object is carried out within the schedule resulting from technical documentation. In many cases intervals between maintenance are defined well enough or are simply satisfying the owner. For tramway vehicles it is often not so. The reason for this are conditions of use, impact of infrastructure and the predispositions of tram drivers. Therefore, the aim of the work is to prepare an inventory of tramway system characteristics may affect its safety.

2. Literature review

2.1. Reliability in railway and tramway systems

From the very beginning of reliability studies in rail transportation system studies mainly focused on vehicles. Apart from testing mathematical models, operational data analyses were conducted concerning damage. The research was narrowed down to a statistical analysis and conclusions drawn therefrom. Rail vehicles consist of systems, assemblies, subassemblies, etc. which may be subject to failure resulting in the entire

vehicle becoming non-operational. Thus when analyzing their reliability decomposition is performed in order to design the models more precisely [31]. Operational studies into vehicle failure rates are used, among others, to determine optimal inspection and repair intervals.

A crucial aspect in the railway engineering practice is determination of the state of infrastructure and relating safety improving actions to it [2]. A crucial group of studies in this aspect involve the so-called Life Cycle Costs analyses [25]. In [15, 19] decision models for determining the right time for technical service of infrastructure at minimum total costs have been designed.

Another group of tasks performed in rail transportation system includes a dispatcher's actions once disruptions occur. One of the possible methods is to regulate the speed by running trains in order to minimize unplanned stopovers (particularly perceived by passengers) and reduce energy consumption [10]. In this approach no structural process changes are proposed, but merely changes in process parameters. In fact, these aspects are related to re-organization of traffic after occurrence of disruptions whose aim is to minimize further propagation of disruptions [6, 34, 35].

A more detailed insight is provided by an analysis of consequences of original and the related secondary damage (excluding the traffic impact) [32]. Chen in [7] presented train services reliability and punctuality models.

The authors [22] proposed a disrupted train traffic management support model. The model is based on the costs of rail traffic reorganization or cancellation of trains in the context of railway employees (engine drivers and train traffic service staff).

The probability of delay suppression is directly related to the so-called "resistant timetables" [23] and resilience [14], i.e. an ability of the system to regain functionality after an event. Vromans [37] narrows the term of rail transportation system reliability down to reliability of transport services. In this regard it does not matter what caused the process failure. Therefore, the unwanted event is treated as a black box. Therefore, the reliability characteristics of system components are not taken into account (infrastructure, rolling stock, train category, etc.).

The previous groups show a tendency to narrow the subject down to one specific aspect. The next group of aspects has a completely different approach in comparison to the before-mentioned ones. They include research in which the impact of catastrophic events on system operation is analyzed. Railway services are in this respect considered Critical Infrastructure System (CIS), whereas conducted analyses focus on serious events with dire consequences. A CIS description contains graph models in which the most basic ones are modelling simply the relations between junctions. The more advanced models include traffic capacity of the edges, travel time, traffic control at junctions, as well as the mode of power supply [11, 12]. In this aspect the term - reliability of railway network infrastructure traffic capacity - is introduced [39].

2.2. Safety in transportation systems

Safety is related to maintenance of the system, that prevents occurrence of adverse events, such as [27]:

- death,
- body injuries,
- tangible property loss,
- natural environment loss.

In [33] a method of barrier identification based on the fault tree was presented. The method is based on the so-called Swiss cheese model, in which the holes must overlap so that an arrow can go through them (for safety failure to take place). A risk situation, which is a peak event is modelled by a classic fault tree with AND and OR logic gates. Once the tree is drawn up the first logic gates are searched for starting from the peak event. The event above a given OR gate is directly related to one barrier and used for determination of a barrier.

In the case of railway transportation system an event tree and a fault tree can be used in adverse event risk analyses. In [1] such an analyses was expanded by addition of risk influencing factors. The problem was shown on an example of a single-track line, for which a peak event was a collision of two trains coming from two different directions. Barriers which aimed at preventing occurrence of peak events were catalogued and then a tree of events leading to the barrier faults were drawn up. Operational risk influencing factors were attributed to the basic events.

The studies [3, 4, 30] explore security engineering in rail transportation system design. Articles discuss the issue of ERTMS (European Rail Traffic Management System) implementation, which in their structure also contain a unified European communications standard GSM-Rail. The problem of security at ERTMS implementation is all the more crucial if we take into account lack of experience in operation of such a system in conditions corresponding to the implementation (for Dutch railways in 2003). The basis for discussions [3] is risk identification for the implemented system. The [4] publication summarizes literature which introduces risk analysis components for a newly designed railway system (ERTMS). For security appraisal of the ETCS system, a slightly simplified ERTMS variant, Functional Hazard Assessment method was proposed in [29].

A crucial aspect in the assessment is identification of Safety Integrity Levels (SIL). In the draft of the European standard [16] a simplified SIL table was used for railway traffic control, communication, data processing equipment and electronic systems significantly influencing the safety of rail transportation. In [5] representing railway transportation risk levels in the form of a table was suggested. In this way unacceptable risk, acceptable risk areas and a border area were obtained. Combinations of frequency and consequences in borderline risk areas were then used for drawing up a risk table based on the SIL table. The proposed table presents frequency of event occurrence and consequences divided into A to E. Group A represents events which can be classified as fail-safe. The remaining groups have been divided in terms of energy accumulated during the event:

- B - concerns consequences of events during manoeuvres,
- C - concerns events at low linear speed values,

- D - events at medium linear speed values,
- E - concerns consequences of events at high speed values.

In [9] risk assessment of hazardous load transportation was conducted by using events/vehicle-kilometers as a measure of event occurrence intensity. In [24] a model used in a risk analysis of hazardous material rail transportation was presented. The risk is determined as the product of intensity of derailment of carriages used for transport of hazardous materials, operational work related to transportation of hazardous materials, conditional probability of hazardous material release after derailment and consequences of hazardous material release from the carriage.

2.3. Human factors

The literature sources point out that the human factor dominates during the occurrence of hazards [20, 36]. In the case of standard rail traffic control devices a situation may occur in which the security system will have to be circumvented to enable further operation of train traffic. Emergency traffic operation is conditioned by improper system operation which constitutes a possibility for unreliability of security [13]. In [18] a model for human error occurrence probability during operation of rail traffic safety system was presented. In the paper were included human error probabilities, intensity of human errors in atypical situations, work conditions influence on failure occurring.

Increased behavioural and cognitive load has an impact on traffic safety (more than 90% of accidents in the rail transportation system occur after taking over the responsibility by a human [30], whereas disasters in transport occur in around 80% of cases due to a human error [21]. A human factor exists in the entire system not only in direct operation of trains by railway traffic control stations [38].

A weighty problem in the use of the rail transportation system is the SPAD (Signal Passed At Danger) phenomenon. The most common cause of this type of events is the machine operator's error. The [17] source says that in 2011 more than 45% of accidents were caused by a train passing a stop signal in a dangerous way. SPAD events were examined qualitatively in [28].

Due to the crucial impact of those events on occurrence of safety failure they are examined in detail by using various methods (e.g. Bayesian networks [26]).
In the context of a human factor a science dealing with safety culture in antropotechnical systems should be noted. Models of the problems were synthetically introduced in [8].

3. Infratsructure qualities

Infrastructure is the system part have main influence on the rolling stock operation and maintenance process is infrastructure. The most important related qualities were presented below.

3.1. Maintenance

Maintenance actions are often realized through outsourcing. The savings resulting from this are reduced by necessary supervision over integrity of work. Key tasks performed while maintaining the tram infrastructure consist of:

- grinding rails, which reduces the noise and vibrations of a moving tram, it also affects the reduction of wheelset degradation,
- welding of degraded rails and switches,
- maintenance, cleaning and diagnostics of switches,
- maintenance of tracks - repairing of broken rails and superstructure, cleaning,
- elimination of derailment consequences.

Welding or replacement of damaged rails is carried out during night breaks in traffic. Sudden repairs are performed most often without breaks in tram traffic. Track worker stops maintenance when a tram arrives give it priority. Such strategy is vulnerable to human errors and may result in a derailment accident with man.

3.2. Diagnostic methods for finding of superstructure conditions

In Poland only one document regulates several aspects of track diagnostics "Technical Guidelines for the design, construction and maintenance of tram tracks", published by the Polish Government in 1983. This document standardizes only a few of the required parameters and measures. There is no reference to speed limits in relation to degradation of the track. There is also no scale of possible parameter values.
Periodic inspections are performed every five years by an external company, that uses own measures an scales.
For the tramway case, there exists no specified and automated diagnostic equipment, like measuring cars. All measurements have to be performed by hand tools. For example measuring equipment which moves on rollers on both rails and collects data related to: gauge length, twist, cant, uneven horizontal and vertical.
In addition, visual inspections are carried out by operator inspectors due to state of ballast, sleepers, etc.

3.3. Rail shapes vs wheel shapes

In Poland, currently are used four types of rails. The first two are specialized tram rails, so-called slot-rails, Ri60N and 180S. The main difference between them is the radius R. In case of rail 180S, the radius is adapted to the radius of wheel type T (conical). For Ri60N, the radius is larger and adapted to wheel profile PST. The PST wheel profile is based on the partial degraded T wheels. Therefore, profile PST is pre-shaped to the T wheel in period of stable operation. However, studies have shown, that mixing of profiles increases the degradation speed of wheels and rails. Another rail used is the S49, which is a solution from the railway. Its geometry is similar to Ri60N rail and wheel profile PST.

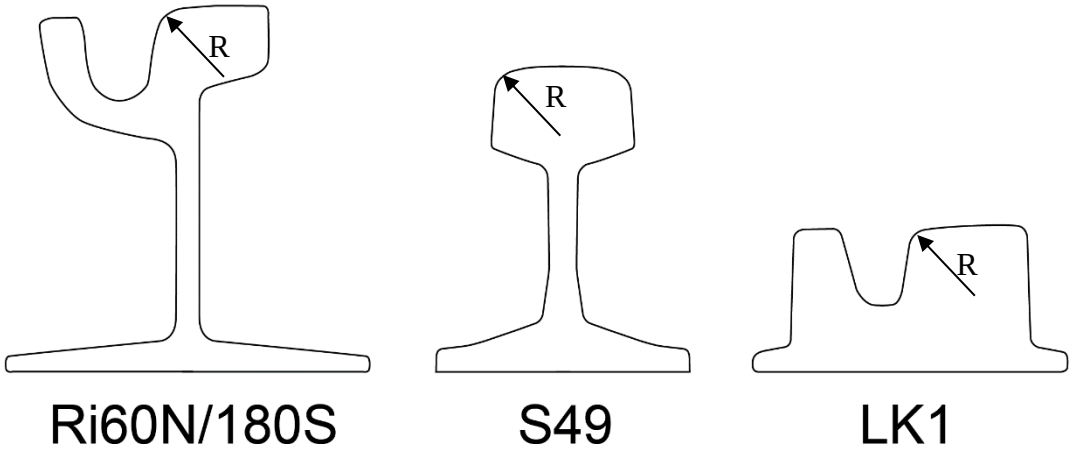


Figure 1. Explanatory figure of rail profiles used in tramway transport.

The third rail, LK1 does not have a long neck. That allows placement of rails in concrete plates without fixing with a mount.

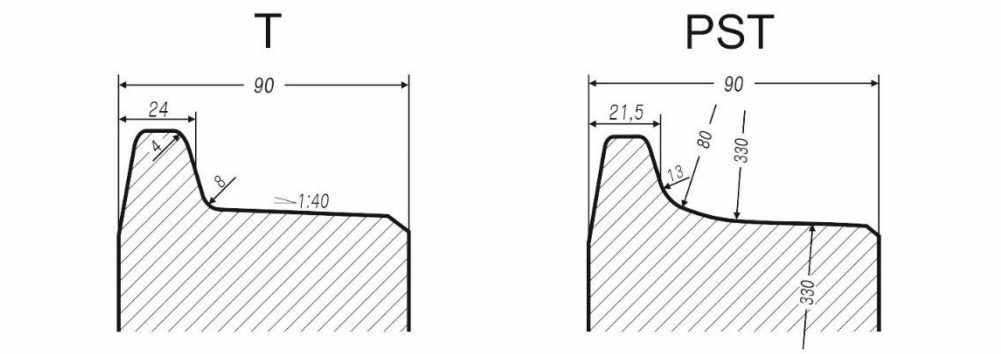


Figure 2. Explanatory figure of T and PST wheels used in tramway transport.

In the Polish standard PN-K-92016 are set out in detail geometric dimensions of wheelsets. The diameter of a new wheel must not be greater than 650 mm, and radial deviations must not be greater than 0.2 mm. The wheel must be replaced when its diameter is decreased to 538 mm.
During operation it is acceptable that the difference of wheel diameters between two wheelsets in a bogie is up to 10 mm. Diameter differences between two wheels in one wheelset must not exceed 2 mm (for new wheels 0,5 mm). Incorrect maintenance can lead to unwanted track degradation, derailments, excessive noise and discomfort for passengers.

The maintenance schedule of wheelsets includes:

- daily inspection - it is recommended to finding sudden damages, which could occur during operation as a result of external phenomena, the method bases on visual diagnostics,
- controlling inspection - measurement tools are used to carry out all important wheelset dimensions,
- middle renovation – includes all previous diagnostics maintenance.

3.4. Superstructure types

Tramway track should be cheap, reliable, durable, quiet and should not be the cause of rolling stock failures. Due to lack of uniform construction standards, a lot of design solutions were investigated. Improving of tramway superstructure was carried out in every Polish city individually. Therefore, there are used the following types:

- railway solution - rails on sleepers,
- track built for road crossings - it allows the passage cars across the tramway,
- rails on concrete base – it has a low durability, because of asphalt as base material, after changing to concrete the noise emission has increased,
- rails in manufactured concrete panels – operation experience shows, that it is impermanent (collapsing rails and cracked asphalt due to high stiffness),
- rails fixed to a concrete base – till now successful,
- rails on concrete base, without benches – improving of the previous solution, it has not enough fixing points, therefore occur vibrations and cracks of the concrete,
- so-called Hungarian track – manufactured concrete panel put on asphalt basement with LK1 rails, it is cost intensive but very durable and generates low noise, the main problem is to repair broken rails,
- rails on concrete base with rubber pads,
- rails on concrete plates - after a year of operation came deformation in bituminous pavement between two rails and unbalanced collapse rails.
- direct concrete casting under the rails – new technology.

Due to the cost of infrastructure, the time between major repairs is relatively long. If the durability will be to small, the rolling stock will probably move through degraded superstructure. Large geometrical deviations and track defects cause accelerated wheelset and moving system degradation. As a result of track defects also appear large water clusters, which can cause damage of vehicle electric system.

4. Human factors – over speed

A frequent case is driving through switches at a speed higher than permitted. This results in uncontrolled and faster infrastructure degradation. Over speed may also result in derailments. Over speed on switches or in curves is often a result of driver's conviction that the vehicle has left the sensitive place. Because of the length of a tramway vehicle it is true only for the train head, but not for the end.
In November 2015, speed of tramway vehicles on switches was analysed. The maximum speed was observed on the tram speedometer when the tram was on a switch by minimum one bogie. The results were shown in Figures 3 and 4.

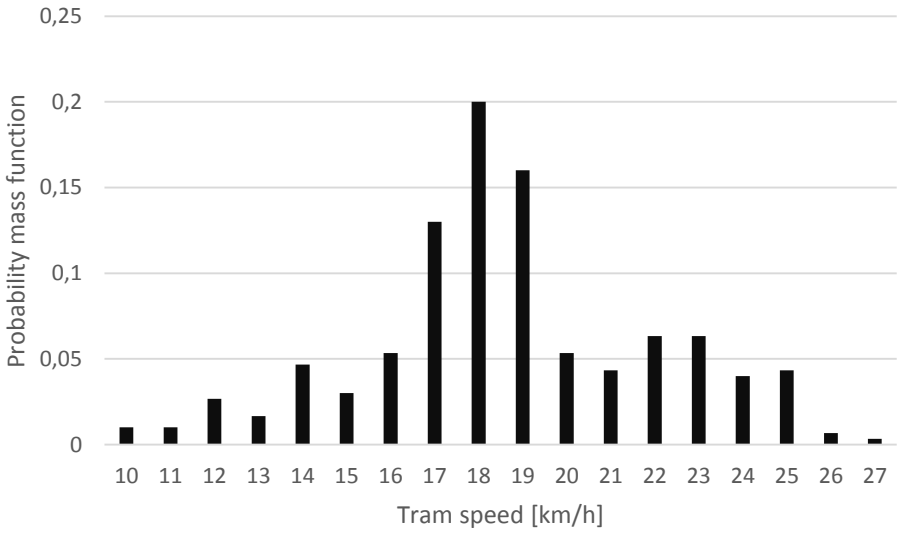


Figure 3. Tram speed PMF – driving straight on a switch (the speed limit is 15 km/h).

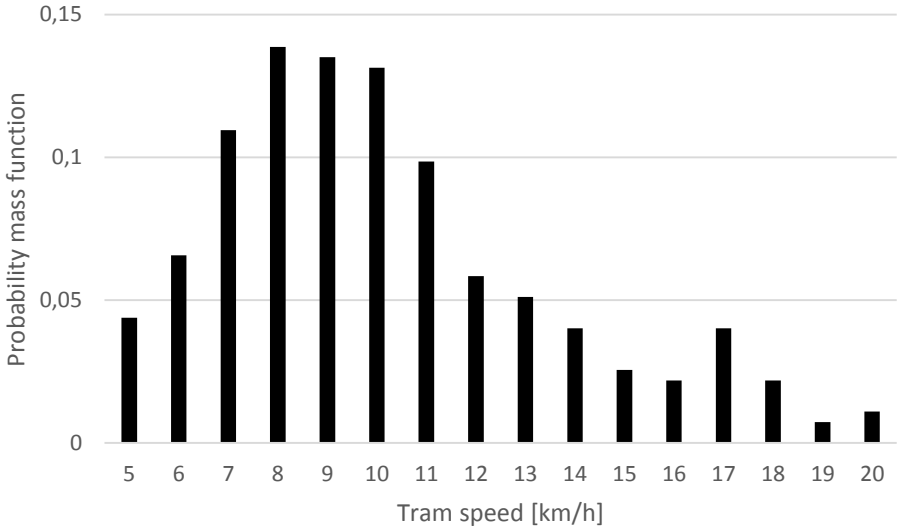


Figure 4. Tram speed PMF – driving sideways on a switch (the speed limit is 10 km/h).

An important notice is the over speed by driving straight ahead in 86 percent of all cases and the over speed by driving sideways at 38 percent. This affects a faster degradation of rolling stock and infrastructure. While, infrastructure degradation will increase rolling stock damages for all vehicles.

Small speeding can lead to derailment when simultaneously the infrastructure is degraded. While significant speeding cause derailments even for good infrastructure conditions.

5. Derailment influencing factors

Over speed and poor state of infrastructure create good conditions for derailments. Tram drivers are advised to take care that all bogies have left a critical place, before acceleration. As the results of speed measurement show, in many cases it is not so. The tram driver should also pay attention on a switch if all bogies move in the same direction. In that case many times they do not do that. In contrast to the railway, tramway switches are not mechanically locked. Therefore, under vibrations switch position changing is possible, and has occurred a few times in Wroclaw.

Looking at accidents can be listed four causes of derailments. The first are poor technical conditions of infrastructure:

- poor technical conditions of rails in curves,
- damages or degradation of switches,
- broken rails.

The next factor is poor technical condition of rolling stock:

- deviations in wheelset geometry,
- severed parts of the body,
- damages to parts of the running gear.

The third factor may lead to derailment is over speed, while the last one are random events. Experts' opinions indicate, that the combination of overspeed and infrastructure conditions creates the most hazardous situation, which can lead to derailment.

6. Planned operation research

Due to diversity track types (rails and substructure) in Wroclaw, studies are planned on selected lines with known qualities. Especially relatively new lines, in very good condition. These are tram lines 31, 7 and 4. The characteristics of these lines are shown in Table 1.

Table 1. Characteristics of tram lines selected for operation research

Line number	Route length [km]	Rail type			Proportion of track in very good condition [%]
		Ri60N [%]	S49 [%]	LK1 [%]	
31	13	73	8	19	72
7	11	62	36	2	39
4	12	61	39	0	66

From the rolling stock set will be selected in four tram units, from two newest types (PESA Twist and SKODA 16T). The tram units will run the same routes. One SKODA and one PESA tram will be equipped with new wheel profiles (PST) and the other two trams will be operated with the old wheel profiles (T).

For all wheelsets of the observed trams, on each wheel rim will be marked reference points, every 45°. For these points would be measured profiles using the profilometer IKP-5T, after each 6000 kilometres (SKODA) or 5000 kilometres (PESA). Such

distances are related to the intervals between preventive maintenance. Figure 5 shows an example of measurement results visualization.

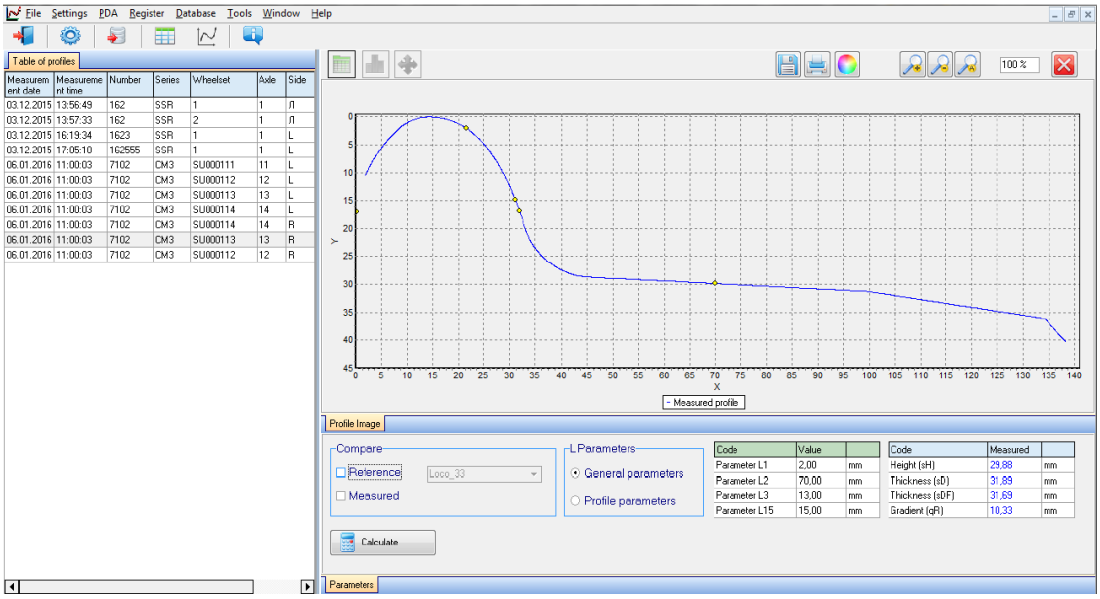


Figure 5. Example of IKP-5T profilometer measurement results on computer screen.

Using the real profile and the theoretical one for eight points per wheel, the wheel degradation can estimated.

The degradation of all wheelsets, of each observed tram unit will be analysed in function of time and driven distance. Re-profiling of wheelsets is typically done after 60 thousand kilometres, therefore there will be available ten measurements (each at eight points) per wheel.

7. Conclusions

The most durable and least problematic are tracks separated from roads, those made from the classic design of railway tracks with ballast. Thus, combined tracks generate problems during operation and can have influence on the degradation speed of rolling stock.

The most hazardous infrastructure places are arches, crossings and switches crossovers. In some cities, the number of crossings and switches is reduced to a minimum. Apart from hazards, the listed infrastructure places create problems in maintenance and tram speed limits.

Derailments in the analysed city are mainly due to poor state of infrastructure. In the accident reports can be seen, that there is lack of analysis of causes. Especially related to track state or other causes of more than one derailment in the same place, during a short period of time.

On the other hand, in some cases of derailments, accident data does not correspond with data on technical conditions of the infrastructure. Derailments occur at points of very good track performance. Therefore, there are also very important human factors, especially train drivers' behaviour.

The main focus of further research is on operation research in cooperation with the tramway operator in relation to the wheel profile problem. During this research it will be investigated possible ways of data gathering for next steps of research. Especially the tram speed in relation to unwanted events. Also horizontal, and vertical accelerations will be helpful for human factor investigations.

Acknowledgements

The publication has been prepared as a part of the Support Programme of the Partnership between Higher Education and Science and Business Activity Sector financed by City of Wroclaw

References

[1] Albrechtsen E., Hokstad P.: An analysis of barriers in train traffic using risk influencing factors. Safety and Reliability, Swets & Zeitlinger, Lisse 2003
[2] Auer F., Schlöpp A.: Substanzermittlung der Oberbaukomponenten. ZEV Rail 9/2012
[3] de Boer J., van der Hoeven B., Uittenbogaard M., Dijkerman E. M., Kruidhof W.: Design based safety engineering applied to railway systems, part I. Safety and Reliability, Swets & Zeitlinger, Lisse 2003
[4] de Boer J., van der Hoeven B., Uittenbogaard M., Dijkerman E. M., Kruidhof W.: Design based safety engineering applied to railway systems, part II. Safety and Reliability, Swets & Zeitlinger, Lisse 2003
[5] Braband J.: On the Justification of a Risk Matrix for Technical Systems in European Railways, FORMS/FORMAT, Part 3, Springer-Verlag 2011
[6] Caimi G., Fuchsberger M., Laumanns M., Lüthi M.: A model predictive control approach for discrete-time rescheduling in complex central railway station areas, Computers & Operations Research, Vol 39, ELSEVIER 2012
[7] Chen H.-K.: New models for measuring the reliability performance of train service. Safety and Reliability, Swets & Zeitlinger, Lisse 2003
[8] Choudhry R. M., Fang D., Mohamed S.: The nature of safety culture: A survey of the state-of-the-art, Safety Science 45, ELSEVIER 2007
[9] Cremonini M.G., Lombardo P., De Franchi G.B., Paci P., Rapicetta C., Candeloro L.: Industrial areas and transportation networks risk assessment. Safety and Reliability, Swets & Zeitlinger, Lisse 2003
[10] Ding Y.: Simulation model and algorithm for train speed regulation in disturbed operating condition. ZEV Rail 10/2011
[11] Dorbritz R.: Methodology for assessing the structural and operational robustness of railway networks. Praca doktorska, ETH Zurich 2012
[12] Dorbritz R., Weidmann U.: Auswirkungen schwerer Störungen auf Bahnnetze. ZEV Rail 6-7/2012

[13] Elms D.: Rail safety, Reliability Engineering & System Safety, Vol. 74, ELSEVIER 2001
[14] Enjalbert S., Vanderhaegen F., Pichon M., Ouedraogo K.A., Millot P.: Assessment of Transportation System Resilience. Human Modelling in Assisted Transportation, Springer 2011
[15] Enzi M.: Der optimale Re-Investitionszeitpunkt für das Gleis unter dem Aspekt der Lebenszykluskosten. ZEV Rail 3/2012
[16] European Standard: EN50129
[17] European Railway Agency: Intermediate report on the development of railway safety in the European Union, France 2013
[18] Goossens L.H.J., Pietersen C.M., den Heijer-Aerts M.: Comparative quantitative risk assessment of railway safety devices, Safety and Reliability, Swets & Zeitlinger, Lisse 2003
[19] Hansemann F., Marschnig S.: Der Gleisprophet – ein Impuls zur Nachhaltigkeit. ZEV Rail 9/2012
[20] Hudoklin A., Rozman V.: Reliability of railway traffic personnel. Reliability Engineering and System Safety, Volume 52, ELSEVIER 1996
[21] Kadziński A.: Wprowadzenie do zagadnień bezpieczeństwa systemów kolejowych pojazdów szynowych. XII Konferencja Naukowa Pojazdy Szynowe, Poznań-Rydzyna 1996
[22] Kroon L., Huisman D.: Algorithmic Support for Railway Disruption Management, Transitions Towards Sustainable Mobility Part 3, Springer-Verlag 2011
[23] Liebchen C. et al.: Computing delay resistant railway timetables, Computers & Operations Research, Vol. 37, ELSEVIER 2010
[24] Liu X., Saat M., Barkan C.: Integrated risk reduction framework to improve railway hazardous materials transportation safety, Journal of Hazardous Materials, ELSEVIER 2013
[25] Marschnig S., Veit P.: Life Cycle Management in der Realität. ZEV Rail 9/2012
[26] Marsh W., Bearfield G.: Using Bayesian Networks to Model Accident Causation in the UK Railway Industry, Proceedings of the European Safety and Reliability Conference, ESREL 2004
[27] Młyńczak M.: Metodyka badań eksploatacyjnych obiektów mechanicznych, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2012
[28] Pasquini A., Rizzo A., Save L.: Quantitative and qualitative analysis of SPAD, Proceedings of the European Safety and Reliability Conference ESREL 2002
[29] Renpenning F., Braband J., Wery S.: Application of functional hazard assessment in railway signalling. Safety and Reliability, Swets & Zeitlinger, Lisse 2003
[30] Renpenning F.: Reliability Prediction in Railway Signalling. Proceedings of the European Safety and Reliability Conference, ESREL 2004
[31] Saat M., Barkan C.: Generalized railway tank car safety design optimization for hazardous materials transport. Journal of Hazardous Materials, Volume 189, ELSEVIER 2011
[32] Schöbel A., Maly T.: Operational fault states in railways. European Transportation Research Review, Springer published online 18.01.2012
[33] Schwartz S.: Identifikation von Sicherheitsbarrieren am Bahnübergang. ZEV Rail 1-2/2010

[34] Törnquist J., Persson J.A.: N-tracked railway traffic re-scheduling during disturbances, Transportation Research Part B, Vol. 41, ELSEVIER 2007
[35] Törnquist Krasemann J.: Design of an effective algorithm for fast response to the re-scheduling of railway traffic during disturbances, Transportation Research Part C, Vol. 20, ELSEVIER 2012
[36] Ugajin H.: Human Factors Approach to Railway Safety. QR (Quarterly Report), Volume 40, RTRI (Railway Technical Research Institute) 1999
[37] Vromans M.: Reliability of Railway Systems, TRAIL Thesis series T2005/7, The Netherlands TRAIL Research School 2005
[38] Wilson J.R., Norris B.J.: Human factors in support of a successful railway: a review. Cognition, Technology & Work, Volume 8/no. 1, Springer 2005
[39] Zheng Y. et al.: Carrying Capacity Reliability of Railway Networks, Journal of Transportation Systems Engineering and Information Technology, Vol. 11, ELSEVIER 2011

Change Point Technique Application for a Wind Turbine Malfunction Detection System.

Miguel A. Rodríguez-López [a], Luis M. López-González [b], Nuria López-Triguero [a], Ángel Marín-Guillén [a] y Antonio J. Fernández-Pérez [a]

[a] Iberdrola Ingeniería y Construcción, S.A.U.

[b] Universidad de La Rioja.

1. Introduction

The use of condition-based maintenance and condition-monitoring techniques in the wind industry, onshore and especially offshore, has clearly improved energy efficiency and reduced the running costs of wind plants.

Using techniques of artificial intelligence in maintenance, it is possible to identify patterns of failure in the equipment and thus anticipate possible failures.

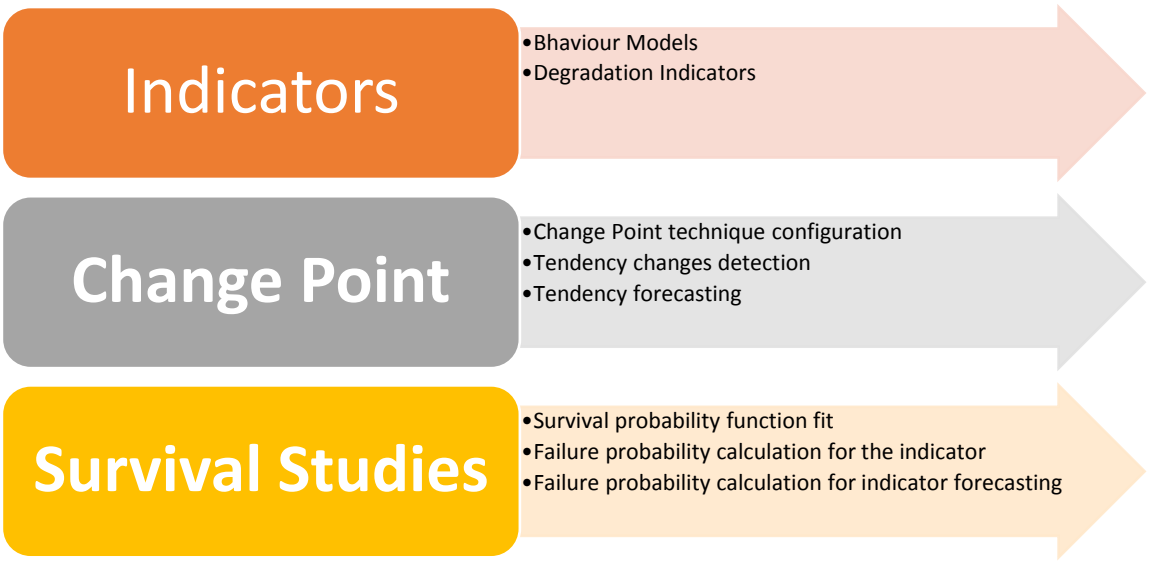
The principle of condition-based maintenance (CBM), also known as predictive maintenance, considers that if it is possible to identify that a component is degraded and might fail in a given period of time, then preventative maintenance can be performed before that failure actually occurs. In the case of a wind turbine, this means increasing the energy produced, since the maintenance task can be performed at a time when any energy that might be generated by the wind is negligible or non-existent. At the same time, it enables maintenance costs to be cut by preventing greater damage were the failure to actually occur.

Knowing what is going to fail makes it possible to optimize store management and reduce the logistical waiting times involved in performing the maintenance task. Moreover, by using these techniques it is possible to extend the useful service life of the assets, so that the operator can continue using the installation even well after its initially forecast depreciation period.

The purpose of this paper is to detect incipient failures or malfunctioning using degradation indicators and its evolution along time. It is presented a tendency change analysis technique, “Change Point”, and tendency forecasting in addition to survival probability ratios, which are useful to evaluate when the normal behavior indicator will pass the normality limits and the provability of failure in each time.

2. General description of the methodology

The methodology seeks to minimize the resources required to develop a system of detection of degradation and evaluation of remaining life of equipment. As shown in Figure 1 below, the process is divided into three phases. On a first stage the operator has to have a set of status or degradation indicators. Secondly, the technique “Change Point” analyzes the evolution of the degradation. Finally, the result of a previous survival analysis will complete the information with a estimation of the probability of failure of the equipment.



[Figure 1]. General diagram of the tendency and failure forecasting.

2.1 Antecedents: Behavior models and degradation indicators

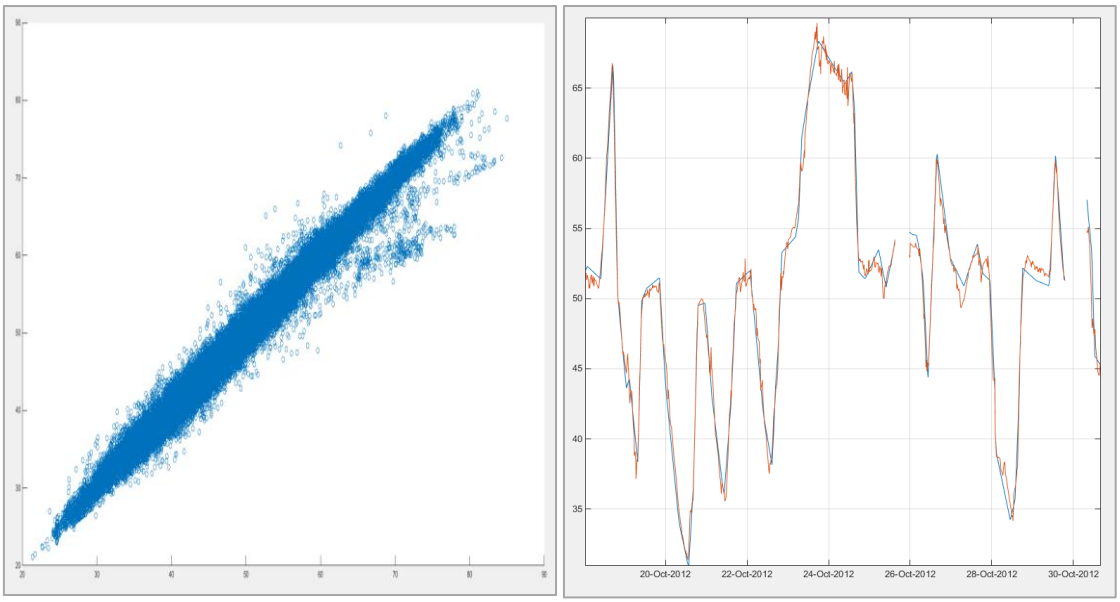
2.1.1. N.N. model

The main advantage of models with neural networks lies in the fact that it is not necessary to know the nature of the dataset to be represented; rather the neural network itself, through the training process, gathers the essential features of the dataset to be represented. For continuous processes in which there are no changes in the operating parameters (boundary conditions) it holds true.

In order to create the NDE bearing temperature behavior model, a neural network of multilayer perceptron (MLP) type can be used. This is a type of one-way neural network in which the neurons are organized in layers, so that the input of a neuron located in an intermediary layer can only be the output of the preceding layer, while its output serves as the input for neurons in the next layer. An MLP neural network can have various hidden layers, although with a single hidden layer, it would be capable of approximating, with an arbitrarily small error, any bounded continuous function (linear or non-linear), and with two hidden layers it could approximate any continuous function.

The current temperature of the NDE Bearing depends not only on the current values of the other variables, but also on the previous values, given the thermal inertia. For this reason, a time-delay variant of the MLP networks was used. Time-delay neural networks are a type of recurring neural network in which connections are established between neurons in a single layer. To model temperature changes behavior, focused time-delay neural networks (TDNN) are recommended. In general all time delayed neural networks have a structure that makes it possible to allow it to retain a memory of the activity of the neurons in the network with prior values from the input vector.

By representing the regression line of the behavior model, it can be seen that the model is very good. Nonetheless, the difference in the errors calculated is negligible. See Fig. 2.



[Figure 2]. Regression Line of the Behavior Model (on the left). Real temperature of the NDE bearing in blue, and estimated temperature in red (on the rigth).

As can be seen from the regression line, some of the data used for validation of this model corresponded to values with a possible state of malfunctioning, since the real temperature (x-axis) is higher than that estimated by the model.

2.1.2. Definition of the indicator

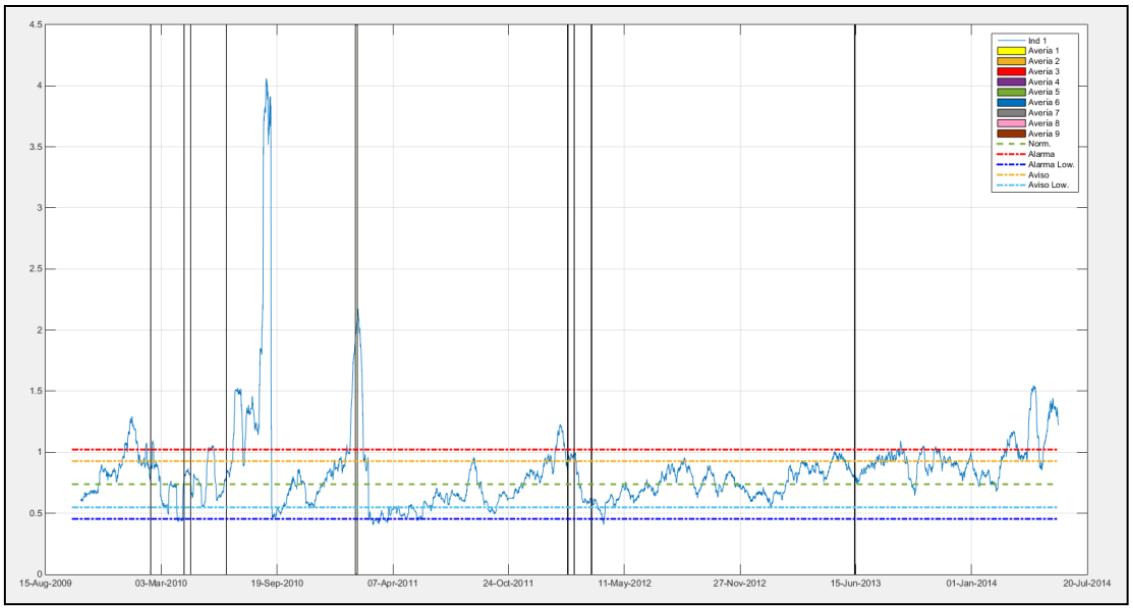
The indicator shown here is based on calculation of evolution along time of the error presented by the model as compared to the real situation.

If the no failure value of the indicator is calculated using a dataset in which the unit has not shown malfunctioning or degradation, the error can be expected to remain constant. The indicator can therefore be expected to remain within certain intervals of variation. However, when a unit is degraded, its behavior will increasingly vary from that of the model. The remainders may therefore be expected to be ever greater and the mean value of the error will therefore be greater.

By calculating the indicator with a dataset in the absence of faults, it was possible to determine the expected normality value of the indicator and its fluctuation intervals – in other words, the maximum and minimum values between which the equipment can be found to continue behaving as in the model. These indicators are therefore valid for determining degradations that extend over time and which generally cannot be detected by the operating SCADA.

The mean value of the indicator for this dataset stands at around a fixed value. If no degradation occurs, the indicator may be expected to remain constant this mean value. The deviation of the indicator has also been calculated and the levels of Warning and Emergency have been determined as the limits of normality. Thus, if the indicator exceeds these values at any point, a signal will be triggered indicating detection of possible malfunctioning.

Examining the reaction of the indicator to the fault in the bearing, it can be seen that there is a reaction, exceeding the limits of normal operation of the indicator several weeks before. See Fig. 3.



[Figure 3]. Fault reaction of the Indicator developed before the fault in the NDE bearing.

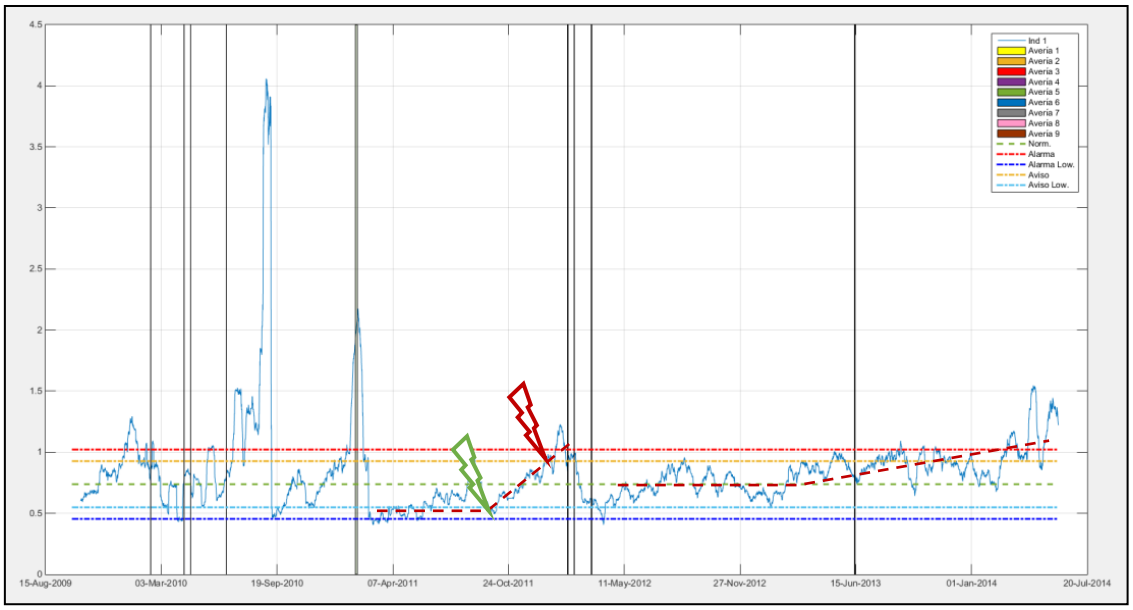
Nonetheless it is considered that the fault might have been detected by first analyzing the trend in the indicator, which leads us to develop the "*Change-point*" technique being developed at present.

2.2. Change-Point Technique

This section describes the "Change point" methodology for determining critical points for trend changes. The purpose of this technique is to detect the beginning of a possible malfunction, which, besides being useful for making a projection of the trend and therefore an estimate of the remaining life of the equipment, it is also used to identify the date when there was a change of behavior of the machine and therefore the operator can analyze what happened during that time, and thus better understand their equipment behavior, and to determine the underlying causes of the failure.

Status indicators react to changes in equipment performance, but do not give the warning signal or alarm until certain thresholds are exceeded. It is possible that once the warning signal is given is too late to act. To solve this problem an analysis of change in trend and projection of it is proposed.

The following figure shows a clear example in which the technique of "Change point" had given a warning long before the status indicator is used alone. In this example, the technique "Change Point" had identified the point indicated (vertical red line) as a change in trend, and from that point to project the trend to date the warning level is exceeded.

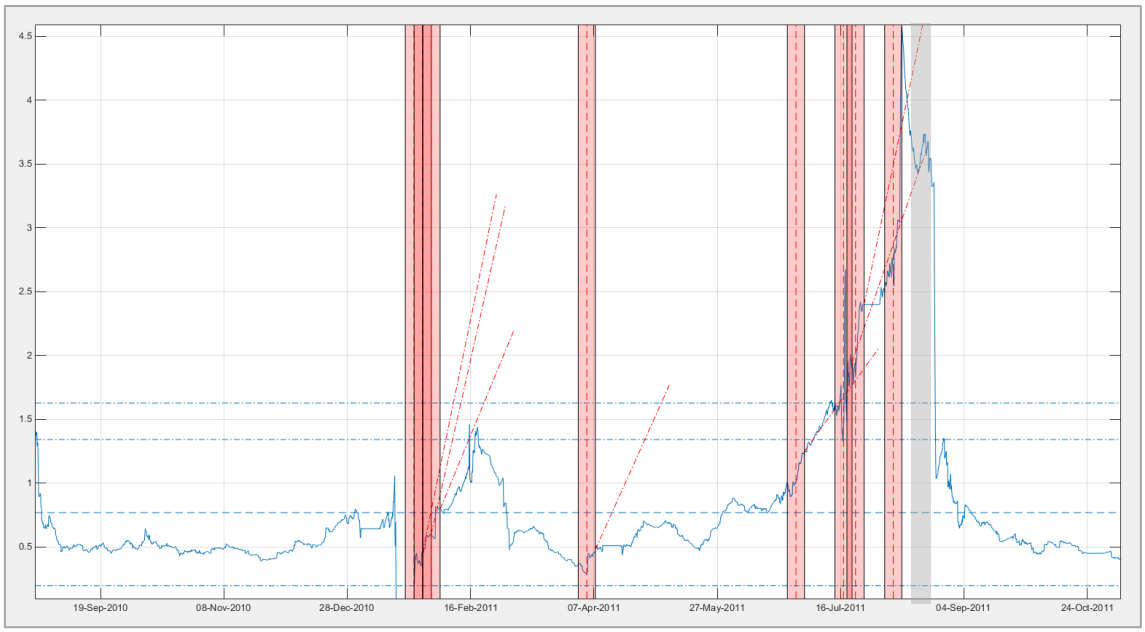


[Figure 4]. **Example in which the use of the technique "Change point" had warned in advance of a possible malfunction (green mark) before a slow response indicator (red mark).**

As the above example, the change of trend would be indicated from the beginning of October 2011 and the projection of the trend estimate that, if this trend continues, on January 2012 warning level will be exceeded. The equipment failed along January so without the tendency analysis the operator would not have time enough to react before the failure. The methodology developed here has the ultimate aim to implant in a production environment, in this environment, the fleet of equipment to monitor is very high, which makes it unfeasible for an operator being looking for a way visual trend changes or specific alterations that occur in an indicator. To solve this problem it is necessary that the system indicates to the operator where to look. Conceptually, the technique of "Change point" consists of a double moving average around a point in time.

Once a date is identified as "Change point", the projection of the trend is made. If over a period the slope remains linearly (red line in the illustration above) from the indicator value in *t*. Each increase of *t*, the slope is calculated, so that as time goes the projection will be tangential to the curve of the indicator is recalculated.

In the following figure has been applied the technique of "Change point" to the indicator. The red boxes indicate the detection window and the straight line and point are straight trend. The vertical line in the center of each window is the "Change point", ie the exact date on which it begins to produce the change in trend. The figure shows the period prior to the fault zone (indicated in grey). A higher concentration of "Change points" is observed in the area next to 20 July 2011. Within the following example without using the "Change point" alarm had been given on July 11, 2011, and the technique "Change point" is predicted on July 2, that around 14 July alarm level be exceeded, ie has advanced detection nine days.



[Figure 5]. Detail above example of applying the technique "Change point" on the indicator in the pre-break NDE bearing period.

These indicators must be accompanied by a survival analysis of the equipment, so that from the value that the indicator presents at the date of breakage, it is possible to fit a function and estimate thus the probability of rupture of equipment based on partial probabilities of different indicators. In the next section the application of this survival analysis applied to the value of the status indicators is presented.

2.5. Survival analysis and Remaining life

So far, to determine a potential failure, it has been calculated the maximum level indicator (alarm level), considering it as the limit of normal values, ie, when the machine does not failure is expected to be within these limits, but, which is the "breaking point"? Where is the endurance limit of my equipment?

It still needed to define which the limiting value of the indicator is before it can be considered as failure, or even the time the indicator should stay above that threshold for not being considered a simple fault of the model or an aberrant data as false positive (transient situation). In this respect, Iberdrola is conducting survival studies of equipment, determining the failure probability f(t). For this, the value of indicators at the time the malfunction occurred, and taking the maximum values of these indicators (local or transient maximum) in the other turbines in which there has been no failure to consider such censored data (right censoring). Once 30 (or at least 10) completed data (values is case of real malfunction) are available, it would be possible to obtain the f(t)[1], F(t) and thus h(t), adding to the indicator a probability of occurrence of damage directly calculating the conditional probability of failure (hazard function):

$$h(t) = \frac{f(t)}{1 - F(t)}$$

[Equation 4]

In the presented study it has been calculated the Weibull distribution function of the probability of damage from the value of 13 completed data and 12 censored data of the indicator. Complete data were taken from the application of indicators at 15 wind turbines of a wind farm that experienced 13 bearing failures, measuring the value of the indicator in the previous instant of the SCADA alarm that triggered the subsequent repair time. Censored data were taken in other wind turbines that did no present no significant generator faults.

1 Fitting to a Weibull function.

Based on this distribution the probability of failure associated with the indicator and included as an additional indicator (hazard function h(t)) was calculated.

We consider that it is necessary to provide more complete data of faults for a more precise Weibull fit. However it is observed as the hazard indicator showed reagent in the days before major bearing failures (the second vertical line in the picture above), and after making a design modification on the generator (third vertical line in previous figure). Keep in mind that after performing maintenance on the equipment, the probability of failure increases, known infant mortality.

4. Conclusions

Companies responsible for operation and maintenance (O&M) of the wind farms that want to make use of their historical data and improve the economic results of the business need to develop a strategy for this purpose, bearing in mind that they must achieve this aim by following a previously plotted path.

The methodology "Change Point" for the trend analysis of status indicators is able to overtake failure detection by detecting a trend change and projecting the indicator within the new trend. After project the trend it is analyzed when the limit of normal operation, or fault, of the component is exceeded.

Generally, the value warning or alarm was defined by the range of variation of the indicator when the machine did not show any malfunction. However, this limit value only defines normality, but not the "breaking point" of the component. To solve this uncertainty, a survival study of the component, based on the values of the status indicators was conducted, and a failure probability was associated with the projection of the trend, so that it is possible to estimate when a component has a failure probability 100% (F (t)).

However, the numbers of registered cases of rupture were not enough to make a Weibull fit good enough (complete data versus censored data). As more cases of failure were registered, the adjustment function would be getting better.

With the use of the techniques presented in this article, the ability to detect a fault, passes made with one or two weeks before months in advance.

5. References

Rodríguez-López MA. A method for smart systems for detecting malfunctions in equipment. Application to wind turbines. Tesis Doctoral (Directores: López-González LM, López-Ochoa LM.). Universidad de La Rioja (España), Logroño, 2015.

Complex Engineering Assets Criticality Analysis for Maintenance Purposes.

Khairy Kobbacy**, Adolfo Crespo*, Antonio Sola*, Pedro Moreu de León*, Juan Gómez*, Samir Shariff**

*University of Seville
Department of Industrial Management, School of Engineering.
Camino de los Descubrimientos, s/n. 41092 Seville, Spain.
adolfo@etsi.us.es, moreu@etsi.us.es, asrasrasr@telefonica.net, juan.gomez@iies.es

** Taibah University. Madinah. Saudi Arabia. MM Binladin Chair of Operations & Maintenance

Abstract

This paper deals with the problem of establishing the criticality of assets when dealing with complex in-service engineering systems. This process is considered as a first required step to review the current maintenance programs. Review is understood as a reality check, a testing of whether the current maintenance activities are well aligned to actual assets objectives and needs. This paper proposes and describers a working process and a model resulting in a hierarchy of assets, based on risk analysis and cost-benefit principles, which will be ranked according to their importance for the business to meet specific goals. Starting from a multi-criteria analysis, the proposed model converts relevant criteria impacting equipment criticality into a single score presenting the criticality level. An example is presented to help the reader to understand the process and to operationalize the model.

Keywords: Criticality, maintenance management, operational reliability.

1. Introduction

In this paper we deal with the strategic part of the maintenance management definition and process (as in [1]), which is related to the determination of maintenance objectives or priorities and the determination of strategies. Part of this strategy setting process, that we refer to, is devoted to the determination of the maintenance strategies that will be followed for the different types of engineering assets (i.e. specific physical assets such as: production processes installations and machinery, manufacturing facilities, plants, infrastructure, support systems, etc.). In fact, maintenance management can also be considered as "…the management of all assets owned by a company, based on maximizing the return on investment in the asset" [2]. Within this context, criticality analysis is a process providing a systematic basis for deciding what assets should have priority within a maintenance management program [3]. On some occasions, there is no hard data about historical failure rates, but the maintenance organization may require a certain *rough assessment* of assets priority to be carried out. In these cases, qualitative methods may be used and an initial assets assessment, as a way to start building maintenance operations effectiveness, may be obtained [4].

In this paper we propose a criticality analysis taking into account the following process design requirements:

1. The process must be applicable to a large scale of in-service systems within a plant or plants for which the business has the same goals;
2. The scope of the analysis should be the one for which the current PM program is developed and implemented;
3. The analysis should support regular changes in the criticality model (this is a must to align maintenance strategy in dynamic business environments).
4. The process must allow easy identification of new maintenance needs for assets facing new operating conditions;
5. General guidelines to design possible maintenance strategy to apply to different types of assets, according to the results of the analysis (criticality and sources of it) should be provided;
6. Connection with the enterprise asset management system to automatically reproduce the analysis over time;
7. The process should be tested in industry showing good practical results.

In the sequel the paper is organized as follows: Section 2 shows first, briefly, the proposed criticality analysis process description. Then, more precisely and in the different Subsections, the notation of the mathematical model supporting the process is introduced, as well as every step of the process to follow, including model equations. Along this second Section of the paper, a practical example helps to exemplify the process and model implementation. Finally Section 3 presents the conclusions of the paper.

2. Process Description and Rational

In this Section we describe a comprehensive process to follow in order to generate a consistent criticality analysis based on the use of the PRN method together with multi criteria techniques to select the weights of factors deriving in the severity of an asset. The process consists in a series of steps determining the following:

1) Frequency levels and the frequency factors;
2) Criteria and criteria effect levels to assess functional loss severity;
3) Non admissible functional loss effects;
4) Weights (contribution) of each criteria to the functional loss severity;
5) Severity categories, or levels, per criteria effect;
6) Retrieving data for actual functional loss frequency for an element (r);
7) Retrieving data for maximum possible effects per criteria;
8) Determination of Potential asset criticality at current frequency;
9) Retrieving data for real effects per criteria;
10) Determining observed asset criticality at current frequency;
11) Results and guidelines for maintenance strategy.

The process followed to assess the criticality of the different assets considered is supported by a mathematical model, whose notation is now presented:

i: $1 \ldots n$ criteria to measure severity of a functional loss,

j: $1 \ldots m$ levels of effects of a functional loss for any criteria,

z: $1 \ldots l$ categories of functional loss frequency,

r : 1…k element or asset analysed

e_{ij} : Effect j of the severity criteria i,

w_i : Weight given to the severity criteria i by experts, with $\sum_{i=1}^{i=n} w_i = 1$,

M_i : Maximum level of admissible effect for criteria *i*, with $M_i \leq m, \quad \forall i$,

MS : Maximum severity value,

v_{ij} : Fractional value of effect j for the severity criteria *i*,

S_{ij} : Severity of the effect *j* for the severity criteria *i*,

pe_{rij} : Potential effect *j* of criteria *i* for the functional loss of element *r*,

f_r : Value for the frequency of the functional loss of element *r*,

ff_z : Frequency factor for frequency level *z*,

fe_{rz} : Boolean variable with value 1 when *z* is the level of the observed frequency of element *r* functional loss, 0 otherwise,

af_z : Average frequency of functional loss for frequency level *z*,

S_r : Severity of the functional loss of element *r*,

C_r : Criticality of element *r*,

re_{rij} : Current probability of the effect *j* of criteria *i* for the failure of *r*,

S'_r : Current observed severity of the functional loss of element r,

C'_r : Current criticality of element *r*,

2.1. Determining Frequency Levels and Frequency Factors

To manage the frequency levels, the analyst may use different options. In this paper a form of Pareto analysis is used, in which the elements are grouped into z frequency categories according to their estimated functional loss frequency importance. For example, for z=4, the categories could be named: very high, high, medium and low functional loss frequency. The percentage of elements to fall under each category can be estimated according to business practice and experience for assets of the same sector and operational conditions. Then, average values for frequencies falling inside each group can be estimated and frequency factors per category calculated (see example in Table 1).

In the model mathematical formulation, if af_z is the average frequency of functional loss for frequency level *z*, then the frequency factor vector is defined as follows:

$$ff_z = \frac{af_z}{af_1} \text{ , for } z = 1...l \text{ levels of functional loss freq.}$$

Table 1. Frequency factors per functional levels

Asset	f/y	Asset	f/y	Category (z)	% (z)	af_z	ff_z
A	1	i	8	Very high	10%	8	6.7
B	2	d	7	High	20%	6.5	5.4
C	5	h	6				
D	7	c	5	Medium	20%	4	3.3
E	3	e	3				
F	1	b	2	Low	50%	1.2	1.0
G	1	j	1				
H	6	g	1				
I	8	a	1				
J	1	f	1				

2.2. Criteria, and Criteria Effect Levels, To Assess Functional Loss Severity:

For the severity classification, this study focuses the attention on both, safety and cost criteria . For the safety severity categories, similar hazard severity categories to the ones used in MIL-STD-882C are adopted. This standard proposes four effect categories that can now be reframed as follows:

- Catastrophic, could result in multiple fatalities
- Critical, resulting in personal injuries or even one single fatality
- Marginal, and
- Negligible

As cost factors, we may select different criteria for which the functional loss effect can be classified in different levels that can, at the same time, be converted into cost using a certain contract or standard that the company must honor. In the example for this paper, the following criteria are selected (assuming that we are dealing with the criticality of a collective passenger's transportation fleet by railroad):

- Operational reliability: measuring the potential impact of a functional loss to the system where the asset is installed. The effects could be classified in different levels like: No Affection (NA), stopping the system less than x min (S <x), stopping the system more than x min (S>x) or leaving the system out of order (OO). Each one of these affection levels can be later translated to cost of the functional loss, and the corresponding factors could be obtained.
- Comfort: evaluating whether the functional loss of the element may: have no affection on comfort (NA), affect a passenger (P), a car (C) or the whole train (T). Again, each one of these affection levels can be later translated into cost of the functional loss, and the corresponding factors could be obtained.
- The "corrective maintenance cost" could be selected as another cost related criteria. Effects could be classified in very high, high, medium and low corrective maintenance cost, and we could proceed similarly to what has been presented in Table1, classifying the elements' costs and finding averages costs and the corresponding factors for each effect classification level.
- Etc.

The process also requires the definition of those functional loss effects that would be considered as "*non-admissible"* for each specific criterion.

In the mathematical model we will use the following notation for this purpose:

M_i : Max level of admissible effect for criteria i ,with $M_i \leq m, \ \forall i$

MS : Maximum value for overall severity and in our example, $[i]$=*safety, operational reliability, comfort, CM cost* and $[M_i] = 3,3,4,4$ as maximum levels of admissible effects for each criteria, finally it will be considered MS=100.

2.3. Criteria Weights and Functional Loss Severity:

To determine these weights, various considerations can be taken into account, for instance:

- Criteria correlation to business KPI's.

- Budget allocated to each cost related criteria within the maintenance budget.
- Impact of each criterion on the brand and/or corporate image. For instance, in the previous example the management (or the criticality review team) could consider that "operational reliability" and/or "comfort" criteria could have also impact on the brand image, increasing its weight versus corrective maintenance cost.
- Considerations measuring the importance of the safety factor considering standards.
- Etc.

Regardless all these considerations, assigning criteria weights may contain a certain subjective judgments from the experts involved. In order to make this judgment as much consistent as possible, AHP techniques can be used, and a model presenting the multi-criteria classification problem in a logic decision diagram, can help to solve the multi-criteria decision sub-problem at the highest decision nodes of the diagram (the reader is referred to Bevilacqua et al. [5] for additional information concerning AHP utilization with this purpose). A major advantage of the AHP approach is that both qualitative and quantitative criteria can be included in the classification scheme. In addition, the assignment of weights to the different parameters is considered as a positive characteristic of the method [6]. On the other hand, the amount of subjectivity involved in the process of pair-wise comparisons is often viewed as the main limitation of this method, another problem arises when the number of alternatives to rank increases forcing to an exponential increase in the number of pairwise comparisons. That´s why we just limit the method utilization to the severity criteria level, not to the asset criticality classification level.
In the example of this paper, w_i, weight given to the severity criteria *i* by experts, resulting from the AHP analysis are assume to be equal to $[w_i]$= 10, 30, 20, 40.

2.4. Determining Severity per Criteria Effect

In the mathematical model proposed, an effects severity matrix is defined, for any element included in the analysis (r), as follows:

$$S_{ij} = \begin{cases} MS, & for \quad M_i < j \le m, \quad \forall i \\ w_i v_{ij}, & for \quad 1 \le j \le M_i, \quad \forall i \end{cases} \quad (1)$$

Where

$v_{ij} = \frac{e_{ij}}{e_{ik}}$, with $k = M_i$ and $j \le M_i$, and with $v_{ij} = 1$ for $j = M_i$ and $\forall i$

And e_{ij} is the effect *j* of the severity criteria *i, and* v_{ij} is the fractional value of effect *j* for the severity criteria *i*.

In the example we are following, the effects matrix is included (last 4 rows) in Table 2, where relative values for the different effects for each criteria are presented. Units for these relative values are based on cost (for *i=2,3,4*) or in a dimensionless rule of proportionality of the effect (*i=1*).

At this point is important to understand that, for a given functional loss, these are maximum possible effects per criteria, but not actual observed effects (later, real observed effects of functional losses, will be considered in the analysis, which are in fact conditional probabilities to reach a certain effect once a functional loss takes place). In the example that is presented, the corresponding effects severity matrix (according to Equation 1, and for MS=100) is included in last for rows of Table 3.

Table 2. Effects matrix per functional loss

Criteria to measure Severity			
Safety criteria (dmnl) (weight:10%)	Cost related criteria (e.g. based on penalization cost and CM budget, $)		
	Operational reliability (weight:30%)	Comfort (weight:20%)	CM Cost (weight:40%)
Category of effects per criteria and functional loss			
Non admissible	**Non admissible**	4,500	300
1,5	10,000	3,000	150
1	5,000	600	50
0	0	0	10

Table 3.Effects severity matrix per functional loss

Criteria to measure Severity (S_{ij})			
Safety criteria (dmnl) (weight:10%)	Cost related criteria (e.g. based on penalization cost and CM budget, $)		
	Operational reliability (weight:30%)	Comfort (weight:20%)	CM Cost (weight:40%)
Category of effects per criteria and functional loss			
100	**100**	20	40
10	30	13.3	20
6,6	15	4	6.3
0	0	0	1,2

2.5 Retrieving Data for Actual Functional Loss Frequency

Actual data for frequency of functional losses can be retrieved and captured in the variables $fe_{rz,}$ these variables conform, for each asset *r,* a vector of *l* elements, once there are $z = 1...l$ levels of functional loss frequency. Thus,fe_{rz} are Boolean variables with values:

$$fe_{rz} = \begin{cases} 1, & \text{When z is the observed frequency category of element r functional loss} \\ 0, & \text{Otherwise.} \end{cases}$$

Example: For functional loss frequencies expressed in Table 1, the criticality analysis review team could retrieve the asset *b* functional loss frequency and this would expressed as:

$$[fe_{bz}]=0,0,1,0$$

The frequency factor to apply to this element would be the result of the following scalar product:

$$f_r = \sum_{z=1}^{z=l} ff_z\, fe_{rz} \qquad (2)$$

In our example:

$$f_b=1x0+3.3x0+5.4x1+6.7x0=5.4$$

And therefore 5.4 would be the frequency to consider for the element when finally calculating its criticality.

2.6. Retrieving Data for Maximum Possible Effects per Criteria

Data concerning maximum potential effects, when a functional loss of an element happens, can be retrieved and captured in the variables pe_{rij}, these variables conform, for each asset *r*, a matrix of *n x m* elements, once there are *i*: 1…*n* criteria to measure severity of an element functional loss, and *j*: 1…*m* levels of possible effects of a functional loss for any criteria. . Thus, pe_{rij} are Boolean variables with values:

$$pe_{rij,} = \begin{cases} 1, & \text{When } j \text{ is the level of maximum potential effect of the functional loss of an element } r \text{ and for the severity criteria } i \\ 0, & \text{Otherwise.} \end{cases}$$

Assume, as an example, that for the effects severity matrix expressed in Table 4, the criticality analysis review team retrieves potential effects of a functional loss of an element *r=b*, this could be represented with the following *potential effects matrix* (for element *b* in Table 1):

$$[pe_{bij}] = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Then, we can model the Severity of the functional loss of element r as follows:

$$S_r = Min(MS, \sum_{i=1}^{i=n} \sum_{j=1}^{j=m} pe_{rij} S_{ij}) \quad (3)$$

And therefore the severity of the asset *b* would result in:

$$S_b = Min(100, 100 + 30 + 13.3 + 6.3) = 100$$

This, in fact, represents a weighted average type of algorithm, where the weights are introduced through the value of the different criteria effects, as calculated in Equation 1. In this way, consistency in the Severity calculation of one element with respect to another is ensured. It has been experience how by giving maximum severity to inadmissible effects, like for instance in our previous example, the different roles of actors represented in the review team are safeguarded (for instance, *safety department* people in the review team of our example), discussions in the meetings are reduced and consensus is more easily reached.

Notice how, in case of good data integrity for frequency and functional loss effects of the elements under analysis, the review team can and must concentrate its efforts in the selection of the severity criteria and in establishing proper weights according to business needs.

2.7. Determining Potential Criticality at Current Frequency

The criticality of the element is finally calculated as

$$C_r = f_r \times S_r \quad (4)$$

Thus, for asset *b* of the example previously introduced:

$$C_b = 1 \times 100 = 100$$

2.8. Retrieving Data for Real Effects per Criteria

Actual data for real element functional loss effects can be retrieved and captured in the variables $re_{rij,}$ these variables conform, for each asset *r*, a matrix of *n x m* elements, once there are *i*: 1…*n* criteria to measure severity of an element functional loss, and *j*: 1…*m* levels of possible effects of a functional loss for any criteria.

re_{rij} = current probability of the effect *j* of criteria *i* for the functional loss of element *r,* with $\sum_{j=1}^{j=m} re_{rij} = 1$.

Assume, as an example, that for the effects severity matrix expressed in Table 4, the criticality analysis review team could retrieve data concerning real element functional loss effects for asset *r*, this could be represented with the following *real effects matrix*:

$$[re_{rij}] = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0.5 & 0.1 & 0 \\ 0.2 & 0.3 & 0.8 & 0.9 \\ 0.8 & 0.2 & 0.1 & 0.1 \end{bmatrix}$$

Then, we can model the Severity of the functional loss of element r as follows:

$$S'_r = Min(MS, \sum_{i=1}^{i=n} \sum_{j=1}^{j=m} re_{rij} S_{ij}) \qquad (5)$$

In the previous example, the severity of asset *b* would result in:

$$S'_b = Min[100, 6.6 \times 0.2 + (30 \times 0.5 + 15 \times 0.3) + (13.3 \times 0.1 + 4 \times 0.8) + 6.3 \times 0.9] = 31.1$$

2.9. Determining Observed Criticality at Current Frequency

The criticality of the element is finally calculated as

$$C'_r = f_r \times S'_r \qquad (6)$$

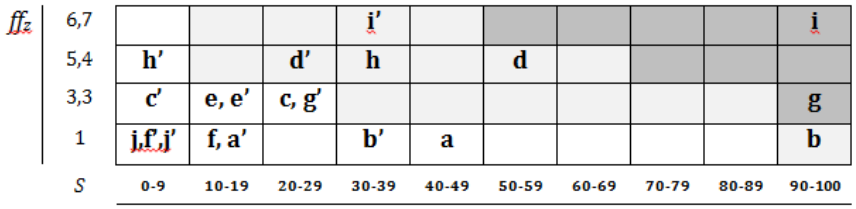
In the previous example presented

$$C'_b = 1 \times 31.1 = 31.1$$

So real criticality is much lower than potential (100)

To easy further analysis, potential and observed functional loss severity can be used to populate a criticality matrix representation (Figure 1). In the matrix in Figure 1 we can compare results obtained in two previous criticality matrices: potential and current, for the different assets under analysis.

Figure 1. Potential and Current criticality matrices representation



3. Conclusions

This paper contains the design of a process and model for criticality analysis with maintenance purposes and specific design constraints. The methodology ensures analysis consistency to business needs and for existing data of in-service complex engineering assets. At the same time, there is an effort to describe how to turn this process into a practical management tool. Issues arising related to extensive data handling and easy results representation is addressed. Finally, guidelines for results interpretation are offered. The authors believe that this type of analysis will become a must for complex in-service assets maintenance strategy review and redesign. Further research can use this methodology for the improvement of specific operational scenarios, or to refine the different steps of the process presented in this work.

REFERENCES

[1] EN 13306:2010, (2010) Maintenance Terminology. European Standard. CEN (European Committee for Standardization), Brussels.

[2] Wireman T, (1998) Developing performance indicators for managing maintenance. New York: Industrial Press.

[3]Crespo Márquez A, (2007) The Maintenance Management Framework. Models and Methods for Complex Systems Maintenance. London: Springer Verlag UK.

[4] NORSOK Standards, (2001). Criticality analysis for maintenance purposes. NORSOK standard Z-008 Rev. 2, Nov.

[5] Bevilacqua M, Braglia M, (2000) The analytic hierarchy process applied to maintenance strategy selection. *Reliability Engineering and System Safety* 70: 71–83.

[6] Molenaers A, Baets H, Pintelon L, Waeyenbergh G, (2012) Criticality classification of spare parts: A case study. *Int. J. Production Economics* 140: 570–578

Do experts agree when assessing risks? An empirical study

Nektarios Karanikas, Steffen Kaspers
Amsterdam University of Applied Sciences / Aviation Academy
Weesperzijde 190
1097 DZ, Amsterdam, The Netherlands

Abstract

Risk matrices have been widely used in the industry under the notion that risk is a product of likelihood by severity of the hazard or safety case under consideration. When reliable raw data are not available to feed mathematical models, experts are asked to state their estimations. This paper presents two studies conducted in a large European airline and partially regarded the weighting of 14 experienced pilots' judgment though software, and the calculation of agreement amongst 10 accident investigators when asked to assess the worst outcome, most credible outcome and risk level for 12 real events. According to the results, only 4 out of the 14 pilots could be reliably used as experts, and low to moderate agreement amongst the accident investigators was observed. Although quite alarming results, this paper does not aim at raising concerns about the skills of experienced employees; rather, we urge organizations to comprehend the distinction between experience and expertise, and focus on training their stuff in published expert judgment methods.

Keywords: expert judgment, risk assessment, risk matrix

1. Introduction

1.1 Background

Every company deals with a variety of risks regardless the field of its operations. Whatever the hazards (e.g., flaws internal to the system, environmental factors) the idea is that if risk is not controlled, it will lead to minor or major losses such as injuries and fatalities, damage in infrastructure and equipment, and decreased customer satisfaction and market share. Safety risk management refers collectively to a process through which organizations aim at eliminating or mitigating hazards, thus reducing their exposure to risks.

The typical risk management cycle consists of hazard identification, risk level assessment, prioritization and implementation of risk controls, monitoring of residual and new risks, and evaluation of preventive measures' effectiveness. The use of risk matrices has been established across many industry sectors though standards and best practice [e.g., 1, 2, 3, 4]. Those matrices are based on the concept that risk is a product of likelihood by severity of each hazard; within the matrix, hazards and threats are placed in a specific cell which corresponds to a particular risk level. The matrix cells are divided into coloured areas that depict the magnitude of risk. Based

on the risk level and area, a decision is made about the acceptance, rejection or control of the risk with the introduction of a variety of barriers and defences (e.g., procedures, training, technology).

The use of risk matrices is accompanied by both advantages and disadvantages. The illustration through risk cells and areas has been negatively criticized because it depicts risks in one-dimension [5]. Although a risk matrix is easy to use due to its graphical and seemingly easy layout, sometimes risk matrices offer low resolution, which may result in difficulties when trying to place a risk in the right segment [5, 6]. Smith, Siefert, & Drain [7] argued that viewing the consequence as a single point in a matrix might be problematic since the same situation might happen again but with implications of different magnitude. Duijm [5] concluded that a matrix might be used differently across professionals, some of them considering the most likely scenario and others thinking about the worst case; the aforementioned author concluded that the manner of representation affects how people accept risk. Hubbard & Evans [6] viewed risk matrices as additive or multiplicative scoring methods, which are accompanied by four drawbacks:

- Their use is subject to cognitive biases, as also Smith et al. [7] statistically confirmed.

- The assignment of probability and severity labels is not standardized across the industry and can be changed to accommodate each organization's risk appetite over time.

- The labels assigned to likelihood and severity affect the results themselves (e.g., a 3-point scale provides a different interpretation of risk compared with a 5-point scale).

- There might be correlations which are not visibly taken into account (e.g., cascade failures).

Available raw data from past cases and events is exploited for risk level estimations (e.g., probabilistic calculations, average costs incurred). Support from experts is requested when data about probabilities and outcomes is unavailable, corrupted or unreliable. Nonetheless, the performance of experts in terms of their judgments' accuracy has been questioned; Camerer & Johnson [8] found that simple models outperformed experts, but subsequent research contradicted these findings [9]. So, it is suggested that both, simple models and expert judgment, should be used as complementary to each other in order to merge their advantages [9, 10]. Weighting the experts has been an additional method for collectively eliciting judgements and provide estimations based on the level of expertise offered by each specialist [11].

1.2 Research scope

Taking into account the literature cited above, this paper presents the results of two studies. Part of the objectives of those studies was:

- The assessment of the level of consistency amongst experts when they were asked to assess possible outcomes and risk levels of real events.

- The weighting of experts as means to facilitate decision making when assessing risks.

The studies were performed in a large European airline and the results indicated extremely low agreement amongst the estimations of experts, and their highly uneven weighting.

2. Methodology

As part of their bachelor thesis, Bloemendaal [12] assessed the level of agreement between experts when evaluating risks and Jánossy [13] calculated the weighting of experts when evaluating event probabilities. Both studies were performed at the same large European air operator; the participants of the two studies were different.

2.1 Assessing agreement amongst experts

Bloemendaal [12] presented 12 Air Safety Reports (ASRs) to 10 experienced accident investigators. The company contemplates those employees as experts and asks for their judgment in the frame of safety risk management. The ASRs dated from October 2014 to May 2015 and were stored in the airline's database; ASRs representing event types with the highest frequency were selected. The airline uses a matrix divided into 25 risk levels (5x5 matrix) with 4 risk areas: low – green area, medium – yellow area, high – orange area and substantial – red area (Figure 1). The company had classified the specific ASRs as follows: 3 low, 7 medium and 2 high.

	PROBABILITY				
SEVERITY	A	B	C	D	E
5					
4					
3					
2					
1					

Figure 1. The risk matrix type used by the airline.

First, the researcher posed to each expert two open questions for each ASR: "What is the worst outcome?", and "What is the most credible outcome?". Second, the accident investigators assigned to each ASR a risk level in the 5x5 risk matrix, indicating thus the probability and severity level of each event, as well its risk area. Intentionally, the experts were not presented with a predefined list of outcomes, in order to minimize anchoring bias. Their answers were qualitatively analysed in order to develop a mutually exclusive and exhaustively inclusive list of outcomes.

Based on the data collected by Bloemendaal [12], we used the Kendall's W non-parametric test for calculating the inter-rater agreement for the worst, most credible outcome, probability, severity and risk levels, and risk area. Kendall's W ranges between 0 (no agreement) and 1 (complete agreement). The significance level was set at to α=0.05.

2.2 Weighting of expert judgment

Jánossy [13] weighted 14 highly experienced pilots in order to indicate the extent to which the judgment of each expert would be considered when assessing event probabilities. The sample was: 5 pilots flying an A330 aircraft type, 5 pilots flying a B777 aircraft type and 4 pilots flying a B747 aircraft type. The Excalibur software [14] was used for weighting the experts based on seven seed questions; the participants were asked to recall numerical data as follows:

1. IATA flights conducted worldwide two years ago.
2. Hull losses of western-built aircraft occurred per 10 million flights two years ago.
3. ASR submitted the previous year by pilots of the specific airline.
4. ASR of the previous year classified as "High" risk in the airline.
5. ASR of the previous year classified as "Medium" risk in the airline.
6. Take-Off Configuration warnings in the previous year within the airline.
7. Rejected Take-Off at a speed rate higher than 80 knots in the previous year within the airline.

The weights were calculated based on the experts' performance on the seed questions. Based on suggestions from literature [15, 16] the "Performance Weighting" option of the Excalibur software was preferred [14].

3. Results

3.1 Agreement amongst experts

Tables I and II show correspondingly the list and distribution of the worst and most credible outcome types the accident investigators assigned to the 12 ASRs. The figures in the cells represent the number of experts that attributed the specific outcome to the respective ASR.

Table I: Frequencies of worst outcomes selected per ASR.

	Worst outcome categories										
ASR	**Death**	**Injury, no hospitalisation**	**Injury with hospitalisation**	**Hull loss**	**Loss of control**	**Runway excursion**	**Aircraft damage**	**Mid-air collision**	**Airprox**	**Hard Landing**	**Short landing**
1	2	1	5								
2	6	1	1								
3	1			6	2	1					
4			1		2		2	5			
5	1	2		1	4		1				
6	7		2								
7	6	2	1								
8	1			5	1	1			1		
9	1			3	1	1				2	1
10	3						7				
11								10			
12	4		1		4			1			

Table II: Frequencies of most credible outcomes selected per ASR

	Most credible outcome categories											
ASR	Injury, no hospitalisation	Injury with hospitalisation	Hard landing with damage	Loss of control	Damage to aircraft	Hull loss	Mid-air collision	Death	Runway excursion	Long landing	Physical distress	Loss of separation
1	1	1	6									
2	6	2										
3			6	1	2	1						
4	1				3		1					
5					4		1					
6	1	2			2			1				
7		5	3									
8		1	1		3				2	1	1	
9				1		1				5		
10		1			7							
11							5					2
12	1	6		1				1				

Tables III and IV show correspondingly the probability (scale A to E in ascending alphabetical order) and severity (scale 1 to 5 in ascending order), and risk level estimations of experts (i.e. the cross reference of severity and probability levels). Each column of Table IV corresponds to the risk area presented in Figure 1. The numbers in the cells represent how many experts assigned each option (i.e. probability, severity and risk levels) to each ASR. The results for the Krippendorff's Alpha and Freidman tests are presented in Table V.

Table III: Frequencies of probability and severity levels assigned per ASR.

	Probability level					**Severity level**				
ASR	**A**	**B**	**C**	**D**	**E**	**1**	**2**	**3**	**4**	**5**
1		2		3	5			4	6	
2	2		3	2	2		3	4	1	1
3	1	4	5					5	4	1
4	5	4				3	2	1	2	1
5	4	3	1			2	1	1	4	
6	4	1	3			2	1	1	3	1
7	4	3	2					5	4	
8	6	2	1				1	3	4	1
9	5	3	1	1		1	4	1	3	1
10	5	3	2				1	3	6	
11	7		1							8
12		1	5	2	2			5	5	

Table IV: Frequencies of risk levels assigned per ASR.

	Risk level (for the respective risk area see Figure 1)																								
ASR	**A1**	**A2**	**A3**	**A4**	**A5**	**B1**	**B2**	**B3**	**B4**	**B5**	**C1**	**C2**	**C3**	**C4**	**C5**	**D1**	**D2**	**D3**	**D4**	**D5**	**E1**	**E2**	**E3**	**E4**	**E5**
1									2									1	2				3	2	
2		1		1								1	1	1									3		
3				1				1	2	1			4	1											
4	3	1		1			1	1	1	1															
5	2			2				1	2			1													

	Risk level (for the respective risk area see Figure 1)																								
ASR	**A1**	**A2**	**A3**	**A4**	**A5**	**B1**	**B2**	**B3**	**B4**	**B5**	**C1**	**C2**	**C3**	**C4**	**C5**	**D1**	**D2**	**D3**	**D4**	**D5**	**E1**	**E2**	**E3**	**E4**	**E5**
6	1	1		2						1	1		1	1											
7			2	2				1	2				2												
8			1	4	1		1	1					1												
9		3	1		1		1		2		1								1						
10		1	1	3				2	1					2											
11					7										1										
12								1					2	3				1	1				1	1	

Table V: Inter-rater agreement results.

Variable	**Kendall's W**	**Significance**
Worst outcome	0.220	0.003
Most credible outcome	0.164	0.027
Probability level	0.305	0.006
Severity level	0.315	0.004
Risk level	0.241	0.000
Risk area	0.550	0.000

3.2 Expert judgment weighting

The results of the Excalibur software are illustrated in Figures 2, 3 & 4 for the A330, B747 and B777 pilots correspondingly. The figures in the column "Normalized Weight without DM" are of interest for the scope of this paper; those represent the proposed weighting of the experts without the advantage of software's Decision Making (DM) function [14].

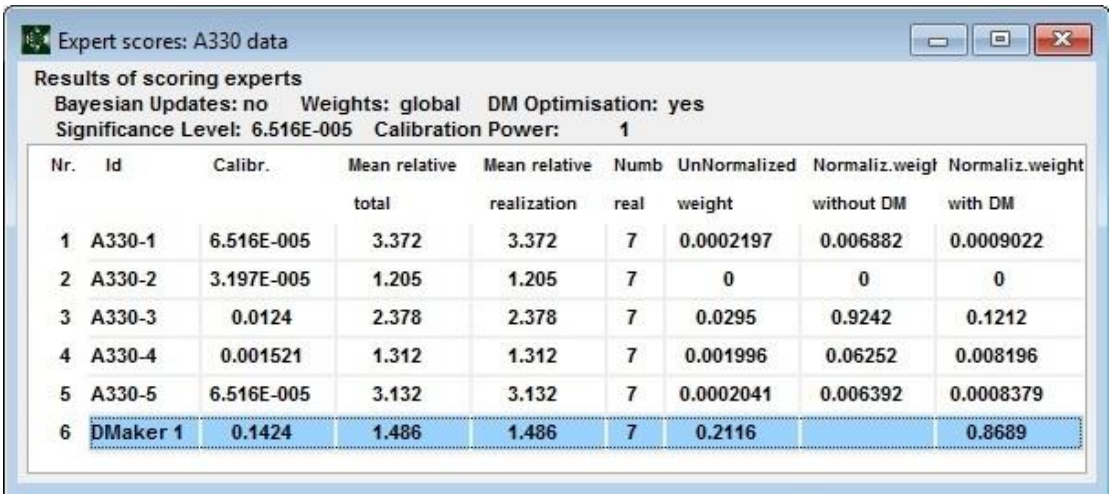
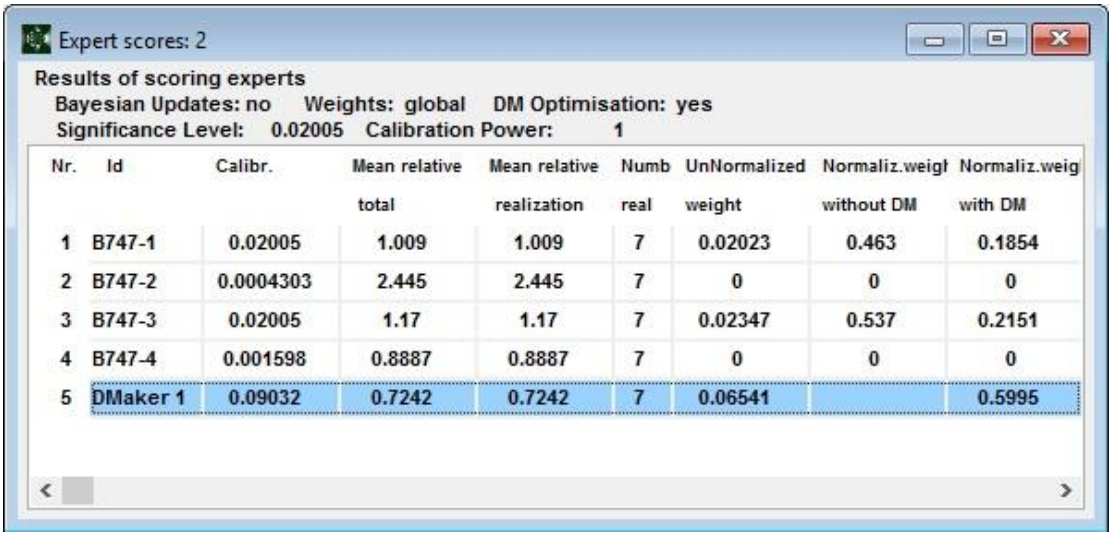


Figure 2. Weighting results for the A330 pilots.

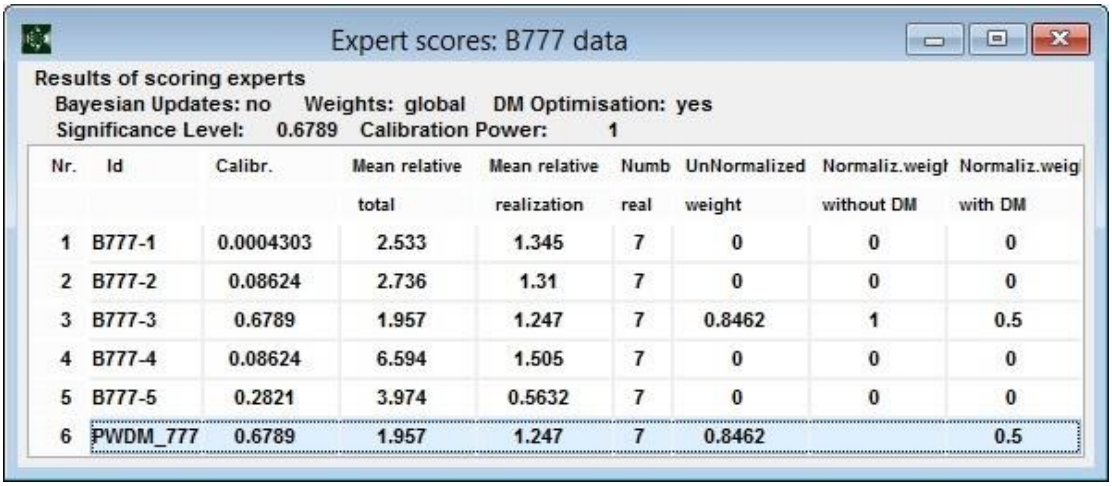


Expert scores: 2

Results of scoring experts
Bayesian Updates: no Weights: global DM Optimisation: yes
Significance Level: 0.02005 Calibration Power: 1

Nr.	Id	Calibr.	Mean relative total	Mean relative realization	Numb real	UnNormalized weight	Normaliz.weigh without DM	Normaliz.weig with DM
1	B747-1	0.02005	1.009	1.009	7	0.02023	0.463	0.1854
2	B747-2	0.0004303	2.445	2.445	7	0	0	0
3	B747-3	0.02005	1.17	1.17	7	0.02347	0.537	0.2151
4	B747-4	0.001598	0.8887	0.8887	7	0	0	0
5	DMaker 1	0.09032	0.7242	0.7242	7	0.06541		0.5995

Figure 3. Weighting results for the B747 pilots.



Expert scores: B777 data

Results of scoring experts
Bayesian Updates: no Weights: global DM Optimisation: yes
Significance Level: 0.6789 Calibration Power: 1

Nr.	Id	Calibr.	Mean relative total	Mean relative realization	Numb real	UnNormalized weight	Normaliz.weigh without DM	Normaliz.weig with DM
1	B777-1	0.0004303	2.533	1.345	7	0	0	0
2	B777-2	0.08624	2.736	1.31	7	0	0	0
3	B777-3	0.6789	1.957	1.247	7	0.8462	1	0.5
4	B777-4	0.08624	6.594	1.505	7	0	0	0
5	B777-5	0.2821	3.974	0.5632	7	0	0	0
6	PWDM_777	0.6789	1.957	1.247	7	0.8462		0.5

Figure 4. Weighting results for the B777 pilots.

According to the results, if the company requested a judgment from those participants the following would apply:

- A330 pilots: The judgment of pilot A330-3 should be taken mostly into account, whereas A330-2 pilot's opinion should not be considered at all.

- B747 pilots: Pilots B747-2 and B747-4 should be excluded and only assessments of pilots B747-1 and B747-3 should be contemplated with about the same weight.

- B777 pilots: Only the opinion of the pilot B777-3 should be counted.

4. Discussion

The results regarding the agreement amongst 10 experienced accident investigators suggested low to moderate agreement in the assessment of all variables considered; Kendall's W ranged from 0.164 for the most credible outcome to 0.550 for the risk area. Even prior to any statistical calculations, the observation of

remarkably scattered figures across Tables I, II, III and IV signified a low agreement amongst the experts.

Interestingly, the results of the expert's weighting with the use of the Excalibur software showed remarkable differences amongst the pilots. Out of the 14 participants only 4 would be considered reliable in their judgments, hence decreasing significantly the pool of experts the specific airline could consult if an assessment was necessary. Aggregated results for all 14 pilots were not available in order to examine possible variances amongst all participants. In addition, it must be noted that in all weighting methods the quality of the seed questions plays a paramount role in the results; in the study of Jánossy [13] the effects of the questions used were not exhaustively examined.

5. Conclusions

Certainly, since both studies were conducted in one airline and limitations in the use of the methods employed might exist (i.e. selection of ASRs and effects of seed questions) we do not claim generalizability of the results. Nonetheless, even under those potential imperfections in the quantification of agreement amongst experts, the qualitative evaluation of the data collected confirm the limitations of probability-severity matrices' usage in risk assessments. However, since cognitive biases are inevitably present in each decision and judgment, the goal of this paper is not to raise concerns about the competencies and the trustworthiness of skilful employees.

Organizations need to realise that extensive working experience is not directly associated with expertise [17]. In line with the literature, we propose that companies consider the consistent use of published expert judgment methods and train their safety professionals and experienced staff accordingly; this way, a combination of hard data and human judgment is likely to support effective decision making. In addition, careful interpretation of the results from relevant software and acknowledgement of limitations such software impose will avoid negative implications on the relationships amongst employees and disturbances in organizational culture.

The powerful and unreplaceable human capabilities have been and will always be crucial for maintaining and improving current safety levels. Diversity must be valued when collecting views (e.g. hazard identification, planning of remedial actions against threats). However, when it comes to assigning risk levels in matrices, which prevail the risk decision making across the industry, sufficient consistency and reliability are indisputably required. If the latter cannot be achieved, risk matrices and other probabilistic risk assessment tools must hold only a supportive role in safety risk assessment, and it is rather time to explore the value of alternative methods and tools.

References

[1] AIRMIC, Alarm and IRM, *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000,* United Kingdom, 2010.

[2] ARMS, *The ARMS Methodology for Operational Risk Assessment in Aviation Organizations,* ARMS Working Group, 2010.

[3] D. Smith, Reliability, Maintainability and Risk: Practical Methods for Engineers, 8th ed., Oxford: Butterworth-Heinemann, 2011.

[4] ICAO, *Safety Management Manual,* Montreal: International Civil Aviation Organization, 2013.

[5] N. J. Duijm, "Recommendations on the use and design of risk matrices," *Safety Science,* vol. 76, pp. 21-31, 2015.

[6] D. Hubbard and D. Evans, "Problems with scoring methods and ordinal scales in risk assessment," *IBM Journal of Research and Development,* vol. 54, no. 3, pp. 2:1-2:10, 2010.

[7] E. D. Smith, W. T. Siefert and D. Drain, "Risk matrix input data biases," *Systems Engineering,* vol. 12, no. 4, pp. 344-360, 2009.

[8] C. F. Camerer and E. J. Johnson, "The process-performance paradox in expert judgment: How can experts know so much and predict so badly?," in *Toward a General Theory of Expertise: Prospects and Limits,* vol. 342, Cambridge, Cambridge University Press, 1991, pp. 195-217.

[9] M. Jørgensen, "Forecasting of software development work effort: Evidence on expert judgement and formal models," *International Journal of Forecasting,* vol. 23, no. 3, pp. 449-462, 2007.

[10] R. T. Hughes, "Expert judgement as an estimating method," *Information and Software Technology,* vol. 38, no. 2, pp. 67-75, 1996.

[11] R. M. Cooke and L. H. J. Goossens, "Expert judgement elicitation for risk assessments of critical infrastructures," *Journal of Risk Research,* vol. 7, no. 6, pp. 643-656, 2004.

[12] M. Bloemendaal, *Increasing objectivity in risk assessments: Integration of accident report data in risk assessment as a means to increase objectivity, Bachelor Thesis (unpublished),* Amsterdam: Amsterdam University of Applied Sciences, 2015.

[13] M. Jánossy, *Expert judgement on accident probabilities in use, Bachelor Thesis (unpublished),* Amsterdam: Amsterdam University of Applied Sciences, 2015.

[14] T. Delft, "Classical Model Software - Excalibur," Lighttwist Software, 2013. [Online]. Available: http://www.expertsinuncertainty.net/Publications/Excalibur/tabid/4386/Default.aspx.

[15] R. M. Cooke, M. E. Wittman, D. M. Lodge, J. D. Rothlisberger, E. S. Rutherford, H. Zhang and D. M. Mason, "Out-of-Sample Validation for Structured Expert Judgment of Asian Carp Establishment in Lake Erie," *Integrated Environmental Assessment and Management vol. 10,* pp. 522-528, 2014.

[16] J. W. Eggstaff, T. A. Mazzuchi and S. Sarkani, "The effect of the number of seed variables on the performance of Cooke's classical model," *Reliability Engineering and System Safety,* pp. 72-82, 2013.

[17] M. W. Wiggins and T. Loveday, Diagnostic Expertise in Orgnizational Enviroments, Surrey: Ashgate, 2015.

[18] K. Krippendorff, "Computing Krippendorff's Alpha-Reliability," 2011. [Online]. Available: http://repository.upenn.edu/asc_papers/43. [Accessed 20 November 2015].

[19] M. L. McHugh, "Interrater reliability: the kappa statistic," *Biochemia Medica,* vol. 22, no. 3, pp. 276-282, 2012.

[20] A. J. Viera and J. M. Garrett, "Understanding Interobserver Agreement: The Kappa Statistic," *Family Medicine,* vol. 37, no. 5, pp. 360-363, 2005.

[21] D. Freelon, "ReCal OIR: Ordinal, interval, and ratio intercoder reliability as a web service," *International Journal of Internet Science,* vol. 8, no. 1, pp. 10-16, 2013.

ZEDB - A Data Base of Nuclear Power Plant Operating Experience of German Design

Yousef Abusharkh
AREVA GmbH, PEPS-G, Safety Engineering
Henri-Dunant-Straße 50
91058 Erlangen, Germany

Günter Becker, Stephanos Camarinopoulos
RISA Sicherheitsanalysen GmbH
Krumme Straße 55
10627 Berlin, Germany

Abstract

The Centralized Reliability and Events Data Base (ZEDB) is a long-term data collection project for reliability measures of nuclear power plants in Germany and other European countries, which started more than twenty years ago with the goal of obtaining trustworthy reliability data for use in probabilistic safety analyses (PSA).

The final evaluation of reliability data considers the operation experience of power plants upuntil December 2014 and has been created and published in August 2015.

This paper summarizes the ZEDB in terms of data base organisation, data contents, properties and capabilities of the data base software, data collection, results generated, and the quality assurance approach applied.

Keywords: Up to five keywords (reliability data, failure rate, ZEDB, PSA)

1. Data Structure and Operating Experience of the ZEDB

The Centralized Reliability and Events Data Base (ZEDB) gathers and analyses operating experience of safety relevant components gained at 19 nuclear power plants in Germany and 2 plants in Netherlands and Switzerland.

The next chapter presents the data structure of the ZEDB database. The data collection is presented in Chapter 1.2.

1.1 Data Structure

The smallest unit examined in the ZEDB database is the component, which is described by means of a plant-specific ID code. The components are characterized by

the fact that they perform an independent function within a mechanical or electrical system. Each component type is defined by a component boundary.

For each component contained in the database, component master data, operating reports and events reports are stored. These reports are essential for the organization of ZEDB data content and are defined as follows:

- **Component Master Data**

The technical attributes of the components, like design and operating parameters, are recorded in the master data. These technical attributes, which are called "aspects" in the ZEDB database, represent the master key to create homogeneous populations. The format of the master data reports is identical for all component prototypes. Most of the attributes are mandatory aspects for the database and are provided by the utilities.

The inspection intervals and observation periods for the component are also specified in the master data, which identify the component and the plants more precisely.
Inspections are considered as component tests to check if a stand-by component will function when required (this concerns failure on demand and stand-by failure rate).

- **Operation Reports**

The operating reports stating the start and end times of the reporting period are stored for each component. The operating time, any disregarded periods within the reporting period, and the demands frequency are also stated.

Start time and end times determine the length of the observation period for the component in the report. The component standby time is then obtained by subtracting the stated disregarded periods and the stated operating time from this time interval.

- **Event Reports**

All events leading to unavailability of a component as a consequence of a failure or malfunction of the component itself are reported in the ZEDB database as a component failure event. The failure events to be considered in the evaluation of the reliability data must occur within the component boundary of a component prototype, and must be capable of being unequivocally allocated to a specific component prototype. The format of the event reports is virtually identical for all component prototypes. The contents of the dropdown lists for the aspects "failure mode" and "subassembly/component part" differ.

- **Queries and Analysis Options**

As the data contained in the ZEDB database are assigned to their respective plants and components by means of the plant abbreviation and component ID, it is possible to perform database queries to select components and events according to certain criteria and to create component populations for which the reliability parameters can be determined. For the evaluation of reliability data, two steps are required:

1. The selection of the component populations according to certain technical and/or operational attributes using the component master data.
2. The relevant failure events for these component populations are selected from the event reports by choosing certain aspects, e.g. failure mode "fails to open".

Using the associated operating reports of the selected components and failure events, the following reliability data can be determined:

- Failure rates per time [1/h] for periods of operation,
- Failure rates per time [1/h] for periods on standby, and
- Failure probabilities per demand.

These parameters are determined by the super-population approach, which enables the evaluation of both generic and plant-specific values. The generic reliability values are obtained using evidence from all participating plants. To obtain the plant-specific values, the data from all plants, with the exception of the particular plant concerned, are firstly used to determine a prior distribution, which is then updated in a second step to obtain a posterior distribution by including the data from the plant in question.

1.1.1 Example of an evaluation

Figure 1 below presents an example of a ZEDB result sheet. The component considered is a generator transformer with the failure mode "no transmission of power". Nine failures of these components have been observed in a total observation period of $4.8317*10^{+06}$ hours. Assuming a homogenous stratum, this would lead to the uncertainty distribution in the table below, which is compared with the hierarchical (2 stage Bayesian) approach used in ZEDB.

Table 1: Comparison of results for homogenous stratum and hierarchical approach

Type	**5 % Quantile**	**Median**	**50 % Quantile**	**Exp. value**	**K**
Homogenous	$1.05*10^{-06}$	$1.90*10^{-06}$	$3.12*10^{-06}$	$1.97*10^{-06}$	1.73
Hierarchical	$3.36*10^{-07}$	$1.45*10^{-06}$	$5.74*10^{-06}$	$2.17*10^{-06}$	4,13

Concerning the expected value results appear not to differ too much, however, the uncertainty ranges differ considerably.

Two out of 15 plants in Figure 1 are outside the uncertainty region of the simple homogeneous calculation, where 0 to 1 such outliers at most are expected. The hierarchical approach used in ZEDB provides a more realistic result, as the uncertainty distribution is broader.

Transformers VGB ZEDB

Components: Generator transformer
Type of transformer: Two-winding
Primary voltage: 220 – 425 kV

Failure mode: **Failure to transmit power**

Analysis: Plant-specific, failure rate (operating time) [1/h]

K.1-2: Generator Transformer, Plant-Specific Failure Rate

Plant	5 % Quantile	50 % Quantile	95 % Quantile	k	Mean Value
1	-	-	-	-	-
2	-	-	-	-	-
3	2.97E-07	1.14E-06	3.23E-06	3.30	1.37E-06
4	1.39E-06	4.10E-06	1.20E-05	2.94	5.07E-06
5	3.06E-07	1.22E-06	3.58E-06	3.42	1.49E-06
6	3.11E-07	1.25E-06	3.79E-06	3.49	1.55E-06
7	-	-	-	-	-
8	8.24E-07	2.56E-06	8.57E-06	3.23	3.34E-06
9	4.87E-07	1.77E-06	5.52E-06	3.37	2.22E-06
10	3.22E-07	1.34E-06	4.39E-06	3.69	1.73E-06
11	-	-	-	-	-
12	-	-	-	-	-
13	3.06E-07	1.22E-06	3.58E-06	3.42	1.49E-06
14	-	-	-	-	-
15	3.06E-07	1.21E-06	3.57E-06	3.42	1.49E-06
16	3.84E-07	1.34E-06	3.38E-06	2.97	1.54E-06
17	3.23E-07	1.35E-06	4.45E-06	3.71	1.75E-06
18	2.95E-07	1.12E-06	3.14E-06	3.27	1.34E-06
19	2.94E-07	1.12E-06	3.13E-06	3.26	1.34E-06
20	3.10E-07	1.24E-06	3.73E-06	3.47	1.53E-06
21	4.48E-07	1.60E-06	4.54E-06	3.18	1.93E-06
generic, empirical	3.36E-07	1.45E-06	5.74E-06	4.13	2.17E-06
generic, lognormal	3.61E-07	1.49E-06	6.15E-06	4.13	2.17E-06

Figure 1: Example: Results for Generator Transformer

1.2 Data Contents

1.2.1 Operational Experience Data.

The total operating experience collected in the ZEDB up until December 2013 corresponds to approximately 336 thousand years.

There are approx. 18200 components in the ZEDB .Table 2 summarizes the number of components for the different prototypes. The distribution over the prototypes is presented in Figure 2

The continuous growth of the operating experience for all thirteen prototypes included in the database for the period 1998-2013 is illustrated graphically in Figure 2. The operating experience's growth rate for the presented prototypes reflects the number of components in the respective prototype, which is given in Table 1. Furthermore, the diagram shows the stability of the growth rate of each prototype over time, which confirms the continuous gapless data delivered by the participating power plants. Due to the shutdown of approx. 40% of the German Nuclear Power Plants, a decrease of the operating experience growth rate can be observed after 2010.

Table 2: Number of components contained in the ZEDB database distributed over different prototypes.

Prototype	**Number of components**
Valves	9763
Circuit breakers	2264
Pumps	1219
Control rods	929
Bus bars	875
Vessels/Tanks	736
Static inverters	575
Fans	496
Batteries	457
Heat exchangers	352
Transformers	326
Emergency diesel generators	144
Rotating inverters	83
Total Number of Components	**18219**

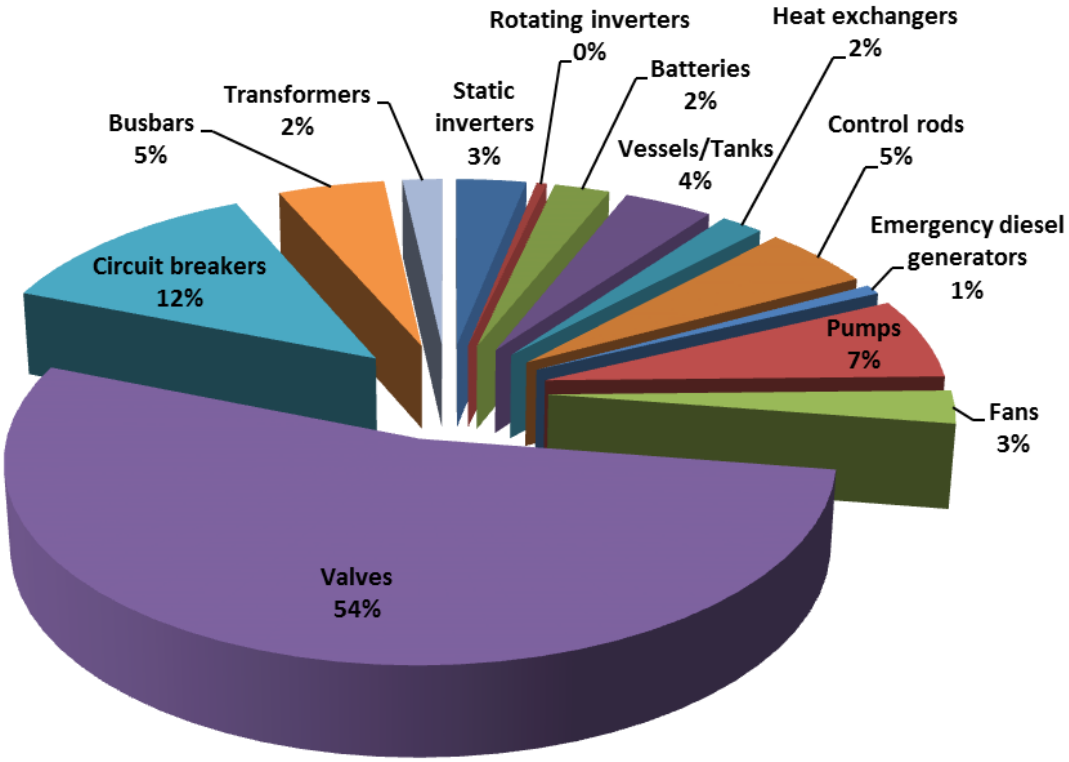


Figure 2: Distribution of the components over the prototypes.

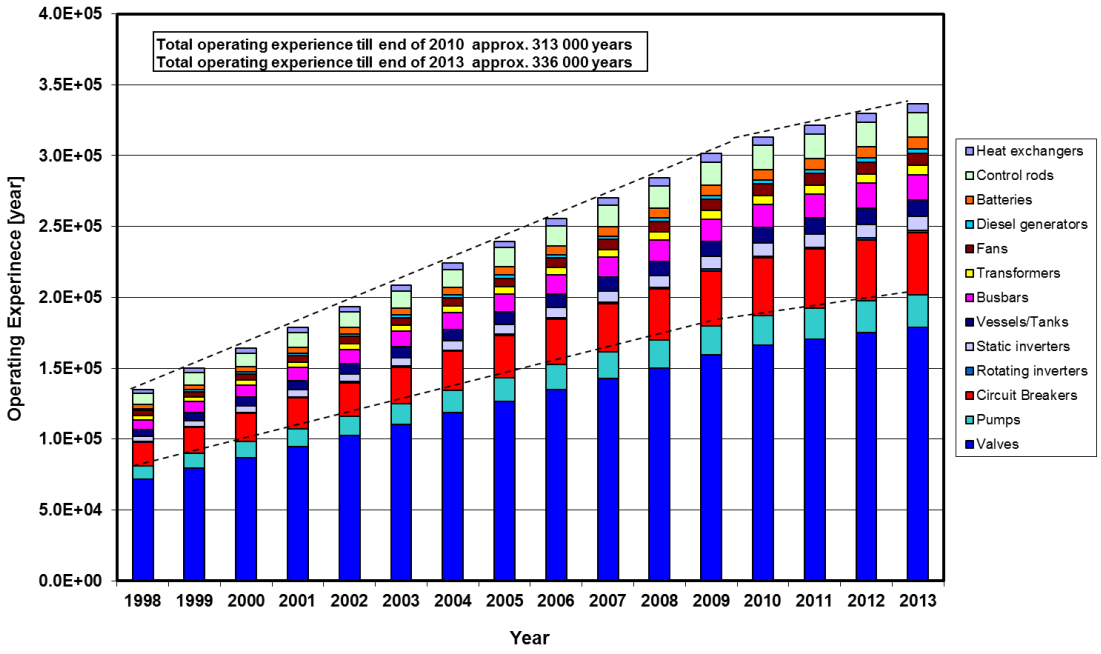


Figure 3: Operating Experience of the Different Prototype over time from 1998 until End of 2013 [1].

1.2.2 Failure Event Data

The total number of critical/non-critical failure events contained in the ZEDB amounts to 3932. Critical failures are those affecting the component such, that they

do not perform the function modelled in PSA. Note that only critical failure events are considered for the evaluation of reliability parameters. Non-critical failure events are included for the sake of completeness. In some cases, regulators demand event reports for failures, which are not relevant for PSA. Such failure is marked as non-critical. The number of failure events assigned to each different prototype is summarized in Table 2.

During the repair time of a component, no further failures are considered until the component has been repaired and normalised. For this reason, replicated failures are extremely rare in ZEDB.

Table 2: Number of critical failure events contained in the ZEDB database for different prototypes.

Prototype	**Number**
Valves	1666
Circuit breakers	182
Pumps	807
Control rods	64
Busbars	48
Vessels/Tanks	13
Static inverters	275
Fans	166
Batteries	18
Heat exchangers	41
Transformers	52
Emergency diesel generators	490
Rotating inverters	110
Total Number of Failure Events	**3932**

2. Properties and Capabilities of the Data Base Software

The ZEDB gathers and analyses operating experience gained at nuclear power plants. The analysis is performed using a two-stage and one stage Bayesian model to calculate plant specific and generic reliability data. ZEDB brings together professionals of diverse research backgrounds, including algorithms, data management, privacy and security, user interfaces, and visualization.

2.1 Introduction

The use of a generic database application is required when an ever-evolving technical task has to be solved, which involves uncertainties regarding development of the structure, scope or level of detail of the data model. The technological innovation in particular for ZEDB is the possibility to manage a central data model which is common for all plants simultaneously with specific model extensions for each individual plant with one software application.

Moreover, the ZEDB facilitates all the functionality required for both data collection at local plants and the demands of the central operator. Keeping this in the same software enables easy maintenance, and reduces problems of compatibility.

2.2 Views in Tables and Forms

The design of the user interface is table-oriented, allowing the user to view and modify data in table views, in addition to a form-based view, which is provided to allow the user to modify data in a more structured manner. Examples of both can be seen in the two figures below.

In Figure 4 a horizontal split of three table views is shown.

1. The component (pump),
2. Operational information and
3. Failure events.

Obviously, this data is interrelated so that after selecting one specific component all related objects of this component are selected, as shown in Figure 4.

Fehler! Verweisquelle konnte nicht gefunden werden. illustrates a form-based view, which contains the specific data for this component.

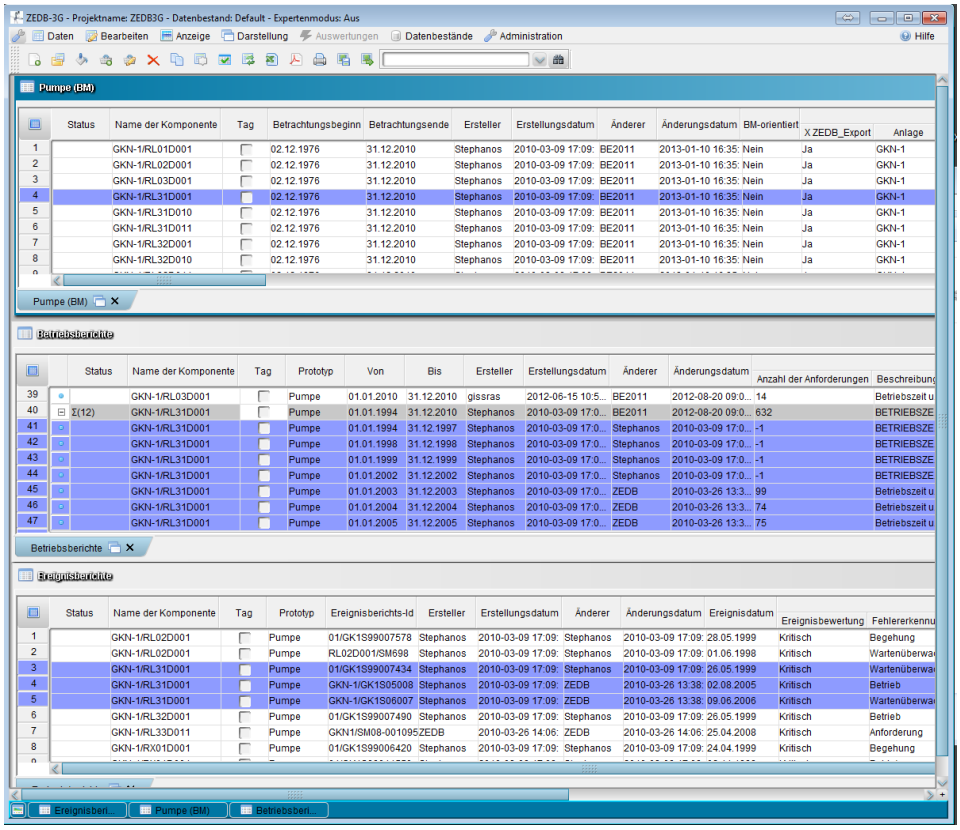
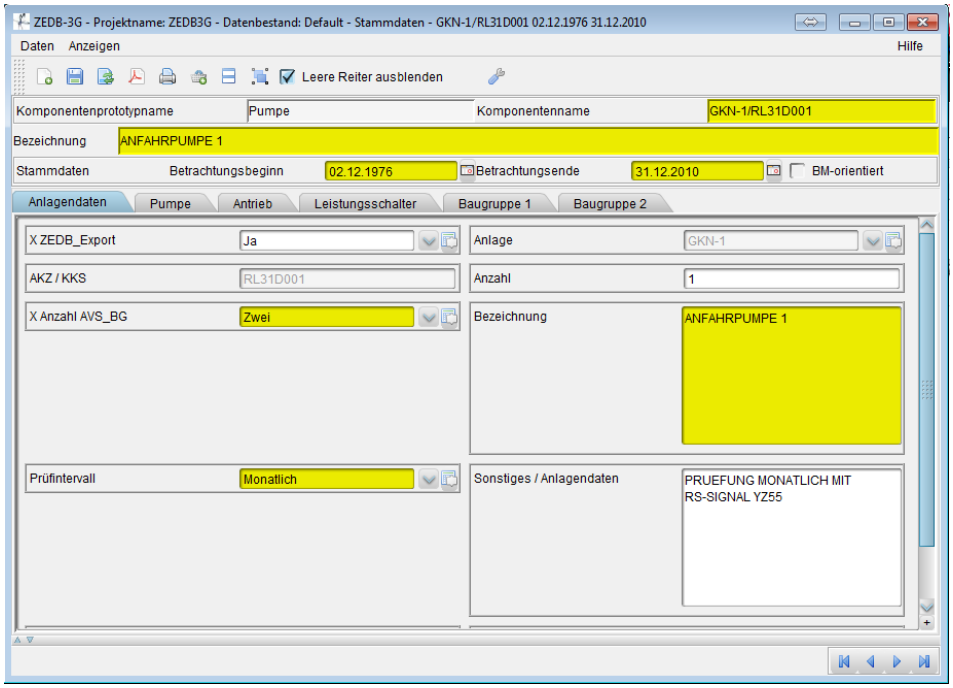


Figure 4: Horizontal split table view in the main application



2.3 Automatic Statistical Analysis

One stage (simple) and two stage (hierarchical) Bayesian approaches were chosen as mathematical tools to analyse the ZEDB data using Bayesian methods. In both cases, the probability distributions of failure rates and failure probabilities per demand are estimated.

Within the simple approach, a lognormal distribution for the failure rates/failure probabilities on demand is assumed. The underlying Likelihood function is the Poisson distribution for failure rate estimations and the Binomial distribution for the estimation of failure probabilities per demand.

The two-stage Bayesian models are standard practice nowadays (see [3] to [7]), although they may differ in their mathematical models and software implementation. The similarity of these applications is the assimilation of data from different sources, as illustrated in Figure 5. This is very attractive in cases where the data from the given plant are sparse.

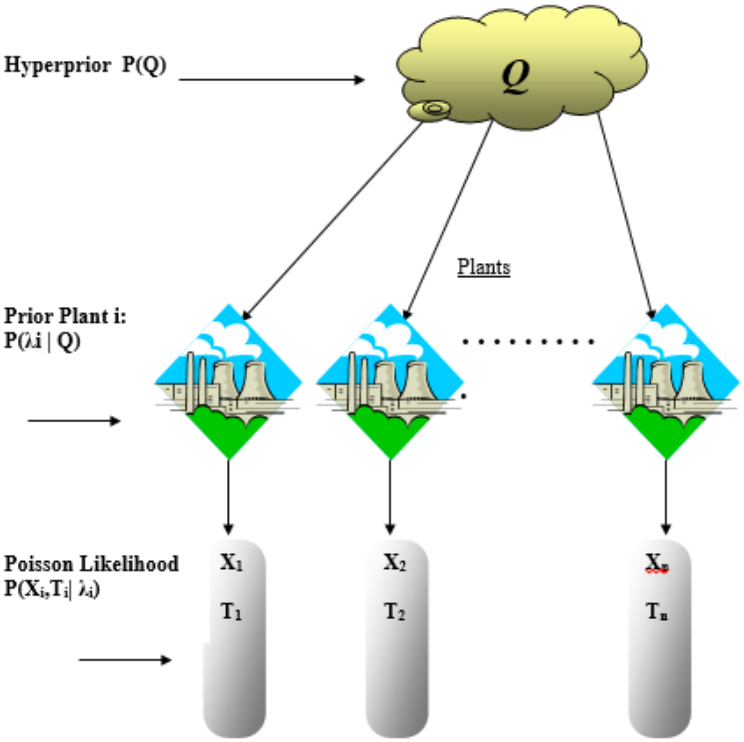


Figure 5: Bayesian Two Stage Hierarchical model

Using these models, the so-called super-population models, the reliability parameter for any component in a particular plant can be assessed with reference to the operating experience from all others. More specific, the general form of the posterior distribution for failure rate λ_0 of a component at plant of interest 0, given failures X_i and observation times T_i of similar components at plants 0, 1, … n is derived. The exposure T_i is not considered stochastic, as it can usually be observed with certainty.
The number of failures X_i for a given exposure follows a fixed distribution type, in this case Poisson. The parameter(s) of this fixed distribution type are uncertain, and are drawn from a prior distribution. The prior distribution is also of a fixed type, but with uncertain parameters. In other words, the prior distribution itself is uncertain. This uncertainty is characterized by a hyper-prior distribution over the parameter(s) of the prior. In Figure 3, the hyper-prior is a distribution P(Q) over the parameters Q of the prior distribution from which the Poisson intensities $\lambda_1,\ldots\lambda_n$ are drawn. In sum, the model is characterized by a joint distribution:

$$P(X_1,\ldots X_n, \lambda_1,\ldots\lambda_n, Q) \qquad (1)$$

To yield tractable models, two types of assumptions are needed. First, conditional independence assumptions are made to factor (1) [8,9]. Second, assumptions must be made regarding the fixed distribution types and the hype-prior distribution P(Q).
Although ZEDB recommends the lognormal model for the prior distribution of λ, both the lognormal and gamma models are supported. The choice of the hyper-prior is based partly on the non-informative rule of Jeffrey and partly on engineering justification [10].

2.4 Interoperability

Due to the heterogeneity of PSA software solutions that are available, ZEDB makes a strong commitment to interoperability. There are flexible interfaces for exchange data with external systems. In addition, ZEDB already includes interfaces to most known PSA software suites (Riskspectrum©, Riskman©, etc.).

3. Quality Assurance Approach

Lots of effort and energy has been invested in the data collection process. Beside the measures mentioned in this chapter, yearly workshops have been held to train the staff from participating plants on how to collect and import the relevant data into the application. At these workshops, the participants gave valuable feedback on practical use of the software to help further develop the whole data collection process.

Whenever demanded, experts from the ZEDB team provided on- and offsite support during the data collection or even conducted the data collection independently on behalf of several operators. A multistage quality assurance procedure beginning from the collecting of component data on the power plants until the evaluation and documentation of the reliability data is applied.

A ZEDB manual [2] has been prepared to provide instructions on how to compile the master data as well as the event and operating reports. This has the aim of ensuring that the data collection is consistent among all participating plants and all submitted data are of the same quality. The manual specifies the component boundaries, describes the component prototypes and explains the dropdown lists assigned to the component prototypes along with the terms contained in them.

The raw data is collected by qualified personnel from various sources at the plant and then input into the local ZEDB3G program. The software only permits the data to be incorporated into the database in a ZEDB-compatible format. To ensure that the data transferred to the database operator are free of errors and inconsistencies, an integrated testing module checks the data.

When the database operator transfers the data supplied by the plant into the central ZEDB database, data is checked via the integrated testing module. If inconsistencies or errors occurr, the incorporation of the data into the database is denied and the database operator is informed by means of a test report about the errors that were found.

The data is then subjected to a plausibility check by qualified staff employed by the database operator. If the database operator should detect incorrect or at least questionable data, the data concerned is sent back to the plant with an explanation and a request for correction or clarification. If the plausibility check is successful and the data content is correct, the data is used for determination reliability parameter.

The documentation of evaluated reliability data is also subjected to a comparative plausibility check by qualified staff employed by the database operator and the release for publishing is performed by the ZEDB Steering Committee.

4. Trend of the Reliability Parameter Estimated with the ZEDB Data

The increase, decrease or constancy of the failure rates estimated in the ZEDB depends on the ratio of the growth of the number of failures events to the growth of the operating time, which mainly depends on the number of components within the considered collective

Based on the observation that the relative increase of the operating experience gradually decreases over time, the relative change of the failure rate is mainly dependent on the relative change of the number of the failure events. Because of the fact that the greater the total number of failure event is, the smaller the relative change of the failure events will be, three representative component populations (with different number of events in 1998) were defined.

For these component populations, the trend of the failure rate has been evaluated for different points in time, starting from 1998 until the end of 2013 with a constant linear step width of one year.

The trend analyses shows that the component populations with a total number of failure events larger than 10, can be considered as rather stable and insensitive to the occurrence of additional failure events. The consideration of additional operational experience less than 10% of the total number of the existing failure events will lead to a reduction of the failure rate. Thus, a further evaluation of these collectives is not strictly necessary.

For component populations with a total number of failure events $1 \leq N < 10$, the most sensitive collective is the one with the total number of failures equal one. This is because of the approximately doubling of the mean value of the failure rate by considering only one further additional failure event.
In contrast, the component populations without previous failure events (are the most sensitive ones. Therefore, a revaluation of these component populations is recommended.

In order to obtain a general assessment of failure rate tendency for all collectives evaluated in the ZEDB, the percentage fractions of the prototype specific collectives depending upon the total number of failure, which defines the trend of the reliability data, is presented in Table III. About 25% of all formed component populations are sensitive against the consideration of further failure of events. About 47% of all component populations with a total number of failure events $1 \leq N < 10$ can be considered as less sensitive. Due to the sufficient operating experience and in particular due to the large number of failure events, 27% of total number of formed component populations can be considered as insensitive against further consideration of operating experience.

Table 3: Fraction of the prototype-specific collectives depending on the total number of failure events

Prototype	**Number of failures**		
	N = 0	**1 <N<10**	**N ≥10**
Static inverters	0%	0%	100%
Rotating inverters	0%	0%	100%
Batteries	45%	0%	55%
Vessels/Tanks	1%	54%	45%
Heat exchangers	38%	23%	39%
Control rods	0%	67%	33%
Emergency diesel generators	0%	67%	33%
Pumps	41%	33%	26%
Fans	75%	0%	25%
Valves	27%	52%	21%
Circuit breakers	69%	18%	13%
Bus bars	50%	50%	0%
Transformers	85%	15%	0%
Related to all component population	**25%**	**47%**	**27%**

Since the operating experience contained in the ZEDB is not going to be further updated, a revaluation of these components population considering the generic prior from other reliability data sources is recommended. There is a free text describing the details of the failure in the database, which can be used to conclude on failure mechanisms and to locate the failure in plant documentation, which may provide additional insight

5. Potential Uses of the ZEDB Data Base

ZEDB comprises a large amount of operating experience, which enables the creation and the evaluation of the most collectives with respect to the component function.

The trend analyses have shown that the evaluated populations with a total number of failure events ≥ 10 are insensitive and that the consideration of further operational experience with additional failure events < 10% of the total number of existing events will lead to a lower failure rate. Furthermore, the ZEDB provides the reliability data for more than 75% of the mechanical and electrical components included in probabilistic safety analyses (PSA) for pressurized water reactors (PWR) and boiling water reactors (BWR). Thus, the ZEDB is the reliable basis for the use in PSA.

As ZEDB considers variability across different plants, the generic results can be used as prior information for other plants, or as a generic basis for a new plant, which has no plant specific information yet.

Specific analysis is possible to analyse whether stand-by time or number of demands influences the failure behaviour.

Specific analysis concerning aging has been performed for Diesel generators [11], though some additional data (times of renewal) had to be collected to perform this task.

Acknowledgements

ZEDB has been financed and substantially supported by Dutch, German and Suisse NPP utilities organised in the VGB PowerTech Service GmbH.

References

[1] ZEDB Evaluation 2014, VGB PowerTech, 2014, Essen, Germany
[2] Handbuch zur ZEDB-Datenerfassung, Version 4.2, erstellt durch AREVA GmbH im Auftrag der VGB, Erlangen 2008
[3] Kaplan, S. (1983) “On a two-stage Bayesian procedure for determining failure rates from experimental data”,*IEEE Trans. On Power App. and Sys.* Vol. PAS-102, 195-202.
[4] Kaplan, S. (1985) “Two-stage Poisson-type problem in probabilistic risk analysis” *Risk Analysis*, 5, no. 3 227-230.
[5] T-Book Reliability Data of Components in Nordic Nuclear Power Plants, ATV Office, Vattenfall, AB, S-162, 87, Vallingby Sweden.
[6] Pörn, K. (1990) *On Empirical Bayesian Inference Applied to Poisson Probability Models*, Linköping Studies in Science and Technology, Dissertation No. 234, Linköping.
[7] Becker, G. and Hofer, E. (2001) Schätzung von Zuverlässigheits-Kennwerten aus der Evidenz veschiedener Anlagen GRS-A-2918.
[8] Iman R. & Hora S. 1990. Bayesian modeling of initiating event frequencies at nuclear power plants, Risk Analysis, vol. 10, no.1, pg. 103–109.

[9] Pörn K. 1990. On Empirical Bayesian Inference Applied to Poisson Probability Models, Linköping Studies in Science and Technology, Dissertation No. 234, Linköping.

[10] Becker, G. 2009. Theorie des zweistufigen Bayes-Verfahrens und deren Implementierung im Programm Bayes20.

[11] Blombach, J., Brahmstaedt, K.U., Camarinopoulos, L., Does ageing of NPPs require the incorporation of time dependent failure rates in PSA models - Verification using operating experience of emergency Diesel generators collected in ZEDB, 31st ESREDA seminary, 2006.

Building Maintenance Optimisation: Current Gaps and Future Opportunities

Samir Shariff and Khairy Kobbacy

MM BinLadin Chair in Operations and Maintenance Technology

Taibah University, Madinah, Saudi Arabia

ABSTRACT

This paper is concerned with research in building maintenance optimisation with particular reference to current gaps and further opportunities. The paper first introduces the history of building maintenance research and its importance, social and economical. The state of the art of modelling in maintenance research is then discussed and an analysis of building maintenance research in comparison to modern "plant" maintenance advances is presented focusing on the gaps between them. The paper then explores how can Building Information Modelling (BIM) be used to support building maintenance given the possible interaction between BIM, Computer Aided Facility Management (CAFM) and Computerised Maintenance Management Systems (CMMS) software.

Key words: Building maintenance, Building Information Model (BIM).

1. Introduction

Building maintenance is acknowledged as an important area that is worthy of study. It is broadly appreciated that the cost of maintenance of a building over its life can be much higher than its initial construction cost. Evans et al [1] study of the long term costs of owing and using buildings suggested a ratio of 1:5:200 relating the initial cost of the building to that of maintenance and operations respectively. Weather this ratio exaggerates the maintenance cost that can be open for debate, but maintenance cost over the life of the asset depends on the type of building and its use. For example in a study of post offices in Japan based on using life Cycle cash flow, the data suggests much lower ratio [2]. The ratio of initial cost to the cost of repair and improvement and to operating cost (utilities and maintenance) of post offices increases from 1: 0.21: 0.55 to 1: 0.65: 1.11 to 1: 1.28: 2.22 for 20, 40 and 60 years old buildings respectively. It is important to note the different terms used by Minami[2] e.g. they refer to maintenance cost as those relating to equipment maintenance, cleaning, security and refuse disposal costs. While this ratio is much lower than that suggested by Evans et al [1] it remains highly significant.

Irrespective of its cost, building maintenance is essential to maintain its functionality. But according to Barbour Index [3] the estimated market for Maintenance, Repair and Improvement (MRI) is £28bn compared with £10bn for new build. Wood [4] presents brief introduction to the recent history of building maintenance in the UK. He discusses the public policy with regard to building construction and maintenance from the focus on reconstruction following WWII, the slum clearance, introduction of building regulations, the modernisation of slums to the privatisation of council houses and the introduction of the Private Finance Initiative (PFI) and the Public/Private Partnerships to organise involvement of the private sector in the public sector construction work that was previously carried out by councils.

The first aim of this paper is to present an analysis of both the modern maintenance advances and the building maintenance research at presented with the gaps between them are identified. The paper then explores how can Building Information Modelling (BIM) be used to support building maintenance given the possible interaction between BIM, Computer Aided Facility Management (CAFM) and Computerised Maintenance Management Systems (CMMS) software. The paper is concluded with a proposed building maintenance framework.

2. Asset Management: The State Of The Art

Maintenance is an important part of operations management of any organisation. In industry, plant maintenance represents the focus of such activities. Its objective is generally acknowledged as being to maintain the condition of plant/ equipment at a state that allows delivery of its functions effectively and efficiently. Apart from industry, other types of organisations also have interests in maintenance of its assets including equipments used, buildings and its contents e.g. air conditioning and lefts.

Generally speaking and until the 1970s, maintenance was viewed as an area that no one wishes to get involved in. Instead, there was a tendency for association with production that produces goods or services that can make positive contribution to the organisation. In fact maintenance was thought of as the last uncontrolled area in the majority of business and a bastion of inefficiency [5].

In the past three decades organisations recognised the importance of maintenance management and researchers developed a huge body of knowledge in this area that ranges from the development of maintenance concepts to the specific management techniques and focus on case studies.

The structure of the Complex System Maintenance Handbook (Kobbacy and Murthy [6]) suggests that one can classify research in this area, excluding case studies, into four main areas: c*oncepts and approaches, methods and technique, problem specific*

models and management. There is a substantial body of knowledge accumulated in each of these areas. More details are shown later in Figure(1).

3. Building Maintenance Research

Little attention was given to building maintenance management and planning until the 1960s. From the mid 1960s studies started to emerge in this area. Examination of two books published in the 1970s on building maintenance reveals the areas of interest and indeed the significant advances achieved by that time. The book on Building Maintenance Management by Lee [7] shows appreciation of the complexity of this area and its social and economical importance and the usefulness of utilising management techniques. The chapter on planning shows appreciation of the increasing cost resulting from the delay in undertaking maintenance actions and hence the importance of inspection and indeed the scheduling and the contingency (planned/ preventive) maintenance. The edited book on Developments in Building Maintenance-1[8] reveals the substantial advancements in this area and the emerging topics that remain to be of current research interest to date. Examples cover the decisions models and statistical aids in maintenance management. Techniques discussed include discounting, cost benefit analysis, mathematical programming and indeed the early models that were developed to optimise maintenance activities e.g. determining optimal inspection activities based on the pioneering work of Jardine [9] which continues to be reprinted to date.

4. The Gap Between Modern Maintenance Advances And Building Maintenance Research

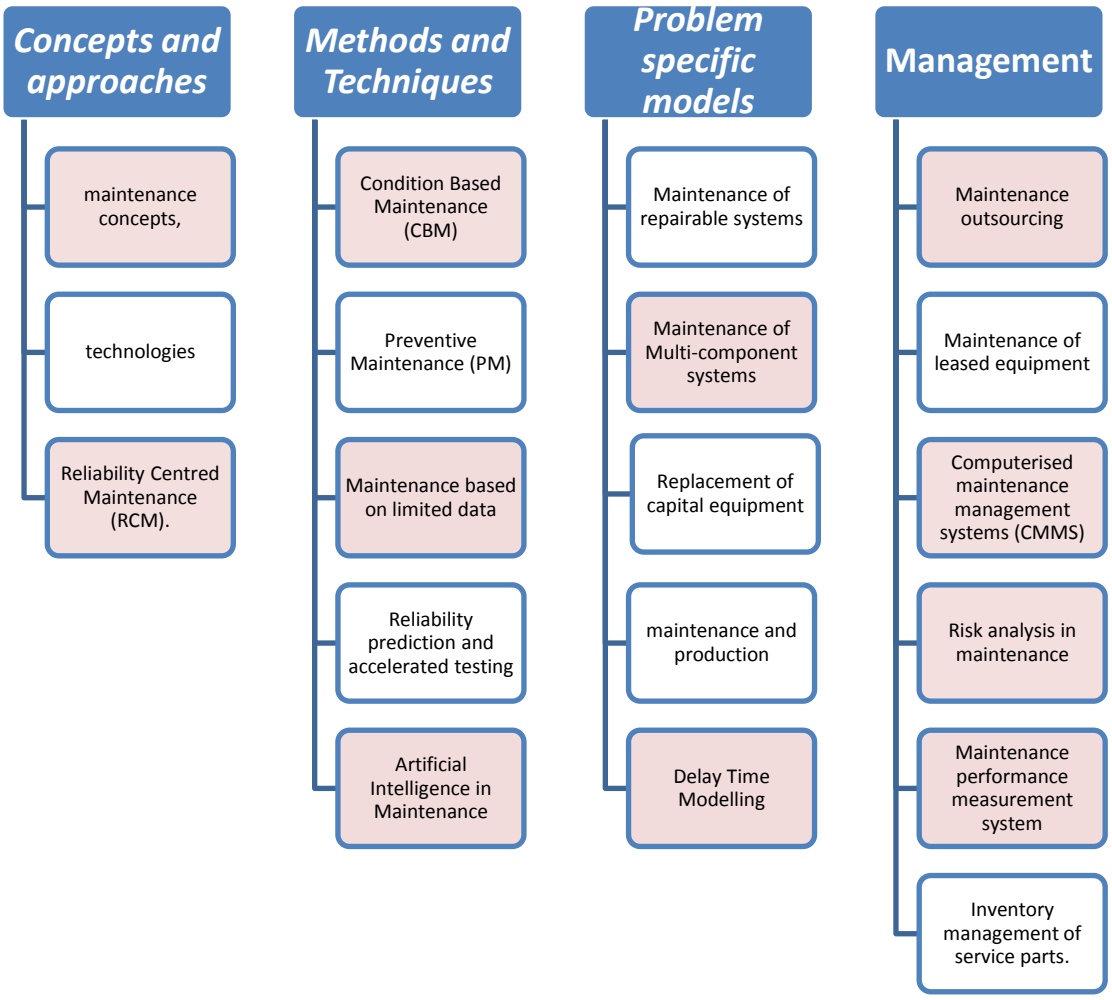
Figure(1) shows the areas of maintenance research according to the classification of Kobbacy and Murthy [6]. A review of the method and approaches developed in the maintenance domain which are typically applied in plant maintenance have identified the methods which are either not been applied or its potential has not been fully explored in building maintenance.

It is important to indicate that many of these methods and techniques while may have not been directly applied in building maintenance situations they are applicable to mechanical and electrical equipment that are used in buildings including lifts, air conditioning systems, water pumps etc. Examples of these techniques include conditions based maintenance, preventive maintenance, reliability predictions and accelerated testing etc. These equipments can typically be grouped under a broad building element namely “services”.

However building maintenance goes well beyond services. For example Elharam et al[10] identifies 11 building elements e.g. floor boards, windows, plaster, walls and doors. Our discussion below will focus on these building elements.

From the previous discussion one can identify the areas that are not explored fully in building maintenance and which have good potential in improving building maintenance. Broadly speaking these areas, which are hatched in Fig 1, include:

1. Maintenance concepts.
2. RCM
3. Condition based maintenance.
4. Maintenance based on limited data.
5. Artificial Intelligence in maintenance.
6. Maintenance of multi-component systems
7. Delay time modelling.
8. Maintenance outsourcing
9. Computerised maintenance management systems (CMMS).
10. Risk assessment.
11. Maintenance performance measurements system



Fig(1) The state of the art and gaps in building maintenance (hatched area indicates potential area of development in building maintenance).

Therefore there is an obvious need to develop a building maintenance concept that guide the strategy of planning and managing building maintenance. An attempt is presented later in this paper. There is also a need to develop more work on the systematic application of RCM in this area.

In the area of methods and techniques the authors believe that a significant benefit can be gained from expanding CBM and the promising area of artificial intelligence techniques. Utilising the most promising statistical techniques on using limited data can be most useful in overcoming typical situations where data are scarce.

Given the complexity and interdependence of building elements it is obvious that utilising the powerful multi-component techniques in optimising building maintenance can be most useful. The same applies to the Delay Time modelling techniques, which were originally developed in the context of building maintenance. These techniques are particularly useful in timing the maintenance action to avoid undesirable and costly failures.

The development and application of maintenance performance measurement systems are essential to assess and develop effective and efficient maintenance policies. Exploring the benefits of maintenance outsourcing is another area that can help in achieving effective maintenance at lower costs. The use of CMMS will be discussed in the next section given the current interest and future expansion in using BIM.

5. Maintenance and Building Information Modelling (BIM)

Building Information Models or BIM was coined in the early years of the 21st Century. There are many definitions for BIM, but essentially it is a digital representation of the physical and functional characteristics of a facility [11]. BIM covers all stages of a building from design and construction to operations and maintenance.

It is expected that maintenance data in BIM models will build-up over the coming few years with the use of BIM which can potentially help more effective building operations and maintenance. The availability of such data will also lead to better managed buildings by reducing both energy use and waste. It is important to start understanding how such information will be used in maintenance management and indeed how the information in BIM can be used to project the maintenance requirements as early as the design phase. In other words the availability of this integrated system will lead to consideration of maintenance requirements at the design stage and hence maintenance cost will influence building design. Furthermore BIM will provide appreciation of maintenance requirements from the design stage. Large organisations now look primarily at facility performance rather than the physical structure [11]. For example the USA General Services Administration

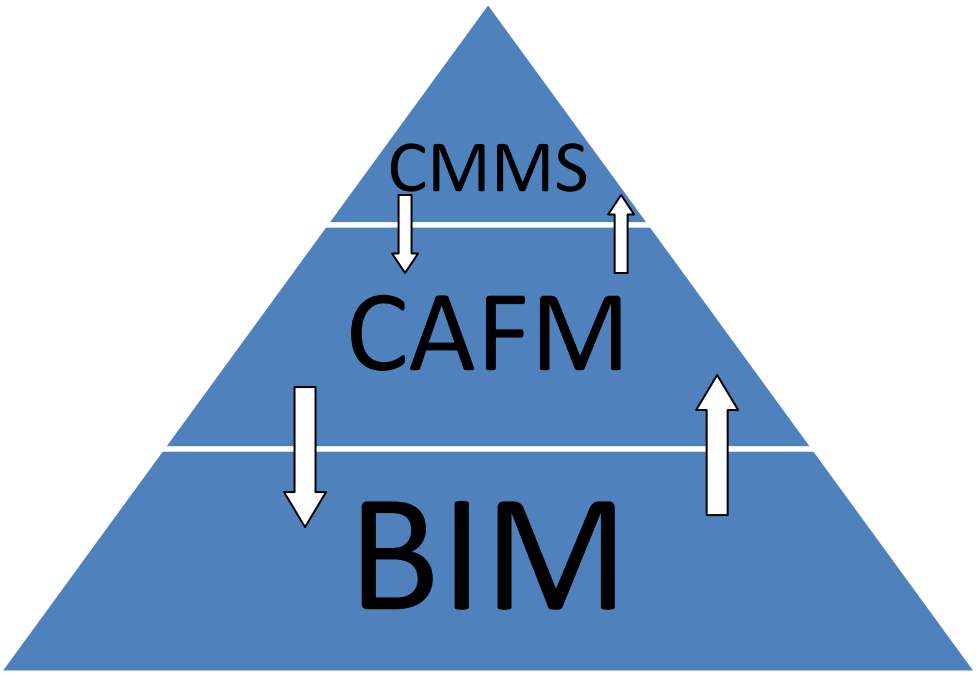
(GSA) has recently awarded contract to design, install and maintain major power facility.

5.1BIM, CAFM and CMMS

These are 3 different categories of computerised systems that can help achieve effective building maintenance; Building Information Model (BIM), Computer Aided Facility Management (CAFM) and Computerised Maintenance Management systems (CMMS). The scope of BIM is broader than that of CAFM which automat many of the FM functions and results in cost savings and improved utilization of assets throughout the entire lifecycle. In particular, CAFM provide and maintain information on floor plans, space utilization, energy consumption and equipment location[11]. CAFM scope is wider than that of the more maintenance specific software CMMS which is a computer software developed to provide support to maintenance managers in planning, management, and administration of the maintenance function with a view to improve its effectiveness. Each type of these software have a role in building maintenance and indeed BIM can be viewed as enabler to both CAFM and CMMS by providing understanding of the facility design and operation, its maintenance requirements and much needed data accumulated while operation.

Integrated CMMSs became the theme for recent development e.g. with asset management systems using costs, production quality, efficiency and facility condition in making decisions about productive and proactive maintenance strategies. Artificial Intelligence (AI) has been identified as a tool to achieve this integration. In a similar manner one would expect the integration of BIM, CAFM and CMMS leading to a more efficient management of buildings throughout its like cycle.

Figure(2) represents the possible interaction between the 3 types of software in supporting the building maintenance and indeed the wider aspects of facility management and other stages of building lifecycle. For example the decision support offered by CMMS can lead to better facility management. It is not surprising, therefore, that some commercial software are classified as both CAFA and CMMS.



Fig(2) Integration of building management tools; BIM, CAFM and CMMS

6. CONCLUSIONS

This paper is concerned with the optimisation of building maintenance. An analysis of the methods and approaches developed in maintenance and building research reveals significant gaps between building maintenance research and the recent advances in the maintenance field typically applied in plant maintenance. We have identified 11 approaches/ areas of maintenance research and development that are either not fully utilised or else not explored in building maintenance. It is hoped that such list will help researchers in developing these areas and exploring its benefits in building maintenance. The potential benefits from the current development and implementation of BIM on building maintenance have been discussed. We believe that over the coming few years with the implementation of BIM significant amount of maintenance data will be accumulated. There is a need to develop methods and approaches that can help integrating BIM with the other computerised systems such as CAFM and CMMS to realise the benefits of BIM implementation in building maintenance. The development of integrated computerised intelligent systems is a potential approach to deal with this issue.

References

[1] R. Evans,R., Haryott,R., Haste, N., and Jones, A. (1998)The long Term Costs of Owning and Using Buildings, Royal Academy of Engineering, London.

[2] Minami, K. (2004) Whole life cost of post offices in Japan, based on a survey of actual conditions and consideration of investment corrections, J of Facilities Management, V2, No 4 pp 328-407.

[3] Barbour Index, (1998) The building maintenance and refurbishment market: summary, Barbour Index , Windsor.

[4] Wood, B. (2005) Towards innovative building maintenance, Structural Survey, V 23, No 4, pp 291-297.

[5] Ward, A. (19880 The micro as maintenance monitor. Account. J. Inst. Chart. Account. Engl. Wales: 127-128.

[6] Kobbacy, K. and Murthy, P. (Editors), Complex Systems Maintenance Handbook, Springer, 2008.

[7] Lee, R., Building Maintenance Management, Crosby Lockwood Staples, London, 1976.

[8] Gibson,E.J., Editor, Developments in Building Maintenance-1, Applied Science Publishers, 1979.

[9] Jardine, A.K., Maintenance, Replacement and Reliability. Pitman publishing, London, 1973.

[10] El-Haram, M.A. and Horner, M.W. (2002) Practical application of RCM to local authority housing: a pilot study, Journal of Quality in Maintenance Engineering, 8(2) pp 135-143.

[11] Ahamed, S.S., Neelamkavil, J. and Canas, R. (2010) Impact of building information modelling in facility maintenance management. The E-SIM 2010 Conference, Winnipeg, Canada.

PSA driven Safety Improvements of Nuclear Power Plants

Jörg Blombach
Ringstr.142
91074 Herzogenaurach
Germany

Hermann Fabian
Franzosenweg 61
91058 Erlangen
Germany

Abstract

This paper recalls the risk studies for nuclear power plants. Following WASH 1400 the German Risk Study for a 1300 MW PWR was performed. The insights from this study led to improvements of safety systems of the analyzed plant and the other PWRs in Germany. Additionally, system modifications were introduced allowing reduction of core melt frequency by plant internal accident management measures for beyond design accident sequences and transferring potential core melt under high pressure into low pressure core melt scenarios before onset of fuel melting. This is quite import with respect to level 2 PSA because the containment integrity is not endangered.
The effectiveness of these measures is presented: reduction of core melt frequency by a factor of 2 and of high pressure core melt scenarios to 50%, 50% being low pressure core melt scenarios.

Keywords: PSA, plant internal accident management

1. Introduction

In addition to the deterministic safety approach probabilistic safety analyses have become more and more important since the 1960s. Reliability methods and programs have been developed allowing nowadays assessing in detail the risk of nuclear power plants quantitatively.

2. Reliability Analyses of Safety Systems

In the 1970s reliability methods such as Event Tree and Fault Tree modelling were developed. The most common quantification was hand calculation and Monte Carlo Simulation. Probabilistic analyses were performed for important safety systems such as

- emergency power supply
- emergency core cooling systems
- auxiliary and emergency feed water systems.

These analyses led to system improvements concerning redundancy and independence of system trains.

3. Risk Studies

The first important risk study (1957) was Wash 740 [1]. The report also known as "The Brookhaven Report" estimated maximum possible damage from a core melt at a large (500 MW) nuclear reactor. The core melt frequency was estimated by expert judgement. The focus was on maximum possible damage (deaths) by exposure from radionuclides after a hypothetical accident.

A milestone was the Reactor Safety Study WASH 1400 [2], 1975). Using the Fault Tree /Event Tree approach (later called PRA or PSA) it estimated the radiological consequences of serious accidents in large U.S Commercial Nuclear Power Plants for a typical BWR and PWR. Within the Individual Plant Examination Program all U.S. nuclear power plants submitted PRAs to the NRC in the 1990s. Five of these were the basis for NUREG-1150, 1991 [3].

Subsequently similar studies were performed in Europe reflecting different plant design, EPS 900 [4] and EPS 1300 [5] in France (1990), German Risk Study in Germany [6], [7] (1980/1989). Probabilistic safety assessment was recognized as powerful means complementary to deterministic safety considerations and used for new plant designs and safety improvement of operating plants by new or modified systems and optimized maintenance.

4. Insights from Risk Studies

In the following some general insights will be addressed and specific insights of the German Risk Study [6] for Siemens/KWU PWRs.

First of all it became apparent that a core melt cannot be ruled out as formerly claimed by deterministic safety assessment. Secondly, it turned out that small primary leaks present a higher risk than the double-ended primary pipe rupture due to its greater occurrence frequency and its more complex demands on safety systems, especially when the cool-down with 100K/h by the secondary side had to be operated manually. Thirdly, the containment can reduce the release of fission products after core melt efficiently, if its rupture by overpressure can be avoided. Fourthly, advanced thermohydraulic accident analyses focused on core degradation resulted in a considerable grace time between loss of core cooling and onset of core melt. Finally, based on these grace times plant internal accident management measures for beyond design accident sequences can reduce the core melt frequency and the amount of radioactive releases using installed systems and their improvements. The most

important measures are:

- automatic cooldown via steam generators with 100 K/h in case of small primary leak
- pressure release of the steam generators and feeding with firefighting pumps
- primary pressure relief via pressurizer safety/relief valves enabling high pressure safety injection and decay heat removal via primary emergency cooling system in case of complete failure of secondary side cooling, in addition prevention of high pressure core melt
- filtered venting of containment preventing overpressure failure of containment
- installation of catalytic hydrogen recombiners in the containment to avoid hydrogen explosions destroying the containment after core melt.

5. Safety improvement by plant internal accident management

Based on the level 1 PSA for internal events of a 1300 MW German PWR which was performed within the periodic safety review in the 1990s [8] the safety improvement by internal accident management is discussed.

5.1 Reduction of core melt frequency

After loss of the secondary side safety systems a core melt can be prevented by

- pressure release of the steam generators and feeding with firefighting pumps – Secondary Side Feed and Bleed
- primary pressure relief via pressurizer relief valves enabling high pressure safety injection and decay heat removal via primary emergency cooling system – Primary Side Feed and Bleed - in case of complete failure of secondary side cooling

The respective emergency procedures are documented in the specific emergency manual. They present the detection signals, the emergency means step by step and the time window for successful application, and they are trained on the simulator.

These emergency procedures are effective for risk dominant Transients and Steam Generator Tube Rupture, as shown in table I.

Overall the core melt frequency is reduced by a factor of 2 which is a remarkable improvement, though for most of the transients the reduction factor is higher. This is due to the fact that both considered accident management means are not effective for Loss of Coolant Accidents.

Table I: Reduction of Core Melt Frequency by Plant Internal Accident Management

Event	Core Melt Frequency without Accident Management	Core Melt Frequency with Accident Management	Core Melt Frequency Reduction Factor
Steam Generator Tube Rupture 2F	6.4E-8/a	3.2E-8/a	2
Steam Generator Tube Rupture 4F	1.0E-8/a	5.0E-9/a	2
Loss of Off-site Power	9.0E-7/a	3E-7/a	3
Loss of Main Feed Water	6.4E-7/a	4.0E-8/a	16
Loss of Main Heat Sink	3.2E-7/a	5.0E-8	6.4
Loss of Main Feed Water & Loss of Main Heat Sink	5.5E-8/a	1.1E-8/a	5
Steam Leak outside Containment	1.01E-7/a	2.4E-9/a	42
Leak Main Feed Water Line inside Turbine Building	3.3E-7/a	1.08E-7/a	1.8
All Events including LOCAs	**3.6E-6/a**	**1.8E-6/a**	**2**

5.2 Risk reduction of high pressure core melt scenarios

Even if the safety injection or the decay heat removal of the Primary Side Bleed and Feed fails, the pressure relief of the primary system as such is a very important measure for accident mitigation. It transfers core melt scenarios to melt down under low pressure thus avoiding high pressure core melt scenarios which could directly jeopardize containment integrity.

The effectiveness of this accident management measure was analyzed in the above mentioned level 1 PSA. It turned out that the contribution of core melt at high pressure could be reduced to about 50% of all core melt scenarios, 50% would be core melt at low pressure.

This is an important improvement with respect to level 2 PSA.

It should be noted that it is a requirement for EPR, a nuclear reactor of the third generation, that high pressure core melt can practically be eliminated [9]. In [10] it is stated "*…a design objective is to transfer high pressure core melt sequences to low pressure sequences with a high reliability so that high pressure core melt situations can be "excluded"*.

6. PSA within the periodic safety review and for new builds

The safety of operating nuclear power plants is reviewed every ten years. This safety review includes a PSA. At the beginning the PSA was a level 1 PSA considering internal events only. Meanwhile the spectrum of initiating events includes fire and site specific external events like flooding and seismic events. Additionally, a level 2 PSA is performed assessing the frequency of large releases. Accident management for beyond design basis accidents using the grace time after loss of safety systems and beginning of core melt are taken into account.

Generally, a full scope level 1 and level 2 PSA is required during design and construction of a new built nuclear power plant comprising

- power operation
- shutdown
- internal fire
- site specific external events

7. Reliability parameters

Quality and results of fault tree analyses depend strongly on the quality of the used reliability data for failure of the considered technical components. In the early stages of fault tree analyses for PSA there was many engineering judgement, but it was evident that reliability data from operating experience was needed. Thus big efforts were made to collect reliability data from operating experience. Important data collections are

- EIREDA [11] (France, French Nuclear Power Plants, 1998)
- T-book [12] (Sweden, Nordic Nuclear Power Plants, regularly updated)
- NUREG/CR 6928 [13] (US, US Nuclear Power Plants, 2007)
- ZEDB [14], [15] (Germany, Siemens/KWU built Nuclear Power Plants, last update 2015)

8. Future improvements

Based on PSA insights the design of safety systems and together with plant internal accident management measures for beyond design accident sequences the overall safety level has been considerably been improved.

However, it is the personal view of the authors that in the future the robustness of the containment as last barrier against large releases should be improved. Especially, the function of the containment should be completely independent from systems that are needed to prevent a core melt, i.e. cooling chains, electrical power supply, safety I&C. Accident management should be planned and incorporated as additional safety level for beyond design accident sequences.

9. Conclusions

After WASH 1400 the German risk study for a Siemens/KWU PWR led to a lot of system modifications by which the core melt frequency could be reduced. Further reduction could be reached by plant internal accident management, primary and secondary side feed and bleed. Pressure relief of the primary system transfers high pressure core melt sequences to low pressure core melt sequences which is relevant for radioactive releases, assessed in level 2 PSA. It became a deterministic requirement for PWRs of the third generation.
PSA has to be performed within the periodic safety review of operating nuclear power plants and serves for continuous improvement of their safety.
Generally, a full scope PSA is required during the design and construction phase of new nuclear power plants providing a well-balanced system design and an acceptable low risk.

10. References

[1] WASH 740 "Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants", USAEC, 1957

[2] WASH 1400 “An assessment of accident risks in U.S. Commercial Nuclear Power Plants", October 1975

[3] NUREG 1150 “"Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants", U.S. Nuclear Regulatory Commission, December 1990

[4] Étude probabiliste de sûreté d’une tranche du Centre de Production Nucléaire de Paluel 1300 MWe

[5] Étude probabiliste de sûreté des réacteurs à eau sous pression de 900 MWe

[6] Deutsche Risikostudie Kernkraftwerke - Eine Untersuchung zu dem durch Störfälle in Kernkraftwerken verursachten Risiko, GRS 1980

[7] Deutsche Risikostudie Kernkraftwerke Phase B, GRS 1989

[8] J. Blombach, Gefährdungszustände und –häufigkeiten DWR-Anlage, KTG-Fachtagung, Karlsruhe, September 25 -26, 2003

[9] Gemeinsame Empfehlungen von GPR und RSK für Sicherheitsanforderungen an zukünftige Kernkraftwerke mit Druckwasserreaktor, Bundesanzeiger, May 5, 1995.

[10] Technical Guidelines for the design and construction of the next generation of nuclear power plants with pressurized water

[11] Procaccia H., Arsenis S.P.,Aufort, European Industry Reliability Data Bank (1998 (Eireda 1998)

[12] Swedpower AB, Stockholm (Sweden) TUD Office (2005). T-book Reliability data of components in Nordic nuclear power plants 6 ed. Sweden: The TUD Office.

[13] NUREG/CR-6928, Handbook of Parameter Estimation for Probabilistic Risk Assessment

[14] H. Fabian, J. Blombach, ZEDB, Zentrale Zuverlässigkeits- und Ereignisdatenbank im VGB-Auftrag, KKW-Betriebsleitertagung, Dezember 1994

[15] J. Blombach, R. Buckermann, B. Schubert, The Centralized Component Reliability Database for PSA Purposes ZEDB – Status, Evaluation 2002, Trends

50th ESReDA Seminar on
25 years of ESReDA seminars : Safety and reliability enhancement throughout Europe : looking back, looking ahead
May 18th -19th 2016, University of Sevilla, Sevilla, Spain.

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

André Lannoy
Institut pour la Maîtrise des Risques
12 Avenue Raspail
94250 Gentilly, France
www.imdr.eu
andre.lannoy@imdr.eu

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.

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, during which 49 ESReDA seminars were organized. The article 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 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.
It should be noted that following the λμ16 Congress of Avignon in 2008, a prospective study on risk management in 2020 was conducted under IMdR (Kahn et al, 2010).

2. Industrial stakes and probabilistic analysis

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,** (and recently) **antifragile** way (Taleb, 2013).

The manufacturer and the operator must demonstrate the safety by the Probabilistic Safety Assessment (PSA, see § 6.1) in which they must answer the following questions (Bedford, Cooke, 2001):

i. What can happen?

ii. How likely is it to happen?

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

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

Level 1: system analysis: it includes event tree, fault tree, human reliability impact, feedback data bases, accident sequence quantification, uncertainty analysis;

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 (US NRC, 1975), concerned the BWR Peach Bottom 2 and PWR Surry 1 nuclear power plants.

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. .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, the probability of rare events, risk analysis, physics- reliability modeling, estimation of consequences, crisis management.

3. Uncertainty

Recall that the ISO 31000 standard (2009) 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 as the work of an ESReDA project group (De Rocquigny et al, 2008) published by Wiley and the recently published book (Lemaire, 2014), 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, ...);

2- lack of knowledge, or the *epistemic uncertainty*, reducible by increasing knowledge on statistics (sample size ...), on the nature of the distribution (which is a subjective choice), on the nature of the model (insufficient physical understanding, uncertainty propagation, ...);

3- *ambiguity* (it can be removed by well adapted definitions, information, …),

4- *indetermination* (case of the extremistan domain, paragraph 6.1 (Taleb, 2010)).

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 which deserves further use). At that time, the Francophone literature is fortunate to have a synthesis work on those methods (Villemeur, 1988). 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 (Rauzy et al, 1997).

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 (§ 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 is a risk of combinatorial explosion by multiplying the number of states. Nevertheless, continuous time Markov processes are used by engineers to describe system dependability in many studies.

Some studies are now performed in the field of dynamic reliability since the early 2000s (Dufour, Dutuit, 2002). The PDMP process (Piecewise Deterministic Markov Process (Davis, 1984)) is a process whose behavior is governed by random jumps at time points, where evolution is deterministically governed between those times (Costa, Dufour, 2010). This process is little used in the industry. Yet the literature indicates that it would be easy 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 (Bouissou, 2008). 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. This method (originally used in automatic, dating from 1962) lists the possible states (in operation, degraded, failed) of a system and the links between them. 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 (Signoret, 2014). 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).

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).

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 becomes also an important stake. 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 (Ligeron, Marcovici, 1974). 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: (Madsen et al, 1986), (Ditlevsen, Madsen, 1996) and (Lemaire, 2005).

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. 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 (1974)) 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). 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 or the most likely failure point. 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 (Rocquigny et al, 2008):

- 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, 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 OpenTURNS in France or PROBAN in Norway.

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; Lemaire, 2014) which is is a non-sampling-based method to determine evolution of uncertainty in a dynamical system, or possibilistic models (Gao, 1996).

Also are emerging new methods, applied to structural reliability, such as Support Vector Machines (SVM) (Li et al, 2006) 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 (Dubourg et al, 2011, as part of a paper related to Reliability Based Design Optimization (RBDO) method).

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 analyse.

ESReDA project groups have been focused on industrial applications of structural reliability. Many ESReDA books have been published. They include (ESReDA 1998), (ESReDA, 2004) on the lifetime management of facilities, (ESReDA, 2010) 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 (ESReDA, to be published).

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 (Andrieu-Renaud et al, 2004) 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 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 (ESReDA, 2001; ESReDA, 2010):

- 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 (Bourgade et al, 1998), 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 (ESReDA, 2014),

- durability and sustainable development have become major issues because of the scarcity of financial resources and environmental protection will.

The RCM methodology appeared in Europe in the late 1980s and has been deployed in industrial systems in the early 1990's. 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 (2012)).

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 (Dehombreux et al, 2004). 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 (Singpurwalla, 1997; Nikulin, Bagdonavicius, 2002). The probability of detection of a defect, 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.

Maintenance decision ultimately depends on:

- the health status of the equipment,
- its predicted physical behavior,
- economic criteria (often the NPV (Net Present Value) is optimized using industrial asset management models).

Reliability proves to be the overriding factor in the decision, leading engineers to examine the effectiveness of maintenance on reliability, until the early 2010s (Procaccia et al, 2011).

The AP-913 approach (INPO, 2001), 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 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) 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, 1993). Attention to ageing appears in the years 1995-2000, almost the same time that 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 and economic optimization decides the lifetime.

The table 1 presents the main trends in ageing studies (IAEA, 2002; Lannoy, Procaccia, 2005).

Numerous studies have thus been developed (ESReDA, 2006):

- detection of ageing by Bayesian techniques (Clarotti et al, 2004); 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) (Klefsjö, 1982);

- 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 (§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 (Bouzaïene-Marle, 2005; ESReDA, 2006); 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, §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 (Sliter, 2003; Lonchampt, Fessart, 2012).

Ageing databases (like the GALL report (US NRC, 2010)) 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.

Table 1 – Main trends of ageing studies.

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**

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 probability 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 (Benavoli et al, 2009) 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 (Bicking, Simon, Aubry, 2008) concerns the modeling of safety instrumented systems design, based on reliability networks, to meet a SIL (Safety Integrity Level, IEC 61508), where optimization is performed by genetic algorithms. Article (Aguirre et al, 2013) 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 (Jensen, 1996) 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 (Weber et al, 2012). 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 (Corset et al, 2006)),
- a probabilistic 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. Its use is also widely used (see §5.5). It can be an alternative to the decision tree (§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) 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 (ESReDA, 1999). 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 (Lannoy, Procaccia, 1994). 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 (Moss, 2005). 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 (Procaccia et al, 1998), 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 safety-related data. 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 these important data for safety are not sufficient for maintenance.

A new collection strategy and a new structure were therefore defined to address maintenance issues (Lannoy, Procaccia, 1994; Sandtorv et al, 2003; ISO 14224, 2006). 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 (§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 a more fine risk analysis. It is a proactive tool, minimizing the risk that an undesirable event occurs or better measuring the consequences.

Knowledge management (KM) and a consideration of the context will improve the detection of weak signals (§ 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, 1998) book.

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.

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 (Procaccia et al, 2011). 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 (Bacha et al, 1998). 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 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 (Clarotti, 1998; Singpurwalla, 2006):

. 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 (1958) which has the property of maximizing the likelihood, the median ranks method of Johnson (1964). 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 analyzes mainly concerned technical but also human aspects. In the late 1990s and beyond, industry were 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 ESReDA (2009). The ambition of these guidelines report is to reflect the state of the art in accident investigation as well to address its future challenges. These 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 are limited. We do not feel that the lessons of the past are effectively acquired by industry.

The challenges are many:

- research the root causes of accidents, which leads to consider the organizational factors and the identification of the factors of robustness and resilience of organizations; AcciMap (Rasmussen, 1997) 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 (Cambon, Guarnieri, 2008); 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 (Kervern, Rubise, 1991; Condamin et al, 2006; Baillif, Planchette, 2013);

- 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 (Welker, Lipow, 1974; Hill, 1975; Deheuvels, 2013): 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 (Morio, Balesdent, 2015) 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 (Cooke, 1991). 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 unapplicable, 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 (Bolado-Lavin, Devictor, 2005):

. 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 (Cojazzi et al, 1998). 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 (Lannoy, Procaccia, 2001).

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 (US NRC, 1975), 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 (Swain, Guttman, 1983) 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 (Sobral et al, 2015) 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; Hollnagel, 1998); a Fuzzy CREAM version has been developed by (Marseguerra et al, 2007),
- the MERMOS methodology (Bieder et al, 1998; Le Bot, 2010) 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 (Gertman et al, 2005), 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. Human factor data is nevertheless essential.

Presumably probabilistic networks, which can take into account interactions and uncertainties can provide valuable assistance to the analyst (Aguirre et al, 2015). 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 (Embrey, 1992) 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 (Clarotti et al, 1994) for the analysis of a maintenance task and determination of its efficiency.

Probabilistic networks are currently used in the humanities, sociology and criminology (Schindler, Wiedmann-Schmidt, 2015). 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 (Forester et al, 2009), 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; Hourtolou, Salvi, 2014) 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 PSA 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?” . 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 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 costly. 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 between 10^{-4}/ year (public) and 10^{-6}/ year (all). 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.

Any risk analysis requires a probabilistic quantification, which is always possible in the uncertainty domain of medianistan, in the domain of the median or of the mean (Taleb, 2010). 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, 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. 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 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 (Beaudouin et al, 1999),
- 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 (Beaudoin, Munier, 2009).

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.

Main popular decision analysis methods are listed in the table 2 hereunder (see also (ESReDA, 2004)). 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.

Table 2 – Main decision analysis methods used in risk management, safety and dependability
(Lannoy, Procaccia, 2014; Merad, 2010).

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

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.

The contribution of ESReDA project groups was important in many themes related to safety, reliability and feedback. The presentation of the works of project groups in seminars or organization of seminars of "exploration" for making a state of the art or identify future works have always been beneficial to ESReDA members as other participants because full lessons. Technical exchanges, benchmarking, objectives and common work save time (and money) to industrial or academic teams.

Understanding the past prepares the future. Risk management and dependability appear with a promising future. Table 3 summarizes the study subjects, considered priority by the author, which could be conducted in the near future. Presumably, some topics could be addressed within the framework of ESReDA project groups.

Table 3 – Priority topics to be developed in the near future.

Topics		List of subjects for the near future
Modeling and propagating uncertainty	Dependability methods, system analysis at the design phase	Dependability of innovative products Modeling complexity Dynamic reliability Organizational and human factors in the design Impact on health and environment
	Structural safety	Industrial applications Processing of data Reliability and robustness Time variant reliability Practical guide
	Maintenance modeling	Maintenance optimized Efficiency of maintenance Failure diagnosis and prognosis, HUMS
	Ageing management	Analysis of degradations Predictive maintenance Diagnosis, prognosis Asset management models Ageing management data basis
	Influence diagrams and belief networks	Belief networks: benefits and difficulties Industrial applications Application to human and organizational factors
Collecting, validating and analyzing uncertain data	Operation feedback: failures and degradations	Big data Automatic treatment of language Text mining HUMS systems Knowledge management
	Frequentist methods and bayesian inference	Fusion of heterogeneous data Practical guide
	Operation feedback: accident analysis	Weak signals Probability of rare events Consequences models International data basis on major events
	Expert opinion	Elicitation, bias, uncertainties, trust in expertise Fuzzy logic Use of expertise: knowledge management
	Human factor data	Methods for quantifying human and organizational factors Text mining International data basis on events and simulator experience to support quantification

Deciding in an uncertain context	Risk analysis, safety, accepting risk	Methods, techniques and tools for risk analysis Safety indicators Efficiency of barriers Acceptance criteria
	Help for decision making	Development and use of MAUT methods Risk informed asset management Practical guide

Acknowledgements

I would first like to recall the memory of my friend and colleague Henri Procaccia, one of the members of ESReDA who promoted ESReDA seminars that have always been very successful.
I would also recall the numerous works of Bob Moss also disappeared.
Thank strongly to the University of Sevilla, to our Spanish colleagues and Antonio Sola.

References

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.

Andrews J. and Moss T.R. (2002), *Reliability and Risk Assessment*, PEPL, Bury.

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.

Aven Terje (2010), *Misconceptions of Risk*, Wiley, 2010.

Bacha M., Celeux G., Idée 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.

Baillif L., Planchette G. (2013), *Sensibilisation aux concepts cindyniques*, AFNOR, MAR-A-I-30-60, avril 2013.

Barlow R.E., Proshan F. (1965), *Mathematical Theory of Reliability*, John Wiley&Sons, Inc. New York.

Barlow R., Clarotti C., Spizzichino F. (editors) (1993), *Reliability and decision making*, Chapman & Hall.

Bayesia software, www.bayesia.com

Beaudouin F., Munier B., Serquin Y. (1999), *Multi-attribute decision making and generalized expected utility in nuclear power plant maintenance*, Interactions and Preferences in Decision Making, Kluwer Academic Publishers, New York, pp 341-357.

Beaudouin F., Munier B. (2009), *A revision of industrial risk management*, Risk and Decision Analysis, vol 1, pp 3-20

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

Benavoli A B. Ristic, A. Farina, M. Oxeham, L. Chisci, *An application of evidential networks to threat assessment,* Aerospace and Electronic Systems, IEEE Transactions, Vol 45, n°2, pp 620-639.

Bicking F., Simon C., Aubry J-F (2008), *Aide à la conception de systèmes instrumentés de sécurité,* Congrès λμ16, 6-10 octobre 2008, Avignon.

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.

Bolado-Lavin R., Devictor N. (2005), CEA-JRC Workshop « *the use of expert judgement in decision making* », Aix-en-Provence, 21-23 june 2005.

Bouissou M., Bourgade E. (1997), *Unavailability evaluation, and allocation at the design stage for electric power plants: methods and tools*, RAMS' 97, Philadelphie, janvier 1997.

Bouissou, M. (2008) *Gestion de la complexité dans les études quantitatives de sûreté de fonctionnement de systèmes*, Lavoisier, Editions Tec&Doc.

Bourgade E., Degrave C., Lannoy A. (1998), *Performance improvements for electrical power plants: designing in the context of availability*, ESREL'1998, Probabilistic Safety Assessment, Cacciabue C., Papazoglou I.A. Editors, Springer and Verlag, Heidelberg, pp 158-162.

Bouzaïene-Marle Leïla, (2005), *AVISE, anticipation des défaillances potentielles dues au vieillissement par analyse du retour d'expérience*, Thesis of Ecole Centrale Paris.

Cambon J., Guarnieri F. (2008), *Maîtriser les défaillances des organisations en santé et sécurité au travail : la méthode TRIPOD*, Editions Lavoisier, Colllection Scieces du Risque et du Danger.

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

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

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.

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*, Colloque λμ 9, ESREL'94, La Baule.

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.

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.

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.

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

Condamin Laurent, Louisot Jean-Paul, Naïm Patrick (2006), *Risk Quantification (Management, Diagnosis and Hedging)*, John Wiley & Sons Limited.

Cooke R.MR (1991), *Experts in Uncertainty, Expert Opinion and Subjective Probability in Science*, Oxford University Press; New-York, 1991.

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.

Costa, O.L.V., Dufour F. (2010), *Average Continuous Control of Piecewise Deterministic Markov Processes*, SIAM Journal on Control and Optimization, 48 (7).

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.

Deheuvels Paul (2013), *Evénements rares et risques extrêmes*, Conférence invitée au congrès Qualita 2013, UTC Compiègne, http://www.utc.fr/fim/fc/video/watch/id/1298/

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.

De Rocquigny, E., Devictor, N., Tarantola, S. et al (2008), *Uncertainty in Industrial Practice – A guide to quantitative uncertainty management*, Wiley.

Ditlevsen O., Madsen H. (1996), *Structural Reliability Methods*, John Wiley & Sons, New York.

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.

Dufour F., Dutuit Y. (2002), *Dynamic reliability – A new model*, Proceedings of ESREL'2002 – λμ 13 Conference, Lyon, pp 350-353.

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

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, Electric Power Research Institute (1993), *Common Aging Methodology*, february 1993.

ESReDA (1998), *Industrial Application of Structural Reliability*. Edited by Thoft-Christensen, P., ESReDA Safety Series No. 2, Det Norske Veritas, Høvik.

ESReDA (1999), *Handbook on Quality of Reliability Data*, edited by Lars Pettersson, Det Norske Veritas.

ESReDA (2001), *Handbook on Maintenance Management*, edited by Lars Pettersson, Det Norske Veritas.

ESReDA (2004), *Decision Analysis for Reliability Assessment*, edited by Tim Bedford, Palle Christensen and Henri Procaccia, Det Norske Veritas.

ESReDA (2004), *Lifetime management of structures*, edited by André Lannoy, Det Norske Veritas, Høvik.

ESReDA (2006), *Ageing of Components and Systems*, edited by Lars Pettersson and Kaisa Simola, Det Norske Veritas, Høvik.

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

ESReDA (2010), *Maintenance Modelling and Applications*, edited by John Andrews, Christophe Bérenguer and Lisa Jackson, Det Norske Veritas.
ESReDA (2010), *SRA into SRA: Structural Reliability Analyses into System Risk Assessment*, editor: Emmanuel Ardillon, Det Norske Veritas.
ESReDA (2014), *Reliability and Maintainability Impact to Asset Management Stakeholders*, editor: Mohammad Raza , Det Norske Veritas.
ESReDA (to be published), *Reliability-based Life Cycle Cost Optimization of Structures and Infrastructures*, editor: Alaa Chateauneuf.
FIDES (2009), UTE-C 80-811 (Janvier 2011) *Guide FIDES 2009* - Edition A – Septembre 2010 : *Méthodologie de fiabilité pour les systèmes électroniques*.
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 Yingzhong (1996), *Modèles probabilistes et possibilistes pour la prise en compte de l'incertain dans la sécurité des structures*, Thèse ENPC, 02 Mai 1996.
Gertman D., Blackman H., Marble J., Byers J., Smith C. (2005), *The SPAR-Human Reliability Analysis Method*, NUREG/CR-6883, US NRC.
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.
Hill B. M. (1975), *A Simple General Approach to Inference about the Tail of a Distribution*, The Annals of Statistics, 3, pp 1163-1174.
Hollnagel G. (1998), *Cognitive Reliability and Error Analysis Method*, Elsevier, Amsterdam.
Hourtolou D., Salvi OO. (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 (1988). Health and Safety Executive: *The Tolerability of Risk from Nuclear Power Stations*. Discussion Document, HMSO, London. Revised edition, 1992.
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 (2008), *Collection and classification of human reliability data for use in probabilistic safety assessments*, Vienna.
IEC 61508: 2010 (2010), *Functional safety of electrical/ electronic / programmable electronic safety- related systems*.
INPO (2001), *Equipment Reliability Process Description*, November 2001.
ISO 14224: 2006 (2006), *Petroleum, petrochemical and natural gas industries – Collection and exchange of reliability and maintenance data for equipment*.
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.
Jensen F.V. (1996), *An introduction to Bayesian Networks*, UCL Press(Ed), London.
Johnson L. (reprint 1974), *The statistical treatment of fatigue experiments*, Elsevier.
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.
Kaplan, E.L. and Meier, P., (1958), *Non parametric estimation from incomplete observations*, Journal of the American Statistical Association, 53, 457-481.

Kervern G.-Y., Rubrise P. (1991), *L'archipel du danger – Introduction aux cindyniques*, Economica, Paris ; (1994) *Latest advances in cindynics*, Economica.

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

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.

Lannoy A., Procaccia H. (2001), *L'utilisation du jugement d'expert en sûreté de fonctionnement*, Lavoisier, Editions Tec&Doc.

Lannoy A., Procaccia H. (2005), *Evaluation et maîtrise du vieillissement industriel*, Lavoisier, Editions Tec&Doc.

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.

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, to be published.

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

Lemaire Maurice (2005). *Fiabilité des structures, couplage mécano – fiabiliste statique*, in collaboration with Alaa Chateauneuf and Jean-Claude Mitteau, Hermès Lavoisier.

Lemaire, M. (2014) *Mechanics and Uncertainty*, iSTE/ Wiley, Mechanical Engineering and Solid Mechanics Series.

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.

Ligeron J-C, Marcovici (1974), *Utilisation des techniques de fiabilité en mécanique*, Technique&Documentation, Paris.

Lonchampt J., Fessart K. (2012), *Investments Portfolio Optimal Planning for Industrial Assets Management – Method and Tool*, IAEA-CN-194-007.

Madsen H.O., Krenk S., Lind N.C. (1986), *Methods of Structural Safety*, Prentise-Hall.

Marseguerra M., Zio E., Librizzi M. (2007), *Human Reliability Analysis by Fuzzy CREAM*, Risk Analysis, vol 27, pp137-154.

Meeker W., Escobar L.(1998), *Statistical methods for reliability data*, Wiley.

Merad Myriam (2010), *Aide à la décision et expertise en gestion des risques*, Lavoisier, Editions Tec&Doc

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

Morio Jérôme, Balesdent Mathieu (2015), *Estimation of Rare Event Probabilities in Compex Aerospace and Other Systems – A Practical Approach*, Woodhead Publishing, Elsevier.

Moss T.R. (2005),*The Reliability Data Handbook*, Professional Engineering Publishing.

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

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

PROBAN software, Sesam probability module, DNV-GL https://www.dnvgl.com/services/sesam-probability-module-proban-2387

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.

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

Procaccia H., Ferton E., Procaccia M., (2011), *Vieillissement et maintenance des matériels et systèmes industriels réparables*, Lavoisier, Editions Tec&Doc.

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

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*.

Reason J. (1997), *Managing the risks of organizational accidents*, Ashgate Publishing Ltd.

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

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

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.

Schindler J., Wiedmann-Schmidt W. (2015), *Im roten Bereich*, Der Spiegel 10/ 2015, http://www.spiegel.de/spiegel/print/d-132040367.html

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.

Simola Kaisa (1999), *Reliability methods in nuclear power plant ageing management*, VTT Publications 379, Espoo.

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.

Singpurwalla N. (2006), *Reliability and Risk – A Bayesian Perspective*, John Wiley & Sons, Ltd, Chichester.

Sliter George,(2003*), Life cycle management in the US nuclear power industry*, SMIRT 17, Prague, 17-22 august.

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.

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.

Taleb N. N. (2010), *The Black Swan - The Impact of Highly Improbable*, The Random House Publishing Group, Second edition.

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).

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

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

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

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

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

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.

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.

Notion and Discussion of a Dynamic Criticality Concept

Joel Adams (*), Vicente González-Prida (**), Ajith Kumar Parlikad (*),
Jayakumar Shambhu (***), Antonio Guillen (**), Adolfo Crespo (**)

(*) University of Cambridge, UK
(**) University of Seville, Spain
(***) University of Stavanger, Norway

Abstract

Most organizations operate in distributed and dynamic environment, which means an asset's criticality will depend on both static and dynamic factors; some which are volatile in nature. From the review of industrial practices, it was clear that an inherent problem with criticality analysis is that it tends to be considered as more or less a static quantity that is not updated with sufficient frequency as the operating environment changes. It is evident, from actual situations, that different demanded conditions can change the assets prioritization in term of their criticality. Therefore, the purpose of this paper is to discuss a step towards dynamic view of the Criticality Analysis (CA) method, considering the criteria (frequency and consequences) as temporary variables and finally obtaining not only one criticality matrix for a specific moment but a more comprehensive picture of those risks resulting more important for the industrial system, according to strategy and over time.
This paper begins with a literature review of previous work and the general characteristics of the CA method. The paper identifies an inherent problem of current criticality assessment methods and discussed the need to adopt a dynamic model for the analysis of asset criticality. Several questions and concerns are raised in the discussion for the need of dynamic re-evaluation of criticality. The reflections showed that while a dynamic assessment is technically possible, the practical usefulness of the implementation of the dynamic criticality methodology for the organization should be justified.

Keywords: Asset Management, Criticality Analysis, Demanded Conditions, Dynamic Criticality, Risk Management

1. Introduction: Criticality analysis and it uses

The need to utilize resources within the organizations efficiently has never been greater as economies around the world struggle with funding and the upkeep for infrastructure and equipment take a back seat. In order to ensure that whatever is spent on maintenance is spent where it does the most good, there is need for a proper understanding of asset criticality – how failure of the asset impact business goals [1]. The relationship between

equipment failure and business performance is an important factor in deciding where and when resources should be applied to maintain or improve equipment reliability. A criticality analysis is a process for determining the relative ranking of items in a system. The purpose of ranking these items is to determine priorities given to the items in a maintenance management program. In industrial environment, these items are generally assets and the resources are labor, materials, tools and schedule priority.

A generic maintenance objective for most organizations will be: "to achieve the agreed plant operating pattern and product quality, within the accepted plant conditions and safety standards, and at minimum resource cost" [2]. Criticality analysis has been applied to different areas of maintenance in an attempt to achieve this objective. According to [3], Some of the potential uses for asset criticality rating are:

- As an input to determine the overall priority for performing a maintenance task (sometimes combined with a "Work Order Priority" entered against the specific task to give an overall priority for the task)
- To determine, at a high level, the type of risk mitigation strategy to be applied to the equipment (e.g. do condition monitoring and defect elimination on high criticality items). An illustration of such concept is shown in Table 1.
- As an input into determining the optimum spare parts holdings required for the equipment item
- To provide input into the capital program so that "high criticality" equipment is given a higher priority for upgrade or replacement
- To guide reliability engineers so that they focus their reliability improvement efforts on the most "critical" equipment.

Equipment Criticality	Mitigation Strategy
Very High	Contingency Plans, Hold Critical Spare Parts, Predictive Maintenance, Preventive Maintenance
High	Hold Critical Spare Parts, Predictive Maintenance, Preventive Maintenance
Moderate	Predictive Maintenance, Preventive Maintenance
Low	Preventive Maintenance
Very Low	Run to Failure – Corrective Maintenance Only

Table 1: **Maintenance Strategy Selection Based on Criticality** [3]

Although criticality analysis promises many potential benefits for asset intensive companies, however, proper use of criticality in developing maintenance strategies and plans is still at a nascent stage in most organizations. Several methods have been developed for doing criticality analysis, most of which are based on static procedures as described in the next section. Hence, the aim of this study is to address the issue of dynamicity in asset criticality due to changing operating conditions and environment and to develop a dynamic model for criticality assessment.

2. Criticality analysis techniques: A review of previous research work

MIL-STD-1629A [5] describes the standard techniques and approaches for criticality analysis during the design phase of an asset. It laid down the procedures for performing Failure Mode, Effects and Criticality Analysis (FMECA) and several other authors have built on this technique as will be described in the following sections. These techniques use, for instance, the Risk Priority Number (RPN) method , fuzzy logic, or approximate reasoning to prioritize failure modes, and not assets [4]. When prioritizing assets for maintenance purposes and during their operational phase [4], a large number of quantitative and qualitative techniques can be found in the [5].

The procedure for FMECA, as described in the MIL-STD-1629A, uses a standard criticality assessment methodology based on calculation of a Criticality Number (CN) for each system failure mode given by [6]:

$$CN_i = \alpha_i . \beta_i . \lambda_p . t \quad (1)$$

Where α is the failure mode ratio, $\beta$the probability of failure effect, λ the failure rate and t the time of operation. It is important to note that since equation 1 does not contain consequence, it should not be applied to a production system in which both probability and occurrence are important.

A second approach which is used to prioritize failure causes is the Risk Priority Number (RPN). The RPN is calculated using linguistic terms to rank the three factors – Severity (S), Occurrence(O) and Detection (D) of failure, such that

$$RPN = S \times O \times D \quad (2)$$

According to Braglia et al [6] while the criticality number technique is common with the aerospace, nuclear and chemical industry, the simplicity of the RPN approach has given it preference in the manufacturing industries. The risk level of each failure is a direct measure of it RPN or CN, thus failure with higher RPN or CN are considered more important and given higher priorities. Unfortunately these FMECA approaches, especially RPN, have several drawbacks when applied in the industry. Some of the limitations of the RPN approach and it criticisms, as reported in [7]–[11], are:

- By using only three kinds of attributes or factors(S, O and D), FMECA is not able to capture other aspects of business effectiveness and risk such as safety, environmental integrity, customer satisfaction, product quality, operational reliability and cost
- Different sets of the three factors can yield the same RPN while their risk implications may be totally different
- The relative weight or importance of S, O and D are not taken into account
- There's no rational justification for the mathematical formulation of RPN, i.e. why S, O and D are multiplied to get RPN
  there's inconsistency in the conversion of the factors. The conversion score for occurrence of failure is linear, but nonlinear for detectability
- Small variation in any of the attributes lead to large change in the RPN

- It is difficult to precisely determine S, O and D. more information can be captured using linguistic terms.

Several new approaches have been proposed in the literature to remedy some of the drawbacks mentioned above. For example, Gilchrist [7] proposed a model which uses expected cost and the basis for ranking failure modes rather than the conventional RPN as shown:

$$EC = C.n\,.p_f.p_d \tag{3}$$

Where EC is the expected cost of failure to the customer, C is the failure cost, n the number of items produced yearly, p_f the failure probability and p_d the probability a failure will go undetected. This model claim to be more applicable practically since the economic aspect of business is considered. But in our view, economics aspects can be accounted for in the "Severity" term of equation 2.

Ben-Daya & Raouf [12] proposed an improvement of the RPN model to address the issue of the relative importance given to each of the criteria, based on the criticisms of Gilchrist model. They suggest more importance be given to the probability of failure than the probability of detection by raising the probability of failure ranking to the power of 2. They also questioned the absence of the severity of failure in the expected cost model. But again just as we pointed out above, the "Cost" term can be seen as failure severity. The authors therefore combined the improved RPN and the expected cost models to prioritize failure modes as well as estimating failure cost to the customer.

Bowles & Peláez [13],[14] described the use of fuzzy logic theory for prioritizing failure in FMECA. This technique uses linguistic terms such as minor, low, moderate, high, and very high for severity for instance. The fuzzy inference system is formulated in terms of "if-then" rules based on expert knowledge. The numerical crisp ratings are fuzzified into the rule base and conclusions are derived whenever there is a match. The conclusions are defuzzified using Weighted Mean of Maximum Method (WMoM). Their technique resolved some of the issues of traditional RPN method, such that: (i) the criticality review team can use linguistic terms to directly evaluate the failure criteria. (ii) Severity, occurrence and detectability of failure are combined in a flexible and more consistent manner. (iii) Qualitative information that is vague and imprecise, together with quantitative data can be used for the risk assessment.

Several other fuzzy inference techniques have been studied in [6], [11], [15] etc. One major issue in the application of this technique is the assignment of weights to the different criteria, a task which is dependent of subjective judgment from the experts involved. Braglia & Bevilacqua [16] proposed the use of Analytic Hierarchy Process (AHP) which uses a logic decision diagram to solve these multi criteria problems. Braglia et al. [6] also introduced a fuzzy version of the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) called fuzzy TOPSIS.

Braglia [10] used the AHP approach to develop a Multi Attribute Failure Mode Analysis (MAFMA) tool. The three hierarchies are the decision attributes which is composed of the four different factors S, O, D and the expected cost, the decision alternatives which are the possible causes of failures and the decision goal which is concerned with selection of failure cause. A pairwise judgment is used to evaluate the factors and

attributes are normalized to give relative weights which are used to rank the possible causes of failures. The sensitivity of the weights was also analyzed.

Sankar & Prabhu [17] introduced the Risk Priority Rank (RPR) technique which uses a scale of 1-1000 possible severity-occurrence-detection combinations. This technique also relies on expert knowledge using the "if-then" rule decision support. Failure with higher rank is given higher priority and the results are represented using a final order matrix.

Chang et al. [18],[19] used the grey system theory and fuzzy logic to address the problem of: (i) linear and nonlinear conversion issues of occurrence and detectability of failure (ii) assigning relative weights to the factors and (iii) complexity of using utility functions. Standard series were defined using the lowest of each of the three factors – S, O and D and for each failure cause the factors information were compared with their standard series to derive a grey relational degree. The higher the grey relational degree, the smaller the effect of the potential failure causes.

Seyed-Hosseini et al [9] developed the decision making trial and evaluation laboratory (DEMATEL) for prioritizing failure modes in systems with many subsystems and components. This method analyses the relationship (direct/indirect) between components and the severity of influence on each other. Alternatives having more effect to another are assumed to have higher priority and called dispatcher and those receiving more influence from another are assumed to have lower priority and called receiver.

Puente et al. [8] presented a methodology which assigns a risk priority class (RPC) to each failure mode. The decision system defines five classes of linguistic rules and the numeric rankings of the three factors (S, O and D) are mapped into their corresponding class. The model is able to obtain the RPC for each failure using a classification from a set of 125 $(5 \times 5 \times 5)$ rules together with the three factors.

Bevilacqua, Braglia, & Gabbrielli [20] modified the RPN using a weighted sum of six parameters (which are maintenance cost, downtime length, failure frequency, machine importance, safety and operating condition), multiplied by a seventh factor i.e. machine access difficulty. The methodology integrates the modified RPN with a Monte Carlo simulation as a way of testing the weights assigned for RPN ranking. The uniqueness of this model is that it gives a stochastic final priority ranking by simulation of the weights. The model was applied at facility level of a power plant to determine which maintenance policy would be most suitable or promising for each facility of the plant.

3. Dynamic criticality

A review of literature and industrial practices showed that criticality is considered as more or less a static quantity that is not updated with sufficient frequency as the operating environment changes. Variations in some factors used for calculating criticality influences change in asset criticality with time and therefore criticality should be modeled as a dynamic process, which is a function of time as shown in Figure 1. But criticality of an asset has been applied in a sense as though it is static and does not change with time. The long-time held myth is: "…we have just concluded our criticality analysis, we can now check that box …" Thus an inherent problem of criticality assessments is that they are static procedures that do not update as the operating

environments and conditions change [21], [22]. In other words, you can just "set it and forget it" and the maintenance strategy remains fixed once commissioned. However, most organizations operate in distributed and dynamic environment, which means an asset's criticality will depend on both systemic factors (such as redundancy) and dynamic factors; which could influence change in an asset's criticality.

As a consequence of this dynamics, there is need for a decision-support system which uses available information in order to propose new maintenance program according to the current enterprise context [23]. It is therefore important to sufficiently review and update the criticality of assets as necessary to ensure maintenance objectives for the assets are aligned to business needs. Unfortunately, current criticality analysis techniques are only static procedures used primarily to identify initial maintenance strategies. Therefore current techniques cannot deal with the issues of real-time asset criticality.

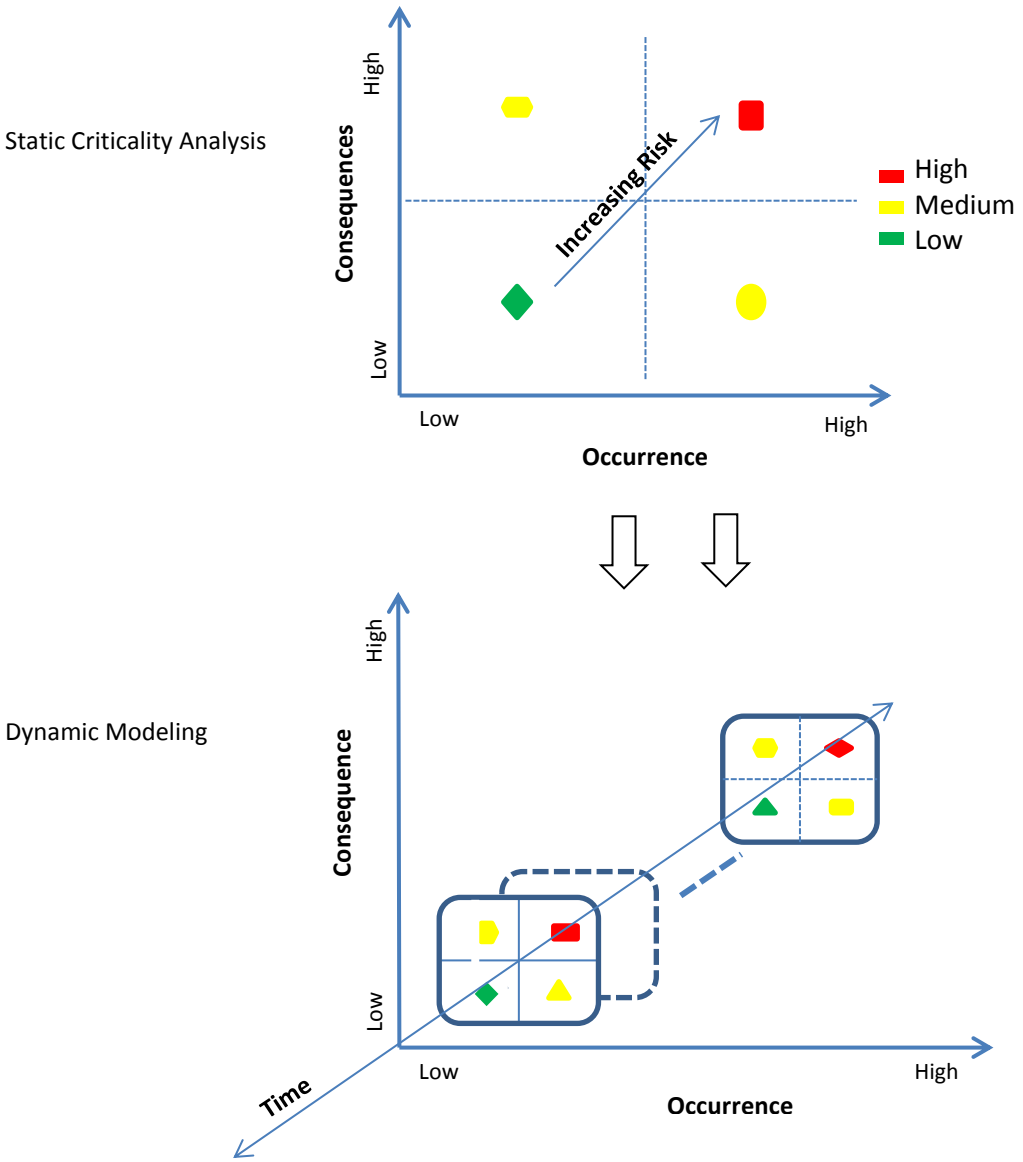


Figure 1: **A step change to dynamic modeling of criticality**

Also note that the risk matrix can change for two different scenarios: when consequence remain the same but occurrence is changing, and when consequence is changing but occurrence stays the same

Objective of the study

The aim of this research area is to propose a dynamic criticality model. Nevertheless, this seeks firstly to address the dynamic nature of assets' criticality by understanding why to model and calculate changes in criticality. One possible approach is the system dynamics technique, an approach to understanding the nonlinear behavior of complex systems over time using stocks, flows, internal feedback loops, and time delays.

4. Notions questions for enabling a dynamic criticality assessment

On order to deal with asset criticality from a dynamic point of view, it is important to consider two aspects:

- How and when can the criticality assigned to an asset be understood to have changed
- How this criticality affects the system and its management (maintenance management and other related areas)

The first aspect concerns the identification of those events or circumstances that result in change of the criticality of one or more assets of the system. In relation to this, there are two issues to solve: the possible methods that can be used to detect and record these events and, on the other hand, the subsequent process or methodology for the re-evaluation of criticality which would lead the event.

In reference to the second aspect mentioned above, an important question may arise – What is the impact of change in an asset's criticality? This is certainly not a minor issue; on the contrary, it is perhaps the most important consideration when planning a dynamic criticality control.

Basically, it is needed to have a clear vision of why it is interesting to re-evaluate the criticality and how often our management requires an updated state (let's say, a "picture") of the assets criticality.

An illustrative example might be to establish an elaborate monitoring system in order to obtain results regarding the availability of criticality values for all the plant assets in "real time." Nevertheless, if the only decision to consider is just to improve the maintenance planning and, on the other hand, the organization allows just one or two changes per year (due to its limitations and organizational resources) in the planning, then one might ask if it is useful at all to know how criticality is changing at every moment. This solution would be far from being useful, but rather it may introduce an over-abundance of information which in itself is a problem for the analysis and management.

It is not intended to disdain the criticality calculation in real time. In fact, it may have a specific practical use. However, it is relevant to affirm the requirement to establish

firstly the specific need for this calculation before forcing the organization to implement it.

The "real time" concept refers implicitly to the ability of monitoring an asset state. Nevertheless, it is important to distinguish the value of criticality measure using other tools from Maintenance Engineering area as the CBM (Condition Based Maintenance). Criticality provides a strategic vision while CBM is a concrete technical solution applied to specific assets. Both tools are therefore at different levels in the structure of maintenance management. In order to understand this difference it is useful to make the following observation: due to the high cost for certain monitoring techniques (like IRIS ultra-sonic technology) and the complexity of the CBM implementation, it will only be justified in those assets of particular relevance. In other words, it is justified for assets with a certain level of criticality. Therefore, the criticality value is used to decide what assets to implement this type of maintenance policies for.

Nevertheless, it is possible to consider the use of a monitoring solution such as the CBM to measure or evaluate an asset reliability in real-time and, thereby, to obtain a real-time measure of criticality. This again raises several issues:

- Would a particular change in criticality lead to a change in the maintenance policy applied in "real time"? It is important to take into account that it is a monitored asset, so, it is supposed it operates with an optimized maintenance policy.
- When an asset is monitored, is it necessary to analyze the monitoring equipment as another asset too, giving a specific criticality level?
- If not all assets will be monitored (as justified before), how would the criticality calculation be interpreted when it is different for assets monitored and unmonitored?

These reflections are intended to illustrate that, while real-time evaluation of criticality is technically possible, the practical usefulness of the implementation of the dynamic criticality methodology for the organization should be justified. Basically, it will depend on the application and will require a suitable solution for each case.

Finally, it is interesting to enumerate those events that may lead to a modification of the criticality in one or more assets of a system. For instance:

- Equipment malfunctions. When a new failure event occurs, its treatment could affect the re-evaluation of criticality, being not homogeneous for every asset or for every stage in the operational life cycle stages of such an asset.
- Changes in operating configuration. Both, by external demand (higher or different production demands, new legal or regulatory constraints, etc.) or internal (changes in business strategy)
- System redesign. Improvements, asset renewal, new auxiliary systems, strengtheners, redundancies, etc.
- Others.

5. Conclusion and recommendation for future work

- From discussions in the previous sections, the following conclusions and recommendation are made:
- From literature and practice, criticality has been understood and used in a static sense. One reason for this could be that "when and "how" failure consequence and probability have not been considered to be dynamic. Therefore current criticality analysis techniques cannot deal with the dynamic nature of asset criticality.
- Two most important questions to address are: "how and when can the criticality assigned to an asset be understood to have changed" and "how this criticality change affects the system and its maintenance management and other related areas".
- Changes in operating conditions and system redesign were identified as some of the events which could lead to a modification of assets/systems criticality.
- It is possible to consider the use of a monitoring solution such as the CBM to measure or evaluate an asset reliability in real-time and, thereby, to obtain a real-time measure of criticality. But this will lead to other issues such as whether to consider the monitoring device as a separated asset and analysis its criticality.
- The need for dynamic criticality analysis has been proposed as a method to monitor, review and update the asset criticality over time and use changes in criticality to review maintenance plan.
- Further work is required in the dynamic modeling approach and will be reported in future publications. For example, the use of system dynamics or dynamic AHP might be suitable techniques for this.
- Further work will also take a look into the field of prognostics (WHEN does the equipment fail) and define its relation with criticality

6. References

[1] J. Adams and A. K. Parlikad, "Dynamic Maintenance Based on Criticality in Electricity Networks," in 5th IET/IAM Asset Management Conference, 2015.

[2] A. Kelly, Maintenance strategy. Elsevier, 1997.

[3] Assetivity - Asset Management Consultants, "Equipment Criticality Analysis – is it a Waste of Time?," 2015. [Online]. Available: http://www.assetivity.com.au/article/reliability-improvement/equipment-criticality-analysis-a-streamlined-approach.html. [Accessed: 15-Oct-2015].

[4] A. Crespo Márquez, P. Moreu de León, A. Sola Rosique, and J. F. Gómez Fernández, "Criticality Analysis for Maintenance Purposes: A Study for Complex In-service Engineering Assets," Qual. Reliab. Eng. Int., p. n/a–n/a, 2015.

[5] A. C. Marquez, The Maintenance Management Framework: Models and Methods for Complex Systems Maintenance, 1st ed. Springer-verlag London, 2007.

[6] M. Braglia, M. Frosolini, and R. R. Montanari, "Fuzzy TOPSIS Approach for Failure Mode, Effects and Criticality Analysis," Qual. Reliab. Eng. Int., vol. 19, no. 5, pp. 425–443, Sep. 2003.

[7] W. Gilchrist, "Modelling Failure Modes and Effects Analysis," Int. J. Qual. Reliab. Manag., vol. 10, no. 5, 1993.

[8] J. Puente, R. Pino, P. Priore, D. de la Fuente, and D. D. La Fuente, "A decision support system for applying failure mode and effects analysis," Int. J. Qual. Reliab. Manag., vol. 19, no. 2, pp. 137–150, Mar. 2002.
[9] S. M. Seyed-Hosseini, N. Safaei, and M. J. Asgharpour, "Reprioritization of failures in a system failure mode and effects analysis by decision making trial and evaluation laboratory technique," Reliab. Eng. Syst. Saf., vol. 91, no. 8, pp. 872–881, Aug. 2006.
[10] M. Braglia, "MAFMA: multi-attribute failure mode analysis," Int. J. Qual. Reliab. Manag., vol. 17, no. 9, pp. 1017–1033, Dec. 2000.
[11] T. R. Moss and J. Woodhouse, "Criticality analysis revisited," Qual. Reliab. Eng. Int., vol. 15, no. 2, pp. 117–121, Mar. 1999.
[12] M. Ben-Daya, A. Raouf, M. Ben-Daya, and A. Raouf, "A revised failure mode and effects analysis model," Int. J. Qual. Reliab. Manag., vol. 13, no. 1, pp. 43–47, Feb. 1996.
[13] J. B. Bowles and C. E. Peláez, "Fuzzy logic prioritization of failures in a system failure mode, effects and criticality analysis," Reliab. Eng. Syst. Saf., vol. 50, no. 2, pp. 203–213, Jan. 1995.
[14] C. E. Pelaez and J. B. Bowles, "Using fuzzy logic for system criticality analysis," in Proceedings of Annual Reliability and Maintainability Symposium (RAMS), 1994, pp. 449–455.
[15] A. C. F. Guimarães and C. M. F. Lapa, "Fuzzy inference to risk assessment on nuclear engineering systems," Appl. Soft Comput., vol. 7, no. 1, pp. 17–28, Jan. 2007.
[16] M. Braglia and M. Bevilacqua, "Fuzzy modelling and analytical hierarchy processing as a means of quantifying risk levels associated with failure modes in production systems," Technol. Law Insur., vol. 5, no. 3–4, pp. 125–134, 2000.
[17] N. R. Sankar and B. S. Prabhu, "Modified approach for prioritization of failures in a system failure mode and effects analysis," Int. J. Qual. Reliab. Manag., vol. 18, no. 3, pp. 324–336, 2001.
[18] C. L. Chang, P. H. Liu, and C. C. Wei, "Failure mode and effects analysis using grey theory," Integr. Manuf. Syst., vol. 12, no. 3, pp. 211–216, 2001.
[19] C.-L. Chang, C.-C. Wei, Y.-H. Lee, C.-L. Chang, C.-C. Wei, and Y.-H. Lee, "Failure mode and effects analysis using fuzzy method and grey theory," Kybernetes, vol. 28, no. 9, pp. 1072–1080, 1999.
[20] M. Bevilacqua, M. Braglia, and R. Gabbrielli, "Monte Carlo simulation approach for a modified FMECA in a power plant," Qual. Reliab. Eng. Int., vol. 16, no. 4, pp. 313–324, Jul. 2000.
[21] R. Smith, "Equipment Criticality Analysis," Analysis, no. 6, pp. 1–20.
[22] W. J. Moore and A. G. Starr, "An intelligent maintenance system for continuous cost-based prioritisation of maintenance activities," Comput. Ind., vol. 57, no. 6, pp. 595–606, Aug. 2006.
[23] M. Cerrada, J. Cardillo, J. Aguilar, and R. Faneite, "Agents-based design for fault management systems in industrial processes," Comput. Ind., vol. 58, no. 4, pp. 313–328, May 2007.

Annex 1

مهندسین مشاور ایتسن مشاور صنایع و تکنولوژی
ITCEN Industrial & Technical Consulting Engineers

European Safety, Reliability & Data Association

Ports and Maritime Organization
General Office of Supply and Equipment Maintenance

Increase MTBF Indicator of Offshore Equipment by applying new technologies in order to increase Availability and Reliability

50th ESReDA Seminar on
25 years of ESReDA seminars: Safety and reliability enhancement throughout Europe: looking back, looking ahead
May 18th -19th 2016, University of Sevilla, Sevilla, Spain

Presenters :
Mr. Abbas Ahmad Zadeh - General Manager of Supply and Equipment Maintenance
Mr. Mohammad Ali Rahbari-Expert of General Office of Supply and Equipment Maintenance
Mr. Dezhangah - Manager of the Department of PAM (ITCEN Consulting Engineers Group)

INTRODUCTION :

The PMO Islamic Republic of Iran in order to increase MTBF indicator and increase its maritime equipment operational level, the use of new technologies in the maintenance and repair of equipment as one of the important goals considered and tries to achieve these goals.

WHAT IS THE UNDERWATER ROBOT (ROV)?

The use of these robots :

1. For the filming
2. diver alternative
3. Carrying out repair and replacement parts
3. Carrying out research plans under water.
4. Discovery of bodies.
5. …

Underwater robot components include:

- **Navigation system**
- **Propulsion system**
- **System for launch in water**
- **Sources of power supply and communication cable**

BUILT ROBOTS

PMO has successfully designed, built and tested three underwater robot :

Persian Gulf probe underwater robot

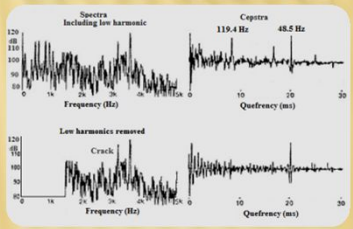
Persian Gulf Basir monitor underwater robot

Persian Gulf gauge underwater robot

PERSIAN GULF PROBE UNDERWATER ROBOT

Specifications and equipment of Persian Gulf probe

Length 126 cm + 90 cm retractable arm
Width 75 cm
Height 68 cm
The number of thrusters 4
Voltage and power consumption of propulsion systems 2X12V, 7SW 2X24V, 1SOW
Floating System – Thruster + Floating chamber + Compressed nitrogen capsule
Sensors: pressure, heat flow
Video system : camera with two degrees of freedom 650 TV line
USB DVR Capture Card + Controller
Lasso Cable length 50 m
Battery: 2 x 7.2A 12V
Control system: The control panel is equipped with a joystick and key commands
Light: halogen 2 x 50W, two power LED, 8W
Pneumatic anchor system: 2 x pneumatic jack with stroke 30 CM
Change and adjust system : sensors position: a with stroke 90 CM



PERSIAN GULF BASIR MONITOR UNDERWATER ROBOT

This probe for measuring health goals, monitoring, non-destructive testing, check the status of bed and leaching bed side walls of Ports, check the status of submarine installations such as optic fiber cables, pipelines and other facilities associated with telecommunication of oil and gas and power transmission as well as protection purposes and passive defense and protection of Coasts & Ports bed is used.

Specifications and equipment of Persian Gulf Basir monitor

Sensor specifications

Body Material	Stainless Steel
Beam angle of curvature	20-degree
suitable speed for imaging	1-8 knots
Data transmission interface	RS 285,1250Kbps
Transmitter operating frequency	400 KHz
Altimeter operating frequency	200 KHz
Altimeter Beam angle	20- degree
Usable depth	0 ~ 100 m

PERSIAN GULF GAUGE UNDERWATER ROBOT

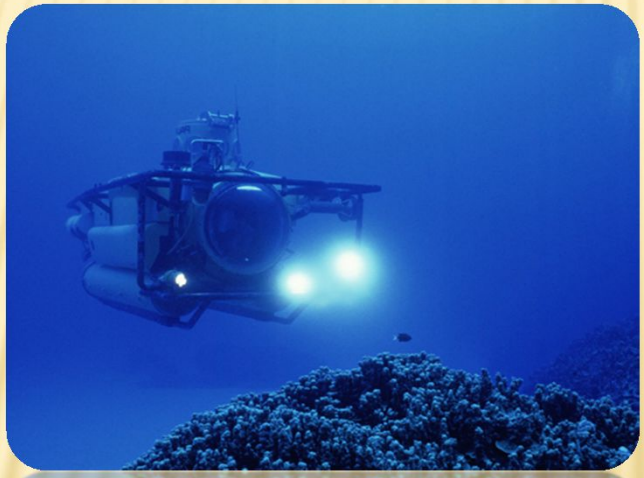
Persian Gulf gauge underwater robot for non-destructive testing (NDT) of ships body and vessels as well as offshore structures is used.

Specifications and equipment of Persian Gulf gauge

System length: 135 CM
Width: 65 CM
Height: 45 CM
The number of thrusters: 3
Dry weight: 33 Kg
Sensors : acoustic sensor+ EML sensor
Thrusters voltage and power : X12VX75W
Battery: 2 x 4.2A 12V

EVALUATE EFFECTS OF THE APPLICATION OF NEW SYSTEM (ROV) IN PROMOTING MARINE STRUCTURES MAINTENANCE MANAGEMENT

One of the most effective and the most important issues in the maintenance and repair of equipment and offshore structures in order to extend the life of structures and prolonging the time between overhaul (failure) or the corrosion issue is MBTF that this issue what in the body of vessel, or marine structures such as docks, oil rig and… imposes irreparable damage to equipment. One of the issues and causes corrosion in the Marine Structures is the discussion of the formation of moss on these structures.



THE WAY FORMATION OF MOSS:

DESTRUCTIVE ROLE OF MOSS AND MICROORGANISMS IN MARINE STRUCTURES

The number of losses inflicted on marine structures formed by moss is referenced below:

Marine Structures concrete demolition
Corrosion of metals
Microbial degradation of colors cover
Facilitate the start pitting
Changing the incline oxygen to create Differential aeration.
Chosen attack of bacteria

EVALUATE EFFECTS OF THE APPLICATION OF NEW SYSTEM (ROV) IN PROMOTING MARINE STRUCTURES MAINTENANCE MANAGEMENT

One of the main problems and disadvantages of forming moss in marine structures can be formed moss on body of vessels that in addition to the vessels body corrosion can cause:

- **Increase the rate fuel consumption**
- **Reduce efficiency and vessel speed rate**

CURRENT METHODS OF MAINTENANCE UNDERWATER OF VESSELS BODY

Vessels on the basis of existing rules and standards, to increase the safety level and the useful life of ships and maintenance of machinery and safety requirements on ships after each period of 2.5 years come out of the transport cycle and to overhaul and lower levels of the water level refer to yard with dry pond or vessels pond.

CURRENT METHODS OF MAINTENANCE UNDERWATER OF VESSELS BODY

Docking Vessel:

The current common approach in order to maintain and repair body of vessels underwater is Dock vessel.

Based on standards and conventions related to marine industry and regulations of rating agencies in terms of maintaining safety, vessels unit every two years and a half would have to visit, repairs and masonry moss, thickness gauging and check the status of anode effluent water transferred. Which immediately after lifting vessels, different stages of work will be done in the following order:

Cleaning underwater body with pressurized water to remove moss

Masonry moss with shovel and spatula

Sand blast of body by sand under pressure

Body wash immediately with fresh water

Paint the first layer

Body repair of underwater, such as: cutting the anode and install new anode, repair chains and...

THE USED MEANS IN THE CURRENT METHOD OF CLEANING THE BODY

Conventional methods in the vessels underwater repairs can include :

- **wire brush method**
- **Shell out with scrub hammer**
- **Rust with flame**
- **Sanders disc**
- **Sweep ballistic**
- **Dry ballistic**
- **Mixed ballistic with water and sand under extremely high pressure**
- **Sand blast**

THE DISADVANTAGES OF THE CURRENT METHODS FOR VESSELS UNDERWATER MAINTENANCE AND REPAIRS

Docking vessel disadvantages can be cited as follows:

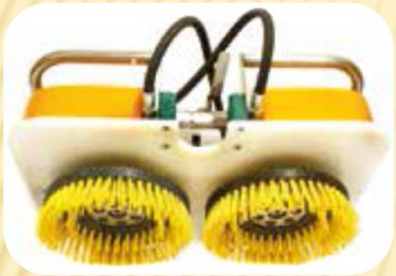
Non-operational vessel from one month to eight months in some cases
The high cost of vessel Docking
Reduce throughput of the port based on the type of vessel services
Reduce availability Indicator
Lack of profit of vessel
Diving risks

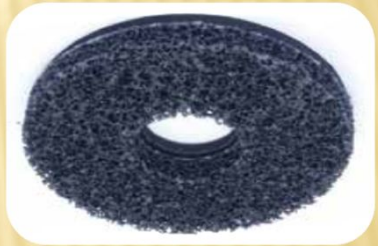
VESSELS BODY CLEANING TO PREVENT THE FORMATION OF MOSS AND METAL CORROSION BY UNDERWATER ROBOT

According to forming a slimy layer on the vessels body within a few days, can be used underwater robot equipped with air cushion in order to stick to the vessel body and specific brush or water jet for cleaning the surface and wipe the slime used. This can be every 10 days, and in the distance going between the two dry ponds for one to several hours depending on the length and width of vessels be done that Practically prevents the formation of moss, body corrosion and reduce speed, Fuel consumption and … and increases color Useful life and body And consequently increases the time between the two docking that this reduces cost and save.

METHODS OF CLEANING THE BODY AND VESSEL BUTTERFLY BY UNDERWATER ROBOT

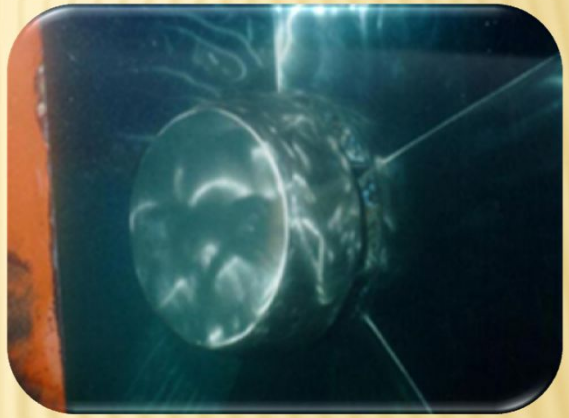
1- By Brush





METHODS OF CLEANING THE BODY AND VESSEL BUTTERFLY BY UNDERWATER ROBOT

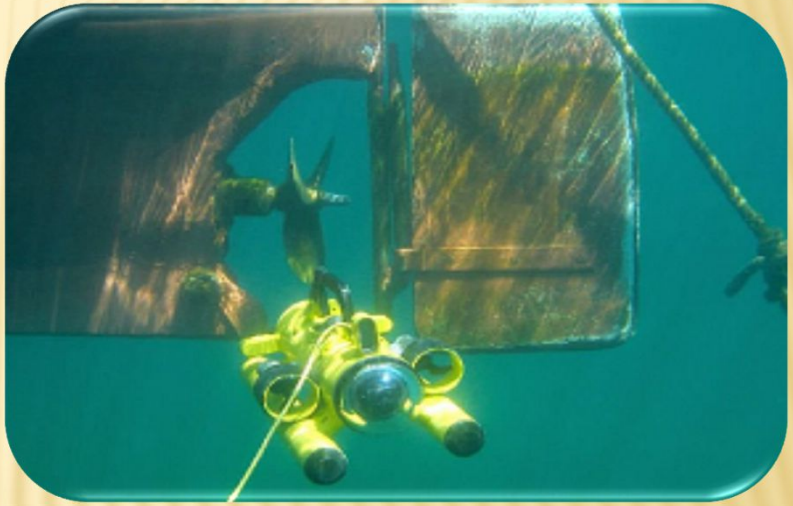
2- Water Jet



THE EFFECTS OF USING THE UNDERWATER ROBOT SYSTEM IN THE MAINTENANCE AND REPAIR OF VESSELS

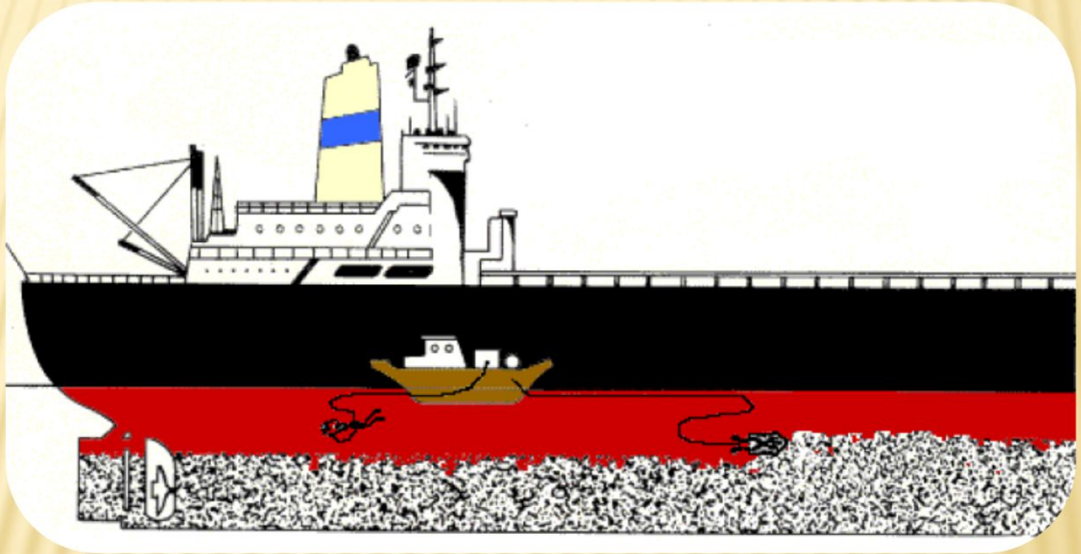
1. Economic efficiency as a result of the inspection and maintenance vessel body

2. Increasing the service



THE EFFECTS OF USING THE UNDERWATER ROBOT SYSTEM IN THE MAINTENANCE AND REPAIR OF VESSELS

Economic efficiency as a result of the inspection and maintenance vessel body



Estimate savings rate resulting from the application of underwater robot system in the maintenance of vessels:

Target vessels first type

Dredger vessel

Trailers vessel

First type target vessels:

Hoveyzeh dredgers vessel- Imam Khomeini seaport

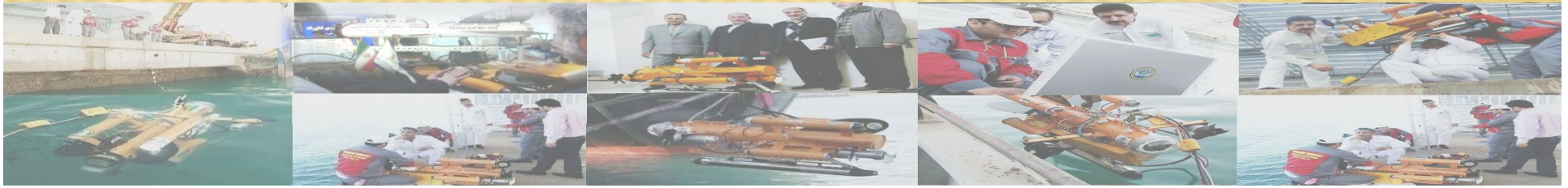
2 Dadman trailers vessel- Imam Khomeini seaport

period of time : 10 years

The number of working days in months: 22 days

Considered Parameters:

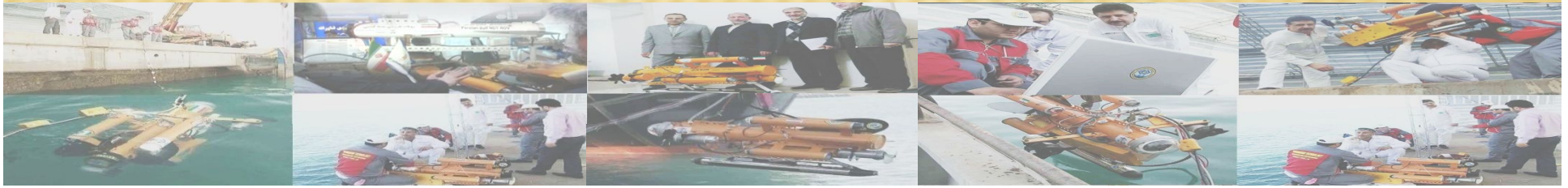
1. The effect on fuel consumption rate
2. Effect on increasing of MTBF
3. The impact of increased operating time of vessel in the result of maintenance by underwater robot
4. Impact on the increase and maintain optimal speed of service vessels



1- The impact rate on fuel consumption using underwater robots:

The duration of service With the same volume of fuel in the non-cleaning body	The duration of service With the same volume of fuel for body cleaning	Free price per ton of fuel (Dollar)	Fuel tank capacity(ton)	Vessel Type	Vessel Name
5 months and 18 days	6 months and 8 days	685	700	dredger	Hoveyzeh
5 months and 15 days	6 months and 18 days	685	150	trailers	Dadman*

*If trailers operate 10 hours a day



1. RESULTS OF THE UNDERWATER ROBOT SYSTEM IN THE MAINTENANCE AND REPAIR OF VESSELS BY THE SAVINGS IN FUEL CONSUMPTION

1- Dredger vessel

Moss effects on Suction Hopper Dredger Vessels :

- Increases dredger fuel consumption by 60 tons in one year. (According to the conducted survey, fuel consumption increased 0.3 per micron layer of slime that this increase in vessel according to the thickness and type of moss is sometimes up to 50%)
- Vessel fuel consumption about 8.5% increases than when it is under control and cleaning the underwater robot .
- Causes vessel efficiency 9% decreased during a year
- 60 tons of free fuel at the price of 69 dollars in a year will be 411000 dollars.

Therefore, in 10 years costs caused by increase in fuel consumption by non-preventing the formation of moss vessel body will be 411000 dollars.

1. RESULTS OF THE UNDERWATER ROBOT SYSTEM IN THE MAINTENANCE AND REPAIR OF VESSELS BY THE SAVINGS IN FUEL CONSUMPTION

2- Trailers vessel :

Moss effects on body of trailers Vessels :

- **Due to moss caused on body of trailers, fuel consumption increases 18 tons.**
- **Causes fuel economy increased about 8.5%**
- **Vessel efficiency will be reduced 12%.**

Therefore, in 10 years costs caused by increase in fuel consumption by non-preventing the formation of moss vessel body will be 247000 dollars.

2. RESULTS OF APPLYING THE UNDERWATER ROBOT SYSTEM IN MAINTENANCE OF VESSELS, THE RESULT OF SAVING INCREASED MTBF UNDERWATER REPAIRS

Number Docking in 10 years	Mean duration of vessel docking	Average cost of docking (Dollar)	Vessel Type	Vessel Name
3	8 month	1199000	dredger	Hoveyzeh
3	3 month	286000	trailers	Dadman

Reviews and calculations in the use of underwater robots in discussions of vessels repair show that With increasing MTBF, 3 times for Docking (current programmed) of about 50% a time dock ,we have reduction of Docking operations over 10 years. This reduces the cost for the target vessels are according to the table above.

For dredger vessels in 10 years will save about 5994000 dollars.

For trailers vessels in 10 years will save about 1427000 dollars.

3. RESULTS OF APPLYING THE UNDERWATER ROBOT SYSTEM IN MAINTENANCE OF VESSELS, THE RESULT OF INCREASED VESSEL OPERATION TIME CAUSED BY THE REMOVAL A PERIOD DOCK IN 10 YEARS

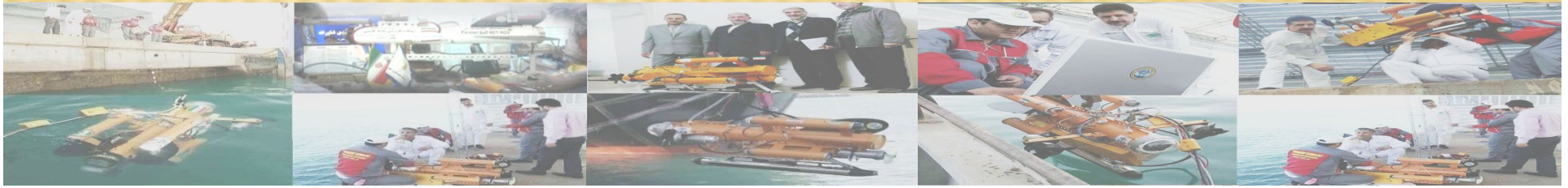
Rate increase in revenue (Dollar)	Increase the duration of the operation time by reducing the turn of dock	Vessel Type	Vessel Name
2717000	4 month	dredger	Hoveyzeh
172000	1.5 month	trailers	Dadman

Due to the increased MTBF and eliminate a target vessels dock turn and with regard to service and being strategic , naturally to the same time of dock, vessels operating time and income are added that from this place significant income will also achieve that above table according to the contract price of 2013 - 2014 has been calculated.

Estimate the savings rate in 10 years due to use of underwater robot system in the maintenance and repair of vessels

Total sum (Dollar)	Increase rate in revenue(Dollar)	Docking cost saving rate(Dollar)	Fuel consumption saving rate (Dollar)	Vessel Type	Vessel Name
3317000	2717000	599000	411000	dredger	Hoveyzeh
561000	172000	142000	247000	trailers	Dadman

According to the operational period considered, the amount of savings resulting from the use of underwater robots in the service and maintenance vessels in the body, just in the issue preventing the formation of moss on the body for a dredger vessel Yearly 332000 dollars and for a trailers vessel 56000 dollars will save. However it should be noted that an underwater robot is capable of serving several vessel simultaneously. So :

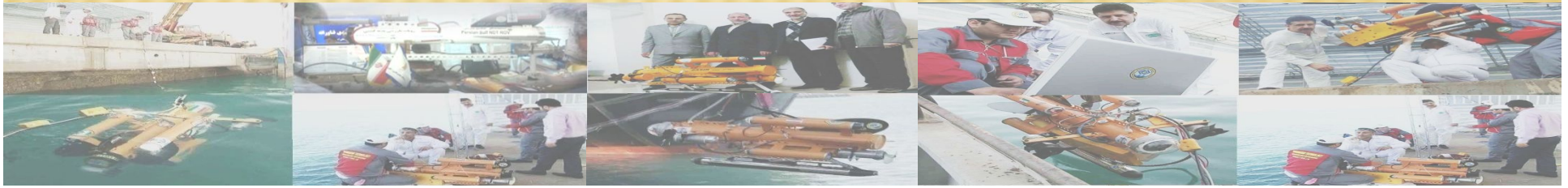


THE SAVINGS RATE RESULTING FROM THE USE UNDERWATER ROBOT TO MAINTAIN A DAILY VESSEL

According to the time required for the formation of moss (between 3 to 6 days) on the floating body and also according to the duration of the vessel body polishing such as Hoveizeh vessel by underwater robot that takes about 5 to 7 hours, on average, predicted that an underwater robot for 6 to 7 suction hopper vessels has throughput that this with a small vessel body increases.

using a robot on a daily for each vessel. Dollar savings due to reduced fuel consumption, increased MTBF and increase the availability and standby vessels and only for a robot :

- The amount 1990000 dollars per year for use in dredger vessels
- 449000 dollars value per year for use at 8 trailers vessels is estimated.

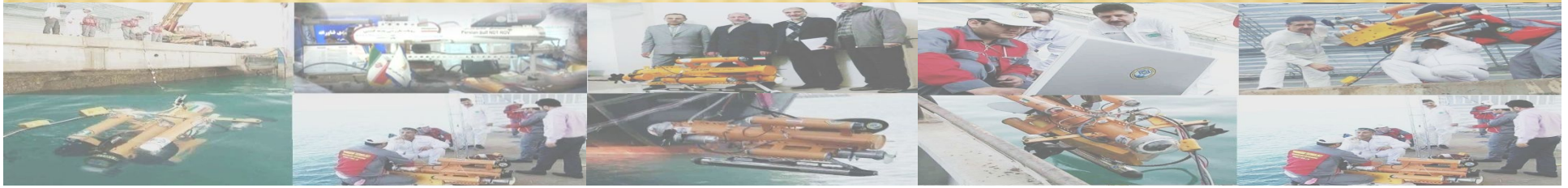


THE SAVINGS RATE RESULTING FROM THE USE UNDERWATER ROBOT TO MAINTAIN A DAILY VESSEL

Per device underwater robot for number of target vessels considered , Certainly in the worst predictions profitability will be the following:

- For Suction Hopper Dredger vessels 995000 dollars per year
- For trailers vessels 225000 dollars per year

However, the price to build an underwater robot is less than 10% above amount of savings.



THANK YOU FOR YOUR ATTENTION