European Commission

ESReDA

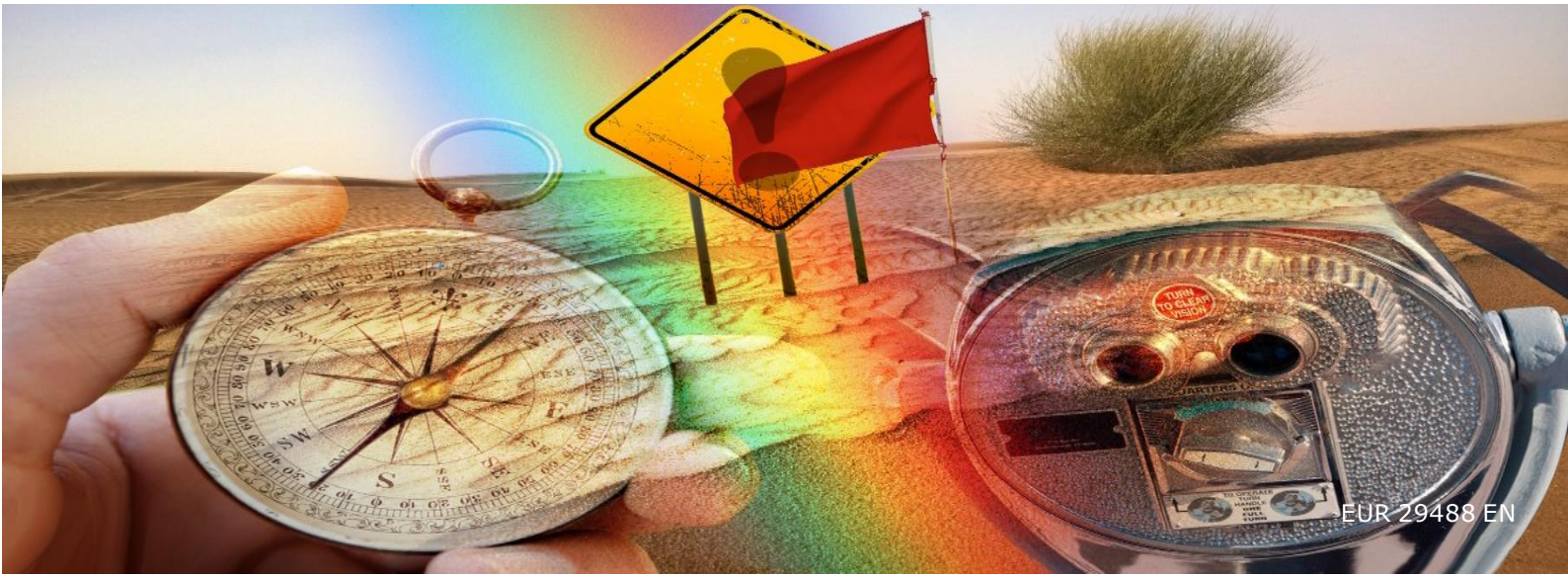
European Safety, Reliability & Data Association

Enhancing Safety: The Challenge of Foresight

Proceedings of the
53rd ESReDA Seminar
Hosted by the
European Commission
Joint Research Centre
14-15 November 2017,
Ispra, Italy

Edited by

Ana Lisa Vetere Arellano,
Zdenko Šimić, Nicolas Dechy



EUR 29488 EN

Legal Notice

European Safety, Reliability & Data Association (ESReDA)

European Safety, Reliability & Data Association (ESReDA) is a European Association established in 1992 to promote research, application and training in Reliability, Availability, Maintainability and Safety (RAMS). The Association provides a forum for the exchange of information, data and current research in Safety and Reliability.

ESReDA membership is open to organisations, privates or governmental institutes, industry researchers and consultants, who are active in the field of Safety and Reliability. Membership fees are currently 1000 EURO for organisations and 500 EURO for universities and individual members. Special sponsoring or associate membership is also available.

ISBN 978-92-79-98156-2
53rd ESReDA Seminar Proceedings, December 2018

For more information and available ESReDA proceedings please consult:
http://www.esreda.org/

Table of Contents

Preface

We live in a world where advancement in technology coupled with human's creative and innovative mind has led to the design of safer and better performing infrastructures (nuclear power plants, chemical process plants, high speed trains, spaceplanes, etc.), which are needed for a modern society. However, due to the interconnected socio-economic and technological landscape that is rapidly evolving, safety continues to have many new challenges (known unknowns, unknown unknowns) that add onto changed variants of the old challenges (e.g. modified known unknowns). Additionally, governance and legislation can be slow to catch up with this dynamic pace of change. At times, overregulation can occur, resulting in a significant resource investment towards compliance for existing infrastructure operators or for aspiring start-ups that would like to enter the market, but end up struggling or even abandoning the sector.

Inspired by this background, the European Safety and Reliability Data Association's *Foresight in Safety* Project Group prepared the 53rd ESReDA seminar with a purpose to launch an open dialogue with stakeholders in the safety arena. Thus, by providing an open forum where experiences in foresight in safety approaches from different sectors could be shared, cross-fertilisation of ideas, such as how foresight could be mainstreamed into safety practice in a more consistent manner, could be discussed.

The seminar offered a technical programme with four keynote speeches from:

- Fabiana Scapolo, European Commision Joint Reserach Centre, Belgium;
- Ana Afonso, European Food Safety Authority, Parma, Italy;
- Antonio d'Agostino, European Union Agency for Railways, Valenciennes, France;
- Lorenzo Fiamma, European Maritime Safety Agency, Lisbon, Portugal.

There were also 23 other presentations made by stakeholders from universities, research centres, industry, government service and safety authorities. The topics addressed were related to foresight from various perspectives: safety, risk assessment, scenarios, resilience, horizon scanning, early warning signals, database management, whistle-blowers, knowledge management, big data, data visualisation, etc., and from various industries: nuclear, chemical, electricity, food, maritime, railroad and aviation.

There were 57 participants from 15 countries (Belgium, Czech Republic, Finland, France, Greece, Italy, Lithuania, the Netherlands, Norway, Poland, Portugal, Romania, Switzerland, United Kingdom and United States).

After the seminar, as a part of a feedback process, participants were asked to provide some keywords about the seminar. The organisers used these keywords to obtain a word cloud shown on the figure below. The project group will build on the seminar result, along with the rich compendium of experiences gained throughout the entire process building towards the seminar. It will take stock of these results and investigate how they could be usedin its future endeavours.

The editorial work for this report was carried out by the Joint Research Centre of the European Commission in the frame of Joint Research Centre support to ESReDA activities.

Ana Lisa Vetere Arellano
EC Joint Research Centre

Zdenko Šimić
EC Joint Research Centre

Nicolas Dechy
Institut de Radioprotection et de la Sûreté Nucléaire

SEMINAR PAPERS

Session 1:
Transferring foresight approaches to the safety domain

A tool to support policymaking and how it can be applied to safety management – Extended Abstract

Fabiana Scapolo

European Commission Joint Research Centre, Foresight, Behavioural Insight & Design for Policy Unit

Rue du Champ de Mars, 21

B-1050 Brussels/Belgium

Extended Abstract

The presentation will start with a brief introduction on why thinking about the future is becoming more and more a necessary activity for many organisations and domains. From there, definition and key characteristics of foresight will be provided together with an overview on what Foresight is and how and when it should be applied to policy making. An illustration on features, requirements and capabilities needed for foresight in a policymaking context to deliver will be delivered.

The presentation will also illustrate a number of possible foresight activities and methods. These include horizon scanning, trend analysis, visions, scenarios, technology assessment. Some examples on how these methods are applied will be provided.

The presentation aims also at reflecting on how foresight could be applied to safety management and risks assessment. It will suggest some practical ways of implementation.

Keywords: Foresight, horizon scanning, trend analysis, visions, scenarios

Uncertain future. Unsafe future? Or foresight in safety – theories, traditions and the ESReDA Safety Approach

Sverre Røed-Larsen

SRL SHE Consulting

Lassonsgate 1

NO-0270 Oslo, Norway

John Stoop

Kindunos Safety Consultancy Ltd

P.O.Box 218

NL-4200 AE Gorinchen, The Netherlands

Abstract

Foresight is a relatively new research discipline, established in the 1960s especially in Japan and United States, and later further developed in many research environments in other countries. The purpose of the use of foresight techniques is to employ a participant-based process for the systematic collection of forward-thinking knowledge and develop visions and future perspectives in a medium and in a long-term perspective. Based on a holistic approach and making use of knowledge of former events - such as results from the investigations of accidents and near misses and knowledge of the present situation - one can improve the current decisions and promote better prevention and harm reduction measures. Unfortunately, foresight methodology has so far been used only to a small degree in a safety context.

The paper will briefly review the evolution of foresight-theories and outline its historical background. It will describe the characteristic elements in foresight and give an overview of the most important methods used. In this context, the basic comprehension forms within the safety thinking are analysed, and it will be argued for changes in the moral and ethical values within safety for technological changes and improvements, as well as for the developing safety as a societal value. It is emphasized that the recognition of a necessary system shift must take place on two levels: as an incremental shift with derivative solutions for known problems, and as a substantial change with disruptive solutions for new problems. In addition to comparative examples of release of energy during aviation and railway accidents, and nuclear

disasters, also the characteristics of so-called "weak signals" are discussed. The necessity of a paradigm shift is underlined.

The paper ends with a brief description of the ESReDA PGs approach to foresight methodology within the safety area, and examples of challenges are given, and recommendations proposed for a new holistic safety management based on feed forward as well as on feedback information and insights.

Keywords: foresight, safety, ESReDA, accident investigation, future

1. Basic attitudes to the future

The human being has always been concerned about its place in existence: the past, present, or future. Many have been especially concerned about the future that lay in front of them as a single man, in front of the family, in front of the genus or in front of the local society. Today we include also the nation, the major regions such as EU and the global community.

The attitude of the future has varied according to which point of view one had: religious, political, social, economic, demographic, commercial and other variables such as ethnicity, age, gender, status, sexual orientation. Some main sections can be:

- The future as fear and threat (religion, but as heaven in a new life!)
- The future as happiness and joy (ideology, religion, social engineering)
- The future as unimportant and immaterial (determinism)
- The future as characterized by risks, probabilities and possibilities (science)
- The future as adaptive and prosperous (technology and socio-technical engineering)

The time horizon may for analytical reasons be divided between short term, middle and long term.

Each of these approaches have been described in religious literature (the Bible), in many philosophical books, in scientific works, in technical papers and books, in novels and poetry, in science fiction etc. Many conceptions about our future destiny form part of our oral traditions. Famous persons who have contributed to futuristic thinking, include i.e. Leonardo da Vinci, Jules Verne, H.G. Wells, Herman Kahn, Johan Galtung, Stephen Hawkin, Aldous Huxley, Robert Jungk, George Orwell, Alvin Toffler, etc.

Some recent examples of global treats include studies made by OECD, studies about opportunities and trends in technology (South by Southwest 2016) and several climate reports. Samsung's SmartThings report[1] about Future living is an example of a very

[1] http://www.samsung.com/uk/pdf/smartthings/future-living-report.pdf

long-time horizon (till 100 year) and how the digital revolution can have massively implications on our lifestyles by changing our homes, our cities and countries.

2. The origins of the foresight scientific approach – the theories and the history

The systematic approach to Foresight Thinking as a science may be dated back to 1950/60-ies with the start of Technology Assessment and Forecasting. Today, modern safety thinking has elaborated in many directions and is used in different connections. Foresight includes the use of a variety of methods and techniques-depending (e.g. 25 methods). The actual notion "foresight in safety" is analyzed and defined in a separate chapter.

The scientific approach labelled as "foresight" is defined in contrast to another discipline which was named future research or futures studies. "Future research/futures studies" was often disputed within scientific circles: could such an approach – which was not based on theories and hypotheses and tested against empirical data, be included as "real scientific research"? Or was it an art?[2] Although a final agreement has still not been reach, it is clear that the studies of futures (possible, probable, or preferable), has neither the traditional characteristics from natural sciences nor the methodology from some social sciences. However, futures studies are now both an academic branch (e.g. environmental/climate sector and dedicated research centres, often with scientific programs) and – much more widespread – semi-commercial (think tanks) or pure commercial bureaus offering a broad repertoire of techniques, such as trend studies/trend analysis, which are widely used in many connections and markets.

As futures studies, strategic foresight studies had many early authors and scientists that initiated or anticipated the more systematic and knowledge-based understanding which were established after the WWII. Strategic foresight studies developed mainly from defence planning as part of the military complex and expanded later to the public sector (state/regional innovation), to large regional organisations (such as EU) to the private sector (such as multi-national companies).

3. Foresight traditions – the middle term and long-term perspective

The foresight approach is part of a wider scientific tradition: to use analyses about the past, about the present situation (diagnosis), to identify future objects and the possibility to reach them (prognosis), and how to reach the future goals (prescription). But here again, the actual studies differ in many ways between the two extremes: on one side pure basic scientific research about the future, and on the other side pure business studies, e.g. in the context of strategic foresight management.

Luke Georghiou (PREST, Manchester University) has defined foresight as an approach overlapping three other disciplines: future studies, strategic planning and policy analysis. Although 'foresight' has been connected to or partly integrated in other research fields, the foresight tradition as a whole has some unique elements.

[2] https://en.wikipedia.org/wiki/Futures_studies

Some characteristics of the foresight approach are[3]:

Process:	cross-disciplinary and cross-sectorial/participation and action-oriented
Time:	medium to long term perspectives (often 5 – 50 years) in contrast to 0 – 5 years for risk assessment (short perspective).
Goal:	aimed at present-day decisions and mobility/joint actions by identifying "possible future developments, driving forces, emerging technologies, barriers, threats and opportunities"
Results	"Outlooks, proposals of future developments, scenarios, visions, roadmaps, action"
Prerequisite:	the world is multi-dimensional and basic uncertain

Scientists that use future techniques in their research (futurists) as well thinks tanks and similar institutions may use a wide range of forecasting methods, which include:

• Anticipatory thinking protocols • Causal layered analysis (CLA) • Environmental scanning • Scenario method • Delphi method • Future history • Monitoring	• Back casting (eco-history) • Cross-impact analysis • Futures workshops • Failure mode and effects analysis • Futures wheel • Technology road mapping	• Social network analysis • Systems engineering • Trend analysis • Morphological analysis • Technology forecasting • Theory U

Both individuals (researchers, authors, scientists etc., see part 1), university institutes and organizations (Foresight professional networks, public-sector foresight organisations, and non-governmental foresight organisations) have allocated resources in order to develop and implement foresight studies and results in many sectors. As examples may be mentioned as networks World Future Society and World Futures Studies Federation, as organizations in the public sector National Intelligence Council and NASA /both US), The Institute for Prospective Technological Studies (EU), Government Office for Science (UK) and Norwegian Research Council (Norway), as NGOs Rand Corporation, Hudson Institute, Copenhagen Institute for Future Studies, Strategic Foresight Group and Project 2049 Institute. The reports and findings may be published in journals like Futures, Journal of Future Studies, Technological Forecasting and Change, and the magazine The Futurist.

Safety seems to be at the edge of a paradigm shift, both from a theoretical and a practical perspective. In the European safety science community, a wide array of new approaches is studied. Some challenge the validity of safety science as a science (Safety Science 2014), while others proclaim new safety concepts and notions, such as Resilience Engineering, a New View on Human Error or Safety I and Safety II. Such

[3] Partly based on op.cit and Raija Koivisto (2009) Integrating future-oriented technology analysis and risk assessment methodologies in Technology Forecasting & Social Change 76 (2009) 1163-1176.

developments challenge and redefine commonly shared notions such as precaution, cause-consequence relations, human performance, cognition and culture with sometimes far reaching consequences for their application. ESReDA advocates the generic value and applicability of safety investigations across industrial domains and scientific disciplines. ESReDA foresees a predictive Foresight on Safety and its integration in a system engineering perspective. In several industrial sectors with a high-tech nature, safety is considered a shared responsibility, superseding a single actor or mono-disciplinary perspective. Life Cycle Analysis seems indispensable for an assessing safety throughout the life cycle of complex legacy systems, addressing specific characteristics of transport, process and nuclear power applications.

4. Safety, investigations and the modern system approach

Within the safety area methods and approaches, such as safety investigation, scenarios, risk analysis and assessment, the measurement of "weak signals" and other indicators, may be useful. Future thinking may be in use in different industrial sectors (such as energy production, the production of chemical substances and products, consumable production, transportation and to some extent also in the consumer-/service sector), but often restricted to a short or medium-term time horizon.

Such new thinking is accompanied by a change in moral and ethical values on safety. Recent developments focus on an additional approach to technical design notions such as failsafe and safe life, crash worthiness, damage tolerance, compartmentation, redundancy and reliability. With the introduction of ICT as a fundamental new technology, new ethical notions such as Value Sensitive design and Responsible Innovation principles have been developed. They deal with complexity, system design and integration of safety assessment by Encompassing Design and Multidisciplinary Design Optimization methods, Knowledge Based Engineering and Value Engineering. New legal definitions dealing with safety assessment and liability have been introduced such as Corporate Manslaughter and Corporate Homicide, shifting social responsibilities for unanticipated consequences back to manufacturers and designers.

The consequences of application of new materials such as composites, technological innovations in ICT, food, system-of-system networks and Internet of Things cannot be predicted and assessed by today's evaluation methods. A new combination of learning from feedback and feed forward is not yet developed and validated. New thinking such the ESReDA Cube has indicated several opportunities to tackle such quests.

Since safety of innovative complex and dynamic systems cannot be assessed based on their past performance, new approaches and notions should be developed. A distinction between socio-organizational and socio-technical system categories becomes inevitable, dealing with their intrinsic, inherent and emergent properties as specific classes of hazard, threats and consequences. A distinction between high energy density systems and dynamic network concepts is necessary to deal with massive instantaneous outbursts of energy of a mechanical, chemical or nuclear nature and the way consequences propagate through networks. A new distinction should be made between normal, undisrupted performance which is highly predictable and controllable, and non-normal situations, emerging from drift, natural growth, aging and exceedance of designed performance envelopes. New mental representations of human performance

become necessary, since Tayloristic models of compliant behavior and rational decision making theories do not provide satisfactory explanations of abnormal behavior in normal situations or normal behavior in abnormal situations. A Good Operatorship notion dealing with competence rather than compliance is under development in several high-tech sectors such as in aviation and the maritime counterbalancing prospects of full automation towards unmanned operated transport systems.

In assessing their safety performance, we can not only deal with new systems and technological innovation. Existing systems in their full maturity have a long and lasting past performance and have gone through a series of decisions, assumptions and modifications that are hardly fully known, let alone documented. The notion of transition management in matured, complex systems with a high level of technological change potential is in its early phases of development. A distinction between disruptive and derivative technology is crucial to understand its dynamic behavior. Due to the very high-performance levels such catastrophic consequences can manifest themselves as very high consequence and very low probability events beyond the responsibility of individual actors and entities. Interferences may occur due to unknown interrelations between components that have been forgotten, neglected or unexplored. In practice, such dynamics are referred to as Unknown Unknowns, but are actually discernable as design induced consequences during operations. Foresight is also knowledge and operational experience based hindsight.
The role of accident and incident investigations can gain a new dimension if such aspects are incorporated in the investigation methodology. A common investigation methodology across industries and disciplines should lay the basis for such a new approach. Supported by a legal recognition and procedural embedment in practice, such as the ICAO Annex 13 approach.

In other articles, these approaches are described and discussed.

Traditionally, many industrial companies have concentrated on learning from past events, such as accidents, production problems, distribution and usage problems, and developed internal safety policies and industry norms after that. Many safety authorities, including regulatory agencies, have also followed this pattern. Feedback to the design of technology and organizations and managing safety during operations have greatly benefitted from such learning. We designed, created and proclaimed a category of Non-Plus-Ultra-Safe systems, such as aviation. There are however, necessities and opportunities to combine feedback and feed forward learning, integrating safety as a social value at all systems levels and life cycle phases.
Safety management based on a systematic combination of learning of past events and issues and analysis and methods for insight into the future challenges seems still not very widespread within several key high-risk areas. This working group aims at reinforcing feedback and feed forwards loops between hindsight and foresight experiences and expertise.

Safety is to be revalued as a strategic societal value, instead of the presently preferred notion as a Key Performance Indicator within organisations, to be assessed against other operational aspects such as economy and efficiency. Safety is a public value, not only a corporate value within an ETTO decision making context on an operator level. A shift back from control to comprehension is inevitable in dealing with modern,

complex and dynamic socio-technical and socio-organisational systems in their operating environment.
Only by re-addressing the context of such systems, a credible foresight on their nature and safety performance can be established.

In safety thinking a transition is taking place from reactive, to proactive, to predictive thinking. Such thinking is twofold:

- in technological developments with respect to technological innovation and disruptive applications

- in socio-economic and social developments with respect to risk awareness, perception, risk acceptance and management.

A Zero Vision paradigm is emerging: no risk is acceptable and lethal accidents are intolerable. At the same time, systems become more embedded, complex and dynamic. The scale is increasing with respect to the volumes, numbers and sizes of the transport means and the energies that can be released from them, while the systems safety performance has achieved a Non-Plus Ultra-Safe level. The law of diminishing returns seem to become dominant with respect to conventional solutions. A preference is noticeable towards new notions that deal with foresight during operations such as Early Warnings, or recovery from non-normal situations, such as Resilience Engineering. Both developments erode the need to remain vigilant and proficient with respect to safety. Investments in road safety have dramatically been reduced. As a consequence, the death toll in Europe is increasing again. Safety in aviation is jeopardized by the limits to growth due to the capacity of the infrastructure, both airside and landside. Such system related developments can be foreseen by analysing their architecture and exploring higher order drivers for change and efficiency, such as business models, policy making and governance.

With respect to socio-technical systems with a non-plus ultra-safe performance level, aviation, railways, maritime, nuclear and process industry can be considered as belonging to a specific category of high energy density systems, capable of creating catastrophic consequences of a physical nature. Preventing accidents of an unprecedented magnitude remains a prime reason for existence for safety investigations.

There is no Golden Bullet with respect to one encompassing safety performance indicator. An analysis of the safety performance in aviation indicates a complex interaction between airworthiness requirements and passenger service performance indicators. Rather than aiming at a further decrease of the overall accident rate as performance indicators, safety enhancement efforts could be invested in a better understanding of the system principles and properties. Safety investigations are a pivotal approach to this purpose.

Recognition of a necessary system change can be acquired at two levels:

- an incremental shift with derivative solutions for known problems

- a substantial shift with disruptive solutions for new problems.

In the second case however, innovation processes and adaptations cannot be implemented by a single actor or from a single perspective or discipline. The concept of Cyclic Innovation needs to be mobilized to achieve sustainable effects, which are if not predictable, at least are descriptive or comprehensible.

The magnitude of energies that are to be controlled during normal operations and can be released during accidents is comparable between aviation, railway and the nuclear sector (see Table I):

Table I: Comparison of energy magnitudes across railway, aviation and nuclear sectors.

	Weight	**Speed**	**Altitude**	**Energy**
High Speed Train	430 tons	250 km/h	ground level	1053 MW
		320 km/h	ground level	1740 MW
A380 Jumbo jet	MTW 575	900 km/h	10.000 m	75 000 MW
	at take-off MTOW 575 tons	260 km/h	ground level	1500 MW
	at landing MLW 386 tons	260 km/h	200m above ground level	1252 MW
Nuclear power plant	Average size			800 MW
	Borsele (Neth)		Sea level	450 MW
	Chernobyl		Sea level	600 MW
	Fukushima		Sea level	784 MW

Weak signals are not weak by definition. Based on signal theory, there are several reasons for a weakness of signals:

- strong signals can be suppressed to weak signals
- the can be misinterpreted by distortion during transmission
- a signal can be missed in the spectrum at the receiving end
- a signal can be overruled by a signal of another nature
- the frequency of transmission can fall beneath a perception threshold level.

In practice such weak signal debates are dealing with either a technical, behavioural or social nature of signals, with primary production processes or secondary processes, while the diversity across actors and stakeholders may create confusion and disagreement of their validity as service providers for user's safety or for technical reliability.

A simultaneous use of feedback and feed forward mechanisms can be underpinned by the Full Information Paradigm of Klir (see fig). According to this paradigm, the acquired body of knowledge and experience collected over decades in a system provides a basis for safety and risk considerations. Such a body of knowledge is overwhelming for legacy systems with a worldwide impact such as energy, process industry and transport, making the NPUS safe, but also reluctant to change. Their

ability to adapt is hampered by vested mental constructs, assumptions and simplifications, expertise and consensus on scientific paradigms, methods, notions and techniques, both theoretical and practical.

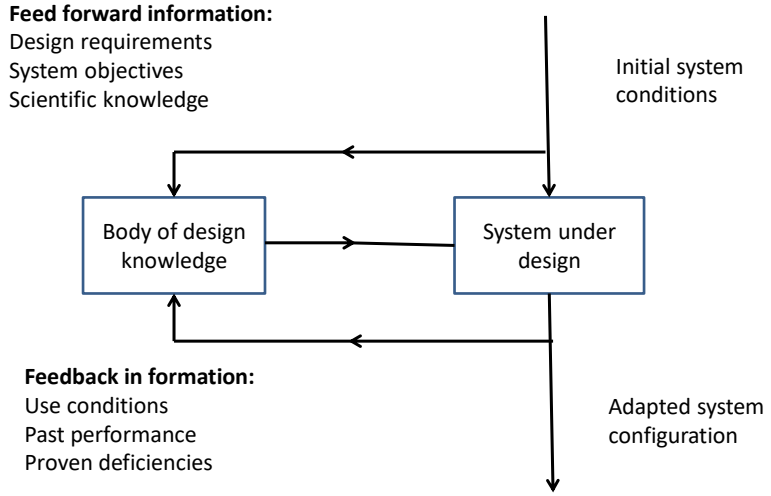


Figure 1. Hierarchical ordered control loops.

'Old views' have to be discarded and abolished in case of a paradigm shift in safety thinking, similar to Schumpeter's 'creative destruction' on economic theory. Otherwise an opaque blending is created by mixing old and new views into a hybrid concept. In the past, we have seen a stall of such a dialectic process by proclaiming A versus B concept of safety, to be replaced by another version of C versus D. Such a debate does not restrict itself to an academic discourse, but may hamper progress. A fall back on old views and repetition of debates across domains and disciplines frequently occurs, allocating public, corporate and personal responsibilities for safety, emphasizing the roles of whistle blowers and regulators.

We advocate the abolition of three obsolete notions:

- replace the application of predefined, simplified accident models by the scenario concept as a consensus basis for reconstructing the course of the event,
- replace the notion of 'human error' by a new view on human behaviour,
- reconsider the notion of 'cause' in the perspective of multilinear interactions.

Abolition of the use of accident models is likely to meet resistance to change due to:

- a lack of understanding of system engineering theory by non-technical scientists and practitioners
- monodisciplinary paradigmatic perspectives in psychology on human performance and cognition
- disciplinary demarcation lines between technical and social sciences and

- cognitive stubbornness and resistance to change at both an individual, corporate and governance level.

5. Foresight in safety; an epilogue

'Foresight' has developed as a scientific research field during the last ten-years and has been more elaborated concerning theories, hypothesis and concepts. Many universities around the world have now foresight research on their research agenda, and some have also established scientific degrees and education programmes. Outside universities, the foresight approach has been used by several public and private institutions, enterprises (esp. multinational companies) and consultancy firms/think tanks etc. The main implementation is connected to change management, strategic analysis and policy development. Corporate foresight has been defined as:

> *"..an ability that includes any structural or cultural element that enables the company to detect discontinuous change early, interpret the consequences for the company, and formulate effective responses to ensure the long-term survival and success of the company"*[4]

5. 1 Preliminary conclusions

- The foresight approach seems to have high potential utilitarian value for exploring safety enhancement on the short term.

- The use of foresight notions and methods have so far only to a small degree been incorporated in systematic safety management at a governance and corporate level

- More research is needed on both national and EU level to identify adequate and appropriate methods and to investigate the utilitarian value of applying foresight in safety in a medium and long-term perspective.

- More emphasise should be laid down on exploring the possible value of transferring experiences and knowledge from the use of foresight methods in other societal sectors in different countries and EU to the safety arena.

Safety is an indispensable strategic value in the transition process from derivative to disruptive solutions in developing innovative as well as legacy systems. The main challenge for safety professionals is to develop new notions, methods, tools and techniques to cope with the challenges that accompany such a transition. These efforts could benefit from unexplored and so far unchartered domains and disciplines. Foresight is a promising prospect.

To paraphrase Richard Booth in his inaugural lecture in 1979: Safety is too important a matter to be left to futurologists.

[4] Rohrbeck, Rene (2010) Corporate Foresight: Towards a Maturity Model for the Future Orientation of a Firm. Springer Series: Contribution to Management Science, Heidelberg and New York.

Session 2:
Foresight challenges in safety management

How did aviation become so safe, and beyond?

John Stoop

Delft University of Technology

Amsterdam University of Applied Sciences

Kindunos Safety Consultancy Ltd

Spijksedijk 8

4207GN Gorinchem, the Netherlands

Abstract

Aviation has been recognized as one of the ultimate safe socio-technical systems. This contribution discusses the conditions and context that moulded the system safety to its present level by applying integral safety, a sectoral approach and safety as a strategic value. At present the aviation system consists of institutional arrangements at the global level, a shared repository of knowledge and operational experiences, feedback from reality, the notion of Good Airmanship, together with the choice of technology as the flywheel for progress. This architecture made aviation a Non-Plus Ultra-Safe system characterized by a safety performance level of beyond 10-7 accident rate. To cross this mythical boundary in legacy systems like aviation, it is imperative to apply game changers such as socio-technical systems engineering, disruptive technologies and innovation transition management. In such a transition, a shift in focus occurs from performance to properties, from hindsight to foresight, highlighted by the case study of the stall recovery device, the Kestrel concept.

Keywords: aviation, system safety, foresight, engineering design, safety investigation

1. Introduction

A Non-Plus Ultra-Safe performance is no reason for complacency. In view of the oncoming growth and expansion in aviation, a further increase of safety is required to maintain the present performance level and to assure public confidence in the system. The size of the 'City in the Sky' at 30.000 feet is prognosed to double from the present 1 million inhabitants to 2 million in 2030 (Boosten, 2017).

To cope with this prognosed growth, abolition of obsolete safety constructs is inevitable. New safety notions are required in a transition from accident contributing

factors to state/space modelling with safety Eigenvectors and multiple solution domains. Despite their low frequency, prevention of physical consequences of major events in such high energy density systems remain pivotal due to their catastrophic and disruptive potential. Application of systems control theoretical approaches should enable a transition from reactive and proactive towards predictive capabilities. Early interventions in the design process enable identification of intrinsic hazards and inherent safety properties that have to be dealt with during normal and non-normal operations and system states.

Incorporation of higher system orders, engineering design principles and innovative and disruptive change enable a combination of both reactive, proactive and predictive responses which facilitate foresight in safety. Because in aviation, we must continue to innovate and improve to safely defy gravity tomorrow.

2. How did aviation become so safe?

2.1 Engines for change

Four engines for enhancing foresight and predicting safe behaviour at a systems level are identified which, each by themselves, are a necessary but insufficient condition for safety enhancement. In addition, they have to occur simultaneously in order to implement a new concept in the aviation sector on a sustainable basis. These engines are:

These engines are:

- Institutional arrangements at the level of the state and its sovereignty in an supra-national context of non-governmental organisations
- feedback from reality, based on precaution and independence of investigations
- system engineering principles, technological innovation and system state transitions
- Knowledge Based Engineering, by understanding empirical and experimental data.

As these engines coincide, a structural need for timely adaptations and system change occurs. Impulses for change can be explained based on internal, structural needs of the sector itself, not only by a public concern on the credibility of a sector. In case of an external impulse, such as with an aviation disaster, sometimes several similar events have to occur before a sector responds. A worldwide implementation of each these engines has not only lead to a significant increase in safety, but also contributed to developing expertise and knowledge about the actual safety performance of the sector. They served as foresight, designed into the system from the start on. A vital issue has been maintaining public confidence in the sector in order to develop a worldwide aviation industry (Kahan, 1998). On one hand, in passenger transport, the public is the customer who puts faith in a safe, efficient and smooth performance of the services rendered. Once this faith is lost, the sector will have to face the fear of going out of

business. On the other hand, the performance of the transport sector is in the public domain. Accidents are visible in the public eye, being bystanders and potential risk bearers in case of a disaster, such as an air crash in an apartment building, a release of hazardous materials or a tunnel fire. Rescue and emergency in incident and disaster handling are public duties in case of a disaster. Independent Transport Safety Boards make public governance at the State level a direct stakeholder in transportation accidents at the systems level in contrast to corporate management of fixed installations in other high-tech sectors such as process industry and nuclear power supply (Vuorio, Stoop and Johnson, 2017). Due to the complexity and high-technology nature, aviation has additional specific characteristics, which necessitate a technical investigation into unexplained failure of such transportation systems. These characteristics are based on the precaution principle, creating a common body of knowledge in aviation.

2.1.1 Institutional arrangements

The first international aviation conference in 1889 raised four fundamental juridical questions with regard to national sovereignty of the airspace and safety of aviation (Freer 1986.1):

- Should governments license civil aviation?
- Should there be special legislation to regulate responsibility of aviators towards their passengers, public and owners of the land where descent is made?
- Should the salvage of aerial wrecks be governed by maritime law?
- Should there be new rules for establishing the absence or death of lost aviators?

Establishing rules for uncontrolled flights in airspace or above territorial waters led to the first international aerial congress amongst 21 states in 1910 in Paris. The First World War spurred aviation technology, leading in 1919 to the International Air Convention on technical, judicial, and military aspects of aviation and the establishment of the International Commission for Air navigation (ICAN) (Freer, 1986.2). The answers to these questions firmly establish safety and the investigation of accidents as a distinguishing feature of the aviation sector.

During the early development of public transport systems, the precaution principle has been applied as the most sophisticated engineering design approach of the 19th century (McIntyre, 2000). This precaution principle is defined in aviation as: first comprehend then control, create foresight by gaining insight. It combines a timely response to failure with an in-depth analysis in order to understand the failure mechanisms. It was only during the Second World War that a probabilistic component in safety thinking was added as a second school of thinking to this approach. Due to a lack of empirical data, probabilistic approaches should reduce uncertainty on new concepts and configurations to facilitate prioritization and cost-effectiveness estimates of safety enhancement measures. After the Second World War, corporate risk management was introduced as a third school in thinking, evolving into a public safety and governance between all actors involved in safety in the transportation area (McIntyre, 2000).

As the flywheel for progress, the level of technical harmonization has been selected focusing on navigation, communication and reliability. The precaution principle and a timely feedback of findings are pivotal. Annex 13 set the terms for cooperation between states which are involved in an aviation accident, namely the States of occurrence, operations, registry and manufacturing (ICAO, 2001). The large-scale introduction of civil aviation required a change in aircraft design. Before the war, civil aircraft were derivatives of military aircraft with respect to their design concepts as well to their construction and materials. After the war, large civil aircraft became disruptive designs because they had to transport great numbers of passengers over long distances, based on regular timetables, putting high demands on endurance, range and comfort. In contrast to these requirements, military aircraft were designed for relatively short-range combat performance, serving as airborne battle stations.

2.1.2 Feedback from reality, separated from blame and state interference

Even before the Second World War, the concept of learning from deficiencies was promulgated in aviation. Safety was viewed as an industry-wide problem, rather than one for any single operator, manufacturer or State. The concept was further developed in wartime aviation. Flanagan et al. (1948) conducted possibly the first study of incidents and "near misses" in aviation when he surveyed U.S. Army Air Corps crews to determine what factors influenced mission success and failure. Anticipating modern insights, he found that the critical factors were to be found more in human performance than aircraft technology. In order to keep public faith in the aviation industry, a common process of learning without allocating blame was deemed necessary. In order to provide a timely feedback to all stakeholders in the sector, accident investigations had to be separated from judicial procedures, which focus on individual responsibilities and liability.

This blame-free approach has clearly borne fruit. Technical investigations into the failure of designing and operating aircraft have seen an impressive development. Based on a limited number of 'showcases' design principles were developed, such as fail-safe, safe life, damage tolerance, crash worthiness, situation awareness or graceful degradation. Several famous cases such as the De Havilland Comet, Tenerife, UA-232 Mount Erebus, TWA-800, Valuejet and Swissair 111 have identified deficiencies in the aviation system, sometimes at some remote from the proximal cause of the triggering event. They have led to many practical changes as well as new expertise on specific academic areas varying from as metal fatigue to human failure, crew resource management or life-cycle maintenance.

During the 1960s, the issue of independence was raised in order to relieve investigations from a dominant influence of the State. During investigations, the influence of State interests, secondary causal factors and circumstantial influences should also be addressed. The debate on this matter can be traced to around 1937, after a series of major air crashes. Arriving at such independence, however, proved to be a long process, and still is not completed. In responding to specific European needs in harmonizing practices current in the States of the Community, an additional procedural arrangement on ICAO Annex 13 has been developed. This development led to the EU Directive 94/56/EC on Accident Investigation, despite fundamental differences between legal systems in the various countries of the Community (Cairns 1961, Smart 2004). Conflicts of interest linked to the issue of double inquiries by technical

permanent bodies and by judicial authorities were recognized, but nevertheless lead to a Community strategy to adaptation of the existing legal and institutional framework, harmonizing national legislation and strengthening cooperation between Member States (ETSC, 2001). As a consequence of the notion that incident investigation and analysis could be a source for safety recommendations, the EU has issued a Directive 2003/42/EC on mandatory incident registration in aviation. So far, the aviation sector has been unique in issuing mandatory, governmental investigations of systemic incidents from its conception on beyond the corporate level of investigations (Vuorio, Stoop and Johnson, 2017).

2.2 System engineering principles

2.2.1 Multiple safety performance indicators

Historically, safety in aviation is not only expressed in institutional arrangements and policy targets, but also in international, technical airworthiness requirements. Taking into account that zero risk is unachievable in any human activity, acceptable safety target levels had to be established in the perspective of an unbalance between safety and expected growth (Hengst, Smit and Stoop, 1998). An array of potential units for measuring risk can be used, discriminating relative safety related to the traffic volume and absolute safety, related to the annual number of fatalities. Differences across fleet segments and services, scheduled, non-scheduled flights and general aviation, accident rates per aircraft class and world region, as well as life expectancy of aircrafts have to be taken into account. Risk acceptance by the general public and personal appreciation of risk depends on convenience and pleasure in the various types of private and public risk taking activities. For each activity, a unit of measurement has to be selected since it makes a large difference whether safety is related to the absolute number of fatalities, a critical flight phase or the distance and time flown. For air services, as the criterion for safety performance the fatality rate per passenger km is used, while for airworthiness the level of safety is expressed per aircraft hour of flight. These two criteria are related by the number of passengers per aircraft, the survivability rate per aircraft and the blockspeed of the aircraft (Wittenberg, 1979).

This relation can be derived from statistics of air transportation quantitative data by:

- Number of passengers km P
- Aircraft flying hours U
- Aircraft flying kilometres S
- Assuming K passenger fatalities in R fatal accidents, the fatality rate per passenger km is K/P and the fatal accident rate per flight hour R/U.

For the relation between these quantities holds:

$$K/P = R/U * K/R * U/P \quad (1)$$

In this expression are introduced:

k = K/R = average number of fatalities per fatal accident

p = P/S = average number of passengers per aircraft

VB = S/U = average block speed

Then for equation (1) can be written:

$$K/P = R/U * k/p * 1/VB \quad (2)$$

Or in words: Pass.fatalities/pass.km = fatal acc./flight hours *fatal per acc./pass per aircraft*1/blockspeed. This dimension analysis shows that the introduction of long haul flights, increased survivability rate per accident, increase in blockspeed and larger aircraft have had a major influence on the decrease of the fatality rate per passenger km. Surprisingly, this dimension analysis indicated that these safety performance parameters are based on air services and airworthiness design parameters and not on safety design principles such as failsafe, safe life, damage tolerance, graceful degradation and crash worthiness.

This dimensions analysis refers to an aircraft design and certification perspective, while later developments applied an operational perspective. Safety management systems and maintenance, repair and overhaul established safety performance indicators for normal situations throughout the operational life of aircraft.

2.2.2 Towards a systems engineering perspective

In addressing the issue of acceptable safety levels, two assumptions are made:

- With the expected increase of traffic volume, safety levels may not fall below the achieved levels for reasons of public acceptance
- The level of growth is linear related to the number of accidents.

Consequently, the percentage of the total growth of the traffic volume expressed in passenger km must be compensated by an equivalent decrease in percentage of the fatality rate per passenger km. In the past, safety improvements have been accomplished by pragmatic changes in technology, aircraft operations and ground equipment. These achievements have been a combined effort of all parties involved: manufacturers, airline operators, authorities and research institutes.

Advocating a more rational tool for establishing a safety level -such as cost-benefit analysis- such approaches are confronted with hardly comparable costs for value of life, operating costs and cost for safety investments. While costs of individual accident are relative low on a sectoral level of costs, the overall safety enhancement measures following from such accidents may be excessive for the sector. A target safety level for aviation based on a rational cost-benefits approach seems hardly achievable (Wittenberg, 1979).

More rational approaches had to be developed in the 1970's for the introduction of civil jet aircraft and new technologies such as the supersonic Concorde and Automated

Landing System development. The allowable probability of failures is inversely related to their degree of hazard to the safety of the flight. No single failure or combination of failures should result in a Catastrophic Effect, unless the probability can be considered as Extremely Improbable, in effect lower than a 10^{-7} accident rate. Interesting in this approach is the total amount of flight hours per year that are produced by the aviation industry as such. Only a few aircraft types can surmount the 10^{7} requirement, accumulating sufficient flying hours. Consequently, accomplishment to the overall safety target of the airworthiness code *can never be proved by actual flight data* but should be settled by a System Safety Assessment approach. Due to the effect of the increase of aircraft speed and aircraft size, the passenger fatality rate expressed per passenger km has decreased in the past far more than the fatal aircraft accident rate per flight hour. In the coming decades, the favourable effect of aircraft speed will not occur and only the effect of aircraft size may remain. This parameter analysis demonstrates that changes in aircraft size and long range flights will consequently have an important impact on the improvement factor required for the fatality rate per *passenger km* versus the fatal accident rate based on the *aircraft flying hours.*

2.3 Knowledge Based Engineering (KBE) design

In assessing the fulfilment of the societal values and acceptance of designs, the prediction of tolerable loads and acceptable behaviour of designs is not so simple and well-defined as it seems. In the striving for excellence, the concept of failure is central to understanding engineering, for engineering design has as its first and foremost objective the obviation of failure (Petroski, 1992). As stated by Petroski, to understand what engineering is and what engineers do, is to understand how failures can happen and how they can contribute *more than successes* to advance technology (Italics added). As a challenge in the Science, Technology and Society debate on Human Values, engineering has as its principal objective not the given world, but the world that engineers themselves create. Extra-engineering motives and considerations of these values result in a continuous change that arises from these challenges. This means that there are many more ways in which something can go wrong than in the given world.
In his analytical study on aerospace engineering methodology, Vincenti indicates the transition from craftsman thinking in experimental progression towards knowledge based design of artefacts (Vincenti, 1990). In the 1930's the empirical and experimental design of aerofoils was gradually replaced by analytical and mathematical understanding of the mechanisms that ruled aerofoil design. Such transition towards a knowledge based design was supported by wind tunnel testing of scale models and flight tests. Scientific research focused on the role of viscosity, transition between laminar and turbulent flow, laminar flow aerofoils and elliptic lift distribution. This application of scientific research in order to reduce uncertainty in the attempts to achieve increased performance created a growth in knowledge. Increased knowledge in turn acts as a driving force to further increase knowledge. As defined by Constant (quote by Vincenti, 1990) the phenomenon of 'presumptive anomaly' may stimulate better understanding of the behaviour of an artefact.

"Presumptive anomaly occurs in technology, not when the conventional system fails in any absolute or objective sense, but when assumptions derived from science indicate either that under some future conditions the conventional system will fail (or function badly) or that a radically different system will do a much better job."

Vincenti concludes that presumptive anomaly, functional failure and the need to reduce uncertainty in design act as driving forces to a growth of engineering design knowledge.

In aviation engineering design, safety investigations have been providing feedback from reality by exploratory reconstructions and analytical interpretations of facts and findings derived from accident investigations. Challenging design assumptions, model simplifications and operational restrictions in examining the validity of this knowledge store have contributed to the growth of design knowledge. Through safety investigations, systemic and knowledge deficiencies were identified, leading to novel safety principles in engineering design. Eventually, this has led to Knowledge Based Engineering as a specific school of design thinking (Torenbeek, 2013).

The search for performance optimization and reduction of uncertainties has created a continuous exploration of design variations and selection of better performing design solutions. This has created generations of commercial and military aircraft designs with similar morphology, configurations and properties. Such solutions can either have a derivative or disruptive nature. Vincenti elaborates on the role of this *variation-selection* process in the innovation of aerospace design (Vincenti, 1994). Developing 'anomalies' should be considered in a historical context of design requirements, gradual changes in the operating context and consequences of design trade-offs. Although 'anomalies' may temporarily deviate from prevailing engineering judgement, specific concerns may force to deviate from this mainstream in exploring innovations. The variation-selection model of Vincenti takes it for essential and unavoidable that any search for knowledge that is new, that is not attained before, must involve an element of what is called 'unforesightedness'. The outcome cannot be foreseen or predicted when the variant is proposed. Foresight on performance has been both tested at the component and subsystem level prospectively by modelling and simulation and retrospectively by flight testing and operational feedback. Such 'unforesightedness' comes with balancing gains as well as costs. The outcomes of such a balancing may favour specific design trade-offs, but should be considered in their historical context and operational demands. As speed increased, drag became dominant in the design trade-offs in designing retractable gears. The generalized knowledge that retractable gears were favourable, was the product of an unforesighted variation-selection process and was valid for a specific class of aircraft designs (Vincenti, 1994). Similar trade-offs in context can be observed in the design of modern commercial aircraft in balancing weight and fuel consumption versus structural integrity and dynamic stability (Torenbeek, 2013). Flight envelope protection was introduced to refrain the pilot from entering the margins of the operational envelope at the cost of loss of pilot situation awareness in critical situations (De Kroes and Stoop, 2012). The application of automation in cockpits has a proven track record of substantial gains in safety, efficiency and accuracy, but comes at a cost of loss of pilot situation awareness in critical situations, increased cognitive task loads and loss of basic flying skills. The notion of 'unforesightedness' has not yet been expanded from the component to the systems level.

3. Socio-technical systems engineering challenges

The driving forces for enhancing safety foresight come from both within a sector and

without. From within, improvements in technology and a need for awareness of potential negative effects of technology drive the need to understand the causes of accidents. From without, public trust, political pressure and international coordination drive the need to prevent and mitigate accidents. For commercial aviation, all of these came together at the same time -as the need for interoperability, punctuality and reliability, international determination of responsibility and responding to the inherent human fear of being in the sky- and converged to demand the highest standards of proactive safety. Such safety foresight had to cope with system properties of both a legal, social and technical nature.

3.1 Legacy systems and 'early warnings' of safety performance

In designing complex socio-technical systems, due to their legacy nature and dependences on other systems, there is no opportunity for real time and full scale testing during introduction and adaptation. Apart from their complexity, there are unacceptable consequences of fault and failure propagation of disruptions through a global network that operates on a 24/7 basis. The vulnerability of such systems is a critical parameter in assessing the consequences of change and adaptation. Such vulnerability is assumed to be caused by unpredictable and unnoticed interactions between system components. According to Dekker, 'drift into failure' is a gradual, incremental decline into disaster driven by environmental pressure, unruly technology and social processes that normalize growing risk (Dekker, 2011).

However, due to a lack of understanding of its incubation, 'drift into failure' inevitably makes a conventional trial and error approach inapplicable in high technology network systems. Such a trial and error approach should be replaced by a predictive approach on a systems level of performance. Applying 'early warnings' of mishaps to prevent a 'drift into failure' during final phases of the design and construction or during normal operations is too late an intervention. Huge costs will occur for control and modification after detection of unacceptable deficiencies and deviations. Consequently, 'drift into failure' is an obsolete construct in controlling and explaining 'emergent properties' in high technology systems. This construct should be replaced by structuring system development and positioning of safety assessment tools and techniques at specific points in each phase of the design, development and operations of such systems. In creating new solutions with predictive potential on safety foresight, several with respect to safety so far unchartered scientific domains and disciplines have to be mobilized. Based on aerospace engineering experiences serious candidates are simulation and prototyping, forensic engineering, value operations methodology and state/space vector modelling (Vincenti, 1990; Torenbeek, 2013).

Analysing the complexity of socio-technical systems, the notion of 'drift into failure' is frequently used as an explanation of 'emergent' behaviour (Dekker, 2011). The underlying notion of the 'incubation period' of such a drift before it emerges as a unanticipated property, remains undefined, unmeasurable and does not cover the dynamics of such a drift. This 'drift into failure' lacks the description and explanation of a triggering event and conditions that sets a sequence of events in motion. The margins and boundaries that separate regular performance from emergent failure remain undefined and hence, uncontrollable. The concept of state/space vectoring of safety events has been conceptually formulated as a potential answer to these issues of

safety margins (Stoop and Van der Burg, 2012). State-space modelling serves the identification of performance boundaries and dissimilarity distances between safe and unsafe performance by introducing vulnerability and margins to system boundaries under specific conditions (Van Kleef, 2017). To communicate about safety, actors have to agree on system states and margins to boundaries, using design requirements and specifications as starting points. Introduction of limit states, operating envelopes and viable envelopes facilitate understanding of margins for prevention and recovery. Such a state/space modelling approach defines safety as a social construct within physical boundaries and operational conditions. Simultaneously, such an approach defines the resilience margins for system recovery and complies with the European codes for technical safety directives and safety integrity levels (Van Kleef, 2017). This state/space vector approach enables quantification of survivability margins to operating limits and a measurable comparison between various system states. Such an approach does neither rely on a normative judgement on acceptability of risks, nor on quality of design or performance.

An adequate definition of the notion of 'state' is given by systems theory. The state of a vector $\vec{x}(t)$ in its present situation can be described, based only on the information and control based on the previous situation. We only need this information to predict the future state of the vector. The dynamics of the system can be described with a state-space equation:

$$\frac{d}{dt}\vec{x}(t) = f(\vec{x}(t), \vec{u}(t), \vec{d}(t), t) \text{ and } \vec{x}(k+1) = f\big(\vec{x}(k), \vec{u}(k), \vec{d}(k), k\big).$$

In this equation $\vec{u}$ is the control vector and $\vec{d}$ the disturbance. This first equation is the continuous time version, while the second is the discrete or event based version, in which k is the actual event.

Rather than just stating *safety factors* we now have a concept of real system safety related *events* having an impact magnitude and a directional bias relative to the dimensions of the system model. The model suggests multi-vectorial design solution spaces which have meaning relative to the dimensions of safety in terms of the contribution or impact within each dimension and the overall resulting orientation or direction of the safety issue being considered. Consequently, safety is significantly elevated from the very basic consideration as a factor, to a new level where it is being quantified as a multi-dimensional quantity with a resulting orientation that defines the choice of the designer or operator relative to their values regarding safety. With reference to the Value Operations Methodology, this leads us to the position where safety can be integrated into the general design approach of the air transport system according to an equation relating KPI to some delta value of the form:

$$\Delta V = \alpha_C(C_1/C_0) + \alpha_U(U_1/U_0) + \alpha_M(M_1/M_0) + \alpha_E(E_1/E_0) + \alpha_P(P_1/P_0) + \alpha_S(S_1/S_0) + \varepsilon$$

where *Cost efficiency* is represented by *C* (revenue/cost), *Utilization* by *U*, *Maintainability* by *M*, *Environmental Quality* by *E*, *Passenger Satisfaction* by *P*, Safety by *S* and finally including an *error* ε, consideration. Consequently, safety as a function of: safety = fn (context, culture, content, structure, time), can be characterised with the individual drivers associated with each dimension so that safety in its vectorial and

most realistic form can be integrated into the overall integrated system of systems design solution space. In shifting from factor towards vector, safety critical behaviour of open and dynamic systems can be analysed by identifying inherent properties during design before they manifest themselves as emergent properties during operations. By doing so, safety can be assessed and optimized pro-actively as a critical strategic value against other system values in a dynamic and complex systems perspective. This approach substantiates the notion of foresight.

3.2 High energy density systems

Socio-technical systems must be safeguarded by design due to their specific characteristics as a distinct category of high energy density complex systems. Management of the operational energy that is stored in the system is a challenge that must be controlled proactively throughout all system states, mission phases and operating constraints.

Due to the increase in size and scale of modern socio-technical systems, the uncontrolled release of energy in a specific event can result in catastrophic material consequences and loss of all lives of a large population at risk, both inside and outside a system. The operational energy stored in complex systems can be expressed in Megawatts as the sum of kinetic and potential energy. The energy content of a High Speed Train and a Jumbo jet that has to be controlled during operations can be compared to nuclear power plants with respect to their catastrophic potential, as depicted in Table 1.

Table 1 Operational system energy content

	Weight	**Speed**	**Altitude**	**Energy**
High Speed Train	430 tons	250 km/h	ground level	1053 MW
		320 km/h	ground level	1740 MW
A380 Jumbo jet	MTW 575	900 km/h	10.000 m	75 000 MW
	at take-off MTOW 575 tons	260 km/h	ground level	1500 MW
	at landing MLW 386 tons	260 km/h	200m above ground level	1252 MW
Nuclear power plant	Average size			800 MW
	Borsele (Neth)		Sea level	450 MW
	Chernobyl		Sea level	600 MW
	Fukushima		Sea level	784 MW

Such an operational energy management strategy is interesting in particular in aviation with respect to the balance between kinetic energy due to the airspeed control and potential energy due to the altitude and attitude control. The operational energy of an aircraft has to be controlled and dissipated back to zero in order to bring the flight to a safe end. This kinetic and potential energy distribution varies across the various flight phases. This means that the energy balance management in the cruise flight phase is based for 25% on the speed control and for 75% on the altitude and attitude control. During final approach and landing, the potential energy reduces from 75% at cruising altitude to 19.6% of the total energy content. The energy ratio between theses phases

subsequently changes from potential energy management towards a predominant kinetic energy management by keeping control over speed and attitude.

3.3 Intrinsic systemic hazards

From the early days of aviation, stall has been an inherent system hazard. Otto Lilienthal crashed and perished in 1896 as a result of stall. Wilbur Wright encountered stall for the first time in 1901, flying his second glider. These experiences convinced the Wright brothers to design their aircraft in a 'canard' configuration, facilitating an easy and gentle recovery from stall. Over the following decades, stall has remained as an intrinsic hazard in flying fixed wing aircraft. Stall is a condition in which the flow over the main wing separates at high angles of attack, hindering the aircraft to gain lift from the wings. Fixed-wing aircraft can be equipped with devices to prevent or postpone a stall or to make it less (or in some cases more) severe, or to make recovery easier by training and certifying pilots.

A further analysis reveals some more fundamental flight performance issues (Obert, 2009):

- All stall recognizing and mitigating strategies have not eliminated the stall as a phenomenon; major stall related accident still occur

- Airspeed indications rely on the use of Pitot tube technology. Applications of a new technology such as GPS provides redundancy in air data information

- In contrast with roll and yaw control, pitch control of aircraft is not redundant. There are no substitute strategies for controlling pitch of commercial aircraft, in contrast with the military, where thrust vectoring is an option

- Angle of Attack in commercial aviation is a secondary parameter, derived from Indicated Air Speed. There is no direct alpha indicator, in contrast with the military

- 4th generation civil aviation aircraft lack the ability to create a negative pitch moment throughout the flight performance envelope by having direct access to speed and attitude as safety critical flight parameters.

Despite all efforts to reduce stall and deep stall to acceptable levels of occurrence, such events still happen occasionally in the commercial aviation community, raising concern about their emerging complexity, dynamics and impact on public perception on safety of aviation (Salmon, Walker and Stanton, 2016). Such events have been subjected to major accident investigations are swerve as triggers for change throughout the industry. Most recent cases are Turkish Airlines flight TK1951, Colgan Air flight 3407, Air France flight AF 447, Air Asia flight 8501 and Air Algerie flight 5017.

In a debate on high-altitude upset recovery, Sullenberger –captain of the Hudson ditching of flight US 1549- described stall as a seminal accident. "We need to look at it from a systems approach, a human/technology system that has to work together. This involves aircraft design and certification, training and human factors. If you look at the

human factors alone, then you're missing half or two-thirds of the total system failure...".

4. Beyond 10^{-7} safety

4.1 Derivatives versus disruptives: the Valley of Death

The responses of aircraft manufacturers to stall have been different. Airbus took a different approach in designing the Primary Flight Display (PFD) than Boeing with eventually, equal safety performance levels. Airbus designed alpha floor protection in the fly by wire concept, which should greatly reduce opportunities for stall by automatically adjusting pitch and power to counteract the stall. Boeing choose to address pilot recognition of an impending stall. The Asiana B 777 accident demonstrated that pilots my fail to recognize low energy states preceding a stall, much as the Air France A330 accident demonstrated that alpha floor protection may fail due to unreliable speed and altitude sensors. By applying existing technology and design features that are incorporated to mitigate stall consequences, neither approaches are fail safe.

The introduction of Glass Cockpits and 3D Flight Displays have improved the navigation task of pilots considerable, but have not simultaneously improved the pilots' attitude towards spatial and situational awareness (Lande, 2016).

Manufacturers have reduced the workload of pilots and introduced the flight envelope protection to avoid entering a stall situation. However, stall and deep stall as a low speed/high alpha flight condition are inherent to the physical properties of fixed wing aircraft, similar to vortex ring state conditions for helicopters. A safe escape from such inherent flight conditions requires basic knowledge of pilots on aerodynamics and flight mechanics. Disorientation and confusion may lead pilots into loss of attitude awareness. The availability of a large and intuitive Primary Flight Display with an Angle Of Attack indicator, integrated in the Basic-T configuration may enable a pilot in a quick regain of control by providing the pilot with situational awareness (Lande, 2016). According to Lande, future PFD's should be based on a synthetic picture of the outside world with overlaid prominent and transparent primary flight instruments, including an AOA indicator. It enables the pilot to gain a 3D attitude awareness. Apart from flying in non-normal conditions spatial disorientation may also be caused by somatogravic and somatogyral illusions. The strongest visual cue a pilot has becomes absent in visual flight in darkness, where reliance on flight instruments becomes critical in absence of a natural horizon.

In the discussion on a recent series of accidents, the focus has been on pilot knowledge and skills and less on Primary Flight Display design. Developments in glass cockpits and data integration provide an opportunity to explore issues in situation awareness, spatial disorientation, automation attitude and team work for a next generation of aircraft handling and cockpit design (Mohrmann et.al., 2015). Trade-offs, based on cost-benefit considerations however, depend on customer acceptance, cost awareness and public confidence in the safety of aviation. Introducing safety enhancement design solutions is submitted to a complex interaction between design, manufacture, operation costs and societal appreciation of safety. The outcomes of such trade-offs define whether it is possible to introduce either a derivative or a disruptive solution. Most innovative and disruptive solutions that are developed technically successful, do not

survive the Valley of Death in their implementation phase due to such considerations (Berkhout, 2000).
In elaborating visual interpretation of information, a series of disruptive concepts can be considered potential game changers in enhancing flight safety. These game changers supersede the level of intervening either in the man or the machine component of complex and dynamic sociotechnical systems. They are frequently discussed in attempts to cross the 10^{-7} boundary. Such concepts deal with Angle of Attack indicators, Intuitive Primary Flight Display, recovery from non-normal flight situations, asymmetric flight, Total Energy Management Systems and Good Airmanship substantiation. These disruptive designs however, died in beauty in the Valley of Death between their invention and implementation due to a lack of a transition strategy and integration at a systems level.
While pragmatic solutions have achieved a high level of sophistication in stall mitigation and recovery, a more fundamental approach to stall avoidance should be developed in order to deal with this intrinsic system property. A new unit of analysis of flight control should be applied, combining both design of man, machine and their interfaces (Woods, 2016). Such a unit of flight control enables integration of disruptive designs into a new man-machine-interface concept. An innovative solution to this more fundamental issue should comply with principles of dynamic flight control over the fundamental forces that are exercised on general aviation and commercial aircraft and the feedback to the pilot in a combined intuitive and cognitive decision making (Stoop and De Kroes, 2012).

4.2 The Kestrel concept

In leaving the Valley of Death, similarities with bird flight control enable a integration of several of the disruptive designs into the Kestrel concept, consisting of:

- Introducing new aerodynamic forces instead of manipulating existing forces
- Introduction of such aerodynamic forces in uncorrupted air flow
- Generating high pitching moments by small forces combined with long arms
- Introducing correcting forces only in case of emergency.

An innovative design is suggested, based on these principles of dynamic vehicle control (De Kroes, 2012). The design combines four building blocks as engines for foresight; understanding flight dynamics, integral systems approach, total energy management and intuitive man-machine-interface design. This design is called the 'Kestrel' concept, aiming at creating redundancy for physical lift generation by stall shields during high Angle of Attack conditions, supported by dedicated software for the integral man-machine-interface flight control unit (see fig 1.).

Assessment of the 'Kestrel' concept as a feasible and desirable innovation can only be done in the early phases of conceptual design on a consensus base. Discussing the issue of stall and remedies for stall related accidents cannot be allocated to a single actor or isolated contributing factor.

Feedback from operationally experienced people such as pilots and accident investigators provide insights in the actual responses of the system under specific conditions that cannot be covered by an encompassing proactive survey during design and development.

Fig 1. The Kestrel concept

5. Conclusions

In answering the initial question, *How did aviation become so safe*, an analysis of the history of aviation shows a preoccupation with safety from the beginning, because of the intrinsic hazards involved in flying. Foresight has been designed into the aviation system from the start on.

Several characteristics have favoured a foresight on safety as a strategic design value, based on retrospective experiences:

- Institutional arrangements at a sectoral level, such as ICAO and its Annexes structure
- Harmonized legal responsibilities at the national State level
- Integral safety performance indicators throughout the system life cycle phases
- Feedback from reality by learning from mishaps, accidents and incidents
- Selecting technology as the flywheel for progress created a shared body of knowledge during design and operations, substantiated in a KBE design methodology
- Application of a 'variation-selection' process in experimental exploration of technological innovation and disruptive design solutions.

In replying to *And Beyond* and to enable crossing the mythical 10^{-7} risk boundary in aviation, innovative strategies should be explored to facilitate a prospective foresight on safety:

- Application of system engineering principles and state-space modelling approaches;
- Shifting from safety performance indicators to system properties and design principles;
- Recognition of game changers and transition strategies in order to surpass Valley of Death traps in implementing innovations and disruptive solutions;
- Exploring disruptive variations to substantiate their integration at the conceptual design level in creating a new unit of man-machine-interfacing design concepts, such as the 'Kestrel' concept.

References

Berkhout, A., (2000). *The Dynamic Role of Knowledge in Innovation*. The Netherlands Research School for Transport, Infrastructure and Logistics TRAIL, June 2000. Delft University of Technology.

Boosten, G., (2017). The (Congested) City in the Sky. The capacity game: Finding Ways to Unlock Aviation Capacity. Amsterdam University of Applied Sciences.

Cairns, (1961) Report of the Committee on Civil Aircraft Accident Investigation and Licence Control. Ministry of Aviation, Her Majesty's Stationary Office, London.

Dekker, S., (2011). Drift into Failure. From Hunting Broken Components to Understanding Complex Systems. Ashgate Publishers

De Kroes J.L., (2012). Commercial plane or flight simulator, adjustable fuselage control surface, computer program product and method. Patent P96519NL0, deposited on 10 Jan 2012

ETSC, (2001). *Transport accidents and incident investigation in the European Union*. European Transport Safety Council. ISBN 90-76024-10-3, Brussels

Flanagan, (1948). *The aviation psychology program in the Army Forces*. Washington D.C. Air Force, 1948

Freer, (1986.1). The roots of internationalism 1783 to 1903. *ICAO Bulletin, Vol.41 No.3, March 1986*, pp.3-32.

Freer, (1986.2). En-route to Chicago, 1943-1944, *ICAO Bulletin, Vol.41, No 7, July 1986*, pp.39-41

Freer, (1994). ICAO at 50 years: Riding the Flywheel of Technology. *ICAO Journal Vol.49 No 7*, September 1994, pp.19-32

Hengst S., Smit K. and Stoop J., (1998). Eds Proceedings of the Second World Congress on Safety of Transportation. 18-20 February 1998. Delft University of Technology.

ICAO, (2001). Aircraft Accident and Incident Investigation, Annex 13 to the Convention on International Civil Aviation. International Standards and Recommended Practices. Ninth Edition, July 2001

Kahan J., (1998). Safety Board Methodology. In: S. Hengst, K. Smit and J.A. Stoop (Eds) *Proceedings of the Second World Congress on Safety of Transportation. 18-20 february 1998*. Delft University of Technology.

Lande, K., (2014). Aircraft Controllability and primary Flight Displays – A Human Factors Centred Approach. European 46th STEP and 25th SFTE Symposium, 15-18 June Lulea, Sweden

McIntyre, G., (2000). *Patterns in safety Thinking*. Ashgate

Mohrmann F., Lemmers A. and Stoop J., (2015). Investigating Flight crew recovery Capabilities from System Failures in Highly Automated Fourth generation Aircraft. Aviation Psychology and Applied Human Factors, Vol 5(2), 2015

Petroski, H., (1992). To Engineer is Human. The Role of Failure in Successful Design. Vintage Books, New York

Roed-Larssen, Stoop and Funnemark (2005). *Shaping public safety investigations of accidents in Europe*. An ESReDA Working Group Report. Det Norske Veritas.

Smart, K., (2004). Credible investigation of air accidents. Special Issue of the Journal of Hazardous Materials. Papers from the JRC/ESReDA Seminar on Safety Investigation of Accidents, Petten, the Netherlands, 12-13 May, 2003. Vol 111 (2004), 111-114.

Obert, E., (2009). Aerodynamic Design of Transport Aircraft. IOS Press 2009

Salmon, P.M., Walker, G.H. and Stanton, N.A., (2016). Pilot error versus socio-technical systems failure: a distributed situation awareness analysis of Air France 447. Theoretical Issues in Ergonomic Science, 17 (1), pp 64-79

Stoop, J.A. and De Kroes J.L., (2012). *Stall shield devices, an innovative approach to stall prevention?* Proceedings of the Third International Air Transport and Operations Symposium 2012. Delft, 18-20 June 2012. Ed. R. Curran, Delft University of Technology.

Stoop, J.A. and Van der Burg, R., (2012). *From factor to vector, a systems engineering design perspective on safety*. PSAM 11 and ESREL 2012 Conference on Probabilistic Safety Assessment June 25-29, Helsinki, Finland

Torenbeek, E., (2013). Advanced Aircraft design. Conceptual design, Analysis and Optimization of Subsonic Civil Airplanes. Wiley Aerospace Series

Van Kleef, E. and Stoop J.A., (2016). *Life cycle analysis of an infrastructural project.* 51th ESReDA Seminar on maintenance and Life Cycle Assessment of Structures and Industrial Systems, 20-21 October, Clermont-Ferrand France

Vincenti, W., (1990). *What Engineers Know and Hoe They Know* It. Analytical Studies from Aeronautical History. The John Hopkins University Press.

Vuorio A., Stoop J., and Johnson C., (2017). The need to establish consistent international safety investigation guidelines for the chemical industries. Safety Science 95:62-74, July 2017

Wittenberg, H., (1979). *Safety in aviation; achievements and targets*. Memorandum M-353, Faculty of Aerospace Engineering. Delft University of Technology.

Woods, D.D., (2016). *Origins of Cognitive Systems Engineering*. P. Smith and R. Hofman (Eds). Cognitive Systems Engineering: A Future for a Changing World.

On some issues related to the safety margin and the process of safety foresight for the nuclear power plants

Dan Serbanescu

Romanian Academy, Division of Logic and Models – DLMFS-CRIFST

Drumul Taberei 35A

061358, Bucharest, Romania

Abstract

The paper presents some insights from the author's research results on reviewed issues related to the level of Risk and Safety Margins (SM) for Nuclear Power Plants, regarded as complex systems. The overarching approach to safety review is presented and it is illustrated on some practical real cases. The focus is on the aspects like the specifics of the SM evaluations for various lifecycle periods, the iterative process of such evaluations, the consideration of human factors, being part of the model itself. It is also illustrated, that for real cases, this approach was (for several decades of the author's experience) the basis for foresight in safety in various projects of nuclear installations in various lifecycle phases.

Keywords: Safety margin, risk, topological space, human factors, nuclear installations.

1. Introduction

There were important developments in the last time in the study of complex systems and the theories derived from applied physics related to them. In this respect, the applied nuclear science, along with the cavalcade of models in modern physics shad a new light on the issue on *"What type of better high energy systems we want to build and how to improve their performance?"*. These goals are tightly connected with the need to build such systems, which have less harmful impact on the population, environment and the workers. As in the fundamental science research, in the nuclear engineering and its associated technologies (artificial intelligence, environment protection etc.) there is a trend to consider fundamental changes in the research and practical engineering activity, i.e. to switch from almost four centuries of the old scientific approach *"Discours de la méthode"* to a new one *("Discours sur la création de la réalité"*[1;2]), in which the observer and the object under design / review / operation are very closely connected and sometimes it is highly difficult to separate them – a speech very well understood by the Artificial Intelligence (AI) specialists and high tech domains increasingly using AI.

One important aspect of this switch is the capability to find new solutions (for improved systems for instance), based on the search for key answers in some deep (miss) understandings / biases / "myths", previously taken for granted, on various issues, including "*How harmful are those systems"* and "*How to evaluate this?"*.
The new approaches allow a *more systematic and preventive insight on the potential safety issues for complex systems*.

In this context and with this new perspective this paper is presenting some insights on significant moments and aspects for a set of specific complex systems (presented in [3]) and their impact on the people, environment and workers: the nuclear power plants (NPP) and the issue of their safety. In previous papers a set of connected aspects to those issues were considered [2; 4], as follows:

- The specifics of risk and safety analyses for NPP

- Interface and sometimes "clashes" with other technologies (like digital in nuclear installations, IT and security issues etc.), as well as combined risks evaluations.

- Realizations on the deep "messages" from natural installations existent before even humans existed, like for instance lessons from natural reactors (Oklo theories and some Mars discoveries)[7].

- *"Oikinomia" as a guiding rule on security of energy supply* and the need to rethink the whole energy lifetime and chain aspects, or in other words lessons from ancient societies to the modern societies on energy issues.

- Interfaces with human factors(HOF) (management approaches changes, safety culture, leadership attitudes changes etc.)

- Real actual acknowledgment of the fact that developers of new nuclear technologies realize that they will be in place in the next century, i.e. in another environmental conditions, *in different societies / civilizations than now, different human generations* and new even totally unknown with communication and living technology available (for example *"How a generation "Z" or "post Z"("Post zet generation") person from (let us say 2085) will look at and use/operate the control room of a 2020 NPP design ?").*

2. Method

The safety of a NPP is measured by functions, which depend on many features, including those defined by the design and operation of a NPP, in a concept of various layers of protection, called Defence in Depth (DiD). An important component considered in the evaluation of the efficiency of the DiD protection is "Safety Margin" (SM). In some type of evaluations this criterion is consider to be in a biunivoc correspondence with another one called "Risk" (Risk is defined as a criterion measuring the damage produced by the challenges to the NPP considering the probability of occurrence of those challenges).

In general, the SM evaluations are performed at the design phase and monitored and reviewed continuously during operation. There are therefore SM obtained in one iteration and SM obtained after a series of iterations, which are dependent of time (the NPP lifecycle time). A sample of such criteria considered for SM evaluations is in Figure 1. As illustrated in Figure 1 the SM criteria are actually defined by groups of criteria, which could be considered of having common features (defining a "facet", i.e. technical facets – 1 and 2 or organizational – society facets 3-6). They define a space of possible variation of the degree of safety included in the 3D figure.

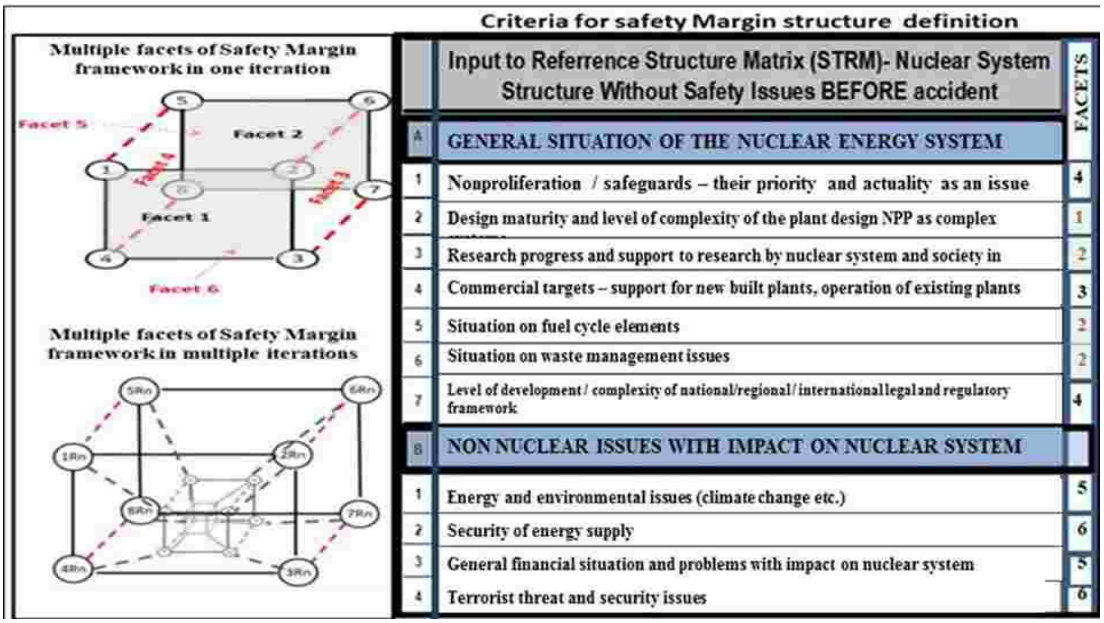


Figure 1. Criteria for defining Safety Margin (SM) in a NPP.

This paper presents two main author's ideas related to the foresight in safety for the case of nuclear power plants (NPP), as regarded from the perspective of an insider involved in various practical projects over a period of three decades:

The **NPP history** is seen as a **history of a technology** (being subject to be described by ***s-curve***). From the perspective of NPP as a technology there were a series of important milestones of the dominant safety approaches in considering Safety Margin (SM) and/or Risk and trying to foresee which the best strategies to cope with safety challenges are. **These milestones are described for the phases of the technology: Creation, Infancy, Maturity, End of Life (EOL).**
For each phase dominant approaches to judge SM and project actions for **safety foresight** evolved as follows:

- Point like reference (setting values as targets not to be exceeded and judging SM based on the distance to a predefined level) - specific for "infancy" period

- Curve like defining an acceptable area for a dominant variable of the definition of SM. Various parameters considered in sensitivity analyses. SM is defined as belonging to an acceptable surface, specific for end of "infancy" and beginning of maturity.

- Sophisticated multivariable description of the SM, were the acceptable zone is defined as an acceptable volume, specific for end of maturity and getting closer to end of life. In the maturity period an attempt to consider HOF is made but the issues lead to the inclusion of the "observer" in the safety model, making foresight difficult if not impossible, due to questionable level of objectivity. On the other side making systems more sophisticated gets to the point where the changes lead to an area of complex system of chaotic behavior, with the warning that there is a limit of safety improvements to increase / improve foresight for safety of a complex system like NPP.

The NPP and nuclear engineering in general has to be considered from what it actually is: a technology. For this technology the evaluations on its evolution, the evaluations on safety and the foresight on its safety have to consider the effect of lifecycle evolutions specific for any technology, as shown in [2;4;5]. Based on the author's experience [2], there are three periods of the NPP lifecycle, which are significant for the approaches used to evaluate their SM:

- Point like reference (setting values as targets not to be exceeded and judging SM based on the distance to a predefined level) - specific for "infancy" period

- Curve like defining an acceptable area for a dominant variable of the definition of SM.Various parameters considered in sensitivity analyses. SM is defined as belonging to an acceptable surface, specific for end of "infancy" and beginning of maturity.

- Sophisticated multivariable description of the SM, were the acceptable zone is defined as an acceptable volume, specific for end of maturity and getting closer to end of life. In the maturity period an attempt to consider HOF is made but the issues lead to the inclusion of the "observer" in the safety model, making foresight difficult if not impossible, due to questionable level of objectivity. On the other side making systems more sophisticated gets to the point where the changes lead to an area of complex system of chaotic behavior, with the warning that there is a limit of safety improvements to increase / improve foresight for safety of a complex system like NPP.

There is an "**End of Life period (EOL)**", when the challenges to consider more and more sophisticated combinations of challenges leads to a degree of complexity of the artefact, that triggers the level after which chaotic behaviour is most probable [2;4]. Those periods and theirs specifics are represented in Figures 2 and 3. The figures illustrate safety paradigms evolutions during the lifecycle and after major accidents and the adopted in each period safety oversight strategies to improve safety. The focus is on the criteria and decisions taken on SM.

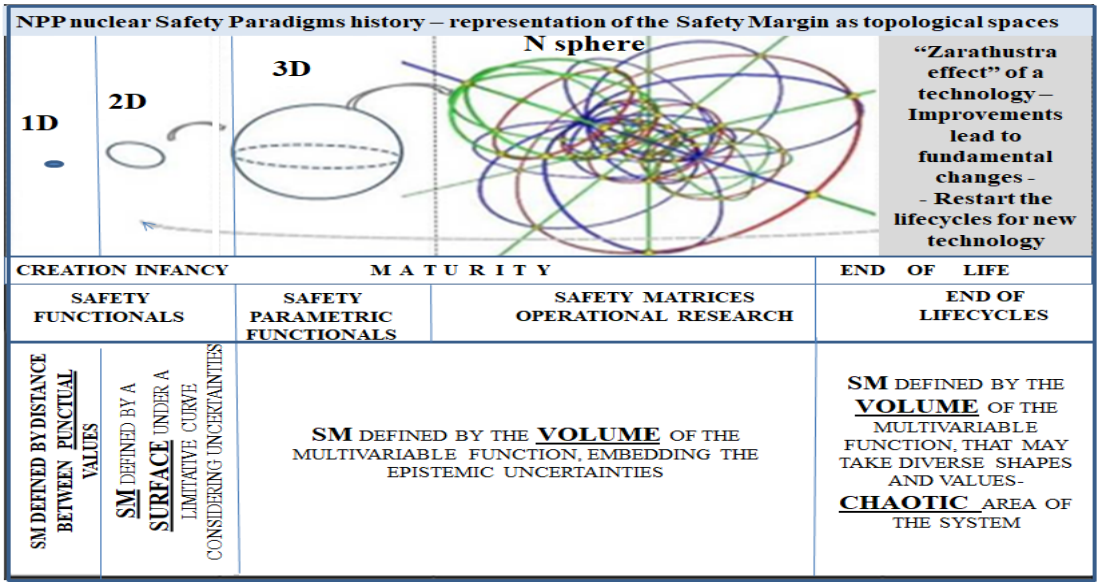


Figure 2. Lifecycle evaluation functional for SM

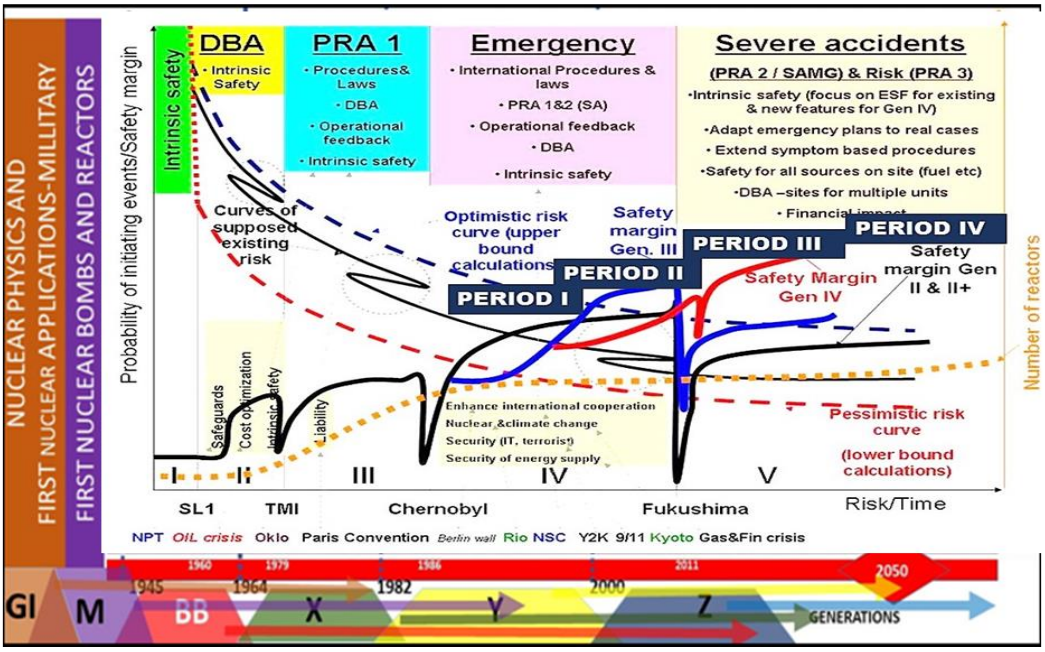


Figure 3. Safety paradigms and SM approaches for NPP [2; 4]. The periods are those reported by the author for the projects in which he participated [2; 4]

The assumptions and the methodological features of the safety evaluations (for the particular case of SM) and on the safety oversight strategies for NPP, as decided during the last decades, have therefore, in the author's opinion, a set of specifics:

- They had to solve a diversity of safety governing issues in various periods and to define strategies for the foresight on safety for the next periods in order to improve safety of NPP. This lead to a diversity of methods. However the consideration of SM from the perspective of NPP technology as an evolving one gives a very

interesting, unifying set of insights on the past history and possible actions for the future.

- A series of actions taken before acknowledgement of the new possible methodological approaches are now very clearly aligned to a series of dominant strategic approaches, as for instance: systemic approach to NPP safety, the need for consideration of complexity, including the HOF impact of high non linearity type on the SM / Risk modelling.

- Improvement of mathematical tools to make them adaptable to a higher complexity of safety evaluations and safety foresight tasks

- Recognition and consideration of the lifecycle period specifics as an important factor to the development of methods.

The result of those specific features leads to a diversity of a "mushroom" type (apparently annoying) of methods, that do not discard in the author's opinion, but enhance the point, that their diversity, governed by some principles mentioned before, makes them specific for the nuclear safety evaluation status of the last decades and for the predictable foresight strategies of the near future.
However even if there is diversity, in the author's opinion based on practical use of safety evaluations, participation in the safety decisions for real NPP cases and foresight on safety for future built, there is a unifying feature of all those diverse methods.

These unifying features consist of the following:

- They had to solve a diversity of safety governing issues in various periods and to define strategies for the foresight on safety for the next periods in order to improve safety of NPP. This lead to a diversity of methods. However the consideration of SM from the perspective of NPP technology as an evolving one gives a very interesting, unifying set of insights on the past history and possible actions for the future.

- A series of actions taken before acknowledgement of the new possible methodological approaches are now very clearly aligned to a series of dominant strategic approaches, as for instance: systemic approach to NPP safety, the need for consideration of complexity, including the HOF impact of high non linearity type on the SM / Risk modelling.

- Improvement of mathematical tools to make them adaptable to a higher complexity of safety evaluations and safety foresight tasks

- Recognition and consideration of the lifecycle period specifics as an important factor to the development of methods.

3. Results

The results applying the diversity of methods on SM / Risk for some real cases of practical value in the last decades are presented in this part.

3.1 SM evaluations for the "Infancy period"

3.1.1 SM evaluations by using Risk and /or equivalent to Risk criteria

SM methods during this period evaluated the dependence of the margin to imposed limits of safe operation on one variable and a set of parameters considered relevant for the impact on SM. For instance if the criterion used is the "Risk "[9;10], then during the late infancy period the area below the curve (the type of variation and its magnitude) was considered to be an indicator on the achieved level of SM.

Various type of plant characteristics as variables of the SM function might be used. In order to make the choice on the dominant parameter, the NPP is regarded from various diverse perspectives. For instance schematic cybernetic representations are made or a model called Reliability Equivalent Diagrams (RED) and accident scenario [2] description are used. In order to evaluate the safety features for such models specific methods were developed, as for instance the method called Probabilistic Safety Analyses (PSA) (from the vast literature the author is mentioning some of its own PSA models [2]).

Another possible set of approaches is to consider NPP model as a cybernetic machine or a thermodynamic machine [4] (as in the case represented in Figure 3 for a generation IV NPP called Pebble Bed Module Reactor (PBMR) [4; 9].

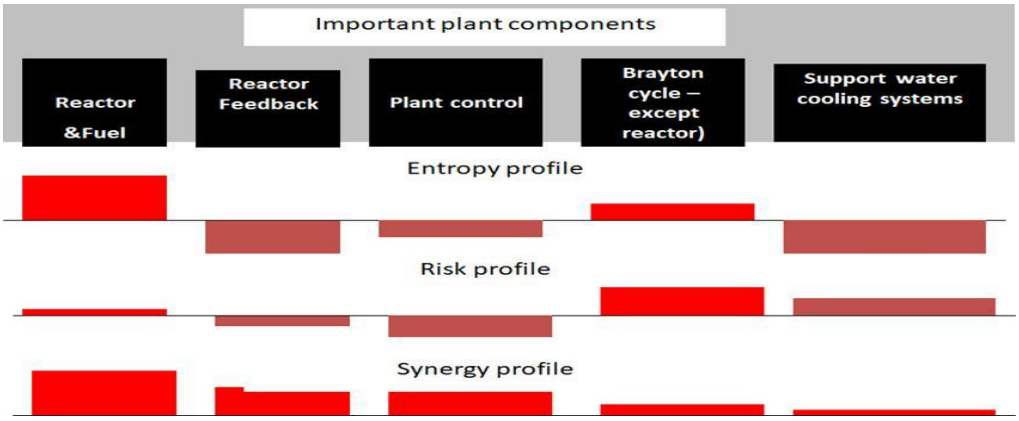


Figure 4. Comparison of various SM functional

NPP may be also considered as a special type of Complex System (CS), as modelled in [4]. In this case, the SM indicator, evaluated using "Risk", may be calculated as:

$$\text{Risk} = f\,(\text{PIE} * \text{PPR} * \text{Pd}) \qquad (1)$$

Where:
PIE - is the probability of the challenge to CAS, called Initiating Event (IE)
PPR - is a probability representing the system pattern for each IE challenge
Pd - is a normalized probability representing the damage produced by a given IE

The risk model is defined by the contribution of various minimal cut sets (MCS) to the global risk frequency. It shows that there is the following type of dependency on a certain probability of a given event:

$$MCS = pIE * (1 - g(pi)) + h(pi)) \quad (2)$$

Where:
pIE - is the probability of the event, for which various changes and impacts are evaluated during a specific analysis;
g(pi); h(pi)) – are functions of the probabilities of basic events other than pi

In [4] an amended risk criterion, defined as "synergy", was used for real cases of SM evaluations. This criterion is using information from the probability of events, the level of damage and the limits in epistemic knowledge, evaluated using the information entropy.

In any of the above approaches the goal is to evaluate a risk criterion (RC-formula (3)) versus the "Total Design and Operation" (TC-formula (4)) criterion (for instance "The delivered energy") and to find the areas were an optimum for both criteria are reached (Figure 5). The SM is evaluated, in this case, for a variable and no parameters.

$$y1 = c0 * e - c1x \quad (3)$$

$$y2 = c2 * xn \quad (4)$$

RC is considered versus TC for the SM evaluation process for a variable and no parameters.

In line with this approach, if parameters impacting on risk are considered, then the risk may be evaluated for a variable and a set of dominant parameters (Figure 5). This approach is illustrated by its use in the NPP risk optimization during the design phase [4], as in a case of PRA study for the generation IV NPP. SM was evaluated by calculating Risk in a study on new plant [4; 9; 10].

The Figure 5 illustrates the fact that, if we consider the parameters during sensitivity studies, then the acceptable space of safe situations of NPP (of PBMR type **is defined by** a 3D volume**, that was called in the study** "Risk Bowl" defined as an aggregate 3D risk criterion. **This is a general presentation of risk calculations of RC type (as per formula (3)) that is performed for all parameters considered fixed.**

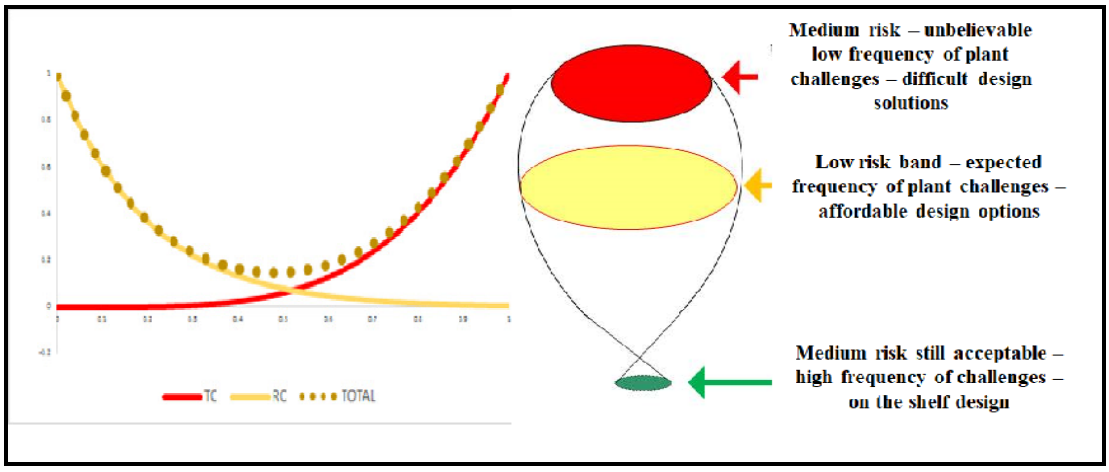


Figure 5. Risk bowl 3D risk representation [4].

3.1.2. SM evaluations by using feedback from operation

In [2; 4] an approach was used for the evaluation on the changes in dominant approaches in SM of NPP after major accidents. For this purpose the NPP history was considered from the point of view of its behaviour as a technology, described by a so called ***"s-curve"*** *(*Figure 6)

During major accidents from the NPP history so far, it was noticed that the **SM were reassessed,** as the real experience showed that **the initial margins** were not conservative [2]. Based on the expert review of the changes in the main directions in SM evaluations and focus after each major accident it was proposed **to consider a set of "safety paradigms"** specific for each phase after such an event [2; 5; 6] **and which were governing the safety oversight process for NPP for the next periods.**

It was also shown that the paradigms were connected with the changes in management structures, management styles, safety culture and leadership attitudes (Figure 3) [8; 12]. **The s-curve has the form for SM as defined by formula (4), while the drop in SM after a major accident is of (5) type.**

$$f_1(x) = \frac{a}{1 + e^{-bx}} \tag{5}$$

$$f_2(x) = c * e^{-x} \tag{6}$$

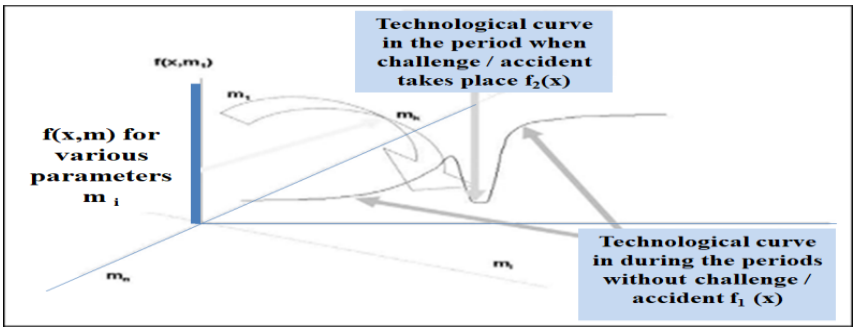


Figure 6. NPP as a technological curve considering challenges and falls of SM [2;4]

3.1.3. SM evaluations by using combined methods

A key issue for a better SM evaluation, prediction and monitoring is related to the method adequacy. From the vast literature on this topic some results obtained by the author will be mentioned [9; 10]. This issue is increasingly more important after each major accident, challenging the used methods for the SM evaluations and searching for their improvements. There are some main types of methods (if we exclude the lessons learnt from past: deterministic (D), probabilistic (O), operational feedback (O), and quantitative risk analyses (R), data-methodology-epistemic uncertainties (U). The combination of those methods leads to a set of "methods of various grouping (Mi) categories" (as illustrated in Figure 7). In [9; 10] it was shown that there are specific areas and criteria were each of the method is best fit (Figure 8).

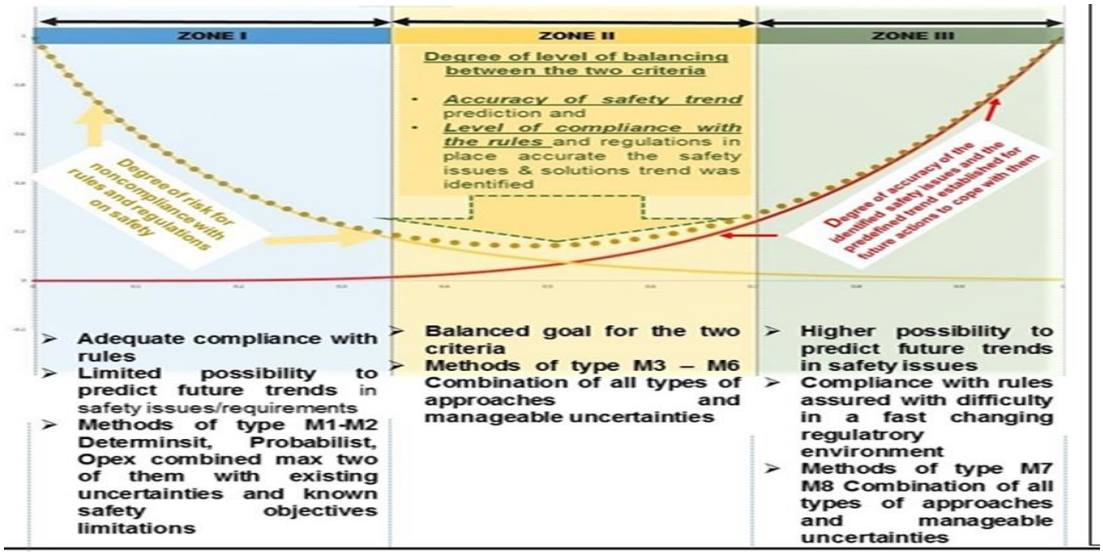


Figure 7. Areas of applicability for various methods in SM evaluations [9, 10]

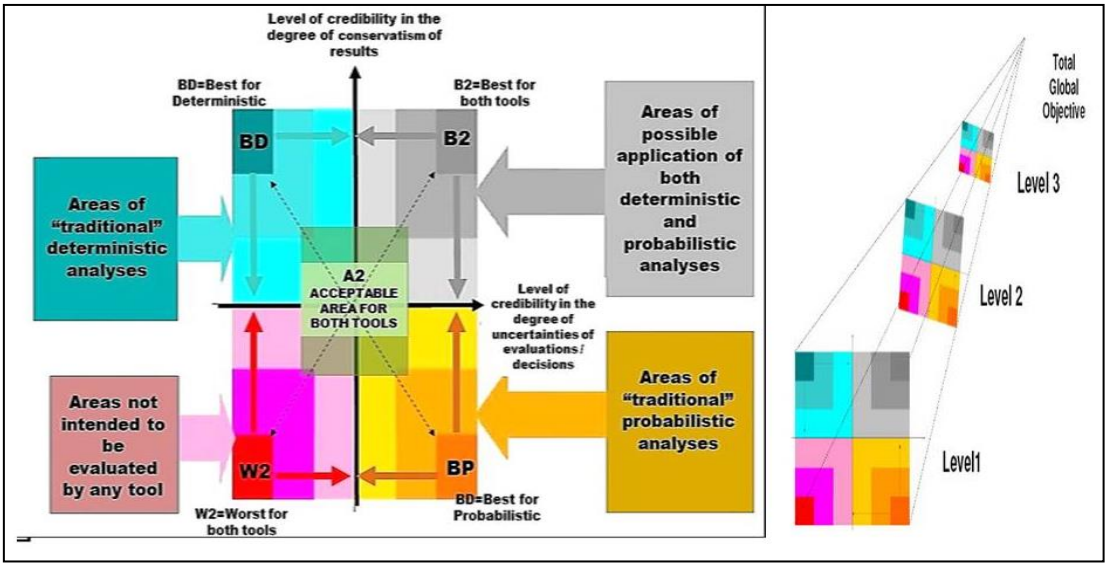


Figure 8. Areas of applicability for various methods in SM evaluations [9, 10]

For this approach of using combined methods, if the NPP model is considered to be a hierarchical one, then the **Risk evaluations are to be performed for the main components of the plant model and for each level and their combination**. The calculations are made by using combination rules for the defined criterion (in this case Risk). In those formulas usually the combination rule is a convolution integral, as the R functional is of probabilistic nature. **The total global criterion is considered after combining it at each level for all components and then it is combined between levels**. [9,10]. Each of those hierarchy levels generates in its turn a Complex System (CS) by itself and therefore, a systematic review of the adequacy of the method and compliance with the object to be **studied are required in order to confirm, that the methods used are compliant with the specifics of the CS.**

On the other side, **the risk evaluations performed using this type of modelling consist of a structured hierarchical process**, starting from defining the model at the first level, evaluating risks at the second level of the process and reviewing compliance of risk metrics with the imposed targets for them. This last level usually leads to a feedback review of the process for more detailed evaluations and / or changes in CS so that the targets will be met.

Multilevel / hierarchical risk model of a NPP [4]. For the author's experience during a set of three periods (Period I – Period III) of SM paradigm changes (as illustrated in Figure 3) a set of practical SM evaluation projects were performed as reported in [2;4]. The criteria used are in Table 1 and the summary of this activity is represented in Figure 9. **The self-assessment** of the SM evaluations as a whole is done by a **multicriterial analysis**. For the same set of evaluations detailed information on the specific methods used (PRA review, deterministic analyses review etc.) are in [9; 10]. The conclusions on the efficiency in safety foresight actions and safety decisions based on those evaluations are illustrated in Figure 9. **The figure illustrates the groups of the strategies adopted during the SM tasks for the projects under review, including a foresight for a specific NPP case for the next 10 years**.

Table I. Criteria of a specific experience in using various SM evaluation methods [9; 10]

Code	Definition of the criteria used for the safety evaluations
CRU	Credibility of uncertainties
CRC	Credibility of the level of conservatism
LEC	Level of conservatism
SM	Safety margin acceptability
DiDA	Defence in depth Acceptance criteria for levels and in general
DiDI	Defence in depth - Independence of levels
CEE	Cliff edge effects
DPC	The adequacy of the type of method acceptable - deterministic (best estimate or not), probabilistic, combined, using operating experience (OPEX)
CHC	Impact of capability to manage change control
CGEN	Impact of generation / technology phase & HOF
CSIT	Impact of site selection predefined criteria
CEP	Emergency Plan and mitigating actions

Figure 9 shows results of the convergence and stability of decisions based on the SM combined evaluations and illustrate for the presented example, on a real case of using safety decisions and paradigms during a period of about 25 years and two major paradigm changes, that the global effect of SM changes and the adopted foresight strategies was a positive one and it lead to stable solutions in SM predictions for diverse cases. However, this evaluation showed that, that are some areas of potential concern, of which the most recent after Fukushima are related to: the modelling of the Human and Organizational factors (HOF), the Change Management versus initial design intent and the modelling of complex highly dynamic systems requiring new theoretical backgrounds.

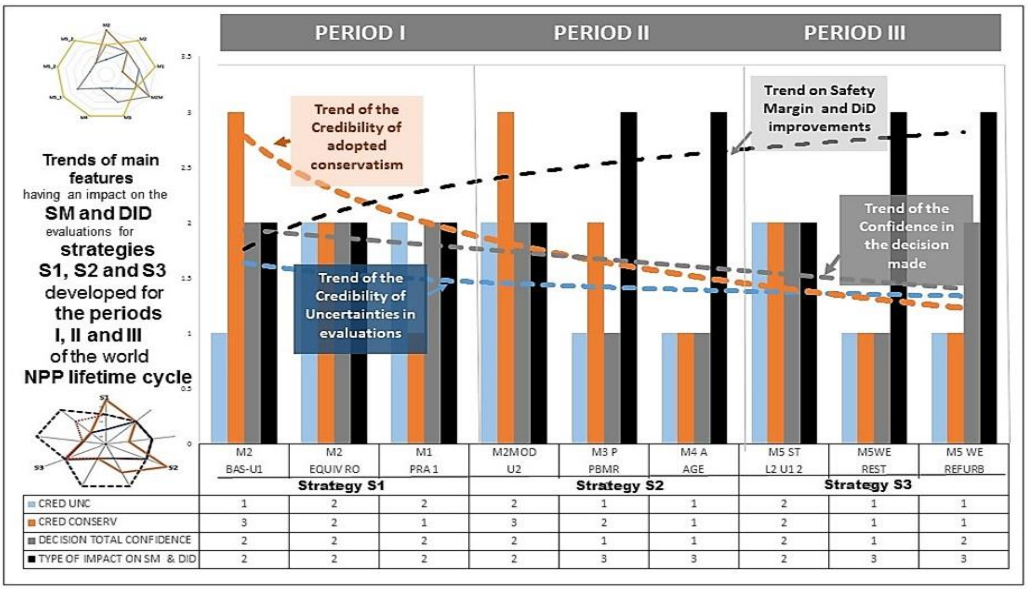


Figure 9. Self-assessment on the results of using diverse SM [9, 10].

3.2 New trends in SM evaluations for the "Maturity period" of the NPP

3.2.1 The extended use of HOF modelling in SM evaluations

One impact of the NPP entering into a "maturity period" was that the SM evaluations needed to focus more on the HOF elements. The HOF elements were presented in [8; 9; 10] as elements of a systemic approach defined for a NPP structure as represented in Figures 10. Figure 10 represents a real case of HOF modelling for a NPP defined by its safety structure, safety culture and leadership components. HOF for a NPP company and its hard and soft safety structure [8;9;10] Evaluation of the weak points of the matrix representation of safety structure and challenges to it for an Emergency Plan of a real plan case lead to the need to get a linear model. This was achieved by using Laplace transforms [9; 10; 12]. After the weak points were defined, a detailed evaluation of it was performed with the EP specific tools and standards.
It is important to note, that the matrices describing those structures are of the type represented in Figures 10 [9; 10] and that the results of the operational research are under a format of eigenvalues of the problem.

The eigenvalues dependencies on the dominant parameters, which are calculated after a series of sensitivity analyses, indicate the optimal values for SM of the systemic description adopted for NPP from HOF perspective. The eigenvalues indicate a set of weak points of the structure, having a clear practical significance [9; 10; 12].

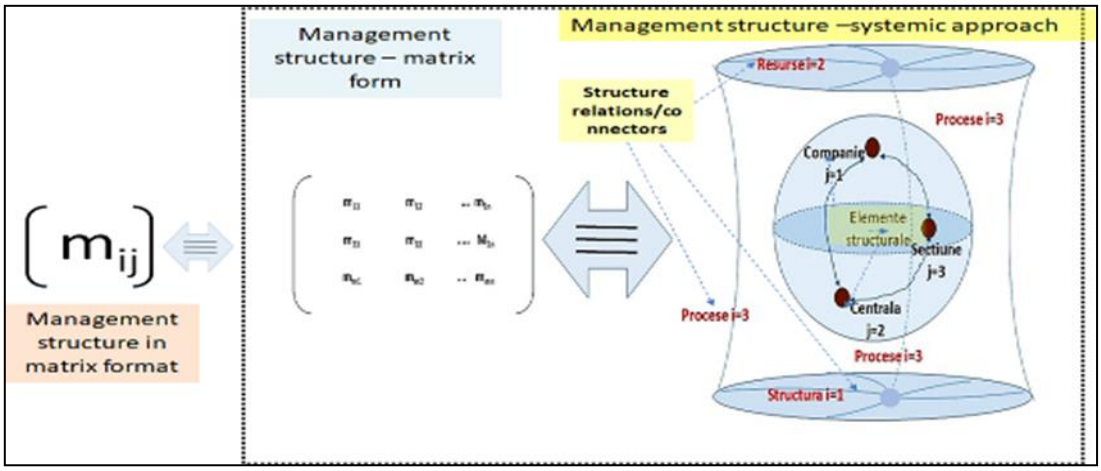


Figure 10. Representation of a NPP HOF model using matrix form [9; 10]. A Specific case of the Emergency Plan optimization [12].

However the results for such evaluations of **SM considering the HOF contributions are reaching in our view the limits specific to the evolution and description of any system, by increasing the level of complexity**. As it was mentioned in other results [2;4], **there is a certain moment of the evolution of the complex system, after which any intended modification leads actually to an area of chaotic, in the sense mainly for SM as unpredictable, response**. And in addition to this aspect the model including HOF elements has a high degree of subjectivity that needs to be carefully considered in safety decisions.

Another example of such evaluations using operational research is illustrated in Figure 11, illustrating a sample of dominant safety aspects to be considered as a foresight for **safety plan after Fukushima accident [2; 4; 6].**

	Issues to be evaluated/Priority in various evaluation options	CATEGORY	Option A	Option B	Option C	Option E
1	Defense in Depth – risk balanced RIDM as method referrence IPE/IPEEE	M-DID&RISK	H	L	L	H
2	Evaluation and /or review of the requirements for classification of systems on various IE (SCC) and on seismic/flood	M-SCC&IE	H	L	M	H
3	Review if considered seismically induced fire/floods	M-S IE&INDUCED	H	L	H	H
4	Evaluation of safety margin for SBO in the case of DBA and BDBA	M-SM DBA & BDBA	H	H	H	H
5	Intrinsic safety and conservative design - Robust (redundancy, diversity, - portable etc) alternative sources of electricity for safety systems after DBA/BDBA	M-INSAF&DBA BDBA	M	H	H	H
6	Review SM for DBA on multiunit plants	M-SM MULTIUNIT DBA	H	H	H	H
7	Review ventilation in containments after severe accidents	M-VENT SA	M	H	M	H
8	Use of PRA level 2 and 3 for Emergency Planning	M- PRA L2&3 EP	M	H	L	H
9	Hydrogen control inside containments and other buildings (spent fuel)	M- HYD	M	H	M	H
10	Spent fuel cooling for DBA & BDBA and reduction of spent fuel inventories	M-POOL DBA & BDBA	M	H	H	H
11	I&C availability for BDBA and severe accidents	M-I&C BDBA	M	H	H	H

Figure 11. Post Fukushima SM evaluations on dominant issues to be followed [2; 4; 6]

Consideration of the safety evaluations and results on SM are also part of the decision making on safety. From this perspective (as shown in [4]) **the Risk Informed Decision Making (RIDM) process with more than two players (Industry, Regulatory Body and Public) has the problem of convergence of adopted decisions, as no stable solution exists for such a game with three players**; the stable solution may be achieved only by **common agreement on the acceptable level** of risk and / or the acceptable level of safety, given the **difference between the calculated SM / Risk and their perceived values**. In Figure 11 there are several options for a basis to the safety decision and foresight on NPP safety after Fukushima, with graded levels of confidence (from lowest – Option E to highest - Option A).

3.2.2. Topological spaces modelling

As it was presented in the previous paragraph the modelling of the complex systems / technologies reaching the end of "Maturity period" leads to the need for more refined description for the variables and parameters of a NPP system, which define the level of SM. Therefore in NPP modelling, as in other industrial areas (like aviation) the need to defined space states of the levels of risk / safety margins appear as solutions for more complex tasks [4].

The use of the space state models is connected with the need to decide on a set of **dominant variables of the SM optimization**.
In energy systems an approach from mathematics was proposed to define this set as **dominant fundamental criteria/ parameters, called syzygies (they are for instance defined by the physical parameters like energy produced, entropy loss, information entropy specific to the control systems etc.)** and examples **were shown for energy systems in [4].** By considering the SM of the NPP as multivariable systems, new approaches are used. These approaches are considering the models of NPP for the last phases of the maturity period as needing the development of more special operational research, able to take into account multiple variables. One of those is called **"topological spaces"** approach.

For such approach the SM is considered in a biunivoc relationship with the internal volume of the resultant multi – D description, obtained after a series of iterations (Figure 12) [1].

The space states produced for the SM are not just volumes, but generalization of volumes in multi-dimensional spaces (Figures 1, 2 and 12). The value of the volumes is indicating the level of SM. The type of topological geometrical figure is an indication if the optimization is on a good track (as the volume depends as indicated in the figures on the type of poliedra) [1].

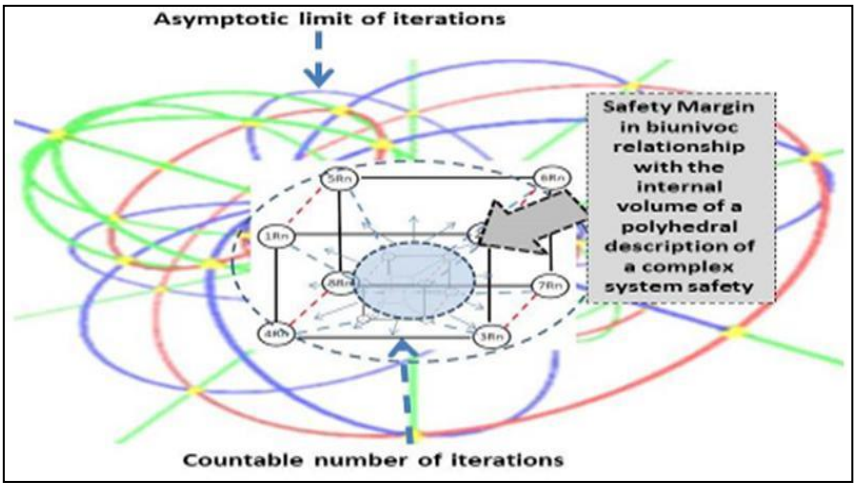


Figure 12 Safety Margin (SM) Topology in a multi-iterative evaluation.

The poliedra are calculated by using the matrix description as presented in [1]. An illustration for the multiunit PSA is presented in Figure 13. Such a representation requires the definition of a series of connections assumed for the evolution of elements of the structure that have to consider their evolution from one iteration to another. The algebraic basis for the poliedra is in the format of octonions) (as illustrated in Figure 13) [1].

GROUPS OF TRANSITION AT THE SAME LEVEL	GROUPS OF TRANSITION BETWEEN THE LEVELS	GROUPS OF MIXED TRANSITION
GR2 = e_{2j}	GR4 = e_{4l}	GR1=e_{1i}
GR7 = e_{7o}	GR5 = e_{5m}	GR3=e_{3k}
	GR6 = e_{6n}	
	GR8 = e_{8p}	

	GR1	GR2	GR3	GR4	GR5	GR6	GR7	GR8
GR1	e_{11}	e_{12}	e_{13}	e_{14}	e_{15}	e_{16}	e_{17}	e_{18}
GR2	e_{21}	e_{22}	e_{23}	e_{24}	e_{25}	e_{26}	e_{27}	e_{28}
GR3	e_{31}	e_{32}	e_{33}	e_{34}	e_{35}	e_{36}	e_{37}	e_{38}
GR4	e_{41}	e_{42}	e_{43}	e_{44}	e_{45}	e_{46}	e_{47}	e_{48}
GR5	e_{51}	e_{52}	e_{53}	e_{54}	e_{55}	e_{56}	e_{57}	e_{88}
GR6	e_{61}	e_{62}	e_{63}	e_{64}	e_{65}	e_{66}	e_{67}	e_{68}
GR7	e_{71}	e_{72}	e_{73}	e_{74}	e_{75}	e_{76}	e_{77}	e_{78}
GR8	e_{81}	e_{82}	e_{83}	e_{84}	e_{85}	e_{86}	e_{87}	e_{88}

	1	2	3	4	5	6	7	8
	Groups of transition between various states							
	GR 1 = e_{1i}	GR2=e_{2j}	GR3=e_{3k}	GR4=e_{4l}	GR5=e_{5m}	GR6=e_{6n}	GR7=e_{7o}	GR8=e_{8p}
1	1-2							10-1
2		2-3						10-2
3	1-3		3-4					
4	4-5			4-6	4-7			
5				5-6		5-8		
6				6-7	6-8	6-9		
7			7-9				7-8	
8		8-9	7-10 10 8-9- 10					

Figure 13. The algebraic description of topological spaces in Figure 12 [1] for a real case [9; 10].

A practical example of the latest results of this approach are in [11], as defined for the modeling of a real case of Multi Unit Probabilistic Safety Analysis (PSA) called MUPSA starting from a Single Unit PSA (SUPSA).

The development of improved integrated models SUPSA-MUPSA lead to the need to define the space of the risk accepted areas in a 3D format, considering the dimension of the SUPSA, the dimension of MUPSA and the common area connecting the two

areas. (as represented in Figure 14). The areas are represented by the dominant minimal sequences of a real case calculation while developing the SM / Risk volume from one unit to more than 2 units. Therefor the the practical future tasks of this type the use of **3D- Reliability Equivalent Diagrams (3D-RED) and 3D – Risk Spaces is foreseen as having a potential impact in improving the prediction capability**.

This is **in line with results obtained from a different approach by the use of the cube [14].**

However, it is expected that, there is for any technology a potential moment of challenge, when any more complicated model (of the object and with the modeller) will produce such products, technical realities, that will be subject to more and more frequent unexpected sharp changes in the safety / risk level.

It is expected that the description of such challenges of very low probability, but high and correlated between them impact events (issue known as a cliff edge effect problem) are specific for technologies entering last phases of their maturity.

An example presented in this paper is on the results obtained so far in MUPSA, indicating that there is a clear limit of possible modelling of such cliff edge effects and this limit is given by the type of plant technology itself, i.e. by its lifetime cycle reaching the End of Life phase (Figure 13).

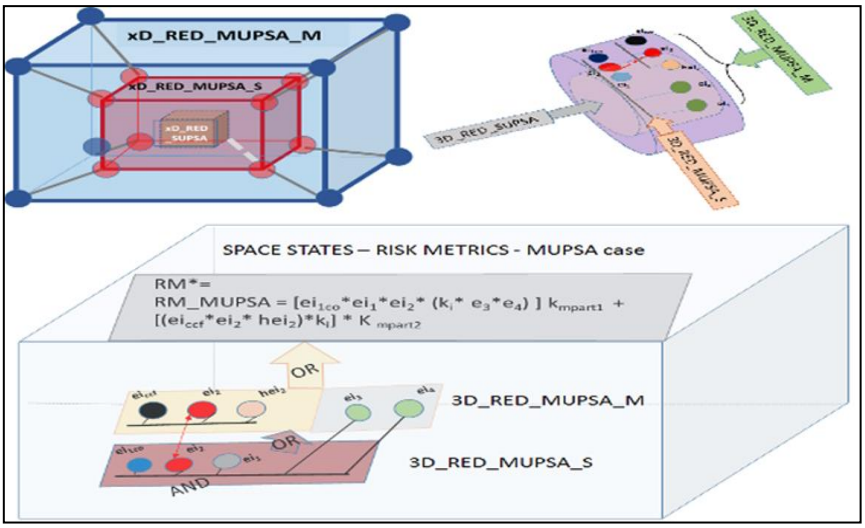


Figure 14. 3D RED for a real case of MUPSA model [11].

4. Conclusions

The paper presents a view on the evaluation of SM for some complex systems (NPP) considering the fact that:

- The history of a complex system is a one of its dominating technology, which has a clear cut of its life cycle periods.

- The evaluation is performed in steps during all this lifetime and in iterations, creating a set / area / volume of acceptable from risk perspective states.

- The SM evaluation for mature period leads to the need of including the modeler into the model of acceptable states, which requires changes in the methodologies and a new view on models and objects.

Further steps of the project considering the SM evaluation in an integrated lifecycle manner are expected to produce more results to support various conclusions for a specific technology (NPP).

References

[1] Serbanescu, D., *An integrated perspective on knowledge and existence*, NOEMA, XVI, 2017, pp.185-218

[2] Serbanescu, D., *Safety paradigm changes and major accidents in nuclear power plants*, SIEN 2017, Bucharest, Oct 2 2017, ISSN 2559-3374 ISSN-L-2559-3374

[3] Serbanescu, D, Understanding major accidents -Shifting paradigms in safety and risk Safety Summit Vienna 27-28 Sept2011, http://www.academia.edu/

[4] Serbanescu, D., Selected topics in risk analyses for some energy systems, Lambert, May 2015

[5] Serbanescu, D., *Systematic biases in event review and their impact on learning* process, 45th ESReDA Seminar on Dynamic Learning from Incidents and Accidents, Bridging the Gap between Safety Recommendations and Learning, 23rd - 24th October 2013, Porto - Portugal

[6] Serbanescu, D., *Systematic biases in NPP event reviews and their impact on learning process*, IA EA-CN- 2 2 7 - 4, International Conference on Operational Safety; Viena 23 - 26 June 2015

[7] Serbanescu,D., *Despre unele sisteme energetice naturale si invatamintele studierii lor, Lights of the World*" A series of events promoting Science, Education and Culture in the context of the International Year of Light 2015 celebrations marking the 70th anniversary of UNESCO Bucharest, 30th October - 1st November 2015, Palace of the Parliament

[8] Serbanescu, D., *Proposed contribution to HOF topics under ESREDA HOF task*, ISPRA, May 2016

[9] Serbanescu,D.,*On some challenges in defining and using Defense in Depth and Safety Margin concepts, as highlighted by the safety improvement process*, IAEA, International Conference on Topical Issues in Nuclear Installation Safety: Safety Demonstration of Advanced Water Cooled Nuclear Power Plants, CN-251, Vienna, Austria, 6 - 9 June 2017.

[10] Serbanescu, D., *A specific experience on some challenges in defining and using defense in depth and safety margin concepts, as highlighted by the safety improvement process*, DOI: 10.13141/RG.2.1.4859.2488 https://www.researchgate.net/publication/316542989, Bucharest, June 2017

[11] Serbanescu, D., *On some aspects of the multiunit probabilistic safety analyses models*, 8th International Conference on Energy and Environment, CIEM 2017, Bucharest 19-20 Oct 2017.

[12] Min, P., *Systematic approach on Human and Organizational factors in the nuclear power plants emergency management*, PhD report 2017, Politecnical University Bucharest

[13] Serbanescu, D., *Report on an IAEA - CNCAN contract "CNCAN Emergency Actions Level Procedure (EAL) -A schematic Flow-path Guidance on the use of the EAL procedure*", May 2014
[14] *Case study analysis on dynamic learning from accidents*, ESREDA, 2015.

The McNamara Fallacy Blocks Foresight for Safety

John Kingston, Noordwijk Risk Initiative Foundation, P.O. Box 14, 2676 ZG Maasdijk, The Netherlands.

Yves Dien, CHAOS, 6, rue Lucien Feuchot, 92190 Meudon, France.

Abstract

Famously, 'what gets measured gets done', but the sociology behind the measurements, particularly those used to manage organisations, are little studied in the field of safety. Yankelovich described a pattern dealing with traps of quantification that he called the "McNamara fallacy" and which has four steps.
Process safety might be particularly vulnerable to the McNamara fallacy because the paradigm of reliance on numbers is very strong in engineering culture. However, as we argue, the McNamara fallacy is less a failing of individuals, than it is an outcome of the forces that produce order in organisations. In this paper after an explanation of the four steps of the "fallacy", we will argue how some failures of foresight are connected to poorly managed quantification, which is, according to Woods (2009), a basic form of organization failure.

Keywords: Measurement, Modelling, Safety, McNamara Fallacy, Quantitative fallacy

> *"There's a quote from T.S. Eliot that I just love:*
> *We shall not cease from exploring*
> *And at the end of our exploration*
> *We will return to where we started*
> *And know the place for the first time.*
>
> *Now that's in a sense where I'm beginning to be."*
>
> (Robert McNamara, speaking to Errol Morris in 2003)[5]

[5] http://www.errolmorris.com/film/fow_transcript.html. Accessed 2nd October 2017

1. Introduction

Foresight is the imagining of future possibilities based on knowledge of the past and present. According to Stark (1961) prediction and foresight are related activities, but they are not the same. In prediction, the emphasis is on judgmental thinking, assigning probabilities, and on accuracy. In contrast, foresight is the awareness of possibilities *"with logic its only constraint"*. Stark points out that foresight "*precedes (or should precede) prediction"*.

Risk analysis is widely practiced across industries, and although it can give good results, the approach has some inherent weaknesses (Dien and Dechy, 2016):

- incomplete identification of risks—a weakness which although generally acknowledged is sometimes lost from sight in specific analyses (see Aulnay et al., 2017);
- it does not take account of the complexity of sociotechnical life (Perrow, 1984)— Interactions between social subsystems and, on the other hand, between social element and technical element are hardly modelled;
- imagination concerning scenarios is censored by plausibility. This creates confusion between impossibility and improbability of occurrence, especially for low likelihood events (see for instance Fukushima);
- worst case scenarios that do not take account of some initiators (see for instance the contribution of bow-doors kept open to the capsize of the Herald of Free Enterprise ferry);
- there is limited updating of analysis in the light of operational experience. Sometimes this is limited to direct and immediate causes (often technical, but with root causes put aside, which often human and organisational aspects).

In the contemporary literature, foresight is often treated as an *organisational* ability (e.g. Osman, 2015; Rohrbeck, et al, 2015). Research on what foresight is, how it might be taught and methodologically supported, seems plentiful, but has yet to find a firm theoretical basis (Piirainen and Gonzalez, 2015). However, even when conceived as an organisational ability, foresight is produced by the minds of individuals.

This paper concerns the conditions in organisations that may affect the quality of foresight. As an entry into the subject, it makes a connection between foresight and the so-called McNamara[6] fallacy. As will be explained, the fallacy describes how foresight can be blinded by corporate overemphasis of a given set of metrics. The present paper considers the impact of the McNamara fallacy, and the mechanisms that mediate it, on the employee's contribution to foresight of safety.

[6] It is a moot point why Robert McNamara's name has been memorialised in this way, but it is likely to be connected to his role as US Secretary for Defence (1961-1968) during the Vietnam War (1955-1975). When Smith wrote his piece in 1972, the public mind still closely associated McNamara with the unremitting destruction being wrought in Vietnam. Only later did contemporary sources reveal that, even by 1966, McNamara bitterly understood the failures of foresight that started and escalated the war. As he said in 2003, *"war is so complex it's beyond the ability of the human mind to comprehend all the variables. Our judgment, our understanding, are not adequate. And we kill people unnecessarily." (http://www.errolmorris.com/film/fow_transcript.html.) See also, McNamara (1995).*

1.1 The McNamara Fallacy and the Fischer's Quantitative Fallacy

The McNamara fallacy was coined by the social scientist, Daniel Yankelovich. As reported by Smith, 1972[7], the fallacy can be stated as:

"The first step is to measure whatever can be easily measured. This is okay as far as it goes. The second step is to disregard that which can't be measured or give it an arbitrary quantitative value. This is artificial and misleading. The third step is to presume that what can't be measured easily really isn't very important. This is blindness. The fourth step is to say that what can't be easily measured really doesn't exist. This is suicide." (Smith, 1972; page 54)

Wikipedia, at the time of writing[8], states that the McNamara fallacy is "also known as the quantitative fallacy". While the present authors agree that there is a connection between the two, we contend that the McNamara fallacy contains lessons for foresight that go beyond those contained in the quantitative fallacy.

1.2 Some lessons for foresight from the quantitative fallacy

What is the quantitative fallacy? Stating it pithily as *"the facts which count best count most"* Fischer (1970) explains that the quantitative fallacy is to behave as though "*facts are important in proportion to their susceptibility to quantification*" (page 90). His critique is aimed at historical analysis, and particularly a trend for advocacy of certain methodologies. It is an attack on the misuse of quantification. As he puts it

> *"Criteria of significance should not be methodological, but substantive in nature. They should always be grounded in the nature of the problem itself and not in the tools of problem solving. The purpose of historical inquiry is not to vindicate a method but to discover what actually happened. Every efficient means to this end is legitimate, but none alone can be erected into a standard of legitimacy."* (Fischer, 1970; page 91)

The erection of 'standards of legitimacy' is one way in which foresight can be limited. Fischer warns that the problem should choose the method. An overriding preference for a particular method, can act as a filter on reality; only those data compatible with the standard are collected, and interpretation will be limited to those future possibilities that are compatible with the standard. As Kingston and Mertens (2007) note, "beware methodolatory".

For example, on February 1, 2003 the space shuttle Columbia disintegrated during its re-entry phase into the Earth's atmosphere after a 16-day mission on orbit around the Earth. The seven astronauts on board died in the accident. The technical cause of the accident is clear. During the launch phase, few seconds after lift-off, a piece of insulating foam separated from the external fuel tank. It struck the shuttle's left wing at

[7] The exact provenance is not certain, but the earliest published source that the present authors could verify is an article in the September, 1972 edition of the Atlantic Monthly magazine. That article was written under the pseudonym 'Adam Smith', but Yankelovich (2012) confirmed that he had discussed the ideas with the journalist in question.

[8] https://en.wikipedia.org/wiki/McNamara_fallacy accessed 2 October 2017

a high speed. The impact holed the leading edge of the wing, a protected area of the Thermal Protection System. During re-entry superheated gases (local temperature more than 2000°C) penetrated into the left wing, leading to the melting of a spar, the loss of control of the shuttle, and eventually its destruction. The hit on the wing was undetected in real time. It was identified on the second day of the mission after analysis of launch photos and films. Nevertheless, the potential for damage caused by the foam strike was known, as were the consequences on shuttle safety during the re-entry phase. So, one challenge to the Mission Management Team was to assess the danger. Indeed it was "*very difficult to even bound the problem and initialize thermal, trajectory, and structural analyses. Their answers* [*might*] *have a wide spread ranging from acceptable to not-acceptable to horrible, and no way to reduce uncertainty*" (CAIB, 2003, page 151). One part of the assessment was carried out using a mathematical modelling tool called *Crater*. It allowed engineers to assess the effects of the impact. However, this tool was not designed for evaluation of large size projectile strikes. During the Columbia mission, *Crater* predicted possible damage, but the Debris Assessment Team assumed, without any validation—and because *Crater* was a conservative tool—that it would predict more damage than would actually occur. Assumptions and uncertainty were never fully presented to the flight decision makers. Furthermore, the team that conducted the analyses had been formed recently, and therefore could be considered as inexperienced. In fact, it was the first mission for which they were solely responsible for providing analysis with the *Crater* tool. In this way, a particular tool was used beyond its applicability limits but with no one really aware of that. It led to fatal decisions of "no-action" regarding the strike on the left shuttle wing.

The impact of the quantitative fallacy on foresight may be more fundamental. A method may impose a filter, but the paradigm from which it is drawn imposes more general limits on foresight. As Patton describes,

> *"The paradigm is a worldview, a general perspective; a way of breaking down the complexity of the real world. As such, paradigms are deeply embedded in the socialisation of adherents and practitioners: paradigms tell them what is important, legitimate and reasonable. Paradigms are also normative, telling the practitioner what to do without the necessity of long existential epistemological consideration." (Patton, 2008, page 423).*

Whereas models and methods are relatively accessible to critique, a paradigm is more deeply integrated into the perceptions and beliefs of its adherents. People looking to the future can change their spectacles, but it is harder for them to change their point of view.

For instance, two senior engineers at Northeast Utilities, which operates nuclear power plants in the USA, were concerned about the way old fuel rods were cooled. They were concerned both by the reliability of the cooling system and by the lack of regulation enforcement concerning refuelling operation. They warned the management, (i.e. they offered new glasses for a better assessment of the situation!) and tried to fix what they considered an obvious safety problem. For several months, managers denied the problem existed and refused to report it to the American Nuclear Safety Authority. They even brought in outside consultants to prove senior engineers were wrong. But

they ended up agreeing with them. Finally, they took the case to the Safety Authority themselves. It also took several months for the safety authority to react (Pooley, 1996).

Fischer's advice is that we should not allow ourselves to be trapped within a paradigm. However, it is probably hard to take the advice. As Patton suggests, paradigms are part of socialisation, and as sociologists[9] have been pointing out for a century or more, individuals readily internalise the norms of a group in order to belong to it. Hence, we should actually assume as normal the situation that Fischer complains about, and recognise that foresight is a function of group identity. Countering the restriction of foresight due to paradigmatic group-think is something to factor-in to the design of our organisations.

Arguably, scientists and engineers are trained to be aware of the grounds on which they make predictions and the limits of their foresight. As Feynman puts it:

> *"The first principle is that you must not fool yourself—and you the easiest person to fool. So you have to be very careful about that. After you've not fooled yourself, it's easy not to fool other scientists. You just have to be honest in a conventional way after that".* (Feynman, 1974; p.12)

However, about scientists communicating with a non-technical audience, Feynman goes on to say:

> *"I would like to add something that's not essential to the science, but something I kind of believe, which is that you should not fool the layman when you're talking as a scientist." ... "I'm talking about a specific, extra type of integrity that is not lying, but bending over backwards to show how you're maybe wrong, that you ought to do when acting as a scientist. And this is our responsibility as scientists, certainly to other scientists, and I think to laymen."*

With fellow scientists and engineers, one can rely to some extent on the scientifically literate scepticism through which the information will be filtered. Arguably, their foresight is stimulated by questioning conditions, as well as by spotting limitations and alternative interpretations of other's results or theories. Following Feynman's suggestion, when scientists or engineers act as advisors to non-scientists there is an additional duty to educate the scepticism of those advised. Perhaps the duty extends even further: to urge the advised to continue searching for other possibilities.

Paradigms define groups and what group members regard as credible evidence. As Patton (ibid) notes, paradigms tell group members what is important, legitimate and reasonable. So, although members of scientific disciplines bear the individual responsibility to conduct themselves as Feynman suggests, their group norms will have some weight in deciding their actual behaviour.

Fischer has a specific warning for groups whose work has a quantitative aspect:

> *"There is an epigram, perhaps apocryphal, attributed to Lord Kelvin that everything which exists, exists in quantity. Enthusiastic quantifiers have*

[9] E.g. Durkheim's *mechanical solidarity,* and Foucault's ideas of *institutions* and *discourse*.

> *amended Lord Kelvin's statement to read, "Unless a thing can be measured quantitatively, it does not exist significantly." Therein lies a fallacy."*

There is a balance then between the conditional trust implied by Feynman and the preference that some groups may have for quantitative evidence. Something like this was at work when NASA and Morton-Thiokol engineers discussed the advisability of launching in very cold conditions given previous observations of O-ring erosion and hot gas blow-by in the boosters. These concerns were raised by Morton-Thiokol engineers in a teleconference on the eve of the space shuttle *Challenger* launch in January, 1986. Morton-Thiokol, who supplied the Solid Rocket Boosters, recommended that the space shuttle launch be postponed until the temperatures warmed-up. They acknowledged that their recommendation was not based on quantitative data "*saying their argument was subjective,* […] *qualitative, intuitively correct*. The NASA managers did not accept this, and *challenged* [Morton] *Thiokol to prove it by* ***quantifying their concerns***[10]***"*** (Vaughan, 1996, p.355). As the opinion of these engineers was not supported by quantitative data, it could be dismissed as an "*emotional argument*". The decision to abandon a launch is not one that NASA could take lightly. In this case, imposing a quantitative standard of evidence might well have been a tactic used to vitiate the qualitative evidence of the Thiokol engineers. However, it demonstrates a belief in quantification by the NASA agents that exceeded their trust in the foresight of the subject matter experts. Vaughan concludes, "*'real' technology conforms to the norms of quantitative, scientific positivism*".

It would be nice to think that scientific or technical input to foresight will always be based on a fresh, objective view of the problem. There is an apocryphal story about technical advice given to a statesman. The advisor had gone on at length, "On the one hand this, but on the other hand that." After the session, President Truman [or sometimes when this story is told, Winston Churchill] turned to his special assistant and said, "The next time I appoint an advisor, remind me to find someone who's one-handed!" Advisors know that not everyone wants to be educated, and in a marketplace, those they would advise can choose amongst advisors.

In summary, the quantitative fallacy highlights three vulnerabilities of foresight:

- the scope of foresight is reduced when numerical convenience is decisive in selecting and processing data. As a consequence, some futures will not be foreseen that otherwise might have;
- the reduced scope of foresight becomes systematic when 'methods choose problems'. Blindsides develop when methodology becomes the test of what is credible;
- these two vulnerabilities will be made worse by a lack of diversity in the population who contribute to foreseeing the possible futures of the organisation.

[10] Emphasis added

1.3 Impaired foresight: what does the McNamara fallacy add to the quantitative fallacy?

The McNamara fallacy is more general than the quantitative fallacy about what and to whom it applies. Rather than the repeated misuse of numerical methods by technical specialists, the McNamara fallacy describes, as a series of steps, a process of degradation in the ability to foresee future behaviour in an organisation. The McNamara fallacy describes a disease of organisational foresight.

The word 'measure' in the McNamara fallacy suggests quantification, but there is reason to interpret it more broadly. Firstly, although measurement often entails numbers, a glance in a dictionary confirms that numbers are a means to an end—to ascertain the state of something. Even were we to restrict 'measure' only to quantification, measurement theory contains quite distinct, theoretically legitimate alternatives about how numbers can be assigned and, therefore, what 'to measure' means in a particular case. As Hand (1996) explains, a measurement scheme might be based on a model that maps to an assumed underlying reality. Alternatively, a measurement scheme might, in fact, not assume any underlying reality, but be a procedure for assigning numbers in a consistent way. The McNamara fallacy is concerned with how actors may misinform their internal representation of the systems they control and, by extension, misinform their foresight of those systems when planning or evaluating change. Later in this paper we explain how some of the hypothetical mechanisms of the McNamara fallacy, misinform the basis of foresight but also its production.

Yankelovich repeats key phrases in his formulation of the McNamara fallacy. The verb 'to measure' is used four times, and the adverb 'easily' modifies it three out of four times. In the quantitative fallacy, Fischer uses the phrase "susceptibility to quantification"; and the present authors regard this as one aspect of 'easily measured' in the Yankelovich formula. However, a broad view of measurement in an organisational setting, suggests that *ease* will reflect other constraints that decision-makers in organisations are trying to satisfy. In addition to the technical ease of measurement, pragmatic constraints such as *administrative ease*, and *political expedience* will factor into the decision about what to measure and how.

To summarise, in contrast to the quantitative fallacy, the McNamara fallacy describes:

- how measurement in its broadest sense can be biased by expediency, and;
- a process of degradation in the quality of foresight available in an organisation.

2. The McNamara fallacy reduces the scope and acuity of foresight

The moral, as it were, of the McNamara fallacy is that measurement schemes tend to become enshrined and inflexible in their organisations. This means that any shortcomings in their validity will also tend to be long-lasting. In this section, the four steps[11] of the McNamara are considered and mechanisms proposed.

[11] The four steps of the fallacy can be found in (Smith, 1972; page 54)

The 'easily measured' part of the Yankelovich formula plays out in numerous ways. 'Easy', from a purely technical point of view, might mean a preference for data readily at hand, or easy to collect or process into a suitable format. As Yankelovich/Smith say, "This is okay as far as it goes" (ibid), however, how far that is may be a function of the design paradox (Frei, 2015). The paradox is that one knows less at the start of a project or design process than at the end. Therefore, if a measurement scheme is set-up early in a design or project lifecycle, unless revised, it will lack validity.

In terms of foresight, if we take Stark's (ibid) point of view, erroneous measurement will create in actors a faulty perception of how the organisation works, and this will be reflected in their view of future possibilities.

For example, in 2014, SNCF discovered that 1,000 of its railway platforms were too narrow to allow adequate clearance for 2,000 new trains it had ordered. A quirk of the sampling methodology meant that measurement of existing platforms focussed on those built in the previous 30 years. However, older stations were built when trains were slimmer and, in consequence, with wider platforms. According to the French minister for transport, M. Frederic Cuvillier "When you separate the rail operator from the train company," he said, "this is what happens." A programme of platform modifications was put in place, an unplanned expenditure exceeding €50 million. (BBC, 2014)

M. Cuvillier's explanation points to the involvement of stakeholders, another issue implied by the McNamara fallacy. At the start of design projects (and this may also apply to projects in ageing systems, according to Horrocks, 2010) the decision-makers involved in defining measurements might not be the same as those working elsewhere, in mature parts of the system, or who inherit the design when it comes into service. If ease does indeed define measurement, then what is easy for the project leaders may create measurement systems focussed on their short term goals or sub-systems rather than the longer-term operational functioning of the whole mature system.

In response to numerous operational problems in the running of public services by contractors, the UK Committee of Public Accounts (CPA) looked into how the civil service managed the contracts. They found there to be a disproportionate emphasis on measuring performance in the early phases of government contracts. Furthermore, not only was there a relative lack of operational performance measurement, there was also a Principal-Agent problem. The civil servants responsible for these contracts usually moved jobs before delivery of the contracted service or product. Therefore, the moral-hazard was for civil servants to set-up measurement of aspects they could control well, but not those that would create difficulties for them. In consequence, CPA recommended that civil servants should "remain accountable for spending throughout the life of contracts". (CPA 2014).

The CPA findings suggest a number of problems for foresight. Firstly, a focus on measurements relevant in the short-term may displace timely consideration of factors that will be relevant in the longer term. Secondly, variables that are *not* measured provide degrees of freedom for decisions. However, if these unmeasured variables turn out to be important later in the lifecycle, decisions taken early in a project may unwittingly trade-off measured variables against those that are unmeasured. Thirdly,

moral-hazard may reinforce self-serving visions of the future that make it harder to foresee problems.

The second step of the McNamara fallacy is to "to disregard that which can't be measured or give it an arbitrary quantitative value". The phrasing suggests that this is seen as a deliberate decision by measurement designers. However, the McNamara fallacy may rely on mechanisms that operate below the level of awareness.

The first mechanism—*skilled unawareness*—is fundamental. As described by Argyris (1999) skilled unawareness screens from consciousness the things the actor is doing to avoid confrontation or protect their own beliefs from dissonance. Some of those things involve subordinating their own views and beliefs, which Argyris calls *skilled incompetence*. Argyris has demonstrated that these defensive skilled routines are common in organisations. This would predict that actors will design measurements that make confrontation less likely or avoid dissonance, and for the same reasons and using the same psychological mechanisms, self-censor criticism of flawed measurements.

Ralph Nader gives an example of self-censorship in car safety. *"There was no Human Factors engineering being the subject of the legal discussion. And then I met a retired engineer from American Motors Corporation, his name was Henry Wakeland. And in my long conversations with him, he told me about the enormous self-censorship inside the industry. And I said, this can't be so. I'm mean, you mean they don't speak up; even in closed doors among themselves? He says, they're all afraid. I said, afraid of what? Afraid of being marked as trouble-makers, non-players on the team. And he gave me a lot of examples"* Nader, 2016.

Avoiding confrontation is not necessarily a goal in itself, and in organisations it may serve a higher purpose: to preserve the political status quo. Lessig (2011) calls this *dependence corruption*. To ensure that the relationships they depend on continue, individuals make complex adjustments in their perceptions. Lessig makes the point that this is not corruption in the sense of bribery, but an aspect of the reciprocity[12] that is fundamental in human relationships. However, in the organisational setting, dependence corruption means that individuals will interpret policies and data, and act in ways that protect the interests of those others who enable the individual to be effective and successful in their work. As well as the risks of measuring what is technically easy, it is likely that *easily measured* is defined in a political dimension. Lessig gives several examples, such as scientific studies of the harmfulness of Bisphenol-A (BPA is a constituent of some soft plastics). He reports that no industry-funded study (n=13) has found evidence of harm, whereas 86% of independent studies (n=163) have. Lessig makes the point that the scientists who found no harm were not dishonest, but consented to work in studies that sought to determine risks of exposure rather than to look for evidence of harm. The overall effect is to make it less certain

[12] Lessig notes that "We all recognize the drive deep in our bones (or, more accurately, our DNA) to reciprocate. Some of it we see directly. Some of it we don't. The subconscious is guided by interactions of reciprocity as much as the conscious. We reciprocate without thinking. We are bent to those to whom we are obliged, even when we believe, honestly, that we are not. What Robert Brooks wrote over a century ago we can repeat today: "By far the worst evil of the present system is the ease with which it enables men otherwise incorruptible to be placed tactfully, subtly, and — as time goes on — always more completely under obligations incompatible with public duty." (Lessig, 2008; p132)

that it is safe or unsafe to use plastics containing BPA. Even better documented is the example of tetraethyl lead (TEL, an additive to petrol) in which, from the 1920s onwards, the scientific evidence for safety was overwhelmingly funded by the industry. In the mid-1960s, independent research *"drew attention to the fallacy of assuming that observed ("typical") lead in foods and bodies of Americans are natural and therefore safe and harmless. He* [Clair Patterson] *used a geochemical argument to estimate that the average (typical) body burden and concentrations of lead in the blood of Americans in the 1960s were at least 100 times above the background values"* (Nraigu, 1998).

Whether subject to unawareness or not, arbitrary measurement or disregarding data that contradicts vested interests may also reflect *organised hypocrisy*. This term was coined by Brunsson (2002) to describe what he found in studies of Swedish public sector organisations. There he saw that decision-makers created situations in which talk and decisions were quite separate from actions. This allowed stakeholder concern about a topic to be addressed, if not resolved, by talk that never transferred into action. Brunsson was not moralising, he was describing a rational means of controlling outcomes when objectives are incompatible. Arbitrary measurement makes it easier to talk rather than act. As Hand (1996; p.453) points out, "*to be useful, the numerical assignment procedure has to be well defined. Arbitrariness in the procedure will reflect itself in ambiguity in the results*." A suitably ambiguous measurement creates a buffer between the world of talk and the world of action. In this way the decision-maker's second step into McNamara fallacy carries the organisation across the threshold into organised hypocrisy.

Most readers will have some familiarity with statistics about the punctuality of the railways. In the UK, until June this year, figures suggested that 92% to 97% trains were on time (BBC, 2017). However, if arrival time is measured more precisely, to the nearest minute, those figures fall to 65%. However, even this does not directly measure the impact on passengers; it excludes missed onward connections, missed or cancelled appointments, and so forth. An attempt to quantify this impact arrived at a figure of 73.47 GBP (about €82) *per minute* of delay (NAO, 2008). Most UK train operators have a policy of compensating passengers for late arrivals at stations of at least 30 minutes, and then for a proportion of the train fare, which in the vast majority of cases will be rather less than €82 per minute.

Technical error of measurement can be hard to spot, even when skilled unawareness is not obscuring it. There is always a chain of arguments that link the conclusions we draw from evidence to the empirical reality we seek to know about and influence. This is true whether the evidence is qualitative or quantitative. Sometimes we are fully aware of this chain, but more often not, especially when some links between the 'map and the territory' are not accessible. As Hand (1996) makes plain, there is plenty of scope for technical errors in constructing and using measurement schemes.

It is one thing to make errors, but another thing not to detect or correct them. One can imagine a number of reasons why systematic errors of measurement, or other problems of validity, would go uncorrected. Firstly, the practical impact of poor measurement might be invisible or inconsequential (even if borne by others in the form of pollution, ill-health etc., if those people lack power or representation).

Secondly, the measurement scheme might be inscrutable. It is quite intimidating to question the validity of a measurement produced by a sophisticated analysis, perhaps even a computer generated algorithm, and based on a huge amount of data. Often the person who might be able to show the steps that connect the map to the territory is not there to explain things, even if such a person exists.

Thirdly, as predicted by Argyris, when a measurement scheme is legitimised at a senior level, it is unlikely to be challenged by subordinates. The misuse of Total Recordable Injury Rate (TRIR) as a general measure of plant safety at the BP Texas City refinery, may be an example of this. As CSB (2007) point out "TRIR and LTIR[13] do not effectively predict a facility's risk for a catastrophic event". Staffing cuts was a factor in that accident, but any adverse effects of this on process safety would not have been visible in occupational safety measurements such as TRIR. Concerning the lack of challenge by subordinates, the Baker Panel concluded that in BP even apparently capable individuals had "weak process safety voices" and that they did "not appear to participate substantially in the critical decision-making process with respect to BP's U.S. refineries" (Baker, et al. 2007).

Fourthly, the simplification implicit in the models which underlie most measurement schemes, may not be recognised as an over-simplification, in the sense that some relevant aspects of the system measured are not represented in the measurement. As Aulnay et al. (2017) note, *"Modelling allows a representation of a system but results in loss of information and especially for liaisons between elements and sub-systems. Nevertheless, level of understanding induced [by modelling] is more important than losses of information."* However, the implication of the McNamara fallacy is that the third step—to presume that what can't be measured easily really isn't very important—leads to the fourth step: *"what can't be easily measured really doesn't exist"*. Modelling is an essential, beneficial activity in safety; and imperfection is not a reason to throw the baby out with the bathwater. The problem is how to maintain vigilance and allocate sufficient resources to closing the gaps between the model and the evolving empirical reality.

3. Conclusions

One goal of this article is to highlight the often subtle ways in which quantification may reduce the scope and acuity of foresight. However, none of the arguments presented deny or minimize the role and importance of quantification in dealing with safety.

The McNamara fallacy describes what happens to foresight if an organization lives on a 'starvation diet' of information filtered through imperfect measurement. There is always scope for improving measurements, but even as good as they could be made, they are filters on reality. The nature of perception, of life in Plato's cave, is that we can never 'peek around the back' and see reality directly.

Foresight is integral to the creative aspect of safety practice. It is particularly evident in the form of hazard identification, which is meat and drink to risk assessment, both

[13] LTIR – Lost Time Injury Rate.

in everyday evaluation of data and in more formal risk analyses. But does foresight contain all the nourishment it needs?

The danger to foresight is that measurement can define our reality, and there are numerous ways in which this can happen. This paper has tried to show that many of these ways are properties of our institutions rather than of ourselves—even scrupulous scientific conduct by individuals is not a complete answer.

The McNamara fallacy seems to be a disease of bureaucracy, not a lapse by individuals. Measurement schemes once established tend to endure, sometimes longer than their creators. And what was too hard to measure reflects not just technical limits, but the political realities of those creators. Does current practice do everything needed to continuously improve measurement schemes? Published accident investigation reports and plant ageing studies suggest not.

Our professions, both as institutions and identities, also have a role. Stopping models and measurements from becoming our masters is something we all need to do. As Feynman (1974) reminded us, we shouldn't fool ourselves. However, we have to take some things for granted, but which things are safely left without 'long existential epistemological consideration', as Patton (2008) puts it?

Afterword

The McNamara fallacy has powerful intuitive appeal, but little basis in empirical research. The authors hope that this paper will sensitise practitioners to the impact of an expedient approach to measurement on the quality of foresight in their organisations. We hope also that it will stimulate researchers to see if the fallacy reflects what they find in the field, and whether the mechanisms proposed here, and others we didn't think of, are valid.

Acknowledgements

We would like to thank Phil Parry, a retired inspector of major hazards installations, for his input to this paper.

References

Argyris, C. (1999) On organisational learning. Oxford, Blackwell.

Aulnay, R., Batiot, B. and Rogaume, T. (2017) Problématique de la gestion des configurations dans l'analyse préliminaire des risques, Rencontre inter-GTR : vers une vision systémique de la maîtrise des risques, Paris, 30 juin

Baker, James et al., 2007. "The Report of the BP U.S. Refineries Independent Safety Review Panel" http://www.safetyreviewpanel.com/, January 30, 2007.

BBC (2014) "French red faces over trains that are 'too wide'" BBC News, 21 May. http://www.bbc.co.uk/news/world-europe-27497727 (Accessed, 2/10/2017)

BBC (2017) "Train punctuality to be measured accurate 'to the minute'" BBC News, 18 July. http://www.bbc.co.uk/news/business-40635372 (Accessed, 2/10/2017)

Brunsson, N. (2002) "The Organization of Hypocrisy: Talk, Decisions and Actions in Organizations" Abrakt Forl: Copenhagen Business School Press, 2002, 2nd ed.

Columbia Accident Investigation Board (CAIB) (2003), Report Volume 1, National Aeronautics and Space Administration and the Government Printing Office

Committee of Public Accounts [UK] (2014) Transforming contract management. Twenty-third Report of Session 2014–15. HC 585.

CSB (2007) Investigation Report: Refinery Explosion and Fire. Report No. 2005-04-I-TX. U.S. Chemical Safety and Hazard Investigation Board.

Dien, Y. and Dechy, N. (2016) L'impensé est-il impensable ? Ce que nous apprennent les accidents industriels, In : M. Merad, N. Dechy, L. Dehouck, M. Lassagne (Edts), Risques majeurs, incertitudes et décisions – Approche pluridisciplinaire et multisectorielle, MA éditions, p. 69-96.

Feynman, R.P. (1974) Cargo Cult Science. Engineering and Science. Volume 37:7.

Fischer, D.H. (1970) Historians' Fallacies: Toward a Logic of Historical Thought. Harper Collins.

Frei, R., Garforth, A., Kingston, J., and Pegram, J. (2015) Using Operational Readiness

to improve the Management of Risk. White Paper 2, Vol 1. Pub. Noordwijk Risk Initiative Foundation.

Hand, D. J. (1996) Statistics and the Theory of Measurement. Journal of the Royal Statistical Society. Series A (Statistics in Society), Vol. 159, No. 3, p.445-492.

Horrocks, P., Mansfield, D., Thomson, J., Parker, K., and Winter, P. (2010) Plant Ageing Study – Phase 1 Report, ESR/D0010909/003/Issue2. A report prepared for the Health and Safety Executive, 27th February 2009.

Kingston, J., and Mertens, F.J.H., 2007. Future directions in accident investigation: lessons from the evaluation research literature. Proceedings of the ESReDA 33rd Seminar, Joint Research Centre, Ispra, Italy.

Lessig, L. (2011) Republic Lost. Twelve, Hachette Book Group.

McNamara, R.S. (1995) "In Retrospect". Random House.

Nader, R. (2016) Acceptance speech to the "Automotive Hall of Fame". https://youtu.be/vSYZNImEkys. Accessed and transcribed on 3 May 2017.

National Audit Office (2008) Reducing passenger rail delays by better management of incidents. Pub. The Stationery Office.

Nriagu, J.O. (1998) Clair Patterson and Robert Kehoe's Paradigm of "Show Me the Data'' on Environmental Lead Poisoning. Environmental Research, 71-78.

Osman, M. (2015) Future-minded: the role of prospection in Agency, Control and other future-directed processes. Frontiers in Psychology. Vol. 6, article 154.

Patton, M.Q. (2008) Utilization-Focused Evaluation. 4th Edition. Sage.

Perrow, C. (1984) "Normal accidents: Living with high risk-technologies", Princeton UP.

Piirainen, K.A., and Gonzalez, R.A. (2015) Theory of and within foresight. Technological Forecasting & Social Change, 2015, Vol.96

Pooley, E. (1996) Nuclear Warrior, TIME magazine, March 4.

Rohrbeck, R., Battistella, C., and Huizingh, E. (2015) Corporate foresight: An emerging field with a rich tradition. Technological Forecasting & Social Change, Vol 101.

Smith, A. (1972) The Last Days of Cowboy Capitalism, The Atlantic Monthly, September, p 43-55.

Vaughan, D. (1996) The Challenger Launch Decision. Risky Technology, Culture, and Deviance at NASA, The Chicago University Press, Chicago.

Woods, D.D. (2009) Escaping failures of foresight, Safety Science 47(4), p. 498-501.

Yankelovich, D. (2012) Personal correspondence with the author (Kingston).

Foresight for Risk Prevention and Resilience:to what Extent do they Overlap? – Extended Abstract

Nicolas Dechy, IRSN, Institut de Radioprotection et de la Sûreté Nucléaire, Fontenay-aux-Roses, France

Myriam Merad, CNRS, UMR ESPACE, Nice Sophia Antipolis University - UMR LAMSADE, PSL*, CNRS, Université Paris Dauphine, Paris, France

Laura Petersen, European-Mediterranean Seismological Centre, Bruyères-le-Châtel, France

Maria Luisa Pestana, EDP DISTRIBUIÇÃO - Energia, S.A., Lisbon, Portugal,

Igor Linkov, US Army Corps of Engineers, Concord, MA, USA

Yves Dien, CHAOS, Collectif Heuristique pour l'Analyse Organisationnelle de Sécurité, Paris, France

Extended Abstract

For several years now, resilience concepts appear to challenge traditional risk approaches. One of the key difference suggested is the way foresight is tackled in both. This paper discusses commonalities, differences and any overlaps in the use of foresight between these two approaches. Several lessons learned from historical cases are used for this purpose (before and after Toulouse chemical disaster, Fukushima nuclear accident, business continuity and crisis management for critical infrastructure). Both approaches are in fact rather complementary in fulfilling certain critical functions, and are less opposed than as claimed by resilience promotors. While the expectations and foresight differ, recovery is included in risk approaches as well as in resilience approaches. Furthermore, risk approaches also deal with unexpected events. The paper concludes with an analysis of the knowns, unknowns and awareness that enables one to distinguish different foresight categories in risk (defensive, reactive, ethical, proactive) and in resilience.

Keywords: Risk, Prevention, Resilience, Foresight, Anticipation

Session 3:
Foresight and technology

Potentials, limitations and problems of technologies for enhancing safety and foresight

Zdenko Šimić

European Commission Joint Research Centre, Dir. G – Nuclear Safety and Security

Postbus 2

1755 ZG, Petten, The Netherlands

Abstract

Technological advances potentially impact all stages of the life cycle of safety related systems. This is increasingly so with advanced sensors, as well as the exponential increase of computing power, communication bandwidth and storage capacity. The design and operation of safety related systems can benefit significantly with potential to continually reduce risk through the application of advanced software and hardware solutions including artificial intelligence (AI). The question is which kind of technological advances are in use and being developed and how they can potentially improve safety?

This paper aims at identifying major existing and emerging technologies with tangible potential safety benefits applicable to different life cycle phases of concerned systems (i.e., design, verification, validation, production, testing, commissioning, operation, maintenance, emergency response and decommissioning). These technologies generally comprise a combination of hardware and software used for e.g.: development, training, operation, monitoring, diagnoses and predictions. Examples are computer aided hybrid development, real time modelling analysis and various artificial intelligence applications. In this preliminary review the aim is to identify potentials, limitations and difficulties associated with the application of these advanced technologies for the enhancement of safety and foresight.

Some of the problems associated with the use of advanced technologies are related to the increased technical complexity that they may bring to the design (e.g., software and digital instrumentation and control validation and verification). In addition, other issues related to the need for connectivity like cyber security and privacy are becoming even more worrying. The open question is what are the limitations or ultimate potential benefits which can be gained by using advanced technology to enhance safety and foresight (considering challenges and benefits)?

Keywords: safety technologies, hardware, software, modelling, artificial intelligence

1. Introduction

We live in the age of rapid digitalisation which is significantly changing our lives. The change to society is mainly digital (new software and more powerful hardware) but it is also complemented with development of novel and inexpensive sensors and systems enabling connectivity and numerous applications, i.e.: communication systems, global positioning system (GPS), and internet of things (IoT), affordable data storage. This change is generally improving everyday life, economy and society as whole. From many impacts safety is of special importance because technological advances potentially impact safety related systems through all stages of the life cycle. A framework for an integrated nuclear digital environment, in [1], illustrates wide potentials and huge requirements. UN Sendai Framework for Disaster Risk Reduction (DRR) 2015-2030 emphasis on using science and technology is another example, [2].

The design and operation of safety related systems can benefit significantly with potential to continually reduce risk through the application of advanced hardware and software solutions. There are many questions about the role of technology in safety and first one is which kind of technological advances are currently in use and development?

This paper portrays a preliminary study, which aims to identify major existing and emerging technologies with tangible potential safety benefits applicable to different life cycle phases (i.e., design, verification, validation, production, testing, commissioning, operation, maintenance, emergency response and decommissioning) of the selected systems described in the paper. The goal is also to identify domains of application and examples of typical potential benefits emphasising potential for foresight in safety, along with their limitations. New technology, while solving problems, can often introduce new safety problems and can also face implementation challenges. This raises many questions about optimal development, regulation and implementation of new technologies.

The paper is organised in the following way: Section 2 describes approach and scope; Section 3 presents findings and discussion; finally, Section 4 contains concluding remarks. This paper is part of the ongoing work in the ESReDA Project Group on Foresight in Safety and it presents initial results from horizon scanning.

2. Approach

Role of technology in safety and foresight is inherently connected to all safety systems and any other use of technology in general. This presents a rich playing field of opportunities for discovering many different applications, approaches, regulations and experience. However, learning about them and properly understanding value for numerous applications in all different domains is a significant challenge. Literature review was selected as approach to gain from multi-domain role of technology in safety and foresight. Considering author's background, main focus was dedicated to the nuclear field; however, other fields are included in an effort to make review more comprehensive. Similar examples from different domains are used in order to illustrate common solutions. Reviewing different domains is also valuable in identifying both generic and unique issues and potential limitations.

Google Scholar (scholar.google.com) online tool was used as it seems to be a very comprehensive and accessible cross-domain literature database. Performing search is as easy as for regular web search with some special functionalities for selecting time range, finding related articles to any selected article and looking for citations (both per google and per Web of Science). This is all web browser based and needless to say hyperlinked. Search was made mostly for the last two years, with only few exceptions, in order to capture most recent development.

Initial search was made with key-words "technology" and "safety". Relevant articles were selected as pointers towards more refined search. Over 100 papers were initially selected and grouped by major domains including "miscellaneous" and "issues". A more detailed review has reduced the number of selected references for this paper to 60. This selection is certainly representative for the role of technology in safety and foresight. However, this is far from the most representative or comprehensive selection considering rapid developments, number of domains and applications.

The next section presents relevant findings across the following dimensions: technologies, domains, applications, life-cycle, foresight, and issues.

3. Findings and discussion

Findings about the role of technology are presented in six different dimensions in order to provide more complete picture. First of all, general groups of technology type were identified. Then, these general technologies are used in different domains. The third dimension is related to specific application of these technologies in different domains. Next dimension is the parts of life-cycle where technologies are used. While all identified technologies are used to enhance safety, initial effort was made to identify foresight as separate dimension. Final dimension is related to all issues preventing use or even potentially introducing new safety problems because of the use of new technologies.

The findings of this study are presented in two subsections: technologies and issues. The six dimensions are presented together in relation to technologies and issues. Finally, the third subsection, with discussion, pays special attention to foresight. The approach was to mainly focus on nuclear examples when available. Examples from other domains were added for completeness.

3.1 Findings about the role of technology in safety and foresight

The role of technology in safety and foresight is reviewed through examples from literature in nuclear and other domains. Findings are presented as short explanations of technology, application, part of the life-cycle and contribution to foresight. Grouping by technologies is imperfect because of numerous applications using several technologies combined.

3.1.1 Computing power and advanced software

Computing power is an enabling factor for better design and for many safety applications. Nuclear power plant design requires highest level of safety and economic competiveness. High performing computing with advanced modelling and simulation is necessary to include multi-physics "core simulation" (e.g., radiation transport,

thermal-hydraulics, corrosion chemistry, etc.) requiring robust numerical solutions algorithms and uncertainty quantification [3].

Plant simulators are a proven tools to train operators for complex systems like nuclear or process plants ([4]) and airplanes. Methods for selecting human system interface are evolving with technology development and it has to go beyond user interface, [5]. Simulators are improving in two different directions in order to make them completely realistic and simple. So called full scale simulators are able to present not just full operational characteristics of the plant but also accident conditions and scenarios, [6]. Simplified simulators are able to run on a single personal computer and still represent most of the plant operation. This improves both education and training for plant engineers and operators, [7].

Virtual and augmented realities (VR and AR) are the most advanced software developments with potential to improve education, training and operation. In [8] and [9] virtual environment and simulation are suggested to improve safety during work and decommissioning in nuclear facilities. In [10] use of augmented reality is evaluated for safety signs in the working environment. Use of AR for generating safety awareness and enhancing emergency response for construction, earthquakes and driving is reviewed in [11].

Visualisation and *multimedia* are demonstrated to be beneficial, for example in the construction industry (e.g, improved safety management and training, hazards identification, monitoring and warnings) [12], and preventing surgery mistakes [13]. *Building information modelling* (BIM) framework is used in construction design, implementation and operation for different domains (e.g., for nuclear [1] and general waste [14]) and applications (e.g., construction risk management [15] and fire protection [16]). BIM is also used for planning and building of first high level radioactive waste final disposal facility by Posiva in Finland, [17]. Risk management potentials for BIM are further enhanced using ontology and web semantic technologies [18].

Knowledge management (KM) concept is increasingly important for complex systems with longer life cycle and has potential to improve operation and decommissioning with better use of knowledge and experience,[19]. KM relies on information systems with databases, collaborative networking, expert systems, ontologies, web semantics and organizational culture.

Computing and software related technologies do not always depend on high computing power or sophisticated software. Sometimes *novel approach/algorithm* could make safety improvement, e.g. central control of trains to avoid rear-end collisions in [20].

3.1.2 Internet, communication, cloud computing, sensors, big data and AI

Sensors are irreplaceable components for proper and safe operation as they are critical help for avoiding dangerous situations and reducing unwanted consequences. Requirements for sensors (e.g., precision, speed, robustness, connectivity and energy consumption) vary greatly depending on the domain and application. One example in security checking for explosives, where both speed and sensitivity are required, is use of thermo-desorption mass spectrometry, [21]. Another example is in food safety (disease detection) and quality, the use of hyperspectral imaging technique for automated non-destructive analysis and assessment applied to wide range of food

products, as reviewed in [22]. Sensor measurement values also depend on software capable to diagnose conditions and predict developments. In [23], the use of distributed equation and artificial immunity system is proposed for online monitoring and prediction in condensate and feed water system of the nuclear power plant.

Internet, as a network of computers, sensors and people, has growing potential of technologies and applications for safety and foresight in many domains. Information about online search queries is used for various applications, e.g.: early detection of food related epidemics, [24]; perception and prediction of viral and other outbreaks, [25] and [26]. Together with sensor equipped smartphones this presents additional potential for safety technologies, e.g.: monitoring health behaviour,[27]; managing construction,[28]; and collision warning while driving,[29]. New software technology, blockchain, has potential to assure records validity which is important for proof of safety parts origin [30].

Geographical information system (GIS) is used for integrated regional risk assessment, [31]. Optical, radar and other satellite data is used as support for emergency response services in natural, technology and social related hazards, [32]. Disaster planning, warnings and response are incorporating the use of social networking like tweets, [33]. Increasing number and combined satellites use could make them more responsive (i.e., in hours) with improved resolution. Global positioning system (GPS) has many applications from industry to personal use, however commercially available resolution still limits some new applications, like autonomous driving, [34]. Video, mobile and other data are used for safety of various applications, e.g. intersection monitoring for safety analysis, [35]. Wearable personal devices with biosensors (e.g., hart beat, movement, sleep behaviour) are able to track physiology data helpful for detecting valuable health related information [36].

Accumulated data from increased number of sensors presents opportunity for better understanding of complex systems and might provide new insights for safety science, [37]. Analysis and interpretation of huge volumes of data ("*big data*") is requiring and enabling use of new techniques like artificial intelligence (AI). AI is machine learning in development with major advances with so called deep learning. Impressive AI results, like winning at GO game and superior medical diagnostics, are showing huge promises. However, timescale and limits for AI potentials are not easy to predict. About 50% of experts believe that high-level machine intelligence will be developed in the next 30 years and superintelligence might be developed 30 years after, [38]. New AI applications automatizing, more or less demanding, human work are becoming available, e.g. restaurants food safety check and news writing, [39].

Modern vehicles are equipped with more and more technologies assisting drivers (emergency braking, blind spot monitoring, line support system, objects recognition, etc.), along with fully *autonomous vehicles*, are expected to be commercially available in several years. Automated vehicles embodies the implementation of leading edge technology solutions, which include a number of different sensors, computing power and AI software [40].

From a large number of safety technologies, a few more are selected as illustration of vast potentials for safety and foresight. *Unmanned aerial vehicle* (UAV, drone) is used for numerous applications in remote monitoring. In [41], 3D radioactive contamination mapping is described for Fukushima-Daiichi nuclear accident. Eye movement recoding

and analysis allow experts, e.g. pathologists to learn and improve themselves, in [42]. Three-dimensional printing is used in many domains for preparation of difficult tasks, producing custom complex parts, and for education and training, e.g. in medicine [43].

3.2 Issues with use of technology for safety and foresight

Great potentials and promises of new technology for improving safety and foresight have to be tested and proven before fully introduced. This is necessary for simple applications like material condition monitoring ([44]) and complex solutions like digital control rooms (DCR), [45]. Example of DCRs shows that potential might be different for various domains depending on many elements, e.g. implementation and operators' age (in [45] potential side effects which reduce operators' reliability in DCRs for nuclear power plants are demonstrated). Verification and validation (V&V) for digital technology is an open problem. While by nature it allows virtual testing of true simulations, the existence of an immense number of possible states makes full testing impossible. This is the case with the autonomous car [46] and nuclear digital instrumentation and control, [47]. Experience proves that hardware and software induced failures are inevitable in complex digital systems and this should always be already factored into the system's recovery plan, [48]. Number of recommendations for research and development prioritisation in development of light water reactor is related to the adaptation of digital technologies (digital power plant) in order to address V&V and other issues, [49].

Internet and social networks are not just incredible resources, but they are also efficient and effective disseminators of fake information. This is an important issue during any emergency situation and it can have detrimental effects, as it was tragically illustrated during and after Fukushima Daiichi nuclear accident, [50]. It is important to always consider imperfect, incomplete and changing state for all online data usage, [51]. Perhaps some "degree of uncertainty" classification could be designed to assist in judging the quality of data.

While smartphones are allowing easy communication and access to information, they are also a distraction for important activities like driving, and could cause accidents, [52]. This is regulated in some countries and supported by apps which are recording activity of smartphone before accident.

Cost is limiting the introduction of some technologies with proven benefits before widely used and fully commercialised, and this depends on many factors. Cost of life in the U.S. and Colombia make a difference when evaluating cost-benefit analysis of commute bus crash avoidance system installation, [53].

Cybersecurity is one of several major issues for many internet and wireless based technologies because ultimate protection is impossible without losing functionality, e.g. for autonomous vehicles [54]. Hacking is an increasing problem on the internet and it might reduce trust in some new technologies like internet of things and artificial intelligence. Some related issues for autonomous vehicles and medical assistance devices are presented in [55].

Solutions for the above-mentioned issues are not trivial and will require additional work. For some of these issues, the solution is technology itself either already built in (e.g. communication for UAV collisions [56]) or complemented with other solutions

(e.g. documenting scientific software for nuclear safety applications [57]). Another part of the solution is learning by doing (e.g. for health IT [58]) after accepting new technology with simple criteria in order to prove that it is at least as good as existing technology. For some issues with new technology it will require developing new methods which will help prevent unwanted consequence, e.g. for detecting promoted social media campaigns [59].

3.3 Discussion about the role of technology in safety and foresight

One way to summarise here presented use of technologies for safety and foresight is to list results across six dimensions. Table I lists findings for all dimensions.

Potential for the role of technology in improving safety seems overwhelming. Prospective to improve foresight in safety looks also vast, e.g.: improved analysis and simulations to identify and anticipate safety issues; higher quality production to improve reliability; adaptive maintenance to prevent failures; continuous improvements with better operating data assessment; accident prevention with timely preparation and response; faster and better emergency response with appropriate organisation and communication [60]; prompt and appropriate accident management with real time assessment; improved learning from accident investigation; preventing societal disruptions with proper communication.

Table I: List of identified technologies and findings for different dimensions.

Dimension	**Findings**
Technologies	computing power, software, cloud computing, sensors, laser scanning, radars, artificial intelligence (AI), smartphones, social networks, internet, internet of things (IoT), geographic information system (GIS), global positioning system (GPS), virtual and augmented reality (VR, AR), 3D printing, big data analytics, knowledge management (KM), blockchain
Domains	transport, power generation, medicine, construction, mining, military, chemical industry, food, weather forecast, security, communication, internet, research & development, smart cities, disasters risk reduction, society
Applications	optimised design without safety compromise; enhanced validation and verification; virtual/augmented experience for better design, operation and emergency planning; improved and effective education, training, operation and maintenance;
Life-Cycle	all phases and activities – concept development, design, production, commissioning, operation, and decommissioning; validation, verification, testing, monitoring, education and training.
Foresight	improved analysis and simulations; quality production; adaptive maintenance; continuous improvements; accident prevention; faster and better emergency response; prompt and appropriate accident management; accident investigation; preventing societal disruptions
Issues	cost, complexity; verification & validation; faster change cycles; cyber security; disinformation; distraction; proving benefits; privacy; AI better than human;

4. Conclusion

Extensive review presents large number of examples where technology is used to improve safety and foresight. Significant evidence exist that various technologies individually and combined could improve safety and foresight. Some benefits are

already in use while others are in development. There are also new issues caused by complexity and quick introduction of new technology. Some of them could be resolved by using technology. These issues will require specialists' solution, but they are also depending on regulation and users perception. New technology adaptation might improve if relative prospective to exiting technology is assumed (i.e. by not increasing requirements) and applying learning by doing approach.

References

[1] Patterson EA, Taylor RJ, Bankhead M. *A framework for an integrated nuclear digital environment*. Progress in Nuclear Energy. 2016 Mar 31;87:97-103.

[2] Aitsi-Selmi A, Murray V, Wannous C, Dickinson C, Johnston D, Kawasaki A, Stevance AS, Yeung T. *Reflections on a science and technology agenda for 21st century disaster risk reduction*. International Journal of Disaster Risk Science. 2016 Mar 1;7(1):1-29.

[3] Turinsky PJ, Kothe DB. *Modeling and simulation challenges pursued by the Consortium for Advanced Simulation of Light Water Reactors (CASL)*. Journal of Computational Physics. 2016 May 15;313:367-76.

[4] Colombo S, Golzio L. *The Plant Simulator as viable means to prevent and manage risk through competencies management: Experiment results*. Safety Science. 2016 Apr 30;84:46-56.

[5] Hugo JV, Gertman DI. *A Method to Select Human – System Interfaces for Nuclear Power Plants*. Nuclear Engineering and Technology. 2016 Feb 29;48(1):87-97.

[6] Li Y, Lin M, Yang Y. *Coupling methods for parallel running RELAPSim codes in nuclear power plant simulation*. Nuclear Engineering and Design. 2016 Feb 29;297:1-4.

[7] NEI. *Educational revolution: An integrated suite of training simulators running on standard PCs is transforming initial training for all types of nuclear workers*. NEI; 2015 Nov 19. (www.neimagazine.com/features/featureeducational-revolution-4731118/)

[8] Jeong KS, Choi BS, Moon JK, Hyun DJ, Lee JH, Kim IJ, Kang SY, Choi JW, Ahn SM, Lee JJ, Lee BS. *The safety assessment system based on virtual networked environment for evaluation on the hazards from human errors during decommissioning of nuclear facilities*. Reliability Engineering & System Safety. 2016 Dec 31;156:34-9.

[9] Liu YK, Li MK, Peng MJ, Xie CL, Yuan CQ, Wang SY, Chao N. *Walking path-planning method for multiple radiation areas*. Annals of Nuclear Energy. 2016 Aug 31;94:808-13.

[10] de Amaral LR, Duarte E, Rebelo F. *Evaluation of a Virtual Environment Prototype for Studies on the Effectiveness of Technology-Based Safety Signs*. International Conference on Applied Human Factors and Ergonomics 2017 Jul 17 (pp. 100-111). Springer, Cham.

[11] Agrawal A, Acharya G, Balasubramanian K, Agrawal N, Chaturvedi R. A *Review on the use of Augmented Reality to Generate Safety Awareness and Enhance Emergency Response*. International Journal of Current Engineering and Technology, 2016 Jun; 6(3):813-820.

[12] Guo H, Yu Y, Skitmore M. *Visualization technology-based construction safety management: A review*. Automation in Construction. 2017 Jan 31;73:135-44.

[13] Dixon JL, Mukhopadhyay D, Hunt J, Jupiter D, Smythe WR, Papaconstantinou HT. *Enhancing surgical safety using digital multimedia technology*. The American Journal of Surgery. 2016 Jun 30;211(6):1095-8.

[14] Akinade OO, Oyedele LO, Munir K, Bilal M, Ajayi SO, Owolabi HA, Alaka HA, Bello SA. *Evaluation criteria for construction waste management tools: towards a holistic BIM framework*. International Journal of Sustainable Building Technology and Urban Development. 2016 Jan 2;7(1):3-21.

[15] Zou Y, Kiviniemi A, Jones SW. *A review of risk management through BIM and BIM-related technologies*. Safety Science. 2016 Jan 23.

[16] Cheng MY, Chiu KC, Hsieh YM, Yang IT, Chou JS, Wu YW. *BIM integrated smart monitoring technique for building fire prevention and disaster relief*. Automation in Construction. 2017 Dec 31;84:14-30.

[17] NEI, *Engaging with BIM*, 2016, Nov 17. (www.neimagazine.com/...-with-bim-5672206/)

[18] Ding LY, Zhong BT, Wu S, Luo HB. *Construction risk knowledge management in BIM using ontology and semantic web technology*. Safety science. 2016 Aug 31;87:202-13.

[19] Wang M, Zheng M, Tian L, Qiu Z, Li X. *A full life cycle nuclear knowledge management framework based on digital system*. Annals of Nuclear Energy. 2017 Oct 31;108:386-93.

[20] Wang J, Wang J, Roberts C, Chen L, Zhang Y. *A novel train control approach to avoid rear-end collision based on geese migration principle.* Safety science. 2017 Jan 31;91:373-80.

[21] Zhao Q, Liu J, Wang B, Zhang X, Huang G, Xu W. *Rapid screening of explosives in ambient environment by aerodynamic assisted thermo desorption mass spectrometry*. Journal of Mass Spectrometry. 2017 Jan 1;52(1):1-6.

[22] Liu Y, Pu H, Sun DW. *Hyperspectral imaging technique for evaluating food quality and safety during various processes: A review of recent applications*. Trends in Food Science & Technology. 2017 Nov 1;69:25-35.

[23] Wang H, Peng MJ, Wu P, Cheng SY. *Improved methods of online monitoring and prediction in condensate and feed water system of nuclear power plant*. Annals of Nuclear Energy. 2016 Apr 30;90:44-53.

[24] Bahk GJ, Kim YS, Park MS. *Use of internet search queries to enhance surveillance of foodborne illness.* Emerging infectious diseases. 2015 Nov;21(11):1906.

[25] Petersen J, Simons H, Patel D, Freedman J. *Early detection of perceived risk among users of a UK travel health website compared with internet search activity and media coverage during the 2015–2016 Zika virus outbreak: an observational study*. BMJ open. 2017 Aug 1;7(8):e015831.

[26] Bates M. *Tracking Disease: Digital Epidemiology Offers New Promise in Predicting Outbreaks*. IEEE pulse. 2017 Jan;8(1):18-22.

[27] Ernsting C, Dombrowski SU, Oedekoven M, LO J. *Using Smartphones and Health Apps to Change and Manage Health Behaviors: A Population-Based Survey*. Journal of medical Internet research. 2017 Apr;19(4).

[28] Azhar S, Jackson A, Sattineni A. *Construction apps: a critical review and analysis*. In ISARC. Proceedings of the International Symposium on Automation and Robotics in Construction 2015 Jan 1 (Vol. 32, p. 1). Vilnius Gediminas Technical University, Dep. of Construction Economics & Property.

[29] Botzer A, Musicant O, Perry A. *Driver behavior with a smartphone collision warning application – A field study.* Safety science. 2017 Jan 31;91:361-72.

[30] Zheng Z, Xie S, Dai HN, Wang H. *Blockchain Challenges and Opportunities: A Survey*. Work Pap. 2016.

[31] Zhao M, Liu X. *Regional risk assessment for urban major hazards based on GIS geoprocessing to improve public safety*. Safety science. 2016 Aug 31;87:18-24.

[32] Denis G, de Boissezon H, Hosford S, Pasco X, Montfort B, Ranera F. *The evolution of earth observation satellites in europe and its impact on the performance of emergency response services.* Acta Astronautica. 2016 Nov 30;127:619-33.

[33] Landwehr PM, Wei W, Kowalchuck M, Carley KM. *Using tweets to support disaster planning, warning and response*. Safety science. 2016 Dec 31;90:33-47.

[34] Murrian MJ, Gonzalez CW, Humphreys TE, Pesyna Jr KM, Shepard DP, Kerns AJ. *High-precision GPS Vehicle Tracking to Improve Safety*. TR-1115, D-STOP, University of Texas. 2016 Sep.

[35] Shirazi MS, Morris BT. *Looking at intersections: a survey of intersection monitoring, behavior and safety analysis of recent studies*. IEEE Transactions on Intelligent Transportation Systems. 2017 Jan;18(1):4-24.

[36] Li X, Dunn J, Salins D, Zhou G, Zhou W, Rose SM, Perelman D, Colbert E, Runge R, Rego S, Sonecha R. *Digital health: tracking physiomes and activity using wearable biosensors reveals useful health-related information.* PLoS biology. 2017 Jan 12;15(1):e2001402.

[37] Ouyang Q, Wu C, Huang L. Methodologies, principles and prospects of applying big data in safety science research. Safety Science. 2018 Jan 1;101:60-71.

[38] Müller VC, Bostrom N. *Future progress in artificial intelligence: A survey of expert opinion*. Fundamental issues of artificial intelligence 2016 (pp. 553-570). Springer.

[39] Thurman N, Dörr K, Kunert J. *When Reporters Get Hands-on with Robo-Writing: Professionals consider automated journalism's capabilities and consequences*. Digital Journalism. 2017 Feb 26:1-20.

[40] McGehee DV, Brewer M, Schwarz C, Smith BW, Jensen M, Tudela A, Row S, Krechmer D, Flanigan E. Review of Automated Vehicle Technology: Policy and Implementation Implications. UoI, RB28-015, IDoT, 2016 Mar.

[41] Martin PG, Kwong S, Smith NT, Yamashiki Y, Payton OD, Russell-Pavier FS, Fardoulis JS, Richards DA, Scott TB. *3D unmanned aerial vehicle radiation mapping for assessing contaminant distribution and mobility.* International Journal of Applied Earth Observation and Geoinformation. 2016 Oct 31;52:12-9.

[42] Brunyé TT, Mercan E, Weaver DL, Elmore JG. *Accuracy is in the eyes of the pathologist: The visual interpretive process and diagnostic accuracy with digital whole slide images*. Journal of biomedical informatics. 2017 Feb 28;66:171-9.

[43] Marro A, Bandukwala T, Mak W. *Three-dimensional printing and medical imaging: a review of the methods and applications*. Current problems in diagnostic radiology. 2016 Feb 29;45(1):2-9.

[44] Boguski J, Przybytniak G. *Benefits and drawbacks of selected condition monitoring methods applied to accelerated radiation aged cable*. Polymer Testing. 2016 Aug 31;53:197-203.

[45] Liu P, Li Z. *Comparison between conventional and digital nuclear power plant main control rooms: A task complexity perspective, Part I: Overall results and analysis*. International Journal of Industrial Ergonomics. 2016 Feb 29;51:2-9.

[46] Kalra N, Paddock SM. *Driving to safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability?*. Transportation Research Part A: Policy and Practice. 2016 Dec 31;94:182-93.

[47] Li Y, Lin M, Yang Z, Hou Y, Yang Y. *Methods of applying nuclear simulation technology to the dynamic site testing of digital I&C system—I: Scheme of OLVT*. Annals of Nuclear Energy. 2017 Jun 30;104:157-65.

[48] Fan CF, Yih S, Tseng WH, Chen WC. *Empirical analysis of software-induced failure events in the nuclear industry*. Safety science. 2013 Aug 31;57:118-28.

[49] McCarthy K. *Research, Development and Demonstration (RD&D) Needs for Light Water Reactor (LWR) Technologies* A Report to the Reactor Technology Subcommittee of the Nuclear Energy Advisory Committee (NEAC) Office of Nuclear Energy US Department of Energy. Idaho National Laboratory, Idaho Falls, ID (United States); 2016 Apr 1.

[50] Utz S, Schultz F, Glocka S. *Crisis communication online: How medium, crisis type and emotions affected public reactions in the Fukushima Daiichi nuclear disaster*. Public Relations Review. 2013 Mar 31;39(1):40-6.

[51] Diaz F, Gamon M, Hofman JM, Kıcıman E, Rothschild D. *Online and social media data as an imperfect continuous panel survey*. PloS one. 2016 Jan 5;11(1):e0145406.

[52] Boudette NE, *Biggest Spike in Traffic Deaths in 50 Years? Blame Apps*. New York Times. 2016 Nov 15. (www.nytimes.com/2016/11/16/business/tech-distractions-blamed-for-rise-in-traffic-fatalities.html)

[53] Mangones SC, Fischbeck P, Jaramillo P. *Safety-related risk and benefit-cost analysis of crash avoidance systems applied to transit buses: comparing New York City vs. Bogota, Colombia*. Safety science. 2017 Jan 31;91:122-31.

[54] Straub J, McMillan J, Yaniero B, Schumacher M, Almosalami A, Boatey K, Hartman J. *CyberSecurity considerations for an interconnected self-driving car system of systems*. System of Systems Engineering Conference (SoSE), 2017 12th 2017 Jun 18 (pp. 1-6). IEEE.

[55] Hengstler M, Enkel E, Duelli S. *Applied artificial intelligence and trust — The case of autonomous vehicles and medical assistance devices*. Technological Forecasting and Social Change. 2016 Apr 30;105:105-20.

[56] Dill ET, Young SD, Hayhurst KJ. SAFEGUARD: *An assured safety net technology for UAS*. In Digital Avionics Systems Conference (DASC), 2016 IEEE/AIAA 35th 2016 Sep 25 (pp. 1-10). IEEE.

[57] Smith WS, Koothoor N. *A document-driven method for certifying scientific computing software for use in nuclear safety analysis*. Nuclear Engineering and Technology. 2016 Apr 30;48(2):404-18.

[58] Fong A, Howe JL, Adams KT, Ratwani RM. *Using Active Learning to Identify Health Information Technology Related Patient Safety Events*. Applied clinical informatics. 2017;8(1):35-46.

[59] Ferrara E, Varol O, Menczer F, Flammini A. *Detection of Promoted Social Media Campaigns*. In ICWSM 2016 Mar 31 (pp. 563-566).

[60] Xie T, Li CD, Wei YY, Jiang JJ, Xie R. *Cross-domain integrating and reasoning spaces for offsite nuclear emergency response*. Safety science. 2016 Jun 30;85:99-116.

Cogeneration: technologies, possibilities, challenges

Tomasz Jackowski, Karol Kowal, Sławomir Potempski

National Centre for Nuclear Research

7 Andrzeja Sołtana Str.

05-400 Otwock, Poland

Abstract

The concept of High Temperature Gas Cooled and Very High Temperature Reactors (HTGR, VHTR) or Dual Fluid Reactors (DFR) are the examples of the attempts for building industrial applications based on the Generation IV nuclear technologies. These applications concern not only generation of electricity, but the production of process heat, hydrogen or hydrazine, which is of great importance for chemical industry. However, the licensing process of the newly designed reactors, comprising safety and reliability issues of the whole processing installations of the chemical plant needs special attention and appropriate research program to solve a number of foresight problems, not considered so far or not treated enough deeply in previous studies. The paper is an attempt to discuss these problems presenting main challenges for the implementation of such technologies, based on the experience gained during last years in Poland and in perspective of anticipated changes of the nuclear industry.

Keywords: Nuclear Cogeneration, High Temperature Reactors, Industrial Applications.

1. Introduction

Industry is responsible for about 24% of EU's consumption of fossil fuels and similar proportion of CO_2 emissions. This includes, among others, the following sectors: iron and steel making, food processing, the chemical industry, ceramics and glass wares and machinery production. The average level of CO_2 emission in different EU industries remains at about 37 Mt. However, in some Member States such as Germany, France, United Kingdom, Italy, Netherlands, Romania and Poland it is much higher, presenting the levels between 50 and 200 CO_2 Mt. This means that the climate policies should be treated as strategic issues with the reduction of such emission as one of the main targets. This also means some strategic steps in the energy sector are supposed to be done, taking into account also needs of the industry.

Such a goal creates very significant economical and societal challenges. Apart from the emissions, the absence of alternatives to fossil fuel consumption leads to often unacceptable geopolitical dependence on supply countries, which is strictly related to energy security. This has been observed, for example, in case of Ukrainian crisis.

In the energy sector the nuclear reactors have been serving for many years as a source of clean energy, with very small greenhouse gases and other noxious emissions. Nuclear energy, however, is known to have a much wider potential than being used solely for the generation of electricity. Especially, it seems desirable that the nuclear reactors should start providing other forms of energy (heat, cold) for industry on a much wider basis than today. This mechanism is known as cogeneration of heat and power. The ideas and technical solutions for non-electric nuclear applications have been developed, although, for various reasons, they have not yet reached the same industrial maturity as for the generation of electricity. Following the progress of the nuclear technologies for non-electric applications, which is manifested by numerous documents on cogeneration and heat production, the International Atomic Energy Agency (IAEA) performed the initial target market analysis [1] which shown that:

- there is increased interest in non-electric applications facilitated by the recent development of advanced reactor concepts;

- the current trend to a market oriented restructuring in the energy sector requires an accurate estimation of the costs and benefits of nuclear applications in comparison with the non-nuclear suppliers of similar services;

- globally, since the use of nuclear energy is at a crossroads, with its prospects ranging between negligible and highly accelerated growth, it is important to identify the potential of the non-electric part of nuclear applications.

When it comes to the nuclear cogeneration of heat and power, there are more than 750 reactor years of experience around the world, but the range of applications was mostly limited to rather low temperatures such as steam production for the paper and pulp industry, district heating and seawater desalination. Nuclear cogeneration has been shown to be highly efficient increasing power plant efficiency even up to 35%.

Taking into account foresight (climate policies, reduction of dependence on fossil fuels, geopolitical issues) on one hand, and available nuclear technologies on the other hand some predictions on future applications of nuclear cogeneration can be made. The concepts of High Temperature Gas Cooled and Very High Temperature Reactors (HTGR, VHTR) or Dual Fluid Reactors (DFR) are the examples of the attempts for building industrial applications based on the Generation IV nuclear technologies. These applications concern not only generation of electricity, but the production of process heat, hydrogen or hydrazine, which is of great importance for chemical industry. However, the licensing process of the newly designed reactors, comprising safety and reliability issues of the whole processing installations of the chemical plant needs special attention and appropriate research program to solve a number of problems, not considered so far or not treated enough deeply in previous studies.

The paper is an attempt to discuss these problems presenting main challenges for the implementation of such technologies, basing on the experience gained during last years

in Poland (among others, the EU program NC2I-R: "*Nuclear Cogeneration Industrial Initiative - Research and Development Coordination*" [2] and Polish program HTR-PL: "*Development of high temperature reactors for industrial applications*").

2. Possible applications of cogeneration

In the nearest future the best opportunities for cogeneration will be application of High Temperature Reactors (HTR) for the chemical industry. In this respect within NC2I-R project [2] a review has been made taking into account the following main processes compatible with HTR capabilities:

- refinery distillation steam;
- refinery distillation superheated steam;
- petrochemicals - reaction enthalpy;
- steam as utility for industrial complex;
- paper steam (drying).

Mapping of industrial sites was conducted in a manner allowing describing the heat market and distinctive European industrial areas. The following data were gathered:

- rated thermal power;
- electric power production and usage;
- fresh steam parameters (temperature, pressure, mass flow);
- process steam parameters (temperature, pressure, mass flow);
- current power production unit characteristics (size, age, fuel);
- others (e.g. environmental factors, regulatory framework etc.).

In total 132 sites were identified within Europe, 57 provided data related to their needs. A significant share of the sample sites uses less than 100 MWth – 20 sites. About the same proportion needed between 100 and 250 MWth. The last significant category was about 500 MWth, in this category include 9 sites. The electrical power demand is distributed somewhat in more uniform manner. The lowest demand – up to 50 MWe was reported by 20 sites. Each of next categories, respectively 51-100 MWe, 101-200 MWe and 201-400 MWe, reported between 4 and 6 sites.

As far as need for process heat is considered it can be estimated as 600-900 GWh per year for temperatures below 250°C, 250-550°C and above 1,000°C. The lowest interval can be accommodated by light-water reactors (LWR). The highest range (above 1,000°C) can be treated as highly prospective due to possible production of hydrogen and hydrogen-based fuel. The steam with temperatures about 500°C is a standard process heat in large industrial plants, mostly chemical. Application of

nuclear reactors should be easier in this case, as they would replace old steam generators (gas or carbon types), still using existing turbines for power generation. For example, in case of Polish industry it has been estimated that there is a need for such a steam in several plants, in total, about 6,500 MWth.

3. Technologies

Based on the valuable results of the German HTR development program up to the late 1980s, significant progress has been made by a several European FP5-7 R&D projects which obtained further leverage through the collaborative participation of European organizations in international projects (NGNP, PBMR, HTR-10) and in Generation IV International Forum (GIF). The most outstanding examples are in the areas of fuel production and qualification, the qualification and coding of high temperature structural materials and new graphite grades (incl. through irradiation testing), component development (e.g. turbomachines, heat exchangers), helium technologies and licensing-relevant modelling (e.g. reactor physics, thermo-fluid dynamics, mechanics, tritium transport, source term calculations, system code integration). In addition, significant improvement was achieved in understanding the market and end-user needs so as to design a power plant accordingly. The European System Integration studies in ARCHER and in NC2I-R, the ANTARES and SC-HTGR projects performed by AREVA, and several other reflect this development.

3.1 High and Very High Temperature Gas Cooled Reactors (HTGR/VHTR)

There are many advantages of HTGRs over conventional water cooled reactors. First of all, the large mass of the graphite moderator provides high heat capacity. Core materials are made of ceramic materials usable at elevated temperatures. The helium coolant is single phase and an inert fluid. Thus, chemical interactions between fuel, moderator, and coolant can be avoided. One of the most attractive features, however, is inherent safety – there is no possibility of reactor core melt [3]. This is due to usage of TRISO fuel and physical characteristics of the reactor causing spontaneous shutdown in case of the loss of coolant.

The TRISO-coated particles have an overall diameter in the range of 500 to 1,000 μm. Each particle contains a spherical fuel kernel (350 to 600 μm diameter) of fissile or fertile fuel materials, usually in the form of uranium dioxide (UO_2), plutonium dioxide (PuO_2), or an uranium oxycarbide (UCO) mixture. Typical fuel enrichments vary from 8 to 20%, as dictated by power rating and safety considerations. The fuel kernels are then coated with successive layers of pyrocarbon (PyC) and silicon carbide (SiC). First, a low-density PyC buffer coating is applied that provides void volume to accommodate fission gas and attenuates fission product recoils released from the fuel kernel. This layer is surrounded by successive coatings consisting of an inner PyC layer (IPyC), a silicon carbide (SiC) layer and an outer PyC layer (OPyC). The irradiation behaviour of the PyC coatings on either side of the SiC provides prestressing to assist in accommodating internal pressure. The SiC layer is the primary pressure vessel and is an effective barrier to fission product release [4]. The coated particles are overcoated with a resinated graphite powder to prevent particle-to-particle contact during either sphere making or compact formation. In the prismatic design, the overcoated TRISO particles are imbedded within a graphite matrix to form cylindrical compacts (Fig. 1).

Approximately 3,200 of compacts are inserted into a hexagonal fuel element. In the pebble bed design, overcoated TRISO particles are also imbedded in a graphite matrix; however, in this case, in the form of a spherical element with hundreds of thousands of them making up the core (Fig. 2). The fuel construction and performance may differ among various HTGR designs [5].

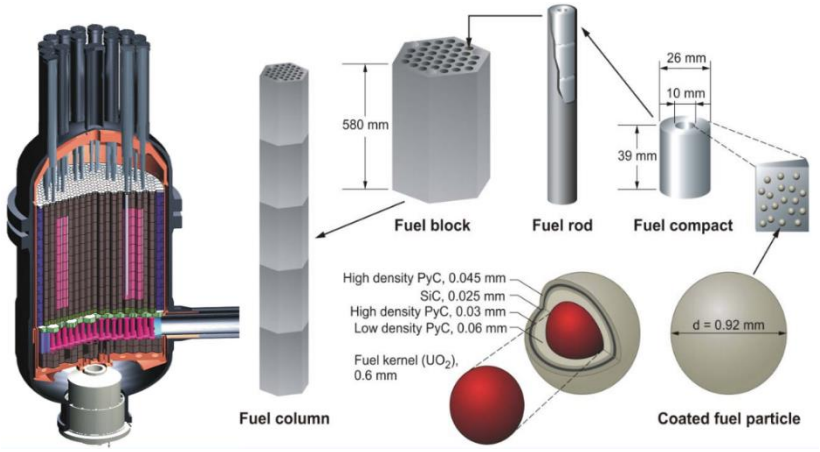


Figure 1. TRISO fuel in a prismatic HTGR [6, 7].

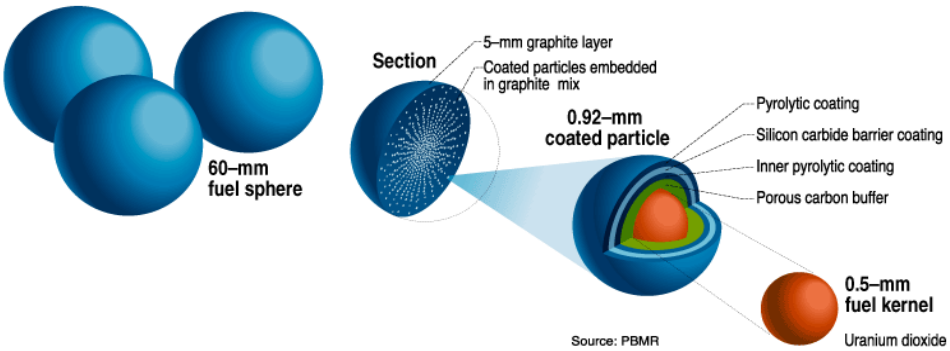


Figure 2. TRISO particles in a pebble bed HTGR [7].

It seems that the gas cooled high temperature reactors are optimal for the production of steam with 500°C is. For practical implementation, however, there is a need for preparing a demonstration project, which requires further work in the areas of system design, based as much as possible on proven technologies. As a part of the activities of just started GEMINI+ project and the US NGNP Industry Alliance, it is intended to obtain a maximum design convergence for a future demonstrator, still allowing for differences where licensing requirements or market needs impose them. For the successful demonstration, a functioning and stable licensing framework is required at an early stage as part of the infrastructure. This will guide the conceptual design and possibly required targeted R&D. This licensing framework must be capable of taking into account the specific safety approach of modular reactors based on inherent safety features of the system and addressing the coupling with industrial processes.

Further development of HTR technology is seen in the new concept of long lifetime Very High Temperature Reactor (VHTR) which would produce outlet temperatures of ~950°C for large-scale hydrogen production, process heat applications, and Brayton

cycle electricity production, while increasing fuel discharge burnup for better uranium utilization. The higher operating temperature conditions and increased burnup may be achieved by replacing the conventional UO_2 fuel kernel with a stoichiometric two-phase mixture of UO_2 and UC_2, namely UCO [4].

3.2 Dual Fluid Reactors (DFR)

The Dual Fluid Reactor is a novel concept, whose key feature is the employment of two separate liquid cycles, one for fuel and the other one for the coolant. A very high power density resulting in remarkable cost savings, and a highly negative temperature feedback coefficient, enabling a self-regulation without any control rods or even mechanical parts in the core, are the most interesting advantages of this new design. In the reference design of DFR proposed by Armin Huke et al. in 2015 [8], the fuel liquid is an undiluted actinide trichloride based on isotope-purified Cl-37, circulating at an operating temperature of 1,000°C. The pure Lead is to be used as a coolant. The coolant liquid is required to have the highest possible heat transportation capability and best neutronic properties. Pure molten Lead has low neutron capture cross-sections, a low moderation capability, and a very suitable liquid phase temperature range. Consequently, a DFR has increased power density, small core and fuel volume, and very hard neutron spectrum that improves the neutron economy and the Energy Return on Investment [9]. Figure 3 depicts the reactor core as well as the fuel loop and the primary coolant loop. The liquid fuel enters the core vessel at the bottom, spreads over a system of vertical tubes where it becomes critical, and leaves the reactor on top towards the Pyrochemical Processing Unit (PPU). The Lead coolant enters the core vessel from the bottom takes the heat from the fuel duct by conduction and leaves the vessel on top towards the heat exchanger. During each cycle the temperature of the Lead coolant changes from 750°C (at the bottom of the core) to 1,000°C (inlet of the heat exchanger) and back to 750°C (outlet of the heat exchanger). Consequently, the temperature inside the fuel (tube centre, not at the walls) is 1,150°C at the bottom and 1,400°C at the top which defines the highest absolute temperature in the reactor core. Depending on the power needed, part of the Lead's heat is taken for electricity production or as process heat.

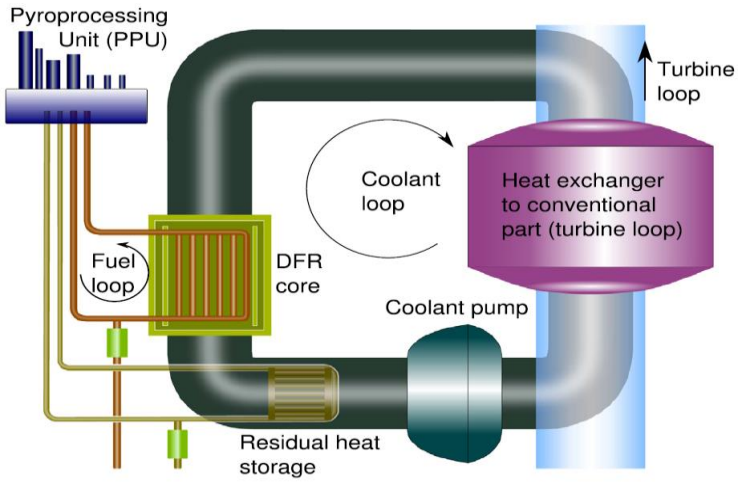


Figure 3. DFR fuel and cooling loop. The fuel circulates between the PPU and the core whereas the coolant loop connects the fissile zone to the conventional part [8].

The high temperature opens many innovative applications of DFR which is depicted schematically in Fig. 4. In addition to electricity generation it can be used in [8]:

- *Process heat generation only*. The conventional part of DFR needs to be modified for this application. The heat transducer to a secondary coolant cycle or a direct heating of a chemical reactor in close vicinity with primary coolant may be used.

- *Mixed process heat and electricity generation*. The first heat exchanger which decouples heat energy at the high operating temperature may be followed by a subsequent heat exchanger which heats at a lower temperature water in a steam.

- *Radiotomic chemical production*. Utilization of intensive radiation for radiotomic induction of chemical reactions requiring high doses [10]. E.g. Nitrogen oxide NO_2 and ozone O_3 can be obtained by irradiation of compressed air; Hydrocyanic acid HCN from methane and nitrogen; CO from radiative dissociation of carbon dioxide. The DFR reference plant may produce $10^{4\text{-}5}$ tons/year of these chemicals.

- *Magneto hydrodynamic generators (MHD)*. There is a possibility for utilization of an MHD generator connected to the Lead coolant loop of the DFR reactor. MHDs transform thermal energy and kinetic energy into electricity. These generators are different from traditional ones in that they operate at high temperatures without moving parts which may be significantly less costly than turbines. Liquid metals are eligible for that because of their high concentration of free charge carriers.

- *Medical isotope production*. One single DFR produces at least 30 kg/year of Mo-99 (a precursor of ^{99m}Tc which is needed for medical diagnostics), and what is even more important, already provides it in a separated form. Mo-99 can be quickly withdrawn in large amounts with no further processing. This strongly reduces the handling so that a complete on-site medical-clean production of the technetium generators are feasible which further simplifies the logistics.

- *The hydrogen-based chemistry*. Production of synthetic fuels suitable for today's vehicles. The low costs make these applications competitive with fossil fuels.

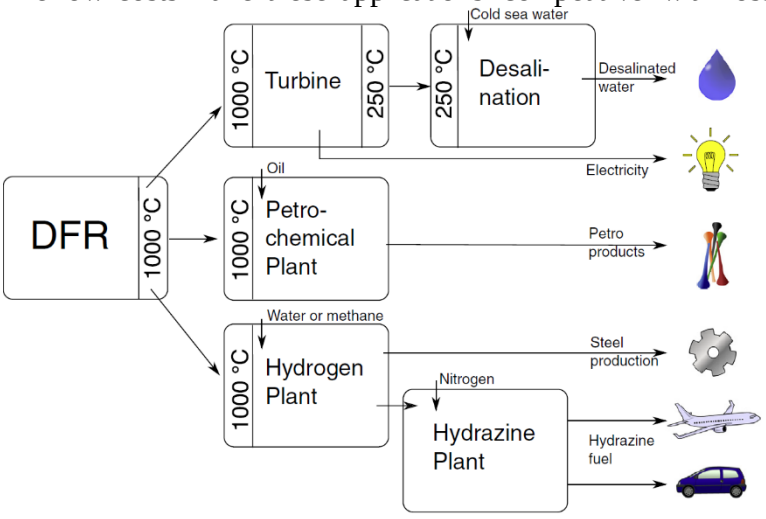


Figure 4. Possible applications for the DFR [8].

4. General approach to licensing issues

The analysis of licensing issues has been made within NC2I-R and HTR-PL projects with consideration of the previous NGNP guidelines [11]. In principle the screening of past and recent cogeneration applications with a nuclear heat source reveals no specific licensing issues beyond the standard licensing requirements of the NPP. However, for some standard requirements a higher effort will be needed to address specific cogeneration related aspects. This concerns such issues like evaluation of external hazards by nearby industrial facilities or fast isolation options for transfer lines out of the NPP site. Regarding other standard requirements, the specific safety features of modular HTR should lead to the improvement of the nuclear safety (e.g. reduced exclusion zone possible because of limited radioactive releases even during beyond design basis events) and of the economic conditions.

For nuclear facilities the limits for the emissions or releases of radionuclides in general are defined in national regulations. It should be expected that for cogeneration applications the aspect of a product free (according to international or national limits) from artificial radioactive contamination will be even more in the focus of the public. This specific care should be met by promoting the radionuclide barriers already applied in modern NPP for normal operation and design based accidents and the additional advantages given by the HTR technology. The tritium contamination issue related to gaseous primary coolant circuit should be also addressed. Tritium, as well as hydrogen, is able to diffuse through the metallic walls of heat exchanger tubes or sheets and therefore the contamination of the secondary coolant circuit with tritium has to be considered in the radiological assessment. It seems that He purification systems proved good efficiency and that additional contamination of the secondary circuit through leaks could be avoided by maintaining the secondary circuit overpressure. Moreover, an additional barrier against the contamination of product stem or product gas by tritium could be provided by a tertiary circuit. Such an additional circuit has been already proposed in the project EUROPAIRS in order to minimize the effort for the licensing process of the prototype HTR. On the other hand, recent investigations in the ARCHER project indicate that reasonable limits of tritium contamination in process steam might also be met without a tertiary circuit. This surely needs further research and clarification. To effectively support the licensing of HTR based cogeneration application and in particular a prototype facility, the NC2I-R consortium recommends that the following activities should be conducted in addition and in advance to the standard licensing procedure:

- in a pre-application phase, early discussion of the safety features specific for a modular HTR (e.g. passive decay heat removal, “vented containment”) with the regulator of the country hosting the demonstrator with the aim to achieve clarity about their consideration in the licensing process;

- a demonstration that cogeneration or process heat application issues are covered by the licensing procedure;

- a gap analysis for further R&D needs under consideration of the results achieved in the gap and SWOT analyses in the ARCHER project.

The licensing of the HTR shall follow the general licensing procedure covering the following main aspects:

- definition of the nuclear facility, its activities and the respective boundary conditions (e.g. dose and discharge limits, action levels);
- siting and site evaluation;
- safety and environmental impact assessment;
- safety demonstration of the proposed technology for all operation stages and accidental conditions;
- public inquiry;
- construction;
- commissioning;
- operation;
- decommissioning.

Because of the prototype issues and the strong interface to the local public, it has been pointed out that a road map should include an extended pre-licensing phase with a strong public involvement to promote a positive acceptance level in the local public. An extended environmental impact study should also be included.

5. Needs for further research and development

Most research needed for the implementation of HTR for industrial purposes concerns rather the choice of optimal solutions for specific technical problem than to overcome basic barriers. The other reason for the need of further research is related to solving licensing issues. The basic directions of research should be the following:

- deterministic safety analysis for HTR, i.e. neutronics and thermo-hydraulics calculations, in particular:
  - integrated models for thermo-hydraulics and neutronics analyses;
  - development of high fidelity models for HTR;
  - validation of numerical tools used for HTR design, concerning neutronics and thermo-hydraulics (distribution of power, neutron flux, temperature).
- probabilistic safety assessment of HTR integrated with chemical installation – integrated risk analysis chemical-nuclear installations, including analysis of interfaces, mutual reactions and interdependencies;
- material science issues: mechanical and thermal characteristics, corrosion effects in specific radiological conditions to determine reactor safety limits;

- determining basic characteristics of HTR like reactivity, distribution of core temperature, changes of pressure gradient;
- development and testing instrumentation of HTR;
- studies for new concepts of fuel and core structure.

In particular, the results of research should answer the following questions:

- Which types of interactions between nuclear and non-nuclear systems have to be considered, concerning safety aspects during normal and accidental situation?
- What can be the impact of non-nuclear incident (fire, explosion, toxic release) for the nuclear part of the installation?
- Is there a need for higher safety standard for nuclear reactor operating as a part of chemical installation?
- Is there a need to modify the strategy of the defence in depth?
- What kind of approach (deterministic, probabilistic, hybrid) is suitable during the design and licensing phase for cogeneration system?
- Which containment characteristics plays a deciding role for safe operation of nuclear reactor in cogeneration system?
- Is there a need for special regulations concerning emergency planning and response for such a processing system?

6. Safety issues

The most important technical problems needed for licensing, identified in NC2I-R project, are related to safety. This concerns the following:

- the evaluation of the fission product transfer coefficients in the fuel coatings and graphite matrix;
- find the means for evaluating the fuel temperature in standard and accidental operation;
- the achievement of a suitable radiative emissivity of the core barrel;
- in service inspection of the primary structures including graphite structures, fuel elements (blocks) and steam generator tubes;
- the evaluation of dust behaviour, distribution in the primary pipes and components (potential for accumulation, plate-out, etc.), resuspension and dust bound fission products phenomena and, in general, the development of a complete chain of computer codes for the modelling of source term in case of depressurisation scenarios.

- Probably the most crucial is to demonstrate passive decay heat removal capability, which is the fundamental safety requirement associated with the HTR concept. This should allow for determining and optimizing safety margins. Taking into account licensing issues the evaluation of normal and abnormal transients, based on both validated codes and tests (for example performed in demonstrator) is an important task. A number of guidelines on these issues were provided so far [12-13]. Uncertainty assessment related to the possibility of accidental radioactive release has to be done, however a conservative approach can be still a reasonable approach anyway.

- Further studies, for future development, are also needed in the field of development of high temperature resistant fuel and material together with efforts for enhancing the fuel quality control and reducing uncertainties on safety parameters (fuel maximum temperature and burn-up).

- Many safety problems concern the mutual dependence of nuclear and chemical parts. In principle the basic assumption is such that HTR and conventional installations should not influence each other in particular in case of severe accidents as explosions or release of corrosive materials. The safety related risk induced by external hazards ought to be independent from the cogeneration components and the end-user facility.

- In this respect the question of appropriate distance between these two parts have to be posed and solved. This concerns, however, two-way interactions. Hence, on one hand, any external hazard for the reactor caused by chemical facility has to be evaluated. On the other hand, any radioactive hazard coming from HTR has to be considered and taken into account while performing risk analysis in chemical installation. This means that radionuclide limits have to be precisely established by estimation of the consequences of the releases for all possible pathways.

Another safety issue is related to thermal hydraulic feedback/transients. Delivered by HTR process heat would represent the major part of the thermal power. One of the attractive features of HTR as a source of the heat is a possibility of processing at power of larger range than conventional systems. However, varying operation conditions at the transfer system or at chemical part will generate feedback/transients to the HTR. These feedbacks and transients have to be considered, evaluated and covered by corresponding safety systems (e.g. compressor chambers).

7. Conclusions

Foresight and technologies include application of nuclear cogeneration. In this respect, a number of advantages for using HTR as a source of process heat can be mentioned – the most important ones are:

- inherent safety features of HTR;

- more flexible operating conditions than in case of conventional systems;

- possible decrease of restricted use zone;

- easier adjustment to the future needs by a possibility of adding new blocks;
- possible shorter construction time due to the modularity.

On the other hand, one can express some disadvantages:

- licensing can be a challenge, because of using new technical solutions not based on currently operating NPP;
- need for new regulations;
- human factor issues have to be considered, taking into account that several modular reactors are supposed to be controlled.

It seems that licensing procedures are the most burning issues as new regulations and procedures have to be developed by the regulator in order to reflect all the features of HTR. This, however concerns not only nuclear part, but also chemical one. Therefore, it seems that development a new framework for integrated approach to the safety of combined nuclear-chemical installations both from technical point of view, as well as, from legislative issues caused by the need for developing appropriate regulations, are necessary for successful practical realization of cogeneration applications.

References

[1] International Atomic Energy Agency (2002) Market potential for non-electric applications of nuclear energy, IAEA Technical reports series No. 410, Vienna.

[2] Nuclear Cogeneration Industrial Initiative - Research and Development Coordination, Periodic Report, (2015)

[3] Brinkmann G. et al. (2006): Important viewpoints proposed for a safety approach of HTGR reactors in Europe. Nucl. Eng. Des., vol 236, pp. 463-474.

[4] International Atomic Energy Agency (2010) High Temperature Gas Cooled Reactor Fuels and Materials, IAEA-TECDOC-1645, Vienna.

[5] International Atomic Energy Agency (1997), Fuel Performance and Fission Product Behavior in Gas-Cooled Reactors, IAEA, Vienna.

[6] Ortensi, J. (2012) Prismatic Core Neutronics Design and Fuel Cycle, IAEA Course on High Temperature Gas Cooled Reactor Technology Tsinghua University, Beijing, October 22-26, 2012.

[7] Windes, W. et al. (2014) Role of Nuclear Grade Graphite in Controlling Oxidation in Modular HTGRs, Idaho National Laboratory techn. report, Idaho.

[8] Huke, A., et al. (2015) The Dual Fluid Reactor – A novel concept for a fast nuclear reactor of high efficiency. Ann. Nucl. Energy., vol. 80, pp. 225-235.

[9] Weißbach, D., et al. (2013) Energy intensities, EROIs (energy returned on invested), and energy payback times of electricity generating power plants. Energy, vol. 52, pp. 210-221.

[10] Stannet, V.T., Stahel, E.P., (1971) Large scale radiation-induced chemical processing. Ann. Rev. Nucl. Sci., vol. 21, pp. 397-416.

[11] NGNP Licensing Basis Event Selection White Paper, September 2010

[12] International Atomic Energy Agency (2003) Considerations in the Development of Safety Requirements for Innovative Reactors: Application to Modular High Temperature Gas Cooled Reactors, IAEA, Vienna.

[13] International Atomic Energy Agency (2008) Accident Analysis for Nuclear Power Plants with Modular High Temperature Gas Cooled Reactor, Vienna.

Session 4:
Risk analysis as input to foresight

Emerging Risks in food and feed, the importance of foresight

Ana Afonso

European Food Safety Authority

Via Carlo Magno 1 A

43126, Parma (PR), Italy

Kenisha Garnett

Cranfield Institute for Resilient Futures (CIRF)

School of Water, Energy and Environment

Building 53, Cranfield University,

Cranfield, Bedfordshire MK43 0AL, United Kingdom

Hub Noteborn

Netherlands Food and Consumer Product Safety Authority (NVWA)

Catharijnesingel 59

3511 GG Utrecht, The Netherlands

Petros A. Maragkoudakis

European Commission, DG Joint Research Centre (JRC)

Directorate F – Health, Consumer Protection and Reference Materials

Via E. Fermi 2749

21028 Ispra (VA), Italy

Abstract

Food is produced, distributed and sold on a global scale. The interconnectivity of the market simultaneously builds resilience in supply chains but magnifies vulnerabilities, so it is more important than ever to have the best possible understanding of the world around us, and how it is changing. Reflection is required on how new technologies transform our global supply chains, trade policies, and future food production. The identification and prioritization of emerging risks is a complex process involving the gathering and evaluation of large amounts of information from different sources and the biggest challenge is to make sense of the complex interactions of different factors and actors in the food system to predict and possibly prevent future risks.

Forward-looking exercises have been employed by organisations, institutions, authorities or governments to enhance policy preparedness and promote prevention-based policy approaches. Foresight employs methods to explore change in the mid-to-long-term future based on the assumption that developments outside the food supply chain and even outside the food system are either directly or indirectly related to the development of a particular food-borne hazard. Typical outputs from foresight studies, specifically scenario planning, are multiple scenarios that model systemic change in the food system in order to reveal potential unknown patterns of food-related challenges. This paper briefly describes the development and use of scenario planning as a foresight methodology, presents specific case studies applied in the area of food safety, and discusses the challenges and opportunities linked to this approach for identification of emerging risks and policy preparedness.

Keywords: Global supply chains, Food systems, Emerging Risks, Foresight studies, Drivers of change, Scenario development, Preparedness.

1. Introduction

A series of food scares during the nineties resulted in consumers' distrust of European Union and National competent authorities to protect public health and ensure food safety. To establish the highest standards of food safety and ensure free movements of goods an innovative regulatory package was put in place. Regulation (EC) 178/2002, also known as the General Food Law, lays down the basic food safety principles and establishes the European Food Safety Authority (EFSA) as an independent scientific body, clearly separating risk assessment from risk management and giving EFSA a mission on risk assessment and risk communication in all fields directly or indirectly related to food and feed, animal and plant health.

The concept of 'emerging risks' is embedded in the regulation: 'The successful identification of risks at their early inception is at the heart of public health and environmental protection. Improved identification of emerging risks may become a major preventive instrument at the disposal of the Member States (MS) and the Community '. EFSA is required to establish monitoring procedures with respect to systematically searching for, collecting, collating, and analysing information and data with a view to the identification of emerging risks in the fields within its mission.

Food is produced, distributed and sold on a global scale. The interconnectivity of the market simultaneously builds resilience in supply chains but magnifies vulnerabilities, and therefore it is more important than ever to have the best possible understanding of the world around us, and how it is changing. Reflection is required on a variety of emerging technologies, and how these exponentially improved new technologies transform fields as diverse as our global supply chains, trade policies, and the distributional implications of future food production. The identification and prioritization of emerging risks is a complex process involving the gathering and evaluation of large amounts of information from different sources and the biggest challenge is to make sense of the complex interactions of different factors and actors in the food system to predict and possibly prevent future risks.

Beyond emerging risks, forward-looking exercises such as foresight studies have been employed by organisations, institutions, authorities or governments to enhance policy preparedness and promote prevention-based policy approaches. Foresight studies are inherently more complex than emerging risk identification, as they need to take into account all developments that might affect the topic at hand, and assess the effects of their combination on a specific system. Foresight studies usually have a longer-term horizon than emerging risk identification, and apply a variety of creative and participatory techniques, such as scenario building, designed not only to describe the future in a methodological and systematic way, but also to facilitate the identification of valuable information from the future that could have relevance for today's decision making.

This paper briefly describes foresight methodologies, presents specific case studies of foresight applied in the area of food safety, and finally discusses the challenges linked to this approach for the identification of emerging risks and policy preparedness.

2. Foresight Studies

The use of early warning systems, such as the Rapid Alert System for Food and Feed (RASFF) of the European Union, are reasonably well developed and effective in identifying and addressing short-term challenges; however, they are usually reactive in nature and at best can identify early 'trends' in emerging risks. Risk assessors, risk managers and policy makers however, must be ready to frame longer time horizons and prepare for developments beyond the typical four steps of the scientific risk assessment cycle (Van Leeuwen and Vermeire, 2007).

In the context of food systems, foresight approaches aim to anticipate emerging risks (and opportunities) that are difficult to characterise since they are the long-term outcomes of a range of operational and environmental factors, some of which may not be fully in play at the present time. Foresight employs methods to explore change in the mid-to-long-term future based on the assumption that developments outside the food supply chain and even outside the food system are either directly or indirectly related to the development of a particular food-borne hazard. Typical outputs from foresight studies are multiple scenarios that model systemic change in the food system in order to reveal potential unknown patterns of food related challenges. Such approaches demonstrate the potential for complementing the extensive and successful systems for monitoring the occurrence of hazards and risks within the food system.

2.1 Scenario planning (scenario development and analysis)

Scenario planning involves the development, analysis and use of scenarios for improved preparedness to emerging risks and strategic planning; i.e. assessing the robustness of strategies and policy approaches that withstand the risks presented by alternative plausible futures. Scenarios are a foresight tool used to explore uncertainty in complex systems. They are defined as a set of plausible, sequentially linked events that might potentially occur in the future (Jarke et al., 1998), and they are designed to understand, analyse and communicate information about the future, often with the intention to clarify current actions in the light of plausible and possible futures (Durance and Godet, 2010; Parson, 2008; Swart et al., 2004). Scenarios provide a framework for considering a wide range of interacting drivers and the potential consequences of events in order to think through possible responses to uncertainties in the future, using this knowledge to support development of effective, forward-looking policies that address risks. Scenarios help understand the social, economic and environmental impacts on food systems, using this knowledge to determine where future intervention is best directed. However, they do not predict the future; they rather aim to explore what the future could look like under the influence of specific driving forces (De Ruijter, 2014).

Scenarios should be: i) plausible and describe events and developments that fall within the limits of what might conceivably occur in the future ii) internally consistent, the combination of elements and factors in each scenario must be logical, compatible and consistent iii) fit for purpose, serving the aim of the foresight study, especially when looking at facilitating decision making, for example, if the aim of the exercise is to test the resilience of a regulatory system or a policy framework, creating a scenario that presents a 'perfect future' that is free of challenges would not serve the aim of the study iv) present multiple futures in order to capture alternative developments and better inform the foresight study. In such a case, care must be taken to ensure that the scenarios are diverse enough from each other, and not just a variation of a central theme, while at the same time not stretching them to such extremes that it threatens their plausibility.

An indicative foresight study process with specific reference to scenario development is indicated in Fig. 1.

Figure 1: Foresight study process

2.1.1 Environmental scanning: defining driving forces

A key common approach to scenario development is to identify those elements that are crucial and can bring change to the topic/system of the study; i.e. driving forces. The methodology used to identify relevant drivers of change can vary between foresight studies, but often employ variants of the PESTLE (political, economic, social, technological, legislative and environmental factors) framework (Brown 2007). Depending on the scope of the study, drivers can be macro/high level (e.g. trade, economic growth, food chain structure, consumer perception or values, food prices, climate change), or detailed and specific to a limited process (e.g. a specific category of primary production in the food chain), or even a combination of both. Once a set of drivers have been identified and clearly described, it is important to gain insights for each driver, current knowledge, trends, potential developments and related future hypothesis. This is usually done via a literature review and in consultation with experts, often through workshops, interviews or more structured Delphi exercises. The objective is to assess varying assumptions about food system conditions in order to reveal areas of uncertainty. Such analysis help to clarify what logical relationships exist between drivers to inform how they may lead to change in the system.

2.1.2 Scenario development: alternative plausible futures

Setting up scenarios is a creative process with no ready-made recipes. The basic principle of scenario analysis is that the full extent of risks and their interconnectedness is assessed. Every potential risk, both on the micro- and macro level, that influences the safety of the food system has to be used in the scenario analysis.

Scenarios are developed using a holistic approach that adopts analytical and deliberative/participatory techniques such as workshops, expert elicitation and computer-based modelling to build a spectrum of plausible alternative futures. A key aspect of the approach involves assessing how the drivers of change, based on factors that currently exist or are likely to emerge, evolve and interact with each other in the future. Usually two drivers are selected, on the basis of their importance and uncertainty, to help construct the scaffolding and axes of a scenario. The scenarios are broadly defined using the extremities of these axes. A 2 x 2 matrix is created, based typically on an assessment of the most critical uncertainties. Each quadrant of the matrix represents the skeleton of a different scenario, where the relationship between other drivers are described and characterised to establish the scenario context. The selection/prioritisation processes to designate the two main drivers, or the procedure to characterise the behaviour of the other drivers, can vary, e.g. by order/score of strength of impact on the system in question, via carefully created scoring criteria, by voting on driver importance and uncertainty, or by specifically selecting drivers that fit the study aim.

Additionally, beyond driver description, scenarios can feature also narratives (i.e. scenario descriptions). Narratives can be stories, days in the life of fictional characters, report-like descriptions of the current situations etc. Narratives help to better visualise a scenario, and offer room for more in-depth technical description of the dynamics of the system. Scenario narratives are developed through deliberation with key stakeholders and subject experts, and relay plausible future developments of the whole system, based on a coherent and internally consistent set of assumptions about key

relationships and driving forces. The shorter the time horizon of a scenario, the lower the chance of uncertainty, excitement and surprise. Scenarios with a longer time horizon make it easier to get people out of fixed mindsets, i.e. to 'step out of the box', which is crucial in forward looking exercises and can prove to be a major hurdle when involving in the process academic/technical experts with considerable experience in a narrow aspect of the topic. However, extensively long horizons undermine the relevance of the scenarios, and make them non-binding. Careful consideration of the scenario horizon to be used is therefore important.

2.1.3 Scenario analysis

Once scenarios have been fully described, information pertinent to the object of the study can be extracted. Problems, issues, challenges, opportunities and specific situations that appear in the scenario can be identified, analysed and used towards the aim of the study, e.g. proposing actions, measures, for today that can tackle or even prevent the problems of tomorrow. In this way, scenario planning establishes a context for dialogue and foresight in decision-making by providing a framework for assessing the robustness of policy approaches and risk governance.

A number of scenario development studies have been applied to assess the resilience of food systems (O'Keefe et al., 2016; Lakner and Baker, 2014; Vervoort et al. 2014; Chaudhury et al., 2013). These scenarios deliberately challenge the mental maps of food system actors, exploring deviations expected from a 'single' future that typically arise from trends and events outside the vision or awareness of those involved in the scenario development process. The following examples showcase how forward-looking studies employing scenarios can inform decision making in the field of EU food policy.

3. Foresight studies in the area of food safety

3.1 Precaution for food and consumer product safety: a glimpse into the future – NVWA (2010)

New and improved products are entering the food supply chain and while emerging technologies help to deal with problems, it is also know that new products can give rise to new problems. The Office for Risk Assessment and Research (BuRO) of Netherlands Food and Consumer Product Safety Authority (NVWA) is interested in emerging technologies that could enter the consumer market at any time in the next 10 to 15 years.

Experts from various disciplines were involved in scenario planning (i.e. workshops, interviews) that provided a glimpse into the future by indicating which innovative technologies are currently under development and could potentially be applied in consumer products and foods in coming years. Case studies were examined on what society could do to prevent unacceptable risks of new technologies while at the same time obtaining the benefits from those technologies.

Subsequently, three future scenarios were built setting out an extreme view on society i) totally safe, ii) risk=business and iii) sharing is knowledge. Each scenario was accompanied by a story describing in which innovative products could play a role in

our lives. BuRO investigated whether it is possible to identify any risks in relation to these innovative technologies at an early stage and ensure preparedness to control the risks (Van Duijne et al., 2010). Applying the risk governance approach of International Risk Governance Council (IRGC) (IRGC, 2009) the potential emerging risks of seven technological innovations were analysed: new generations GM crops, nanocomposites and polymer nanoparticles, synthetic nanoparticles in foods, functional foods, new food packaging and bioactive coatings, home diagnostics and new solar cells.

The scenario planning approach generated new topics for the research agenda and the guideline for the elaboration of a risk profile for the seven innovative products.

3.2 Plausible future scenarios for the UK food and feed system: exploring future pressures on food system actors – UK Food Standards Agency (2014)

A scenario development project for the UK Food Standards Agency was undertaken to investigate how the UK food system may evolve under a different set of assumptions about future developments. The scenarios produced have been used to explore long-term challenges for the food system to inform future food policy, providing information upon which to test the resilience of policy options against the scenarios.

The study relied on evidence from the academic literature, published reports and the knowledge of experts, gathered through workshops and interviews, to produce a range of plausible scenarios for the UK food and feed system in 2035. Over 60 stakeholders, representing government agencies, academic institutions and the food industry were involved in the process. A wide range of expertise, including economics, social science, food preparation and retail, and risk management, and those at all levels of the organization (e.g. operational, middle and upper management staff) were involved to gather a range of perspectives about the long-term challenges, key trends and drivers of change.

Employing morphological analytical methods (Voros, 2009), three scenario states were developed: Reference scenario (constant rate of change), Global Trading and Resource tensions; each describing different pathways that the UK food and feed system could take over a twenty-year period. The scenarios were exploratory and qualitative in nature, illustrating the consequences of trends and drivers of change on food system actors. There was an iterative process to validate the scenarios, involving interviews with a number of experts that reviewed how well the scenarios sit within a complex policy space. This form of validation allowed for refining the scenario frame, extending current thinking in a way that is both challenging and revealing. See Garnett et al. (2014) for a full description of the scenario process.

The implications of the scenarios were explored for different actors within the food chain (i.e. from production to consumption) with a particular focus on consumer food safety. While food safety is one of the priorities for the UK Food Standards Agency, other challenging issues such as the affordability of food, food security and sustainability were also considered. The issue of food safety was further explored in case studies of three different food types (e.g. cereals, soya, meat and sandwiches) to illustrate how the scenarios could be used to assess policy implications for different actors.

The research outlines the strategic issues and offer insights into intervention that may safeguard against risks to the food (or feed) chain, and assist in developing future food policy. The case studies were of added-value in that they enabled further reflection on the issues at stake, and provided insights into interventions that may safeguard against impacts on the food (or feed) chain, and support consideration of appropriate regulatory response (e.g. safety standards or controls).

3.3 Drivers of emerging risks and their interactions in the domain of biological risks to animal, plant and public health - EFSA (2014)

The study objective was to develop a structured approach for the identification of drivers of emerging biological risks and their interactions in order to improve EFSA capacity for identification of relevant biological emerging risks. Biological risks are an outcome of natural processes which may be influenced by human activities or autonomous developments. The anticipation of emerging risks should therefore be based on the identification of drivers.

A consultation of the Animal health and welfare (AHAW) and Biological hazards (BIOHAZ) Panels was conducted through an adapted Delphi approach. The experts were provided with a briefing note with background information on the objectives of the exercise and asked to identify drivers and emerging biological risks to animal and public health in the next 5-10 years. Subsequently a group of experts participated in a workshop focused on identifying most relevant parameters concerning viral agents associated with the food chain relevant for human and animal health, and how they interact. A parameter influence analysis was conducted to measure and visualise how the parameters interact: drivers (strongly influencing but not strongly influenced), passive (strongly influenced but not strongly influencing), critical (both strongly influenced and strongly influencing) or buffers (neither strongly influenced nor strongly influencing. In order to have a better understanding of the applicability of the general morphological analysis methodology (GMA), it was decided to work on a series of historical cases: Norovirus (since 1968), thermophilic Campylobacter spp. (since 1972), Shiga-toxin producing Escherichia coli in beef, mutton and vegetables (since 1980s), BSE and vCJD (since 1987), infectious salmon anaemia (late 1980s), outbreaks of Trichinella spp. in horse meat (late 1980ties), pandemic of Salmonella enteritidis in eggs (since 1990s), foot and mouth disease and classical swine fever outbreaks (1990s and 2000-2010), Asian Longhorned Beetle, Anoplophora glabripennis (starting in the EU in 2001), Tuta absoluta in tomato (2006), bluetongue spreading from the Mediterranean to northern Europe (2010), and enterohaemorrhagic E. coli in sprouts (2011).

A scenario modelling framework was developed for those parameters shown to be 'critical' in the parameter influence analysis. These scenarios included: i) present trends, ii) collapse of EU, iii) small scale farming, iv) large scale farming, v) positive development: good mix of parameter states leading to decreased risks.

It was concluded that there is potential to the use of GMA methodology but further work was necessary in developing scenarios which can inform EFSA's strategy for emerging risk identification.

3.4 Delivering on EU Food Safety and Nutrition in 2050 - Future challenges and policy preparedness – European Commission (2016)

The European Commission's (EC) foresight study entitled 'Delivering on EU Food Safety and Nutrition in 2050 – future challenges and policy preparedness' (European Commission, 2016) aimed to assess the resilience and readiness of the current food safety and nutrition policy and regulatory framework to address future challenges, thus contributing to ensuring that the EU citizens will continue to enjoy high standards of safe, nutritious and affordable food. The study was jointly developed by the Directorate General (DG) for Health and Food Safety (SANTE) and the DG Joint Research Centre (JRC). Drawing from the valuable experience of a previous JRC foresight study that aimed to identify research priorities for diet in health for 2050 (European Commission, 2014), the JRC-SANTE study also employed scenario development methodology.

Key to the development of the study were two participatory technical workshops, featuring recognised experts of various thematic backgrounds coming from EC services, EFSA, EU Member States national food and health authorities, academia, private food sector industry and professional associations, as well as non-governmental/consumer organisations.

The four study scenarios were based on the developments of specific drivers that can bring change and significantly impact the food system: diverging developments in global trade, food values, EU economic growth, agro-food chain structure, technology uptake, and social cohesion were meaningfully combined to create four diverse and fit-for-purpose food system scenarios for EU food safety and nutrition in 2050. Climate change impacts, natural resources scarcity and world population growth provided a constant background for all four scenarios. The four scenarios were: 'Global Food', 'Regional Food', 'Partnership Food', and 'Pharma Food'.

Food safety and nutrition challenges were identified from all scenarios and prioritised based on importance of impacts and likelihood to occur. These challenges were then mapped to the current EU policy and regulatory framework in food safety and nutrition, and, where gaps where identified and scenario-specific policy options that could address them were put forward. Finally, where required, research needs were also proposed to complement and facilitate policy options.

Within the boundaries of the study, the EU legal framework resulted robust; certain elements however would need further attention to strengthen the systems resilience, such as: harmonisation and streamlining of risk assessment procedure, which should include also risk-benefit assessment, need for a benchmarking system to measure regulatory performance in food safety and nutrition, an effective early-warning system for identifying emerging risks, potential adaptation of official controls and inspection mechanisms for diverse future needs, provision of clear food information to the public, as well as investment in food and nutrition education.

4. Discussion

Environmental scanning for defining driving forces constitutes the backbone of scenario planning. Expertise on different drivers of change covering a wide range of subject areas, often not present in a single institution needs to be available to ensure the

development of plausible scenarios. Identified drivers are highly connected, but may show effects on different timescales that need to be considered. Experts contributing to the study should have in-depth experience in their own field of work, recognising that it is not easy to 'step out of the box' to consider a radically different the future, while at the same time retaining and communicating their knowledge of historical and current trends that inform us of possible developments of the system in the future. It is crucial that creative techniques are used to help participants envisage the future and relate this back to their knowledge and expertise in order to develop highly plausible scenarios that gain 'traction' in the review of policy and strategy.

Integrating qualitative and quantitative data of different levels of uncertainty, (e.g. trade trends and expert knowledge views) is also necessary to reduce uncertainty and develop baselines and indicators of change. Analysis of drivers requires predictive modelling of large complexity. Bayesian network analysis is being used to investigate multifactorial issues, but issues related with quality of data and underlying assumptions must be expressed in a transparent manner.

- Scenarios describe a potential range of futures, but this does not mean that other futures cannot exist. Scenarios are a tool to identify challenges; it is the alternative futures that are described in all scenario studies, and not a single one, that is important for policy preparedness.

- Scenarios often describe worlds that are unpleasant, or that may not fit with the desires and vision that an individual may have. This can often lead to difficulty in accepting a scenario, and even a tendency to discredit it, or to even have the opposite effect, i.e. an attachment to a single scenario while ignoring the rest. Scenarios are not meant to be likable, and in fact it is probable that each member of the audience will not feel the same way towards a specific scenario. It is the usefulness of a scenario that is important, and the implications it may have for the system, and under such a scope even scenarios which are undesirable to some, hold a lot of value for effective policy preparedness.

- Highly disruptive events and 'black swans' often do not make part of scenario development, and, although nobody argues that such low-probability and high impact events can indeed take place, they change the system in such a way that it may invalidate the scope and aim of the foresight study, it is perhaps better to address them specifically via appropriately designed and aimed studies.

5. Conclusions and recommendations

Foresight studies promote a prevention-oriented and pro-active risk policy approach, which considers food systems as a whole; such a holistic view is crucial to achieve risk governance efficiency and coherence in a field that is often addressed by different policy areas (e.g. agriculture, health, internal market) and by different government levels (e.g. EU, MS, local authorities).

Scenarios present decision-makers with other perspectives and possible future options that reveal unfamiliar factors of developments across the food system, and raise awareness about inherent uncertainties. Moving from scenarios to action is the ultimate

measure of success of any scenario project. Often this requires scenarios be applied to (Henriques et al 2015):

- Test the current (or alternative) food strategy/policy/delivery mechanisms against numerous scenarios
- Understand and apply robust responses that address food safety issues revealed across numerous scenarios
- Determine what would be a good strategic position to take in response to critical areas of uncertainty regarding food safety, or indeed risks and opportunities presented, across numerous scenarios

The scenario development process itself offers a unique opportunity to engage a wide range of key actors in the supply chain in strategic conversations about food system developments (including changes in legislative and policy frameworks), thereby creating opportunities for the process to inform policy development. Engaging decision makers during scenario building is often a challenge but necessary to support the communication of findings. In the area of food safety and to improve the use of foresight approaches to policy development it is fundamental to stimulate the:

- Development of indicators for monitoring change;
- Analysis of impact of scenarios on strategy and decision making;
- Continuous review and identification of key drivers and necessary response measures/actions.

Acknowledgements

The UK Food Standards Agency scenario project was funded as part of the Defra Futures Research Partnership (Project ID: SD0339).

References

Brown, D. (2007). Horizon Scanning and the Business Environment - the Implications for Risk Management. *BT Technology Journal, 25*(1), 208-214.

Chaudhury, M., Vervoort, J., Kristjanson, P., et al. (2013). Participatory Scenarios as a Tool to Link Science and Policy on Food Security Under Climate Change in East Africa. Regional Environmental Change, 13(2), 389-398.

De Ruijter, P. (2014) Scenario Based Strategy: navigate the future Gower Publishing Limited 1e edition, 2014. pp. 1- 188, EAN: 9781472437174

Durance, P. & Godet, M. (2010). Scenario Building: Uses and Abuses. Technological Forecasting and Social Change, 77(9), 1488-1492.

EFSA (European Food Safety Authority) 2014. Drivers of emerging risks and their interactions in the domain of biological risks to animal, plant and public health: a pilot study. EFSA supporting publication 2014: EN-588, 44 pp.

European Commission, Joint Research Centre (2014). Tomorrow's Health Society – Research Priorities for Foods and Diets. JRC Foresight Study

European Commission, Joint Research Centre (2016). Delivering on EU Food Safety and Nutrition in 2050 - Future challenges and policy preparedness. JRC Science for Policy Report

Garnett, K., Delgado, J., Lickorish, F., Shaw, H., Rathe, A., Chatterton, J., Prpich, G., and Pollard, S.J.T (2014). Plausible Future Scenarios for the UK Food and Feed System – 2015 & 2030. Report for the Food Standards Agency (FSA). https://www.food.gov.uk/strategicevidenceprogramme/x02projlist/fs246007.

Henriques, C., Garnett, K., Weatherhead, E. K., et al. (2015). The Future Water Environment — using Scenarios to Explore the Significant Water Management Challenges in England and Wales to 2050. Science of the Total Environment, 512, 381-396.

International Risk Governance Council(IRGC) (2009). Nanotechnology applications in food and cosmetics. Available online at www.irgc.org

Jarke, M., Bui, X.T. & Carroll, J.M. (1998). Scenario Management: An Interdisciplinary Approach. Requirements Engineering, 3: 155-173.

Lakner, Z. & Baker, G. A. (2014). Struggling with Uncertainty: The State of Global Agri-Food Sector in 2030. International Food and Agribusiness Management Review, 17(4), 141-176.

O'Keefe L., McLachlan, C., Gough, C., et al. (2016). Consumer Responses to a Future UK Food System. British Food Journal, 118(2), 412-428.

Parson, E. A. (2008). Useful Global-Change Scenarios: Current Issues and Challenges. Environmental Research Letters, 3(4), 045016.

Regulation (EC) No 178/2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety. Official Journal of the European Communities, L31/1

Swart, R. J., Raskin, P. & Robinson, J. (2004). The Problem of the Future: Sustainability Science and Scenario Analysis. Global Environmental Change, 14(2), 137-146.

Van Duijne, F. et al. Precaution for food and consumer product safety: a glimpse into the future, Food and Consumer Product Safety Authority (VWA), Office for Risk Assessment and Research, The Hague, March 2010. Available as pdf on www.nvwa.nl

Van Leeuwen, C.J., Vermeire, T.G. (2007) Risk Assessment of Chemicals: An Introduction. Springer Science & Business Media, 686 pp.

Vervoort, J. M., Thornton, P. K., Kristjanson, P., et al. (2014). Challenges to Scenario-Guided Adaptive Action on Food Security under Climate Change. Global Environmental Change, 28, 383-394.

Voros, J. (2009). Morphological Prospection: Profiling the Shapes of Things to Come. Foresight, 11(6), 4-20

Roles of Incident Scenarios in Foresight

Milos Ferjencik

University of Pardubice, Faculty of Chemical Technology

Studentska 573

CZ-53210 Pardubice, Czech Republic

Abstract

The article is focused on visibility of early warning signs. It describes how the incident scenarios can be used as a supporting tool for foresight. Possible appearance of the incident scenarios represents a starting point. The use of scenarios for the identification of early warning signs and for the prioritization of early warning signs is shown. Uses of both predictive and retrospective scenarios are analysed and common features of both the types are identified. Ways of the use of scenarios are illustrated by examples. According to the article, visualisation of hazard realizations represents the common principal purpose of the use of scenarios. Relation of the visibility of hazard realizations to the visibility of early warning signs is discussed and demonstrated. Methods of hazard identification and risk analysis and methods of incident cause analysis are brought to mind in the article.

Keywords: predictive analysis; retrospective analysis; causal factors; underlying causes.

1. Introduction

1.1 Hypotheses

Kate and William are married; William stays at his parental leave. He takes care about children and also he cooks. He likes cooking. In connection with cooking, he frequently makes small changes – hopefully improvements – in the kitchen.

Kate is glad that William likes cooking. But she does not respond only positively to his improvements in the kitchen. For instance she does not like the bottle with oil in the close proximity of stove, or a heavy bowl in the shelf above the ceramic hob. Also she hates William's custom to leave the frying pan on the stove unattended. See Figure 1.

When they had a controversy over this the last time, William was arguing that nothing had happened yet. Kate answers that all these changes are indicators of problems that

could lead to an incident. In accordance with [1] she calls them warning signs or early warning signs (EWS) and insists on that William should avoid them.

William replies that he does not see anything serious in these changes. Kate states that this is because he does not imagine any accident scenarios. She imagines the scenarios of possible fires in the kitchen and therefore she perceives these EWS as unacceptable.

Kate says:

- Scenarios make it possible to see the risk comprehensively.
- Scenarios are a practical tool for thinking about risk.
- Early warning signs (EWSs) can be derived from scenarios.
- Scenarios make EWS visible through the visualisation of the role of hazards and controls of hazards.
- Scenarios are a practical tool for identifying and prioritizing the EWS.

Figure 1. William's kitchen.

1.2 Objectives

Let us move from the kitchen into the more industrial environment. As an example we will use an object for production of emulsion explosive charges. Figure 2 shows basic arrangement of this plant. Protective walls surround light building inside of which the automatic filling machine produces explosive charges from the explosive paste. In this environment, William may play a role of personnel and Kate represents his manager.

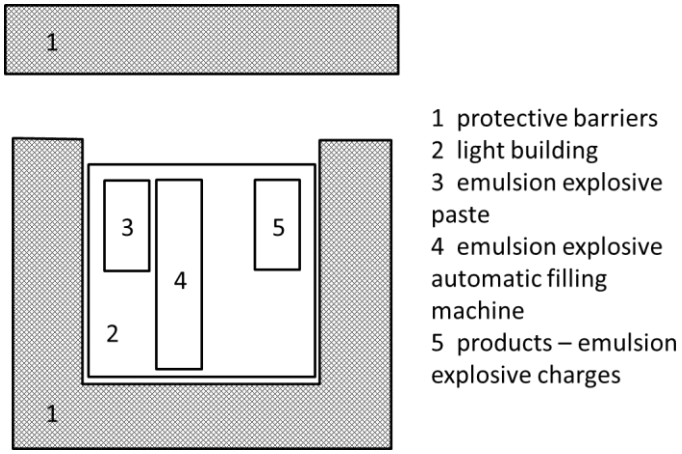


Figure 2. Object for production of emulsion explosive charges (bird's view).

We note that someone simply sees early warning signs and other people do not see them similarly as Kate sees them and William does not see. Let's examine Kate's statements from the preceding section. Kate's hypotheses about the visualisation of risk and early warning signs are to be proved in the following sections. Their applicability is to be shown. We want to find out how scenarios can help us perceive EWS, improving so our foresight and contributing so to Enhancing Safety.

2. Scenarios make it possible to see the risk comprehensively

2.1 Hazards represent the starting point

Origins of danger are called hazards. Definition from book [2] states that hazard is a physical or chemical condition that has the potential for causing harm. Hazards in the industrial environment have usually the form of a presence of dangerous substance or a possibility of undesirable reaction or an accumulation of energy.

In case of William's kitchen the three forms of hazards can be represented by the bottle with oil in the close proximity of stove, by possibility that the oil in the frying pan ignites, and by the heavy bowl in the shelf above the ceramic hob. In case of industrial object from Fig. 2 three groups of hazards are represented e.g. by the presence of volumes of explosives, by the possibility of decomposition reaction in the explosive, or by the energy of compressed air in piping of filling machine.

Hazards can be systematically identified. Number of suitable techniques was developed for this purpose. Probably the most universal techniques for hazard identification in industrial installations are FMEA and HAZOP. See [2].

2.2 Hazards are not a risk

Mere identification of hazards however does not say too much about the risk that is connected with a process or with an operated system. Presence of the bottle with oil in the kitchen means only that the risk connected with the use of kitchen cannot be zero, but nothing more. Three reasons exist why mere knowledge about present hazards is not enough:

- Already the article [3] reminds us that risk increases with the increasing presence of hazards, but it also decreases according to measures which are intended to keep control over hazards. Some of such measures may prevent realizations of hazards, and others may mitigate the effects of realizations. Various types of these measures are called barriers, safeguards, regulations, or layers of protection. Here we will mostly use the term controls or preventive/mitigative controls.

- The risk is not only influenced by the interaction of hazards and controls, but also by the interaction of hazards among themselves. This refers to the terms domino effect or knock-on effect. For example, the ignition of the oil in the pan can develop into the ignition of the oil inside the bottle.

- The magnitude of the risk is also influenced by local environmental conditions that change regardless of hazards and controls. For example, the development of a fire in the kitchen may be different depending on whether the door and/or the window are open. The risk of the plant varies according to how the conditions for the propagation of the shock waves and the clouds of the flue gas change in the atmosphere.

2.3 Scenarios show more than just the hazards

Scenarios describe how the situations can develop when a hazard starts to realize. According to book [4] the above word "realization" means an event or events by which the potential in a hazard system becomes actual. In accordance with this idea the scenarios are sequences of events in which the first event (initiating event) starts the realization of a hazard. The sequence can but does not have to include other - developing - events in addition to the initiation event. See Figure 3. Developing events may be events in the hazard, failures or successes of different controls, application of different environmental conditions, or escalation of development to other present hazards.

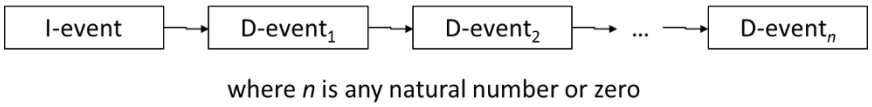


Figure 3. Scenario.

In the kitchen, Kate appears to think about fire scenarios; in the charges production plant she would imagine explosions. For example in the kitchen a scenario may start by the ignition of the oil in the frying pan; continue by extinguishing of fire or by escalation of fire to other hazards including the oil bottle in the vicinity of the stove; and develop until the fire spreads to the entire fire load in the kitchen.

Such scenarios deserve the name incident scenarios since they always cause non-negligible damage. Such scenarios have two substantial properties:

1. Each scenario represents one possible interaction of real conditions in the process/ system. The scenarios not only take into account the hazards in the process/ system but also the ways in which these hazards realize, how the controls fail or succeed,

how the hazards interact and how environmental conditions contribute to the development of the incident.

2. Each scenario represents one contribution to the risk of process/ system. Each incident scenario represents one possibility how damage may arise in the process/ system. Or each scenario represents one part of the risk according to the classical definition [3].

Kate obviously has in mind both these two properties when saying that scenarios make it possible to see the risk comprehensively. In accordance with article [3], the risk of process/ system is for her a set of all conceivable incident scenarios in the process/ system.

3. Scenarios are a practical tool for thinking about risk

3.1 Incident scenarios are a natural tool

Kate is one of the people who consider thinking about danger with the help of scenarios as something natural. The experience with the behaviour of hazards serves as a stimulus for this thinking. The experience does not need to be personal; knowledge-based experience will be enough. When Kate for instance sees Figure 4, she realizes that any heavy object above the ceramic hob is a hazard, and starts thinking about scenarios initiated by falls of heavy objects, and about relevant preventive/ mitigative controls.

This is quite a common way of thinking. It is possible that the ability to respond to experience with the behaviour of hazard by spontaneous development of incident scenarios is a result of evolutionary selection. For example, we know that for our ancestor living in the cave, the presence of the sabre-tooth tiger in the neighbourhood represented a hazard. It is undeniable that the ability to imagine a scenario initiated in this hazard (ability to predict what can happen if a tiger lurks in front of the cave) and the ability to prepare appropriate preventive/ mitigative controls in order to minimise the damage caused by the realization of this hazard was the advantage during human evolution.

Figure 4. Empirical information about a hazard and its behaviour.

Today's designer or an operator of industrial system may think about the realization of hazards just like Kate thinks about heavy objects over a ceramic hob or like a caveman thinks about a lurking tiger. For such thinking it is necessary to know the behaviour of the relevant hazards, to understand them on the basis of natural science or to have experience with them. The effectiveness of such thinking can be enhanced by adopting appropriate techniques.

Incident scenarios can arise in two ways: as a result of prediction (risk analysis) or retrospection (incident analysis). These two options will be discussed in more detail.

3.2 Incident scenarios may be results of prediction

Predictive scenarios arise by developing initiating events in hazards. Event trees are commonly used to represent and create them (see [2]). Example event tree is in Fig. 5. Figure 6 contains the same list of scenarios as the event tree in Fig. 5.

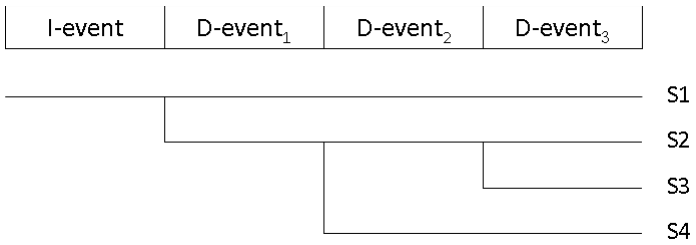


Figure 5. Event tree.

When an analyst constructs an event tree, he starts from a known initiating event in a hazard, knows the behaviour of hazards, and is aware of controls and environmental conditions. He usually begins by considering how and in what order after the initiating event, the controls and environmental conditions should be applied to minimize the damage caused. This sequence of events is called success scenario. Success scenario defines heading of event tree. In Fig. 5 it consists of the initiating event and three developing events.

The analyst then considers what the negations of controls and environmental conditions may cause in the development of an incident. He records the findings in the tree graph below the heading. Such a way he creates a list of predictive incident scenarios which start with the selected initiating event.

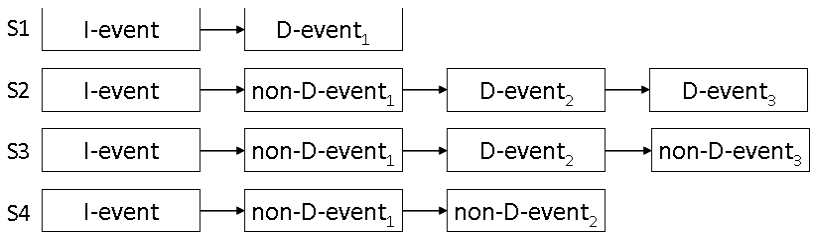


Figure 6. List of incident scenarios from ET in Fig. 5.

3.3 Predictive analysis of incident scenarios

Analysis of incident scenarios using event trees uncovers possible interactions of real conditions in the system, i.e. interactions of present hazards, controls and environmental conditions. For most of the events in the tree it is valid that they can change within a certain range without changing the scenario. For example, if in the tree in Fig. 5 the initiating event is the ignition of oil in the pan, and the first developing event is a fire intervention with a lid, then the fire intervention can take place at any time within a certain time interval of about tens of seconds without changing the course of the scenario. An event tree analyst considers the ranges within which the events can be changed. Individual scenarios from the tree thus represent whole classes of somewhat different scenarios, which however do not differ in qualitative terms, i.e. by the type of events involved. The event tree thus contains representative accident scenarios. For more details see, for example, article [5].

Predictive scenario analysis can be used even before the precise form of the individual conditions in the process/ system is known. Once an initiating event is defined, all the safety functions that are required to mitigate the incident must be defined and organized according to their time of intervention (see book [6]). In the case of ignition in the frying pan, we could consider immediate fire fighting, limitation of propagation, delayed fire fighting, and extinguishing by an external fire brigade. Defining safety functions can be very useful in the design phase because it can be used to define controls.

Predictive analysis typically seeks to investigate systematically all initiating events and related incident scenarios. Scenarios created by predictive analysis take the form of conjunctions of events from which no event can be removed. When thinking about risk, events in scenarios that represent degradation of control over hazards are at the heart of interest. If the convention is kept that the tree heading contains a success scenario, then events that represent degradation are both initiating events and all events that negate successes from the heading, i.e. all the events starting in Fig. 5 and 6 with the word "non".

Guidelines [7] define causal factor as a negative event or undesirable condition that if eliminated would have either prevented the occurrence (= incident scenario) or reduced its severity or frequency. This is exact description of both initiating events and negating events. Thus initiating event and negating events in the event tree can be called causal factors.

Therefore, predictive analysis using event trees can serve as a tool for the systematic identification of all possible causal factors in the process/ system.

3.4 Incident scenarios may be results of retrospection

Retrospective accident scenarios are created as a result of the reconstruction of incidents in the system/ process. According to [8], such reconstruction is always necessary regardless of the method to be used to analyze the causes of the incident.

If the analysis of the retrospective scenario is aimed at preventing the repetition of the same or similar scenarios, it must focus on those events in the scenario that worsen the control over a hazard. And these are causal factors as defined in [7].

Retrospective analysis of the accident thus reconstructs the incident scenario and serves as a tool for identifying the set of causal factors for this particular incident.

3.5 Comparison of prediction and retrospection, role of causal factors

Causal factors are crucial (necessary and sufficient) conditions for the form of incident scenarios. While predictive analysis attempts to predict all possible causal factors that might occur, retrospective analysis identifies the combination of causal factors that actually occurred. If predictive analysis is flawless, then retrospective analysis should result in one of the scenarios created by predictive analysis.

Actually, if we have a set of possible incident scenarios created by a predictive analysis for the process/ system, it is not certain that the scenario generated by the incident retrospection in this process/ system can be quickly identified with one of the predictive scenarios. There may be several reasons for unsuccessful identification:
1) retrospective analysis may mix several scenarios that took place concurrently;
2) scenario events in retrospective analysis are determined in more detail than those in predictive scenarios;
3) certain conditions that worsen the control over a hazard in the process/ system may be omitted in predictive analysis.

The most important common finding is as follows: In both predictive and retrospective scenario analysis, the main outcome in terms of safety is always a set of events that represent a worsening of control over the hazards to which our attention should be focused. In other words, our interest focuses on events called causal factors.

4. Early warning signs (EWSs) can be derived from scenarios

4.1 Scenarios make visible the threatening conditions in the process/ system

The previous section has shown that incident scenarios can be understood as a combination of causal factors, a necessary and sufficient combination of events worsening the control over the hazards. The causal factors can be represented by the initiating event in the hazard, or by the failures of the measures intended to mitigate the realization of a hazard, as well as by the failure of the measures intended to prevent the realization of additional hazard, as well as the events adversely affecting the environmental conditions influencing the realization of hazards.

This result shows that the scenarios make visible the ways in which hazards realize in a particular system/ process. They visualise the real role of hazards and related controls and environmental conditions in a particular system/ process. This visualisation is the basic purpose of both risk analysis and undesirable event analysis.

4.2 Better than prediction or retrospection is the combination of both

Retrospectively, i.e. based on experience with specific undesirable events, only specific accident scenarios can be revealed within the incident cause analysis. From logic point of view, this is an inductive process. Its advantage is that it identifies the real weaknesses of control over the hazards, usually the most likely. It may also reveal weaknesses that within risk analysis remain hidden from our eyes for their delicacy. The disadvantage is that it reveals only some weaknesses and scenarios, not necessarily those that most contribute to risk. The disadvantage may also be that, in the analysis, causal factors are not identified in a sufficiently general manner. The results may mistakenly adhere only to the partial weakness, which is only a contribution to the general causal factor.

Predictively, i.e. based on a system/ process analysis, the risk analysis can reveal theoretically all possible incident scenarios. From logic point of view, this process is deductive. (This means, of course, that it also contains the inductive component - general rules on behaviour of hazards and controls based on experience). The advantage of this approach is that it systematically searches for all weaknesses in the control over the hazards. It is able to reveal all the weaknesses and scenarios, including those with low frequencies. It can also reveal weaknesses that, by mere application of experience, remain hidden from our eyes. The disadvantage of the predictive approach, however, is that the analysis can not avoid various neglects and simplifications because of which some substantial interactions of hazards and controls may be omitted. Hence, the outcome of the prediction may appear to be complete, but in reality, substantial scenarios are missing.

Since it is difficult to avoid above-mentioned errors when using these approaches, combination of a predictive and a retrospective approach seems to be a practical and realistic approach to identifying scenarios.

4.3 Early warning signs are causes of causal factors

We realized in the previous steps that a set of scenarios makes the risk of the system/ process visible as a set of sets of causal factors. As we have already mentioned in Introduction, the essence of foresight is the ability to see EWS or indicators of problems that could lead to an incident. In the context in which the risk is decomposed into incident scenarios and incident scenarios are decomposed into causal factors, the foresight means ability to see the signs that some identified causal factors could actually occur. In particular, we would like to be able to see signs of possible occurrence of causal factors that contribute most importantly to the risk.

It follows from the previous paragraph that the concept of EWS can be identified with the causes of causal factors. However, the concept of causes does not have clear and unambiguous content. If we talk about the causes, we can talk about many kinds of events and ideas. In technical practice, at least direct causes and underlying causes are usually distinguished. Lower differences exist with respect to direct causes. They are physically detectable failures, errors, states, conditions, the combination of which causes an occurrence of causal factor. But there are quite different ideas in different approaches to incident analysis about what are the underlying causes. In relatively common root cause analysis (RCA) methods the underlying causes are called root

causes and represent deficiencies in the implementation of a safety management system. They could also be referred to as organizational causes. Improved RCA such as in [9] would include also the underlying causes in safety culture or attitudes of local management. Symptoms would be identified within ESReDA analysis [10] and failing processes within Leveson's analysis [11].

This diversity means that EWSs can have very variable forms. While these differences in our understanding of causes can discourage us, they all point to the same general fact: EWSs can be determined from incident scenarios as (partial) causes of relevant causal factors.

5. Scenarios make EWSs visible through the visualisation of the role of hazards and controls of hazards

5.1 Steps to the identification of EWSs

Scenarios can help see the EWSs in two steps. In the first step, we determine the causal factors in the incident scenarios; in the second step we determine the causes of the established causal factors.

In predictive analysis, causal factors are determined as:

- events in hazards that initiate realization of hazards
- events in hazards that escalate damages
- events that represent failure of controls over realized hazards
- events that allow damage escalation by setting up adverse environmental conditions.

The determination of causal factors is very easy in conventional event trees. Four causal factors are present in Fig. 5: I-event, non-D-event$_1$, non-D-event$_2$, and non-D-event$_3$.

Various techniques and approaches can be used for the identification of causes of causal factors. Fault tree analysis (FTA) that is recommended in book [7], is very productive in predictive analysis. Fig. 7 shows possible results of application of FTA to two causal factors. It flows from Figures 5 to 7 that cause1, cause2, and cause3 represent EWSs for all scenarios S1 to S4. Cause4 and cause5 are EWSs only for scenario S3. Cause2 indicates the possibility of formation of both causal factors at the same time. Cause2 may represent a sort of common cause failure. Typically, the EWSs with common-cause nature may be the deficiencies in local safety management system.

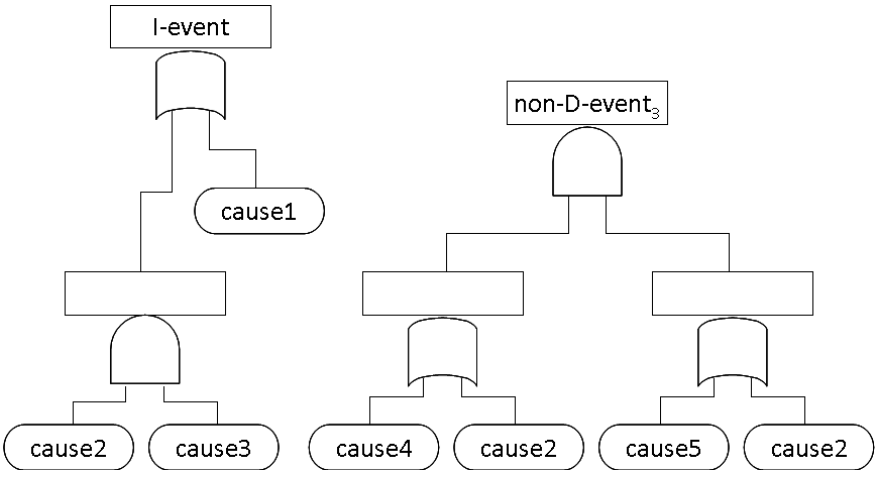


Figure 7. Causes of two causal factors from Fig. 5 and 6.

In a retrospective analysis, causal factors are selected as events that meet the definition of causal factor. Determination of direct causes is usually the result of an incident reconstruction. A hierarchy of checklists called root cause map is often used to determine underlying causes in RCA and improved RCAs. See book [7].

5.2 EWSs are gradually made visible

The path to visible EWSs begins when the incident scenarios are constructed. Scenarios allow the identification of causal factors. They make visible the realization of hazards, which is the main purpose of the construction of incident scenarios. They make visible the roles of hazards and controls of hazards. Once causal factors are known, a way to make EWSs visible is open. Therefore, the visibility of the EWSs emerges through the visualisation of the role of hazards and controls of hazards.

6. Scenarios are a practical tool for identifying and prioritizing the EWSs

6.1 Predictive scenarios are appropriate for the identification of EWSs

Example 1: A frying pan filled with oil is a hazard in the kitchen. Kate worries that the oil in the pan may ignite - she considers the ignition of the oil in the pan to be a possible initiating event. Rapid extinguishing by laying the lid on the pan minimizes damage after the initiating event. If this does not happen, further development depends on whether there is another hazard near the pan - a plastic bottle of oil. If it is not there, the damage is minimized: It can be expected that the oil in the pan will burn out, the smoke will cause damage, but the fire will not expand further. If the bottle is present and stays nearby, it is a matter of time when a large amount of burning oil is spilled on the stove and on the floor. At this point, the rapid use of a suitable fire extinguisher can minimize damage. If the extinguisher is not used quickly, the fire will spread across the room. Further development depends on whether the door is opened into the adjoining dining room or whether it is closed. Closed door minimizes damage in the sense that when the fire breaks out the window and becomes noticeable from the outside of the house, no further rooms are hit so far. If a fire-fighting car arrives in time, it will save

most of the house from the fire. The success scenario consists of an initiating event and five developing events.

Three of the developing events are the use of controls, one event is the realization of another hazard, and one can be considered to be the application of environmental condition. The entire event tree (Figure 8) contains seven incident scenarios.

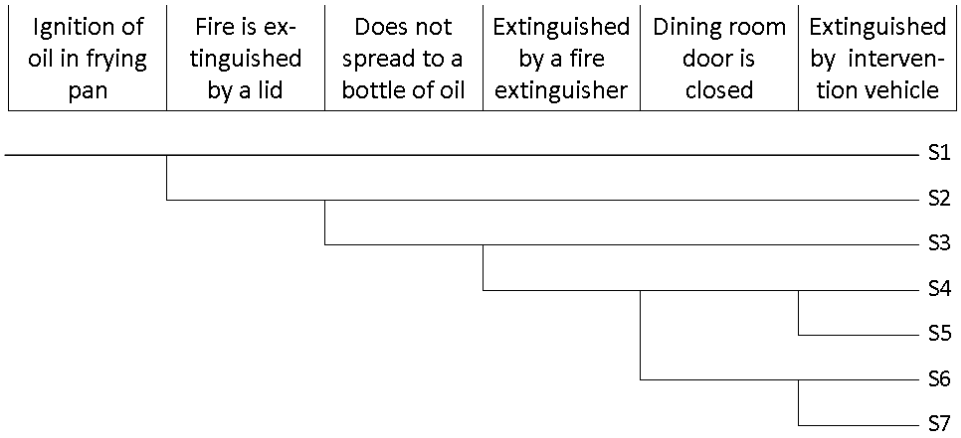


Figure 8. Analysis of possible developments of ignition of oil in frying pan.

Causal factors are determined. Based on causal factors, EWSs in the kitchen can be determined. For example, William's custom to leave the frying pan unattended may contribute to the causes of the initiating event and is the cause of the failure of the first developing event. It is therefore a clear early warning signal.

Example 2: Initiation of detonation during the start of filling machine represents a possible initiating event in object for production of emulsion explosive charges. Resulting event tree is shown in Fig. 9. EWSs that correspond with the identified causal factors are over-limit amounts of explosives, inappropriate deployment of explosives, and insufficient resistance of object.6.2 Retrospective scenarios are appropriate for the identification of EWSs

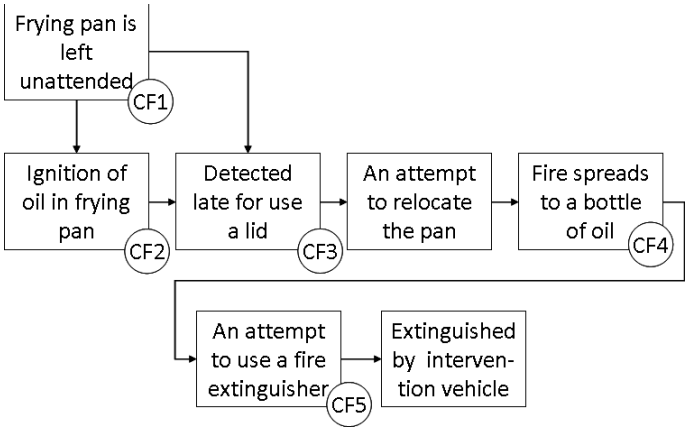


Figure 9. Scenario of real incident in William's kitchen.

Example 3: Fig. 10 shows a real incident scenario in the kitchen. The scenario reminds scenarios S5 and S7 from Fig. 8. Because the information about the dining room door status is missing in the scenario, it is not to be expected that this reconstruction of the incident could identify the EWSs causing the door to be opened. On the contrary, the causal factor CF1 is identified in the reconstructed scenario, which is missing in the scenarios in Fig. 8. The reason for the extra causal factor in the scenario corresponds to point 2 in section 3.5. Causal factor CF1 is the cause of causal factors that we find in scenarios S5 and S7 from Fig. 8.

Example 4: Fig. 11 shows the scenario that actually occurred in object for production of emulsion explosive charges. The scenario contains causal factor CF3 that is not identified in the event tree in Fig. 9. In this case, the real event revealed a deficiency in the predictive analysis of Fig. 9. As stated in section 3.5, point 3, it was overlooked that controls during the start of filling machine should also include the care of the absence of surplus persons in the building. In this case, the retrospective analysis reveals EWSs that predictive analysis was not able to detect.

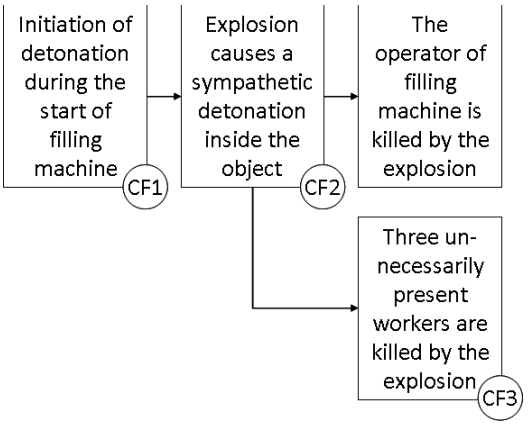


Figure 10. Scenario of real incident in object for production of emulsion explosive charges.

6.3 Scenarios allow the prioritization of the EWSs

Prioritization of EWSs can be done analogously as determination of quantitative importances of components according to [12]. Let us assume that predictive analysis of the process/ system results in the list of incident scenarios S_i, where i = 1 to N. Let us assume that a point estimates of frequency f_i and of damage x_i are determined for each scenario. Point estimates of scenario frequencies are determined with the use of point estimates of frequencies of causes of individual events in scenarios. Point estimate of risk of the process/ system R can be determined as a sum of all products $f_i \times x_i$ for i =1, ..., N. Let us determine a modified point estimation of risk R(EWS) as a sum of products $f_i(EWS) \times x_i$ for i =1, ..., N, where frequencies $f_i(EWS)$ are determined with the use of point estimate of frequency of EWS = 0/year. Priority of cause EWS is p(EWS) = R - R(EWS). The higher the priority, the greater the risk reduction can be achieved by suppressing the occurrence of the EWS.

7. Conclusions

Foresight cannot take place without determining the EWSs. The article shows that incident scenarios may play useful roles in making the EWSs visible. This way, Kate's hypotheses from Introduction are proved. Early warning signs (EWSs) can be derived from scenarios. Scenarios make EWSs visible through the visualization of the role of hazards and controls of hazards. Scenarios are a practical tool for identifying and prioritizing the EWSs.

EWS can be determined from scenarios obtained by predictive or retrospective analysis. The path to the determination of the EWSs leads through the determination of causal factors. Causal factors make EWSs visible. Thus they improve foresight and contribute to enhancing safety.

With the use of incident scenarios, it is possible 1) to make visible the events that are to be considered EWSs in the process/ system, and 2) select EWSs that deserve special attention (such as real-time monitoring).

References

[1] AIChE Center for Chemical Process Safety (2012) *Recognizing Catastrophic Incident Warning Signs in the Process Industries.* John Wiley & Sons.

[2] AIChE Center for Chemical Process Safety (2008) *Guidelines for Hazard Evaluation Procedures, Third Edition.* John Wiley & Sons.

[3] Kaplan, S. and Garrick, J. (1981) On the Quantitative Definition of Risk. *Risk Analysis*, Vol. 1, pp. 11-27.

[4] Marshall, V. and Ruhemann, S. (2001) *Fundamentals of Process Safety.* Institution of Chemical Engineers.

[5] Kaplan, S., Haimes, Y. Y. and Garrick, B. J. (2001) Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and a Resulting Refinement to the Quantitative Definition of Risk. *Risk Analysis*, Vol. 21, pp. 807-819.

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

[7] AIChE Center for Chemical Process Safety (2003) *Guidelines for Investigating Chemical Process Incidents, Second Edition.* American Institute of Chemical Engineers.

[8] Johnson, C.W. (2003) *Failure in safety-critical systems: a handbook of incident and accident reporting.* Glasgow University Press.

[9] Ferjencik, M. (2014) IPICA_Lite—Improvements to root cause analysis. *Reliability Engineering and System Safety* Vol. 131, pp. 1–13.

[10] ESReDA working group on accident investigation (2009) *Guidelines for safety investigations of accidents*. (See also ⟨http://www.esreda.org⟩).

[11] Leveson, N. (2004) A new accident model for engineering safer systems. *Safety Science* Vol. 42, pp. 237–70.

[12] Vesely, W.E., Goldberg, F.F., Roberts, N.H., and Haasl, D.F. (1981) *Fault Tree Handbook NUREG-0492*. U. S. Nuclear Regulatory Commission.

Foresight in process industry through dynamic risk assessment: implications and open questions

Nicola Paltrinieri

Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology NTNU

S. P. Andersen vei 5

7465 Trondheim, Norway

Abstract

Risk analysis is about to enter an era of larger and more complex data sets (big data), where the main challenges are represented by the ability to provide continuous acquisition, effective process and meaningful communication of information. However, most of the methods for quantitative risk assessment allow for static evaluations of risk in a frozen instant of the system life. Research on how to dynamically assess risk in process industry has been carried out, but no real implementation has been attempted. Some open questions are still undermining this approach and should be directly addressed to provide reliable models and exploit new technology opportunities. i) Which strategy should be adopted? ii) How early warnings and past events should be assessed and connected to the overall risk? This contribution aims to give an overview on preliminary answers and highlight possible uncertainties of future developments.

Keywords: dynamic risk assessment; process industry; process safety indicators; information modelling

1. Introduction

An era of larger and more complex data sets (big data) is around the corners for risk analysis methods. For instance, "Google Trends" shows that the number of Google searches for the term "big data" has increased about 100 times since 2011 and today it has reached its peak (Google Inc. 2016). However, despite the increasing availability of new-generation wireless sensors, powerful computers and optical fibres, the main challenges remain related to continuous acquisition, effective process and meaningful communication of information. The term "dynamic risk" had its peak on "Google Trends" in 2009 and today its popularity on the search engine has decreased of about one third (Google Inc. 2016). Many factors may affect such trends and they do not represent the actual applications. However, this behavior may reflect the challenges of dynamic risk assessment to find its place in industry standard approaches. While dynamic risk management has become a common practice in finance in response to the

financial crisis in 2008 (this explains its popularity peak one year later), most of the methods for quantitative risk assessment in industry only allow for static evaluations of risk. Research on how to dynamically assess risk in process industry has been carried out, but no real implementation has been attempted. Some open questions are still undermining this kind of approach and should be directly addressed to provide reliable models and exploit new technology opportunities.
This contribution provides an overview on what can be considered as big data in process safety and how this information can be processed by advanced techniques of dynamic risk analysis. A discussion on the benefits and limitations of such approaches is also carried out, in order to clearly identify related uncertainties and potential ways forward.

2. Big data of process safety

2.1 Process indicators

Increasing attention has been dedicated to evaluation and monitoring of early deviations through appropriate indicators, as a way to foresee the occurrence of major accidents (Paltrinieri et al. 2016). A number of indicator typologies have been theorized and used.
For instance, Health and Safety Executive (2006) identifies two main categories of indicators: leading and lagging indicators. Leading indicators are a form of active monitoring of key events or activities that are essential to deliver the desired safety outcome. They represent early deviations from the ideal situation that can lead to further escalation of negative consequences. Human and organizational factors often (but not always) represent such underlying causes. Lagging indicators are a form of reactive monitoring requiring reporting and investigation of specific incidents and events to discover weaknesses in the system. Lagging indicators show when a desired safety outcome has failed, or has not been achieved.
Øien et al. (2011) affirm that we can refer to risk indicators if: they provide numerical values (such as a number or a ratio); they are updated at regular intervals; they only cover some selected determinants of overall risk, in order to have a manageable set of them. The latter feature has quickly become outdated due to the extensive collection that is being carried out in industry and the attempts made to process and elaborate larger numbers of them (Paltrinieri & Reniers 2017). For instance, for the first time since the first Seveso directive was issued in 1982, Seveso III mentions specific procedures for safety performance indicators and/or other relevant indicators, to use for monitoring the performance of safety management systems (European Parliament And Council 2012). The main aims of the Seveso directives are prevention, preparedness and response to accidents involving dangerous substances in industry in the EU.
Lagging indicators in the form of past events are collected by the competent authorities of all EU member and associated countries (European Parliament And Council 2012) and may indicate themselves the safety performance of a Seveso site. One of the most complete monitoring approaches is suggested in the United Kingdom, where the competent authorities require also the collection of safety performance indicators, which may include leading indicators. Such information is periodically reviewed based on a priority classification of Seveso sites (UK Secretary of State 2015; HSE 2015; COMAH Competent Authorities 2013; COMAH Competent Authorities 2012). In addition, Italian and Dutch relevant regulations address safety performance monitoring

based on indicators and their trends (Consigio dei Ministri 2015; Staatssecretaris van Infrastructuur en Milieu 2015).

2.1.1 Techniques for development of indicators

Several approaches are used for the development of safety/risk indicators. Paltrinieri et al. (2016) identify four classes of methods.

Class I is characterized by a retrospective perspective, where indicators are developed on the basis of the effect of Technical, Human and Organizational (THO) factors in past accidents, and correlation with the overall safety is assumed (Table I). However, major accidents are rare events and the correlation between critical indicators and safety may not be conclusively demonstrated.

Class II is characterized by a predictive perspective, where indicators are defined on the basis of risk models (such as Quantitative Risk Analysis – QRA) for the potential accident scenarios addressed, and the connection to the overall risk level is logically supported by these models (Table I).

Class III groups approaches aggregating the information provided by the indicators, allowing for relatively reliable evaluation of risk on a real-time basis (Table I). Limited sets of risk indicators may not allow comprehensive coverage of THO factors.

Class IV also groups approaches aggregating information from ad hoc indicators, which have been specifically developed for proactive risk assessment (Table I).
Table I shows representative approaches for the development of indicators. Several of these approaches for the development of major hazards indicators were primarily defined for the nuclear power industry. However, the chemical process and petroleum industries have contributed with the definition of specific techniques [11].

Table I: Representative approaches for development of technical, human and organizational indicators

Indicators or approaches for their development	**Class**	**References**
Operational safety indicators	I	(IAEA- International Atomic Energy Agency 1999)
Safety performance indicators	I	(Holmberg et al. 1994)
Risk indicators based on Probabilistic Safety Assessment	II	(IAEA- International Atomic Energy Agency 1999)
Resilience-based Early Warning Indicators	II	(N. Paltrinieri et al. 2012)
Indicators for risk-based inspection	III	(American Petroleum Institute 2000)
MANGER method	III	(Pitblado et al. 2011)
Risk Barometer	IV	(Hauge et al. 2015)

2.2 Iteration of risk assessment

As mentioned by Villa et al. (2016), several efforts have been recently devoted to the development of dynamic risk assessment and management approaches considering the evolution of assessed process. Such evolution may be described by the class III or IV indicators previously introduced.

Some of the first attempts to simulate the dynamic nature of system behaviour were made by Swaminathan and Smidts, who proposed a methodology to extend the application of event sequence diagram (ESDs) to the modelling of dynamic situations and identification of missing accidental scenarios (Swaminathan & Smidts 1999). Čepin and Mavko developed an extension of the fault tree analysis to represent time requirements in safety systems (Čepin & Mavko 2002). Similarly, Bucci et al. (Bucci et al. 2008) presented a methodology to extend fault trees and event trees in a dynamic perspective.

The first complete dynamic risk assessment methodology for process facilities, named Dynamic Failure Assessment, was developed by Meel and Seider (Meel & Seider 2008). This approach aims at estimating the dynamic probabilities of accident sequences, including near misses and incident data (named as Accident Sequence Precursors – ASP), as well as real-time data from processes.

Kalantarnia et al. (Kalantarnia et al. 2010) integrated Bayesian failure mechanisms with consequence assessment. Starting from this foundational contribution, several methodologies have tried to improve the approach by introducing slight modifications. For instance, Hierarchical Bayesian Analysis (HBA) widened the field of application for DRA also to rare event, due to a two-stage Bayesian method (Khakzad et al. 2014). System hazard identification, prediction and prevention methodology (SHIPP) is another derived approach specifically addressing accident modelling, which integrate technical and non-technical barriers (Rathnayaka et al. 2011). Another mentionable contribution is the Dynamic Operational Risk Assessment (DORA) methodology (Yang & Mannan 2010), which included conceptual framework design, mathematical modelling and decision-making based on cost–benefit analysis.

Benefits from iteration of risk assessment are also well known by authorities. Relevant regulations (e.g management regulations by the Norwegian Petroleum Safety Authority (Petroleum Safety Authority Norway 2011)) require iteration of QRA every 5 years or in case of system changes. Most of the risk management frameworks also mention the need for continuous update (NORSOK z013 (NORSOK 2010), ISO 31000 (ISO-International standardization organization 2009), risk governance framework by International Risk Governance Council IRGC (IRGC - International Risk Governance Council 2009), etc.).

DNV-GL has also worked on the topic (Falck et al. 2015) and CGE Risk Management Solutions has released an updated version of their software BowTieXP with an add-on on real-time monitoring of safety barriers performance (no risk assessment though). Attempts have been carried out by the Norwegian oil and gas industry (e.g. Technical Integrity Management Programme by Statoil, iSee by ConocoPhillips and Barrier Panel by ENI Norge), but they only address safety barriers performance monitoring and does not provide risk levels.

3. Dynamic risk assessment

3.1 Hazard identification

A specific method named Dynamic Procedure for Atypical Scenarios Identification (DyPASI) was developed in order to obtain comprehensive hazard identification including accident scenarios that are "not captured by hazard identification methodologies because deviating from normal expectations of unwanted events or worst case reference scenarios." These scenarios are defined by Paltrinieri et al. (2012) as “atypical”. DyPASI is a hazard identification method aiming at the systematization of information from indicators related to past accident events, near misses and literature studies. It supports the identification and the assessment of atypical potential accident scenarios related to the substances, the equipment and the industrial site considered. DyPASI is one of the results of the European Commission FP7 iNTeg-Risk project (Paltrinieri et al. 2013), which addressed the management of emerging risks.

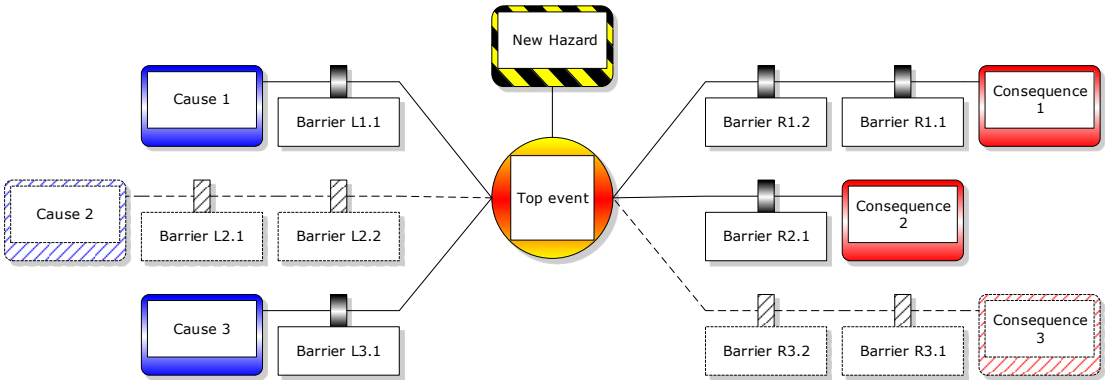


Figure 1. Graphical representation of Bow-Tie diagram with integration of branches newly identified through DyPASI

The application of DyPASI entails a systematic screening process that, based on early warnings and risk notions, should be able to identify possible Atypical Scenarios available at the time of the analysis. The well-established approach of the Bow-Tie Analysis (Delvosalle et al. 2006), which aims at the identification of all the potential major accident scenarios occurring in an industrial site, is taken as a basis to develop the methodology. Specific branches may be integrated consistently with the Bow-Tie Diagrams and related safety barriers defined for the newly identified scenarios (Figure 1).

DyPASI may be suitable for application in each phase of the process life-cycle. It is a tool specifically defined for the continuous improvement of risk management, providing a procedure to enable systematic updating of the hazards identified and managed in the process. DyPASI may be used either as a “stand-alone” technique or may be coupled with existing conventional techniques. In the latter case, it may effectively integrate the existing hazard identification methods to obtain more exhaustive results. In particular it provides a structured and yet dynamic approach in the retrieval of information from early warnings and atypical scenarios. The format of the results from DyPASI allows for integration with the hazard identification techniques based on fault tree and event tree analysis, effectively extending the

applicability of DyPASI from the preliminary hazard analysis to the detailed assessment of complex systems.

3.2 Risk analysis

Two different approaches may be adopted for dynamic risk analysis, which primarily focus on evaluation and update of accident frequency. Such approaches are generally based on either reactive or proactive assessment. Several dynamic risk analysis techniques are available in literature, but only two representative techniques are presented by this work: the reactive Bayesian Inference-based Dynamic Risk Assessment (BIDRA) technique and the proactive Risk Barometer technique.
BIDRA is a methodology for dynamic risk assessment based on Bayesian inference and its objective is achieved by monitoring and processing data on incidents and near misses during the system lifetime (Khakzad et al. 2016). Its goal is to refine failure probabilities of safety barriers and consequently update potential accident frequency values. The updating of the prior probability P of a safety barrier failure θ based on new evidence E (where $L(E|\theta)$ is the likelihood function of θ), is performed as follows:

$$P(\theta|E) = \frac{P(\theta)\,L(E|\theta)}{\sum_{\theta} P(\theta)\,L(E|\theta)} \tag{1}$$

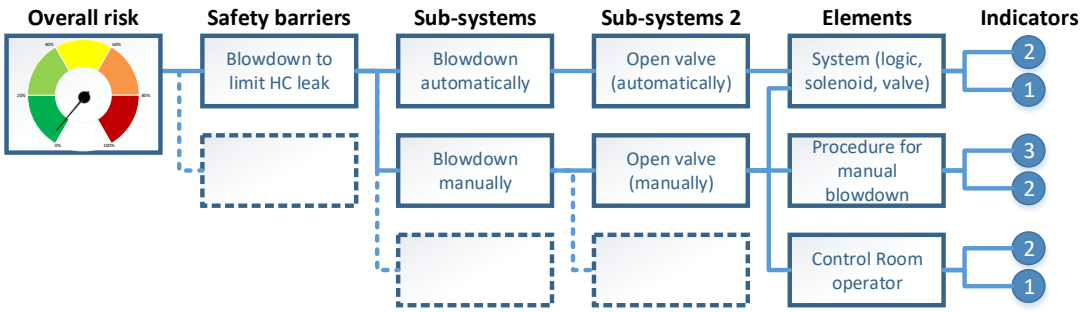


Figure 2. Risk barometer aggregation of indicators

The Risk Barometer is based on the definition and real-time monitoring of relevant indicators, in order to continuously assess the health of safety barriers and evaluate their probability of failure (Paltrinieri et al. 2016; Hauge et al. 2015). Such indicators monitor not only the technical performance of barriers, but also the associated operational and organizational systems. In this way, the Risk Barometer aims to capture early deviations within the organization, which may have the potential to facilitate barrier failure and accident occurrence. In order to aggregate the information expressed by the indicators and assess the performance of barrier systems, barrier functions and plant areas, the indicators are quantitatively weighted and combined by means of weighted summations (Figure 2). Weighting and quantification depend on input from subject matter experts. This process of calibration is carried out by means of a series of workshops, where validation with real data from the plant is advisable. However, continuous control and improvement of the indicators and the related weights should be continuously carried out.

3.3 Establishing the risk picture

Visualization of risk assessed on a dynamic basis may represent an important support to decision making and allow overcome some of risk metric limitations. An example of this is represented by the Risk Barometer (Edwin et al. 2016; Hauge et al. 2015), where the barometer is used to visualize the real-time risk of a system (Figure 3). In addition, the risk trend over time can be visualized to evaluate positive or negative trends and compare the current risk with past values (Figure 3). The y-axis scale is coloured according to the risk tolerability/ acceptability levels used in the barometer.

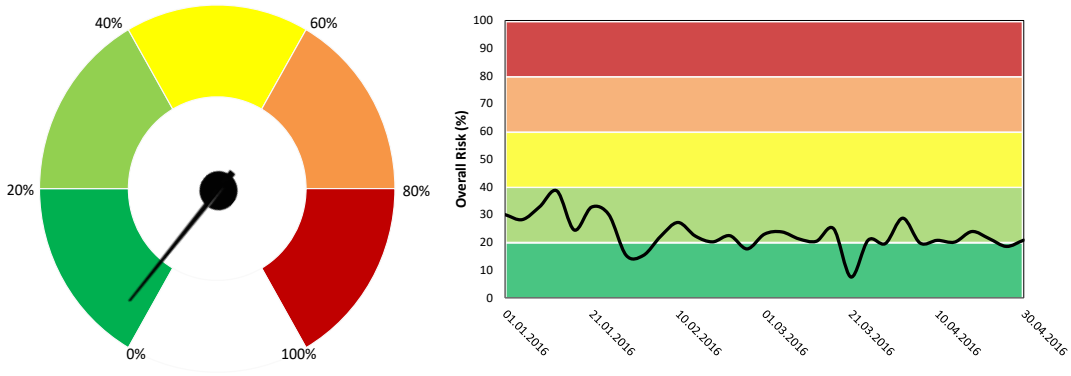


Figure 3. Generic Risk Barometer and risk trend. Adapted from (Edwin et al. 2016)

The risk level is a function of the status and condition of the different barrier functions and associated barrier systems. Each barrier system is modelled and measured through a set of indicators. For this reason, drill-down capability should be enabled to move through the hierarchy of the model, from the area to the barrier and further to the indicator level (Figure 3). Information about the overall risk, its progression and underlying causes can be continuously traced, providing intuitive understanding of the causes of risk variations and supporting definition of priorities related to risk mitigation and control. Moreover, in order to improve decision-support in operations, the Risk Barometer visualizes a list of top risk contributors using real-time sensitivity measures. Such list highlights which barrier functions and associated barrier systems are contributing the most to the risk level at the given point in time.

4. Discussion

The ISO 31000 standard on risk management (ISO-International standardization organization 2009) assigns a pivotal role to knowledge by defining risk as "the effect of uncertainty on objectives". Uncertainty is the driving force of dynamic risk analysis, demanding for continuous calibration of the risk picture and progressively filling lack of knowledge with new evidence and information. Moreover, awareness of the knowledge dimension, as theorized by Aven (Aven 2013) and Aven and Krohn (Aven & Krohn 2014), not only gives credit to dynamic risk analysis, but also improve its understanding.

As discussed by Paltrinieri et al. (2013), the DyPASI technique not only addresses knowledge management, but also complies with the five principles of hazard

identification identified by CCPS - Center for Chemical Process Safety (2000): completeness, reproducibility, inscrutability, relevance of experience and subjectivity. However, the possibility to capture atypical scenarios during the initial hazard identification phase heavily depends on the experience of the user. The DyPASI method was built to systematically approach the issue of critical event identification, screening and organizing available information. The systematic approach of DyPASI should limit the possibility of failing in the identification of some relevant accident scenario, so as to give the analyst a chance to obtain or update comprehensive results. Knowledge on *when* data is collected and risk is assessed in Dynamic Risk Analysis is also fundamental to understand the limits of such approach. In fact, the distinction between reactive and proactive approaches reflects different projections in time for the risk assessed. Reactive approaches respond to an event that is directly associated with the overall risk picture (e.g. failure or success of a technical safety system) and presumably closer in time to a potential accident – if not the accident itself. Whereas, proactive approaches include in the analysis also relevant early deviations from the optimal condition, which have a lower degree of causality on a potential accident (e.g. worsening or improvement of organizational factors).

The BIDRA technique is based on sound statistical theories and falls under the definition of reactive approaches (Khakzad et al. 2016; Scarponi & Paltrinieri 2016). In fact, it updates the risk picture of the system considering information on past events indicating failure or success of safety barriers. For instance, the example of application proposed in the previous chapter shows how this technique can identify worsening in the safety system, or a negative drift towards risk conditions, through the registered failures in the regular tests of safety instrumented systems. Due to the specific characteristics of the data used as input to BIDRA, technical information on the performance of safety equipment is relatively more suitable. This performance may affect the probability of an accident on a higher degree than operational and organizational factors, because closer in the causality chain. However, not only incidents and near misses can be of input to BIDRA, but also results of regular technical tests, which would allow constant update with known lag. The main requirement for BIDRA inputs is a certain degree of objectivity allowing for distinction between success and failure of safety barriers, providing for relevant and critical basis for the analysis.

The Risk Barometer is a recent technique (Paltrinieri et al. 2016; Hauge et al. 2015). It is relatively adaptable to the degree of available information present for the case. The evaluation of the relative importance of the system safety barriers (and the omission of parameters representing the little influential safety barriers) should be preferably performed based on previous risk and barrier analyses. In case pieces of information are not available, the evaluation may be based on expert judgment and subject to a higher level of uncertainty. Poor judgment may result in the exclusion of critical parameters. The indicators collected are heterogeneous and should be translated into mutually comparable scores. Their different nature affects the time lag with which risk is dynamically updated. In fact, they have different collection frequencies, which may alter the overall result. The Risk Barometer characteristic of proactivity resides in its capacity to consider and process also underlying operational and organizational factors, which may affect the performance of safety instrumented systems during operations. Such factors may be earlier in the causality chain than a technical failure and, for this

reason, are defined as early deviations in the sequence of events leading to an accident. Their link with the overall risk is not as direct as technical indicators and they are relatively challenging to define, which may lead to omission or double-counting. For this reason, the Risk Barometer accounts for the relative importance of indicators in respect of the overall risk by means of specific weights and weighted summations. Such weights are defined on the basis of expert judgment. This may be time-consuming and lead to new uncertainties.

It is worth noticing that the terms "reactive" and "proactive" cannot be rigidly apply. In fact, BIDRA does not only collect information from previous events (near misses or incidents), but also consider the results of tests of safety instrumented systems, which provides a certain degree of proactivity in the analysis. Whereas, the Risk Barometer elaborates both reactive and proactive indicators and its applications have proved to be relying on the formers on a higher extent. For this reason, such classification may be reductive and the overlapping between the two techniques may turn considerable in some cases.

Important differences between the techniques stand out concerning the risk updating process. BIDRA considers the components of the process at a rather superficial level. It may evaluate the current failure probability of a safety barrier based on its behaviour in the past. Such information may support maintenance planning and lead to corrective maintenance or risk management in general and lead to additional safety barriers. However, the technique does not allow investigating on the possible underlying causes of malfunctioning. On the other hand, the Risk Barometer provides a deeper insight of the causes. It focuses on factors affecting the general behaviour of the system. In this way, it makes possible the identification of a negative drift at an early stage of the cause consequence chain leading to an undesired event.

The Risk Barometer represents a further development of BIDRA. In fact, the Risk Barometer takes into account underlying factors (addressing organization health and operations) in addition to the test results and past events considered by BIDRA. This provides more details to the overall risk picture and approximate assessment results to the real system conditions.

Complementarity may reside in the potential of one technique to (partially) validate the other. Despite the possible uncertainty in the definition of variance, the mathematical model of BIDRA is more solid and it is based on definite events of technical success and failure. Whereas, the Risk Barometer uses relatively simple aggregation rules for heterogeneous indicators, organized in a hierarchical structure and weighted on the basis of their relative importance. The definition of this risk model is strongly affected by subjective judgment and experts should be consulted for most of the Risk Barometer steps. For this reason, BIDRA results may be compared with risk values from the Risk Barometer. However, such validation is solely related to the Risk Barometer capability of treating technical indicators, because, for the sake of consistency, the technique should be deprived of organizational and operational indicators.

Finally, this work presents some solutions for dynamic risk visualization. Clear hierarchy should ordinate all the elements and allow the potential user to browse among the risk analysis results and drill down to the aggregated details. In fact, the ultimate

purpose for such visualization solutions is improving the support for critical decision-makers, from risk managers to daily planners. In this case, the risk barometer aims to not only offering graphical user interfaces for risk communication, but also continuously updating the risk picture on a real-time basis and providing detailed information of the subsystems involved.

5. Conclusions

This contribution shows that risk analysis in the process industry is evolving. The concept of dynamicity has gone beyond time dependence and online monitoring. It now encompasses progressive calibration/ refinement of nonlinear repetitive processes, reacting and adapting to changes and new information flows. However, the main uncertainties are related to the process of available information. Proactive approach is desirable, but its reliability should not be compromised. Moreover, such tools should be able to provide effective operational support to provide real impact for process industry.

References

American Petroleum Institute, 2000. API Publication 581. Risk-based inspection base resource document.

Aven, T., 2013. Practical implications of the new risk perspectives. *Reliability Engineering & System Safety*, 115, pp.136–145.

Aven, T. & Krohn, B.S., 2014. A new perspective on how to understand, assess and manage risk and the unforeseen. *Reliability Engineering & System Safety*, 121, pp.1–10.

Bucci, P. et al., 2008. Construction of event-tree/fault-tree models from a Markov approach to dynamic system reliability. *Reliability Engineering & System Safety*, 93(11), pp.1616–1627.

CCPS - Center for Chemical Process Safety, 2000. *Guidelines for Chemical Process Quantitative Risk Analysis*, New York, USA: American Institute of Chemical Engineers (AIChE).

Čepin, M. & Mavko, B., 2002. A dynamic fault tree. *Reliability Engineering & System Safety*, 75(1), pp.83–91.

COMAH Competent Authorities, 2012. *Process safety performance indicators (Operational Delivery Guide)*, Bootle, United Kingdom.

COMAH Competent Authorities, 2013. *Site Prioritisation Methodology*, Bootle, UK.

Consigio dei Ministri, 2015. Decreto legislativo 26 giugno 2015, n. 105. *Gazzetta Ufficiale*.

Delvosalle, C. et al., 2006. ARAMIS project: A comprehensive methodology for the identification of reference accident scenarios in process industries. , 130.

Edwin, N.J., Paltrinieri, N. & Østerlie, T., 2016. Risk Metrics and Dynamic Risk Visualization. In *Dynamic Risk Analysis in the Chemical and Petroleum Industry*. Elsevier, pp. 151–165.

European Parliament And Council, 2012. Directive 2012/18/EU of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC - Seveso III. *Official Journal of the European Union*, pp.1–37.

Falck, A., Flage, R. & Aven, T., 2015. Risk assessment of oil and gas facilities during operational phase. In *Safety and Reliability of Complex Engineered Systems - Proceedings of the 25th European Safety and Reliability Conference, ESREL 2015*. pp. 373–380.

Google Inc., 2016. Google Trends. *Google Search*. Available at: www.google.com%5Ctrends [Accessed December 28, 2016].

Hauge, S. et al., 2015. *Handbook for monitoring of barrier status and associated risk in the operational phase, the risk barometer approach. SINTEF F27045.*, Trondheim, Norway.

Health and Safety Executive, 2006. *Developing process safety indicators* First., United Kingdom.

Holmberg, J. et al., 1994. Safety evaluation by living probabilistic safety assessment and safety indicators. In TemaNord, ed. *The Nordic Council of Ministers*. Copenhagen, Denmark.

HSE, 2015. *The Control of Major Accident Hazards (COMAH) Regulations* Third., London: Health and Safety Executive (HSE).

IAEA- International Atomic Energy Agency, 1999. *Management of Operational Safety in Nuclear Power Plant.*, Vienna, Austria.

IRGC - International Risk Governance Council, 2009. *Risk Governance Deficits. An analysis and illustration of the most common deficits in risk governance.* International Risk Governance Council, ed., Geneva.

ISO-International standardization organization, 2009. *ISO/FDIS 31000:2009: Risk Management - Principles and Guidelines*, Geneva, Switzerland: International Standardization Organization.

Kalantarnia, M., Khan, F. & Hawboldt, K., 2010. Modelling of BP Texas City refinery accident using dynamic risk assessment approach. *Process Safety and Environmental Protection*, 88(3), pp.191–199.

Khakzad, N. et al., 2016. Chapter 5 - Reactive Approaches of Probability Update Based on Bayesian Methods. In *Dynamic Risk Analysis in the Chemical and Petroleum Industry*. Butterworth-Heinemann, pp. 51–61.

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

Meel, A. & Seider, W., 2008. Real-time risk analysis of safety systems. *Computers & Chemical Engineering*, 32(4–5), pp.827–840.

NORSOK, 2010. *Standard Z-013, Risk and Emergency Preparedness Analysis.* Third Edit., Lysaker, Norway: Standards Norway.

Øien, K., Utne, I.B. & Herrera, I.A., 2011. Building Safety indicators: Part 1 - Theoretical foundation. *Safety Science*, 49(2), pp.148–161.

Paltrinieri, N. et al., 2016. Chapter 6 - Proactive Approaches of Dynamic Risk Assessment Based on Indicators. In *Dynamic Risk Analysis in the Chemical and Petroleum Industry*. Butterworth-Heinemann, pp. 63–73.

Paltrinieri, N. et al., 2013. Dynamic Procedure for Atypical Scenarios Identification (DyPASI): A new systematic HAZID tool. *Journal of Loss Prevention in the Process Industries*, 26(4).

Paltrinieri, N. et al., 2012. Lessons Learned from Toulouse and Buncefield Disasters: From Risk Analysis Failures to the Identification of Atypical Scenarios Through a Better Knowledge Management. *Risk Analysis*, 32(8), pp.1404–1419.

Paltrinieri, N., Oien, K. & Cozzani, V., 2012. Assessment and comparison of two early warning indicator methods in the perspective of prevention of atypical accident scenarios. *Reliability Engineering and System Safety*, 108, pp.21–31.

Paltrinieri, N. & Reniers, G., 2017. Dynamic risk analysis for Seveso sites. *Journal of Loss Prevention in the Process Industries*, 49, pp.111–119.

Petroleum Safety Authority Norway, 2011. *Regulations relating to health, safety and the environment in the petroleum activities and at certain onshore facilities (the framework regulations).*, Stavanger, Norway.

Pitblado, R. et al., 2011. Frequency data and modification factors used in QRA studies. *Journal of Loss Prevention in the Process Industries*, 24(3), pp.249–258.

Rathnayaka, S., Khan, F. & Amyotte, P., 2011. SHIPP methodology: Predictive accident modeling approach. Part I: Methodology and model description. *Process Safety and Environmental Protection*, 89(3), pp.151–164.

Scarponi, G.E. & Paltrinieri, N., 2016. Chapter 8 - Comparison and Complementary between Reactive and Proactive Approaches. In *Dynamic Risk Analysis in the Chemical and Petroleum Industry*. Butterworth - Heinemann, pp. 93–101.

Staatssecretaris van Infrastructuur en Milieu, 2015. Besluit risico's zware ongevallen 2015. *Overheid*.

Swaminathan, S. & Smidts, C., 1999. Identification of missing scenarios in ESDs using probabilistic dynamics. *Reliability Engineering & System Safety*, 66(3), pp.275–279.

UK Secretary of State, 2015. COMAH - The Control of Major Accident Hazards Regulations - 2015 No. 483. , p.44.

Villa, V. et al., 2016. Towards dynamic risk analysis: A review of the risk assessment approach and its limitations in the chemical process industry. *Safety Science*, 89, pp.77–93.

Yang, X. & Mannan, M.S., 2010. The development and application of dynamic operational risk assessment in oil/gas and chemical process industry. *Reliability Engineering & System Safety*, 95(7), pp.806–815.

Horizon scanning approaches for early sensing of cyber-physical threats to water utilities

Eivind Okstad, Øyvind Dahl

SINTEF Technology and Society

S.P. Andersens vei 5

N-7465, Trondheim, Norway

Abstract

Safety- and security (cyber) assessment of critical infrastructures is essential contribution to ensure robustness of urban water systems. In a risk management context, the quality of risk identification and risk evaluation processes are critical to achieve appropriate risk pictures for risk-reducing purposes. Cyber-attacks related to ICT systems in combination with physical safety aspects of water and waste water systems constitute an emergent threat landscape for water utilities and the society. Horizon scanning and related methods are suggested to improve awareness and collective sense-making capabilities in, and between water utilities, cooperating companies and stakeholders. Horizon scanning is a collective term of approaches capturing weak or early warning signals for use in political discourse and decision-making. An initial literature review of approaches has been carried out, with a pre-evaluation and discussion of the effectiveness of such to uncover types of hidden and emerging threats to water utilities.

Keywords: Water utility, Horizon scanning, Cyber security, Risk management

1. Introduction

This paper deals with safety and security aspects (cyber) related to the control- and surveillance systems of water utilities. Cyber security can be described as elements of an emergent threat landscape. The paper discusses whether horizon scanning methods are possible means to sustain robust urban water systems. The main intention is to review the appropriateness of such approaches to water systems. Horizon scanning share similar challenges and opportunities with other foresight techniques. Here, we refer to horizon scanning as the processes of collecting and assessing varying sort of vague information, or early signals (warnings) about the future, and how this could be translated into useful knowledge for policy-, strategy-, or operational decision-making.

This work is based on an initial activity of the new-started EU-project STOP-IT[14], for which the protection of water infrastructures from cyber-physical threats are addressed. A limited literature review of horizon scanning approaches is presented, followed by a discussion of the usability and appropriateness of approaches to water-supply and sewage systems (water utilities).

Complexity and interconnectivity of socio-technical systems, the social development, and urbanization increases the vulnerability of important societal functions. Critical infrastructures, like water supply and sewage handling, are no exception in that respect. In a risk management context, the quality of risk identification and risk evaluation processes are most important to achieve accurate risk pictures for risk management purposes. Risk identification is typically regarded a 'static' task that takes place a few times during a system's life-time, e.g. in the early planning phases. It is crucial, on a more regular basis, to inform policy- and decision-makers about upcoming opportunities and threats by some other means, having them prepared or making them aware of possible changes and surprises/shocks (Anamatidou et al. 2012). A relevant approach for this purpose is horizon scanning, which is defined as:

> *the systematic examination of potential (future) problems, threats, opportunities and likely future developments, including those at the margins of current thinking and planning. Horizon scanning may explore novel and unexpected issues, as well as persistent problems, trends and weak signals. (Van Rij, 2010).*

National horizon scanning activities have been carried out quite recently, e.g. in the UK, in the Netherlands and in Denmark (Van Rij, 2010). A national horizon scanning activity also took place in Singapore under a risk assessment- and horizon scanning programme. The programme led to continuous end-to-end capabilities to collect and classify data, analyse and understand relationships, and anticipate emerging issues that could have strategic impacts on Singapore. A relevant cyber-event example, is the Maroochy Shire cyber event from Australia, year 2000 (Abrams & Weiss, 2008). It was a targeted cyber-attack on a SCADA radio-controlled sewage system that caused 800,000 litres of raw sewage spilling out into local parks, rivers and grounds. Marine life died, the creek water turned black and the stench was unbearable for residents. The main investigation report concluded that personnel were not trained in preventing, recognizing, or responding to any kinds of cyber-related attack at that time (Anamatidou et al. 2012).

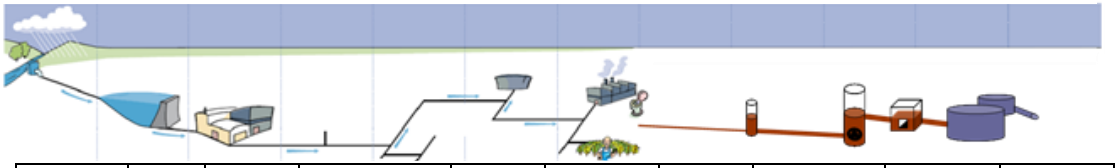
1.2 Objective

The main objective of this paper is to demonstrate whether horizon scanning methods could fit in sensing emerging cyber-physical threats to water utilities. How, and to what degree would such methods enforce early warning capabilities, increase awareness and cooperation in the water sector as a means for policy- and strategic decision-making?

[14] Strategic, Tactical, Operational Protection of water Infrastructure against cyber-physical Threats (STOP-IT), EU-project funded by H2020.

2. Description of water utilities with operational concerns

In the following we will describe a typical Norwegian water utility, with the water- and waste water systems (Johnsen & Røstum, 2015). Water utilities involve both technical- and management systems, but also organizational and human cultures that will be elements in a holistic risk management. Figure 1 shows an example of water- and waste water routes, from the precipitation areas via the water treatment and distribution networks, to the waste water networks and systems. Critical systems or components are identified, e.g. the pumping stations with its control system. In addition to physical systems, information and communication technology (ICT) for system control-integration and communication are significant. ICT systems have become a central building block in every critical infrastructure. Systems are then highly dependent on the security, stability and integrity of these ICT systems. Thus, the attention of industry actors and policymakers towards critical infrastructure protection has grown remarkably (Alcaraz & Zeadally, 2015).



Precip.	Dam	Water treat.	Water distribution	Elev. basin	Building consum.	Sewer piping	Pump stations	Sewer purific.	Recip.
Common infrastructure: ICT net (adm./technical net), links to the Internet, operational centre									

Figure 1. Context: Objects in a typical water and sewage utility, following water from the precipitation areas to recipients

Figure 2 illustrates some of the process control and ICT administrative objects. Programmable logic control (PLC) systems are established for process control. Along with the ICT infrastructures, data network, operational control centre and adm. network, these objects constitute a totality. In addition, we have the organizational responsibilities of the company that also involve subcontractors, ICT departments and the individual employees with their specific knowledge and attitudes.

Operational control system)	Operational control centre	Adm. systems	El. power, cooling

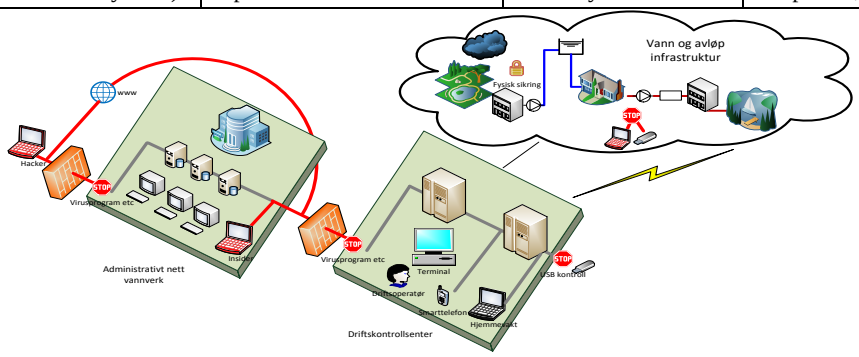


Figure 2. Example of process control, ICT and adm. network found in a water utility

3. Horizon scanning as policy- strategic decision support

The literature identified is based on a general search for articles on the subject horizon scanning through Google Scholar. We have also searched for articles that link scanning methods to the planning and operation of critical infrastructures such as the water supply and waste-water systems.

The following description draws attention to horizon-scanning approaches and methods from this literature. The main concepts presented here are based on the previous SESTI project[15] (Anamatidou et al. 2012).

Horizon scanning implies a search process, which is extended at the margins of the known environment and possibly beyond it (Loveridge, 2009). Horizon scanning aims to identify emerging issues, signs, events or trends which may present themselves as threats or opportunities for the society and policy. Könnölä et al. (2012) regarded horizon scanning as a creative process of collective sense-making. Typically, it builds on concepts aimed for identification of weak, and/or early warning signals within frameworks of political discourse and decision-making.

3.1 Kinds of scanning approaches

There are different approaches which underpin the scanning process. One way to categorize the different approaches is to differentiate between *exploratory* and *issue-centred scanning* (Anamatidou et al. 2012).

3.1.1 Exploratory scanning

The exploratory scanning approach concentrates on assembling potential emerging issues from a wide variety of data from different signal sources. The aim is to identify a long list of signals that are precursors for emerging issues, only demarcated by the policy domain selected (e.g. healthcare or energy). At the end, the long list of signals is clustered into potential emerging issues. Text-mining is an example of a tool that can be used to identify clusters.

3.1.2 Issue-centred scanning

In issue-centred scanning, a hypothesis is evaluated, i.e. a hypothesis of emerging issues. Preliminary descriptions of issues are used as a core to identify potential additional signals that could either confirm, or deny the real emergence of the issue. It starts from the wide range of existing and potential emerging issues (hypotheses) and searches for weak signals to strengthen, or question the specific hypotheses. As a starting point, a frame of reference is conceptualised for the chosen policy domains. Signals are then sought that give a full or substantial future narrative with high impact for a certain policy level. These signals are referred to as primary signals, which could appear in form of articles, presentations or videos. Only documented items with "full storylines", connecting factual findings or plausible assumptions in a logical way with a foreseen future high impact, are considered. These storylines usually imply, either implicit or explicit, elements that could be used as indicators for the realisation of the

[15] The SESTI-project (Scanning for Emerging Science and Technology Issues) was funded by the EU commission through the seventh European Framework Programme.

storyline. It should be clear that issue-centred scanning does not predict any issues. Rather, it provides tools to alert for potential impact-rich issues that need policy attention.

3.2 Methods and tools

3.2.1 Sources of information and tools

Both the exploratory and issue-centred scanning approaches use the internet as the main source of information. The SESTI-project utilized the following scanning tools:

- Web-based search engines as Google, Google News, etc.
- Timeline, Google Insight and Bing
- Expert reviews and surveys
- Visits to conferences and seminars
- A special 'SESTI' wiki to evoke contributions to the scanning process
- Active use of blogging and micro-blogging (Twitter)
- Text-mining
- Expert/stakeholder workshops

Some of the methods above are suitable for obtaining specific information like the expert reviews, surveys and visits to conferences and seminars, while other tools like the initiation of a wiki and the active use of blogs and micro-blogging can encourage wider participation and dialogue. Methods could be grouped per various levels of participation and automation in identification, processing and analysis of weak signals and emerging issues. Such a grouping is shown in Figure 3.

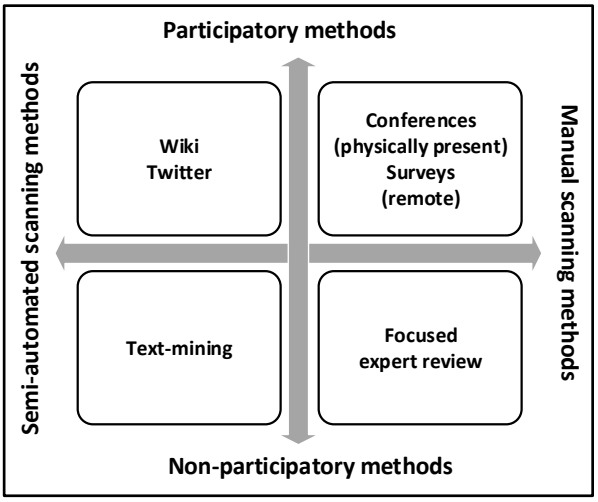


Figure 3. Grouping of methods with respect to level of participation and automation (Anamatidou et al. 2012).

Focused expert reviews are based on internet scanning, which is performed by professional scanners.

3.2.2 Scanning processes

The main phases of the SESTI scanning process are (Anamatidou et al. 2012):

Phase 1 Identification of weak signals. Emerging issues are usually formulated based on searches in different sources, and/or expert interviews.

Phase 2 Processing of weak signals according to the following steps:
- Step 1 Selection of the broader area where emerging issues will be examined
- Step 2 Clustering of weak signals
- Step 3 Assessing the significance of clustered weak signals
- Step 4 Framing the connected weak signals into clustered topics
- Step 5 Tentative modelling of signals/topics into possible emerging issues
- Step 6 Identification of the most significant emerging issues

Phase 3 Analysis and interpretation of emerging issues in policy-making.

Rather than being antagonistic, the exploratory and issue-centred scanning approaches are complementary. Exploratory scanning mainly refers to the first scanning phase (identification of weak signals) while issue-centred scanning spans throughout both phases 1 and 2 of the SESTI-scanning process. The method of focused expert review could be used for the entire scanning process. Within the issue-centred approach it is a useful tool to identify potential emerging issues, like potential problems, threats, opportunities and likely future developments, in a fast and cost-efficient manner. It also enables identification of potential secondary signals that can be used to contextualise issues and to monitor their further development. Database tools that are connected to search engines such as Google News Timeline, Google Insight, Web of Science, etc. could be used for this purpose. As an assessment of the tools used in the scanning process in the SESTI project, the rates presented in Table I were given to each of the tools about their appropriateness and usefulness to the scanning phases.

Table I: Comparison of tools for use in scanning (Anamatidou et al. 2012)

Tool	**Phase 1**	**Phase 2**	**Phase 3**
Focused expert review	High	High	High
Wiki	Low	Low	Low
Twitter	High	Low	Low
Surveys	Low	High	High
Conferences	Low	Medium	High
Text-mining	Low	Medium	Medium

3.2.3 Policy implications and decision criteria

A proper assessment of weak signals should be translated into policy recommendations. At this stage, workshops should provide space for discussions between experts, as well as policy-makers about the findings on emerging issues.

The main objective is to draw conclusions about possible implications of the week signals and clusters of such for policy, and/or strategic planning.

3.3 Assessing, combining and clustering information

There is always a need to link the horizon scanning process more directly to strategic risk and uncertainty management in an organisation. To make it more a decision tool there has been an attempt to complement horizon scanning with strategic risk analysis (SRA) methods and techniques. This was a way to appropriately assess and prioritise the importance/likelihood and impact of emerging issues found on policy, strategy and delivery mechanisms (Pollard et al. 2004; Prpich et al. 2011, 2013). A further development of this is an approach that uses a qualitative weight of evidence (WOE) framework (like Linkov et al., 2009) to establish a more systematic process for filtering information (Garnett et al. 2016). As explained earlier, information is continuously retrieved from the web to capture 'real-time' data on the changing environment and policy landscape. This knowledge and information on emerging issues should be cross-referenced with academic and non-academic literature and through expert reviews, using the WOE framework. It implies a comprehensive analysis of the external macro environment (big picture) to detect and understand the early (weak) signals of change. This is further distilled through informal and formal networks (e.g. within the water or food supply domain) to identify emerging trends and understand the broad, long-term implications on an area (e.g. water quality).

3.3.1 Prioritisation methods

Risk prioritisation methods, participatory workshops and consensus Delphi techniques could be used (Linstone and Turoff, 1975). Additional clustering methods such as network analysis (Konnola et al., 2012; Saritas and Miles, 2012) are relevant to capture cross-cutting issues and priorities to better inform decision-making. Another online collaborative tool, PearlTrees (Padoa et al., 2015; Licurse and Cook, 2014), was successfully used to assess the 'information landscape', to extract and categorise pertinent information per key factors.

3.3.2 Expert reviews

Collective intelligence from a wide range of domain experts to question and challenge current mind-sets is preferable. Stakeholder workshops are employed to engage widely and at all levels, reflecting a critical part of intelligence gathering. Active engagement of policy officials at workshops encourage buy-in and create opportunities for workshop outputs to inform/impact on policy development and other institutional change in the long-term. Finding the right mix of 'experts' to participate is crucial and should thus, include a wide range of stakeholder and interest groups, e.g. from the academia, industry, government and non-governmental organisations, and wider public entities. Claims of bias or poor representation of expertise in workshops may be challenging that de-legitimised outputs, resulting in dissatisfaction with the scanning processes and/or the outputs of such. Therefore, the selection of experts is critical to address concerns about bias.

The following factors have been considered important in selection of the review experts (Rathe et al. 2013):

- *Heterogeneous grouping* - wide range of expertise defined by different value systems (e.g. coverage of broad range of interests, mix of sectors, type of organisation and demographics).

- *Expertise* - internationally or nationally recognised expert (e.g. recognition in field; extensive/recent publications; recognised by professional or trade associations).

- *Interest, familiarity and commitment to process* – individuals with a demonstrable interest in the topic, familiarity and commitment to the process (i.e. analytical, open-minded thinking among participants is encouraged, and effort is taken to eliminate candour or rejection of ideas based on participants' status or association with an organisation).

4. An application - foresight capabilities in the water sector

The following example from Scotland applies scanning approaches to reveal types of threats and opportunities affecting decisions in the water sector. More specific, it is about factors, like climate-change and land-use policy, and influences on the water quality (Dunn et al. 2014). Climate and land-use drivers were used to depict possible future climate- and land-use change scenarios, and evaluating their changing effect on the water quality risks. A simple approach for horizon scanning was thought of for the implications of these scenarios on the water quality.

The objectives of the study were:

- To identify key drivers of water quality in terms of broad characteristics of the climate that dominate hydro-chemical transport and qualitative relationships between different land uses and various pollutants.
- To develop a qualitative spatial methodology to integrate these drivers.
- To demonstrate the method by application of a simple set of climate and land-use scenarios for Scotland evaluating qualitative impacts on a range of key pollutants.

Water quality is for sure affected by a broad range of factors in the environment. Examples of such are basic physical nature attributes like the soil type, geology and topography. Together with the climate, properties of these factors determine the natural chemistry of water draining from an area. Key drivers of the water quality may be the climate-change impacts on increased rainfall intensity, with implications on pollutant transport and bioavailability of the nature.

Whilst climatic characteristics are primarily responsible for the transport of pollutants from the land to water bodies, it is the 'land use' and its management that largely determines the sources and availability of pollutants. In broad terms, different pollutants can be associated with different land uses, although detailed aspects of management and site situation can be extremely influential in determining the risk of pollutant losses. In the study of Dunn et al. (2014), five primary categories of land use in Scotland were identified: 1) arable, 2) grassland, 3) woodland, 4) semi-natural vegetation and, 5) urban/rural habitation.

As part of the methodology (Dunn et al. 2014) the impacts of climate and land use change are taken as interrelated, but a pragmatic distinction is adopted to the methodology to make it as simple and transparent as possible. The two key data sources required are the baseline and future climate, and land use. Two different sets of groupings linked to the climate change and land use change drivers together form the basis of a qualitative model of risk, and a series of matrices were developed to translate the various drivers into a set of pollutant responses. Three sets of transition matrices were developed, which described the relationships between:

- Key climate change drivers and expected pollutant responses
- Impacts of changing land use on pollutant responses
- The relative importance of climate change drivers versus land use change drivers on pollutant responses

A classification system was used within the matrices:

- −2 refer to a large decrease,
- −1 refer to a small decrease,
- 0 refer to neutral,
- +1 refer to a small increase,
- +2 refer to a large increase.

For each pollutant group and driver, values from −2 to +2 were assigned to the matrix based on expert judgement, or developed from the literature and prior knowledge for the predominant rural land use groups in Scotland. This step was initially undertaken by kinds of scientists with expertise in the relevant disciplines.

As indicated, changes in land use can have either a positive or negative impact on water quality. For example, a change from arable land to woodland would be expected to be primarily positive with respect to water quality. Similarly, whilst some small negative responses would be expected with a change from low intensity semi-natural habitat to coniferous woodland, a change to arable production is possibly the biggest negative change that could impact on water quality. As results, a set of maps are produced showing the pollutant responses to the specific (alternative) climate- and land use change scenarios. Reference is made to Dunn et al. (2014) for more details on how the metrics worked for the different scenarios.

5. Evaluation and discussion

5.1 Scanning – challenges and gains

The two examples described in Section 4 may be characterized as issue-centred scanning in the way the approaches substantiated the emerging issues. In exploratory scanning of potential problems, threats, opportunities and likely future developments, a somewhat broader basis is considered from the start, e.g. by internet search or text-mining. One restriction seen from the use of internet scanning methods is the fact that professional scanners may have biases in their searches and interpretation of findings. These aspects are typically addressed in foresight approaches (Truffer et al. (2008). While processing of information or expectations depend on individual experiences, priorities and positions, they are at the same time the result of social interaction. Actors' expectations are shaped by their position, but also by the specific social discourses they are actively or passively taking part in, e.g. particular professional discourses or media discourses. Some expectations even become very widespread across different actor groups thereby becoming shared points of orientation. That is, for some actors they become taken-for-granted presumptions. But even if actors are more sceptical, they tend to take these widely-held expectations into account, because they know that others share these expectations. Thus, expectations can be subject to strong social dynamics.

Teams of scanners with different backgrounds would help to overcome this kind of pitfall. Expert surveys can in fact be quite useful in the processing and analysis phases having an explicit focus on certain fields and issues. By comparing the SESTI experience with experiences from other horizon scanning processes, it seems that surveys are especially useful when areas are specified and the scanning starts from a well-defined field or sector, such as energy, water supply, or general science and policy (Czaplicka-Kolarz et al. 2009; Smith et al. 2010; Sutherland et al. 2010; 2011). Focusing on a specific field, surveys can deliver additional information on various side-aspects related to the core issues.

Timing is a general challenge with early signal analysis. Due to the novelty of issues the evidence basis at the beginning is rather weak while the impact may be tremendous.

5.2 Evaluation criteria

The evaluation of the different approaches and methods faces several challenges. First, each of the methods described above has advantages and disadvantages depending on the specific circumstances under which they are applied. Some methods are better for the initial phases of the scanning process, while others fit better into the analysis phase (Table 1). In this regard, an evaluation across the different approaches and methods is difficult as their success is highly contextual. However, common criteria can be identified reflecting the information needs and interests of policy-makers, and the degree to which they are met by the different tools and approaches.

Some criteria were defined by Anamatidou et al. (2012):

- Connections, clustering of weak signals and degree of relevance to a specific area

- Duration of weakness of signal, also associated with time at which signal is observed
- Origin (stakeholder(s) behind them) and novelty of weak signals
- Rising ethical, legal, societal or cultural issues
- Existence of a strategy already concerned with specific weak signal(s) and emerging issues by a government or industry, political party or lobby, or international organisation
- Positive and negative impacts and associated policy implications
- Policy recommendations

Following the framework of tools and methods presented in Figure 3, certain combinations of methods can be created to provide a complete evaluation along the scanning process. Three combinations defined by Anamatidou et al. (2012) are:

- A) Twitter/wiki scanning which is complemented by processing of weak signals.
- B) Focused expert review which is complemented by text-mining.
- C) Focused expert review which is assisted by expert's survey, literature review and attending conferences.

In Table II, two of the above criteria are combined with the different approaches, and their appropriateness is addressed.

5.3 Societal contexts of scanning

Horizon scanning is not merely about searching for signals and their factual evidence. It is also about analysing and understanding the societal contexts behind the entire process of initiation, communication, (r)evolution and dissemination of issues, as well as their early recognition and monitoring. That means, not only the evidence-based plausible storyline in the identified future narrative counts. It is also crucial to collect information about who initiated the signals or issues, who followed, who opposed them, when and why. Then we consider the interests, emotions and attitudes of the different stakeholders as well as experts.

Overall, it can be said that the added value of emerging-issue scanning lies in the strategic combination of available tools to broaden the spectrum of possible signals and to interpret them in a functional way for decision-makers. In addition, the human intelligence is a valuable necessity, either as a collective, or single experts, especially for the alerting function of the horizon scanning process.

Another interesting aspect is to see to what degree scanning results are considered by present policy-making processes compared to model-based forecasting. It seems that model-based forward-looking results are considered a bit more seriously than horizon scanning results, even though economic models completely failed to forecast the

financial crisis of 2007–2008. On the other hand, horizon scanning in the Netherlands and UK spotted the financial crisis two years before it started.

Table II: Analysis of combined approaches across evaluation criteria (adapted Anamatidou et al. 2012)

Framework/approach (Figure 3)	**Semi-automated, participatory**	**Semi-automated, non-participatory**	**Manual combined**
Comb. of methods	**A**	**B**	**C**
Policy implications assessment	Medium	High	High
	Associated policy implications of emerging issues are analysed by comparing emerging issues identified with topics in previous published thematic foresight reports and policy documents.	Text-mining can show the policy related terms. In focused expert review narratives in the primary scanning, usually contain policy implications or even policy advice of the author. A secondary scanning usually gives ideas on elaboration of proposed policies or of critics.	As reported in survey responses and in literature. As facilitated by narratives in focused expert review. Conferences are useful to recruit potential policy workshop participants.
Policy recommendations	Medium	High	High
	Through discourses, networking, interaction with experts. Also via examination of relevant thematic foresight reports and recently published policy documents.	Meta descriptions of issues can be discussed in workshops with experts and stakeholders, which usually lead to recommendations.	As reported in survey responses and in literature. As facilitated by policy workshops.

5.4 Impact on water utilities

Horizon scanning as a strategic approach for single water utilities seems to be challenging of several reasons. Anyhow, it must be provided as an opportunity for the business, and resources must be allocated for the scanning process. In short of knowledge, resources and time in own organisation, it may be an idea for the water utilities to collaborate on this in sector-associations or similar. Another opportunity is to engage a third party for the data collection.

Post-assessment of the information can however, take place in teams consisting of operating personnel from facilities in addition to the supporting personnel, relevant suppliers and others. Based on pre-assessments, the most relevant scanning methods seem to be expert reviews and surveys.

As seen from Dunn et al. (2014), the analysis of data could be designed as a tool for interaction with stakeholders, e.g. for horizon scanning a range of different pollutants

under different scenarios. In this case, to obtain mapped outputs depicting the qualitative responses to pollutants. In the example, the pollutant responses were based on expert judgement both in terms of the key climate and land use change drivers, and the degree to which these drivers could influence the response. Similar approaches may be applied to other problem areas connected to water utilities as well.

6. Conclusion

In the present paper a description of approaches, and discussion of horizon scanning approaches related to cyber-physical threats to water utilities have been presented. Horizon scanning is generally seen as an instrument with two main functions: 1) the alerting function, and 2) the creative function. For the alerting function, comprehensive methods are needed to scan and assess early warning signals that may indicate potential emerging issues. The information origin span from a variety of published information, media and digital sources. For the more creative function, scanning methods need to be complemented with tools and participative processes that, on one hand, focus on clustering and synthesis of the scanned information and, on the other hand, human imagination and creativity.

As explained, different approaches to scanning, identifying and assessing potential emerging issues exist. The issues found from scanning processes are however, highly dynamic, social constructs that are partly evidence-based, and partly the results of the imagination, thinking and debating that takes place within different organisations and segments of society. The applicability to the water sector is therefore a matter of organisational concern, the ability to play on some 'extended' knowledge and resources, both within and outside the operating business.

7. Acknowledgements

The work with this paper was partly funded by the H2020-program through the STOP-IT project.

References

Abrams, M., Weiss, J. (2008) Malicious control system cyber security attack - Case Study: Maroochy Water Services, Australia. An analysis on controls that might have prevented or mitigated the event. NIST- National Institute of Technology and Standards.

Alcaraz, C., Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, 8, pp. 53-66.

Amanatidou, E., Butter, M., Carabias, V., Könnölä, T., Leis, M., Saritas, O., Schaper-Rinkel, P., and van Rij, V. (2012) On concepts and methods in horizon scanning: lessons from initiating policy dialogues on emerging issues. *Science and Public Policy* 39, pp. 208–221.

Czaplicka-Kolarz, K., Stanczyk, K. and Kapusta, K. (2009) Technology foresight for a vision of energy sector development in Poland till 2030. Delphi survey as an element of technology foresighting, *Technological Forecasting and Social Change*, 76, pp. 327–38.

Dunn, S.M., Towersa, W., Dawsona, J.C., Samplea, J., McDonald, J. (2014) A pragmatic methodology for horizon scanning of water qualitylinked to future climate and land use scenarios. *Land Use Policy* 44 (2015), pp. 131–144.

Garnett, K., Lickorish, F.A., Rocks, S.A., Prpich, G., Rathe, A.A., Pollard, S.J.T. (2016) Integrating horizon scanning and strategic risk prioritisation using a weight of evidence framework to inform policy decisions. *Science of the Total Environment* 560–561, pp. 82–91.

Johnsen, S.O., Røstum, J. (2015) SINTEF Report: (Title in Norwegian) Eksempel på mal for risikovurdering knyttet til informasjonssikkerhet og drifts-kontrollsystem for vann og avløp, SINTEF Technology and Society.

Konnola, T., Salo, A., Cagnin, C., Carabias, V., Vikkummaa, E. (2012) Facing the future: scanning, synthesizing and sense-making in horizon scanning. *Science and Public Policy* 39, pp. 222–231.

Linkov, I., Loney, D., Cormier, S., Satterstrom, F., Bridges, T., (2009) Weight-of-evidence evaluation in environmental assessment: review of qualitative and quantitative approaches. *Science of the Total Environment* 407, pp. 5199–5205.

Linstone, H.A., Turoff, M., (1975) Delphi Method: Techniques and Applications. Addison-Wesley Publishing, Boston, USA.

Licurse, M., Cook, T. (2014) Pearltrees web-based interface for teaching informatics in the radiology residence. *Progress in Biomedical Optics and Imaging - Proceedings of SPIE 9039*, 90390N.

Loveridge, D. (2009) *'Foresight: The Art and Science of Anticipating the Future'*. New York and London: Routledge.

Padoa, C., Schneider, D., de Souza, J., Medeiros, S., 2015. Investigating social curation websited: a crowd computing perspective. *IEEE 19th International Conference on Computer Supported Cooperative Work in Design (CSCWD):* pp. 253–258.

Pollard, S.J.T., Kemp, R.V., Crawford,M., Duarte-Davidson, R., Irwin, J.G., Yearsley, R., (2004). Characterising environmental harm: developments in an approach to strategic risk assessment and risk management. *Risk Analyses* 24, pp. 1551–1560.

Prpich, G., Evans, J., Irving, P., Dagonneau, J., Hutchinson, J., Rocks, S., Black, E., Pollard, S.J.T., (2011) Character of environmental harms - overcoming implementation challenges with policy makers and regulators. *Environmental Science Technology* 45, pp. 9857–9865.

Prpich, G., Dagonneau, J., Rocks, S.A., Lickorish, F., Pollard, S.J.T., (2013) Scientific commentary: strategic analysis of environmental policy risks - heat maps, risk futures and the character of environmental harm. *Science of the Total Environment* 463-464, pp. 442–445.

Rathe, A.A., Prpich, G., Shaw, H., Delgado, J., Garnett, K., Chatterton, J. C., Lickorish, F. and Pollard, S.J.T. (2013). *Annual Key Factors Report 2013*. Cranfield University, UK, at: http://www.cranfieldfutures.com/wpcontent/

Saritas, O., Miles, I. (2012) Scan-4-light: a searchlight function horizon scanning and trend monitoring project. *Foresight 14*, pp. 489–510.

Smith, J., Cook, A. and Packer, C. (2010) Evaluation criteria to assess the value of identification sources for horizon scanning, *International Journal of Technology Assessment in Health Care*, 26, pp. 348–353.

Sutherland, W. J., Clout, M., Coˆ te´ , I., Daszak, P. et al. (2010) A horizon scan of global conservation issues for 2010, *Trends in Ecology and Evolution*, Vol 25, pp. 1–7.

Sutherland, W. J., Fleishman, E., Mascia, B., Pretty, J. and Rudd, M. (2011) Methods for collaboratively identifying research priorities and emerging issues in science and policy, *Methods in Ecology and Evolution*, 2, pp. 238–47.

Truffer, B., VoB, J.P., Konrad, K. (2008) Mapping expectations for system transformations-lessons from sustainability foresight in German utility sectors, *Technological Forecasting & Social Change*, 75, pp. 1360–1372.

Van Rij, V. (2010) Joint horizon scanning: identifying common strategic choices and questions for knowledge, *Science and Public Policy*, 37, pp. 7–18.

Session 5:
Tools and methodologies

Analysis and management of accident precursors in manufacturing industry – Extended Abstract

Micaela Demichela, Gabriele Baldissone

Department of Applied Science and Technology – Politecnico di Torino

Corso Duca degli Abruzzi 24,

10129 Torino, Italy

Salvina Murè

Aria S.r.l.

Corso Mediterraneo 140

10129 Torino, Italy

Extended Abstract

The present work deals with the development of a new Accident Precursors Management System, starting from the HFACS taxonomy and the Fuzzy Application Procedure – FAP, already devised for the industrial risk analysis. The methodology proposed is composed by a data collection procedure, carried out in situ and that requires a short interview to the personnel involved in the observed events. Afterward, a data analysis tool, based on the Fuzzy Logic Approach, allows to obtain the preventive measures suitable to cope with the accident precursors analysed. The methodology described is generic and it does not depend on the working site type. It has been tested in a real industrial workplace and the results obtained are shown.

Occupational accident prevention has been historically approached by Safety Management using ex-post accident analysis in different working fields. This "learning from the experience" approach promotes different reporting and analysis systems for the accidents, as fundamental tools to identify causes and to help of planing the prevention measurement.

Beside the Accident Analysis, several authors suggest to improve the risk prevention with an effective Near Miss. The "Zero Accidents Vision", recently adopted especially by companies characterized by few occupational accidents, addressed the Safety Management activity to support the occupational accident analysis with the accident precursors identification and reporting. The accident precursors can be defined

referring to the accident definition of the Event Tree Analysis as a truncated accident sequence. According with this definition, the concept of accident precursors can include Near Miss event and both Unsafe Acts of personnel and Unsafe Conditions of working places. The difference between these three categories is the closeness to the complete accidental sequence. A full adoption of a Safety Management system, including precursors management, according with Zero Accidents Vision, allows a better control and reduction of occupational risk, meanwhile a careful control of the working conditions and personnel acts should prevent accidents and improve operational efficiency.

Near Miss Management system could not be designed as a simple expansion of Occupational Accident Analysis System. The number of Near Misses is higher than accidents, and their hidden nature requires a different skill of identification compared to an accident that shows evident consequences. These factors suggest that a Near Miss Management system requires higher resources displacement to be reported and analyzed due to the large number of data. Initially, the Near Miss Management system has been developed in process industry and medical sector, then the system has been extended to the construction field and the manufacturing industry. Near Miss Management system usually is characterized by four steps:

- NM identification;
- Assessment and Prevention measurement planning;
- Prevention measurement application;
- Feedback.

- This structure is, generally, adopted with two possible approaches: such as the bottom up approach and the centralized approach. The first approach entails that the Near Misses from a plant are reported by the onsite workers and supervisors, while the Health and Safety office may help in analysis and feedback activities. In the centralized approach, instead, the Near Misses are reported by the Health and Safety personnel or by external personnel that manage all the activities.

- In this work, a new Accident Precursors Management system has been developed starting from the structure of the Near Miss Management system based on the centralized approach. The Accident Precursors Management system has been developed as a general method for detecting and reporting accident precursors in a wide range of working activities. It has been designed as a decisional supporting tool for the HSE service, and it is based on the following structure:

    1 Occupational accident precursors identification and reporting (Unsafe Acts and Conditions and Near Misses);

    2 Data analysis;

    3 Prevention measurement planning and application;

    4 Feedback.

The first step is performed as a collection of data supported by a methodology based on the specific taxonomy (HFACS) applied to external personnel and requires also a short interview to the workers involved. This interview has to be performed in order to identify, as soon as possible, the root causes of the accident precursor observed and it is completed by a preliminary assessment (classification) of the event. The second step is based on the Fuzzy Logic Approach: a tool initially developed for the occupational accident risk assessment that has been modified to be used in case of the accident precursor analysis. It allows an aggregate approach to the accident precursor assessment and leads to the preventive measurement planning in accordance with the HSE service. The last two steps have to be designed case by case, as they are strongly dependent on the characteristics of the workplace.

The paper is organized as follows: a first a description of the data collection methodology and of the data analysis with Fuzzy Logic Approach is given, then a case study application is presented and results are discussed.

Keywords: Accident precursors; workplace risk management; preventive measures; risk-based decision making

Enhancement of Safety Imagination in Socio-Technical Systems with Gamification and Computational Creativity

Antonio De Nicola, Giordano Vicoli, Maria Luisa Villani

ENEA – Centro Ricerche Casaccia

Via Anguillarese 301

00123, Rome, Italy

Andrea Falegnami, Riccardo Patriarca

"Sapienza" University of Rome

Department of Mechanical and Aerospace Engineering

Via Eudossiana 18

00184, Rome, Italy

Abstract

We present a novel framework to enhance safety imagination in socio-technical systems with gamification and computational creativity. This relies on the usage of the Functional Resonance Analysis Method (FRAM) for systemic analysis of socio-technical system. In our proposal information on the system structure and organization both as-imagined and as-actually done is elicited from sharp-end operators by means of a gamified and participatory approach and through an iOS app. Then such knowledge is organized as a domain ontology compliant with FRAM and is used to feed a computational creativity system (i.e. Creativity Machine) and to support the analyst in conceiving FRAM models. Even if the approach is general, here we address a case study concerning healthcare and, in particular, an accident happened during an abdominal surgery.

Keywords: Safety, FRAM, participatory modelling, healthcare, ontology.

1. Introduction

Analytical methods for safety analysis of socio-technical systems require the definition of models representing the relevant aspects of the system to be analysed. An example is the Functional Resonance Analysis Method (FRAM) (Hollnagel 2012), a recently developed method for systemic analysis of socio-technical system, where models represent the functional relationships among the various system's elements. In case of large systems, e.g. systems with many human-based activities, technological artefacts, and procedures, building these models can be demanding in terms of having a clear and complete understanding of the system structure and organization both as-imagined and as-actually done. In particular, for understanding work-as-done, information is usually gathered from informal or structured interviews, observations or other interaction means. These activities imply the collaboration of various systems stakeholders, including sharp-end operators, who generally have limited time to be involved in a strenuous knowledge elicitation project and may not be enough stimulated to collaboration. On the other hand, subjective interpretation of the gathered information could be error prone or lead to incomplete descriptions.

To deal with these problems, we propose the FRAMboICE (FRAM-based ontology for safety Imagination through Collaborative Environment) framework consisting of a gamified and participatory knowledge gathering approach to boost engagement of systems stakeholders and of a formal semantic repository to organize the collected information, upon which performing automatic reasoning to support users in thinking unimagined situations that may occur and that are relevant to safety analysts.

Indeed, gamification, intended as the use of game design elements in non-game contexts, aims at increasing users activity and creativity and it is being used in various contexts, such as training in enterprises and open innovation. The second aspect of the approach refers to the capability to generate coherent conceptual representations of the users information concerning systems functions and their inter-dependencies (e.g., couplings in the FRAM notation), including unexpected situations, at various levels of abstraction, taking advantage of a FRAM-based domain-specific ontology and of semantics techniques.

The approach is supported by the FRAMboICE mobile app to manage the gamified information collection process from the users and by a novel software application, named Creativity Machine (Coletti, De Nicola, & Villani, 2017) implementing computational creativity techniques to automatically suggest concepts describing FRAM functions and realistic situations affecting their performance, selected from the FRAM-based ontology. This approach is discussed through a healthcare case study, adopting a safety-oriented perspective.

The rest of the paper is organized as follows. Section 2 briefly describes the FRAM method for safety analysis. Section 3 describes the healthcare case study. Section 4 presents an overview of the safety imagination framework and its components. Finally Section 5 closes the paper with some considerations on the safety imagination problem and some future research directions.

2. FRAM for Safety Analysis

FRAM is a systemic method to analyse complex socio-technical systems. The aim of FRAM consists in describing the work-as-done in everyday practices as a means to manage the complexity and understand where potential criticalities may emerge. Since the FRAM is a method rather than a model, its first stage of application consists in developing a model of the specific activity that is the focus of the analysis. Once developed the model, the second stage consists in developing instantiations of the activity for the analysis of the complexity itself.

2.1 FRAM principles and building steps

The FRAM relies on four principles, which acknowledge the need to manage - rather than reduce – the complexity of work domain, in line with Safety-II and Resilience Engineering (Hollnagel 2012).

- Equivalence of failures and successes. Failures and successes emerge from a common source, i.e. everyday performance variability. The variability is what allows both things go right and things go wrong, depending on local and global interactions among system's components.

- Principle of approximate adjustments. Human beings as individuals, groups (or even organizations) adjust their performance to deal with the complexity of the operating scenario. These adjustments become usually unavoidable, due to the variability of work conditions, partly intractable and underspecified.

- Principle of emergence. In complex systems, it is not always possible to link one (or multiple) linear static causes to effects. More specifically, many events are emergent rather than resultant from a specific combination of fixed conditions. Transient combinations of factors might not leave detectable traces for a posteriori analysis.

- Functional resonance. The functional resonance represents the detectable signal emerging from the unintended interaction of multiple signals. This variability is not random at all, but it often depends on recognizable behaviours of the agents involved in the analysis, which act dynamically, based on local rationality.

A FRAM model is generally developed following four steps (Hollnagel 2012):

- Step 1: define the functions of interest, adopting a functional perspective. In FRAM, a function represents an activity necessary to produce a certain outcome. The outcome of this step consists in describing what an agent (individual, group, equipment, organization) does, by means of FRAMs' fundamental aspects, i.e. Input (I), Output (O), Time (T), Control (C), Precondition (P), Resource (R), see Figure 1.

- Step 2: identify function variability. Each function has to be explored in terms of its variability, which can be endogenous, exogenous and/or deriving from upstream–downstream coupling (discussed in detail in Step 3). The description of variability can be expressed by means of different phenotypes (e.g. timing,

precision, speed) depending on the specific function. The outcome of this step is the basis for characterising the expected (potential) variability of the activity as carried out in the everyday work environment (see Step 3).

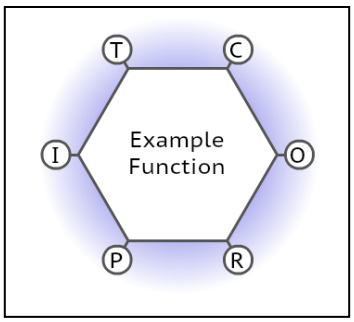


Figure 1. A FRAM function represented as a hexagon.

- Step 3: aggregate the variability. This step aims at understanding how system performance affects and is affected by the coupling variability. The upstream–downstream interaction is described exploring the model paths identified by actual or hypothetical events. For this step, it is possible to use information gathered from real case situations (e.g. an accident analysis), as a means to suggest one or more instantiations of the model, i.e. potential aggregation of variability in a specific scenario. These instantiations can be analysed to find an explanation of why something happened (as in accident analysis) or a plausible scenario of what may happen (as in risk assessment)

- Step 4: manage the variability. Acknowledging the need for a portion of variability in complex socio-technical systems, this step aims at understanding the most effective way to manage it, rather than simply eliminating it, as for traditional approach labelled as Safety-I approaches. Depending on the specific scenario, variability can be damped, amplified or just monitored, addressing the need to add a safety-related indicator.

2.2 Gathering data from developing a FRAM model

Since the FRAM aims to understand the variability of everyday work, it is necessary to explore the nitty-gritty of work, developing the analysis in strict relationship with sharp-end operators. On this path, observational studies represent a commonly used technique for acquiring knowledge of a naturalistic context. In particular, for FRAM-oriented analyses, open-ended naturalistic observations, i.e. pure observations, are adopted frequently to observe work without any preconception as an approach for informal conversation with practitioners (Patton, 2002). In addition, for developing a FRAM model, conversational or semi-structured interviews are used frequently (or complementary to observational studies), even if they require an expert interviewer able to ask open-ended questions (Hackos and Redish, 1998). However, even if these kinds of data collection techniques are used in FRAM model development, they require efforts, which usually become time-consuming. It is also necessary to underline the

central role of the observer/interviewer, who must have fresh-eyes to inspect a work domain with limited bias, and interviewing skills to steer the discussion in a convenient and meaningful direction. For these reasons, developing an automatic or semi-automatic technique for data collection in collaboration with sharp-end operators would generate relevant benefits in terms of model development.

3. Case Study: Safety Imagination in Healthcare

New challenges constantly affect healthcare practices, mainly due to the instrumental, procedural and organizational innovations of recent years (Woods and Cook, 2002). Furthermore, in everyday activities, work conditions are underspecified, as well as functioning principles, due to scenario's variability (e.g., individual patient state, need for specific resources, unique case presentation) (Hernan et al., 2015). For all these reasons, even a simple practice in healthcare is not that simple, and consequently neither its representation. When the purpose is to describe meaningfully a hospital's dynamic relationships, variabilities and agents it is not enough to simply make unstructured content and data analysis available, rather they must be previously adapted to a common ontological layer. This latter allows the analyst to gather, understand and eventually rearrange those relationships, variabilities and data belonging to the healthcare domain.

For example, considering the process of administering drug, there are several types of drugs, different for primary goal (e.g., antibiotic, sedative, metabolic…), methods of administration, side effects, and so on. In addition, different healthcare operators interact with the same drug in a different way, i.e. transferring it, preparing it, administering it, checking its state. Since one solution might be understanding ontologically different data under the lens of FRAM, we must build an ontology based on the FRAM method's structure.

For the purpose to explore this possibility, we propose a taxonomy built from a simple pilot case study: an abdominal surgery, in which disposable materials might be forgotten in patient's body. This scenario may represent a typical accident, and thus it is a valuable candidate as a seed from which developing a base ontology. This paragraph summarizes a case study following an example presented in the FRAM handbook (Hollnagel 2012).

As reported, the team included two specialist surgeons: main – who knew well the procedure – and assistant surgeon. Both agreed with the personnel management to operate simultaneously on more than one intervention (event that occurs occasionally when the facility is short of staff). In this case, the main surgeon had to leave after the suture completion to execute another operation. Akin to the main surgeon, the assistant had to leave the ongoing surgery twice – first after a tissue sample removal, and second after stopping an haemorrage. Since during the procedure the bleeding had been problematic, stopping it had required a multitude of sponges. The scrub nurse always counts all the instruments and material used, but this time had missed a sponge and a disarp still in the patient's abdomen, and had did not signal it to the surgeon. Since the patient was participating in a study, the scrub administered a special analgesic to him. Once the assistant surgeon had removed the disarp. He asked the main surgeon to suture the wound by himself, and left the operating room for the second time. At this point,

the main surgeon was awaited in another operating room, and in hurry. He started suturing the patient assisted by the scrub nurse, but no one checked materials. During this, after checked the study's papers, the supervising nurse realized that the analgesic prepared was wrong. The three present nurses discoursed about which analgesic to use. After that the scrub nurse prepared a new syringe with the right analgesic. The operating room's phone rang to notify to the main surgeon he had to leave. Supervising and scrub nurses did a final check of the instruments and realized that a sponge and a disarp were missing. Everyone was summoned again and the patient, already extubated and whom wound had been suturated, had undergo to a new surgical operation. Fortunately, after all those mischievous episodes the patient remained unharmed.

The FRAM analysis is continued by describing each aspect of each function identified above. When the output description of a function corresponds to the description of one of the five left over aspects of another function a coupling is established among these two functions, thus the order in which is done does not matter, only completeness does. The counting of instruments and materials happens twice in the example, one before and one after the suturing, thus two distinct functions are needed. As depicted in Figure 2, some functions are grey, representing the boundaries of the analysis, they are so-called "background functions". For ours aims background functions can be used as placeholders to expand incrementally the underlying ontological framework, and thus, the taxonomized model.

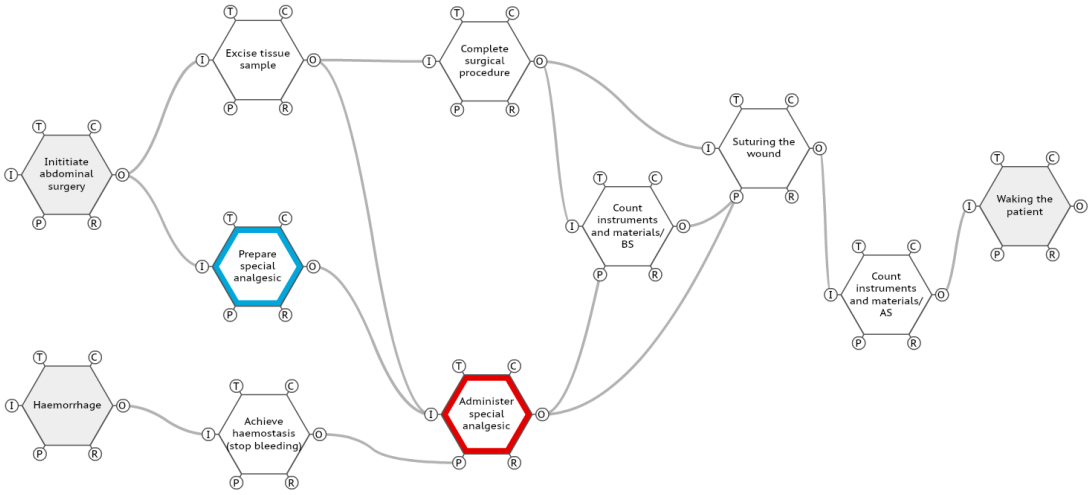


Figure 2. A simplified FRAM instantiation of an accident in healthcare; a valuable starting point to develop an ontology.

While other techniques and tools may be used to build a FRAM instantiation, sharp-end operators' reluctance for reporting about their job activities cannot be overlooked. This problem arises specifically in healthcare, and thus could be overcome through a gamified data gathering by means of healthcare operators' mobile devices.

The check of model's consistency and completeness is a time-expensive issue of FRAM method, that with the FRAMboICE app can be solved letting each of human

(i.e., healthcare operators, ontology master, FRAM analyst) and artificial (i.e., FRAM-based ontology, FRAM designer) agents doing it autonomously repeatedly at several different points of the model development process. The consistency is ensured checking that aspects are described using the same names over the distinct functions. On the other hand, the completeness is checked spanning through each function one at time assuring that all aspects described in the instantiation can be found at least in two functions, is to say that no dangling aspect can exist.

4. A Safety Imagination Framework based on FRAM Semantics

Here we present the safety imagination framework aiming at supporting the FRAM model definition process from the elicitation of knowledge from sharp-end operators (e.g. healthcare personnel) to the design of a FRAM model. The framework includes a FRAM-based ontology, the FRAMboICE iOS app, and the creativity machine. The ontology, which is a formal specification of a shared conceptualization (Borst, 1997) (Gruber, 1993), gathers concepts and their relationships modelling an application domain, as the healthcare.

Figure 3 depicts the whole process for the healthcare case study. The healthcare personnel provide information about their domain of interest by using the FRAMboICE app, which leverages a gamification approach. This relies on the upper model of the FRAM-based ontology and is fed by predefined ontology concepts (step 0 and step 4). By means of the FRAMboICE app, FRAM functions are described (step 1) and collected in a repository (step 2). Then the ontology master (De Nicola & Missikoff, 2016), an ontology engineer with decisional role, reviews the functions and updates the ontology (step 3). Finally, the FRAM analyst builds FRAM models (step 7) by accessing the ontology with semantic queries (step 5) conceived to support creative activities (step 6), as combination or transformation of functions and their aspects and similarity reasoning on function aspects.

4.1 FRAM-based ontology for healthcare systems

The FRAM-based ontology for healthcare systems aims at representing knowledge concerning the healthcare domain structured according to an upper model derived from the FRAM method. To this purpose we identified the FRAM Upper-level Model (FUM) representing the most relevant FRAM concepts and the ontological relationships linking them. A FRAM-based ontology is obtained by extending FUM with domain-specific concepts. With respect to other existing upper level ontologies, as SUMO (Niles & Pease, 2001) and DOLCE (Gangemi, Guarino, Masolo, Oltramari, & Schneider, 2002), FUM is not general purpose and is conceived to support engineering of FRAM-based ontologies to be used to support the process of designing FRAM models.

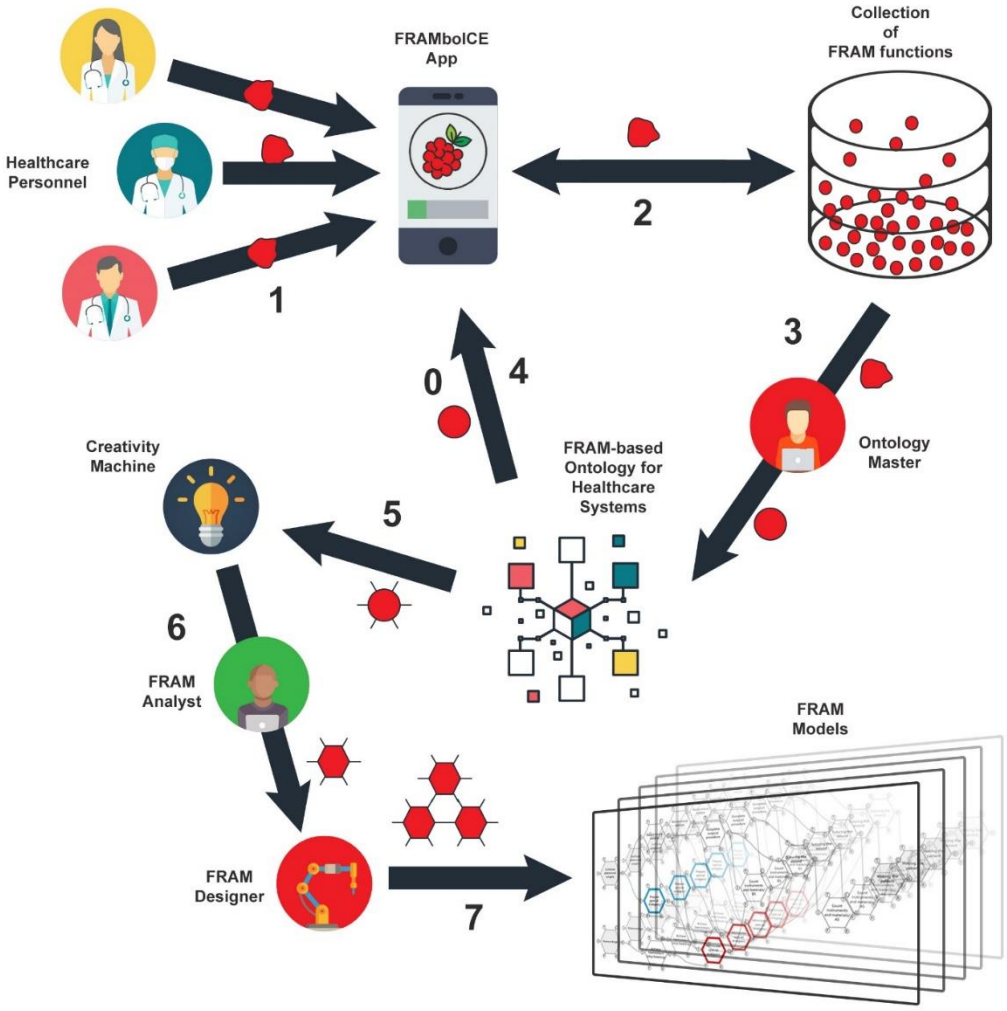


Figure 3. Safety imagination framework based on FRAM semantics. The numbers represent the sequencing of activities needed to define FRAM models.

The FUM upper level concepts are derived from the FRAM modelling entities. Among them, *FRAM_Element* is the generic concept that is specialized in *Agent*, *Aspect*, *Function*, and *Phenotype*. Then *Coupling* allows representing how two different functions link together and *Coupling_effect* models the corresponding effect, which could be *Amplifying*, *Damping* and *No_effect*.

The FUM relationships are modelled in the ontology as object properties. The *hasAspect* object property relates two *Aspect*s. It is specialized in the *hasControl*, *hasInput*, *hasOutput*, *hasPrecondition*, *hasResource*, and *hasTime* object properties. *hasFunction* is the inverse relationship of *hasAspect*. The *hasPhenotype* object property relates an *Output* with its *Phenotype*. The *hasDownstreamAspect* object property between *Coupling* and *Input* and *hasUpstreamAspect* object property between *Coupling* and *Output* allow to specify the role of the aspects in a coupling. Finally the *hasEffect* object property relates the *Coupling* concept with the corresponding *CouplingEffect*.

Figure 4 shows an excerpt of the *Function* concept specialization hierarchy for the healthcare case study. This is depicted by using the OWLViz plugin of the protégé ontology management system (Stanford, 2016).

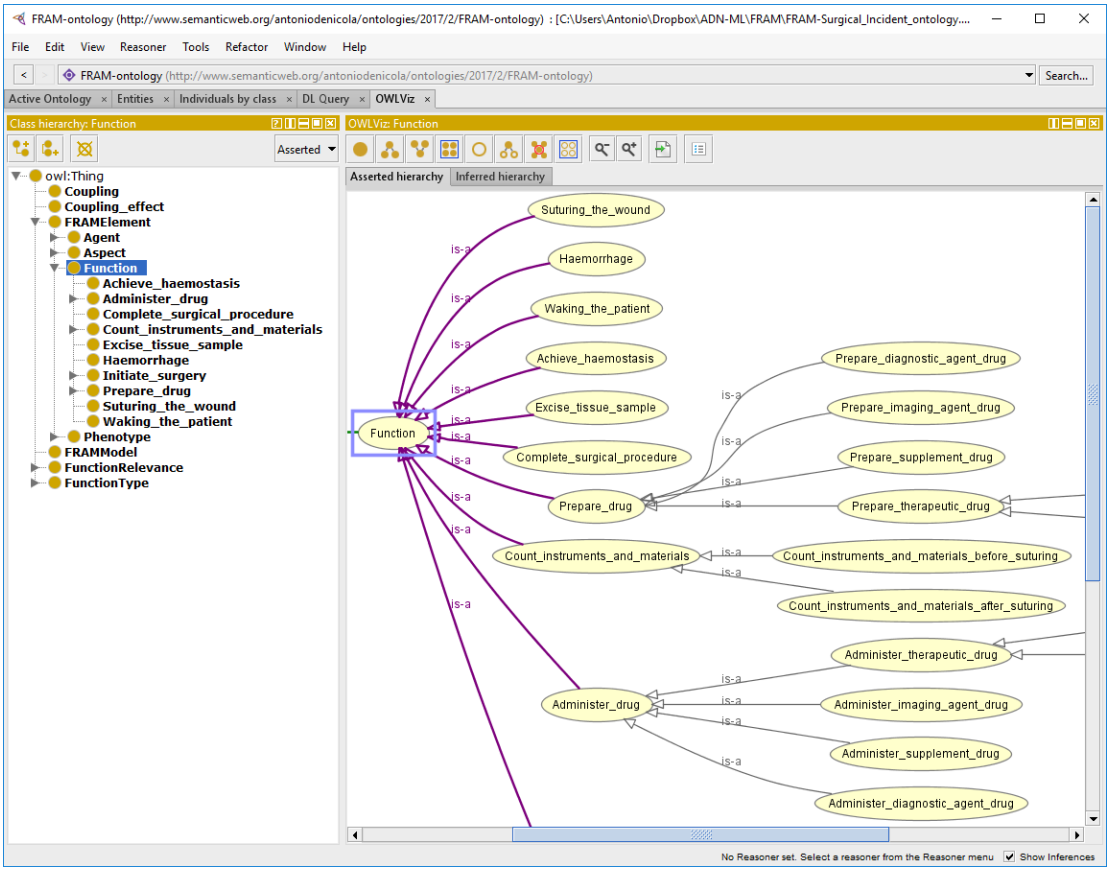


Figure 4. An excerpt of the function taxonomy for the healthcare case study.

4.2 A gamified app for elicitation of sharp-end operator knowledge

Our proposal is based on the assumption that sharp-end operators participate in the process of collecting knowledge on a specific domain of interest, as the healthcare. This is rarely the case as this process could be seen as a strenuous, time-consuming and annoying activity. Hence our objective is to increase engagement of experts by means of a gamification approach supported by a software application where game elements (Reeves & Read, 2009) are introduced to support knowledge elicitation. We deem that a gamified application used in a non-entertainment context could unleash a broader participation of experts and an increased capacity in collecting knowledge. This would lead to safety, security and economic benefits. To this aim we selected seven game elements and we adopted them in a knowledge elicitation workflow. These are: (1) avatars, (2) points and leaderboards, (3) feedback, (4) rules, (5) teams, (6) parallel communication systems, and (7) time pressure.

In the following we describe the game mechanics supported by the FRAMboICE app. We envisage three different roles: the coordinator, the FRAM function proposer, and the FRAM function contributor (for the sake of concision we refer to them in the

following as contributor and proposer). The coordinator is in charge of starting and ending the FRAM functions harvesting activity, and/or may decide its duration. Indeed, the FRAMboICE app provides flexibility to organize a game session lasting a few hours, as in the case of traditional participative FRAM assessment workshops, or days/weeks to give participants more time to define the functions, or even an indefinite time, until the coordinator decides to close the activity. The coordinator is also in charge of deciding whether a FRAM function should be accepted or rejected. As this decision affects assignment of points to the participants, this role should be given to a participant trusted by the community of experts. All the participants can be both proposer and contributor.

The coordinator starts the process by initiating FRAM functions harvesting. Hence, proposers create FRAM functions by means of the ICE app. Other participants can read the proposed FRAM functions and decide to contribute by modifying one of them or, simply, accepting it. In case of modification, the corresponding proposer can decide to accept or reject the update. Once the proposer deems that his FRAM function is valuable, he sends it to the coordinator who may decide to reject it or to use it to update the collection of FRAM functions. It should be noted that, to perform this decisional activity, the coordinator can be supported by a committee of experts (if available). Once the FRAM function is accepted, contributors can still decide to endorse it.

Both proposers and contributors of the FRAM functions harvesting process win points by performing the above-mentioned activities. The idea is that participation is rewarded and that the larger the participation on defining a FRAM function the more points are collected by the team members.

Figure 5 shows the interface of the FRAMboICE mobile app.

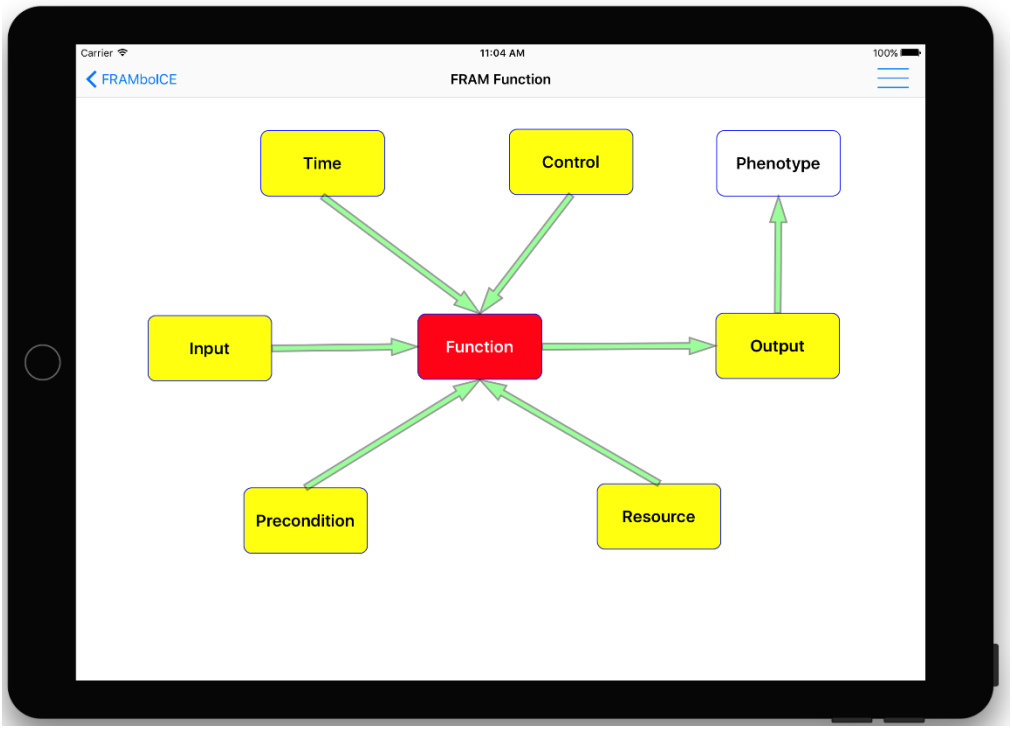


Figure 5. User interface of the FRAMboICE mobile app.

4.3 Computational creativity support

The FRAM-based ontology for healthcare systems collects semantic descriptions of potential functions that an analyst may define when designing FRAM models for specific healthcare safety analysis problems. The FRAM-based ontology allows organizing such function descriptions in a knowledge base that can be used by the analyst to search information through semantics-based query functions. More interestingly, such formalized knowledge may suggest input parameters for FRAM models leveraging automatic reasoning methods, such as concepts/function models subsumption relations and similarity/dissimilarity metrics, as well as contextual or design related constraints. This task is accomplished by the Creativity Machine component of the safety imagination framework that implements methods of computational creativity, a subfield of Artificial Intelligence aiming at defining computational systems that create artifacts and ideas (Colton & Wiggins, 2012).

Generally, computational creativity methods address the problem of thinking something new, e.g., a risk situation, by varying and/or combining one or more aspects of what already exists, e.g., old experiences of incidents or normal situations. For our application, we initially focus on the following methods: the *transformation* method, defined as the process that modifies the form of some particular features of an existing design; and the *analogy* method, defined as the process where specific aspects of the conceptual structure of one problem or domain are matched with and transferred to another problem or domain. In particular, we apply these definitions to the design of a FRAM function and of its couplings.

Given a collection of "ground-level" function semantic descriptions, a task of the safety analyst is to identify all the functions to include in a model, to define the aspects of each FRAM function and its couplings with the other functions. Indeed, the information from the healthcare personnel could be incomplete, and they could miss unusual or abnormal situations that are relevant to the FRAM analysis.
Thus, following the analogy method, support to specify aspects of a given FRAM function can be provided, for example, by showing to the analyst the aspects of similar functions. The description of the function "administer special analgesic" in the abdominal surgery model of Figure 2, with details like the choice/availability of the right analgesic as in the case study, could suggest aspects for "administer epidural anesthetic" function while analyzing labor for childbirth process.

As a FRAM coupling is automatically realized by identifying pair of aspects of different functions addressed by the same name, whenever two aspects refer to concepts that are in a subsumption relation in the FRAM-based healthcare ontology (i.e., they belong to the same taxonomy), the system may suggest the FRAM analyst a coupling between the two functions, or to abstract/further detail one of the two aspects/functions.

The transformation method can be implemented by suggesting changes to function aspects or to couplings. In the example of Figure 2, "count instruments and materials before suturing" could be de-coupled from "suturing the wound" to suggest the analyst a situation that may occur that could be taken into account in the analysis, like that task is forgotten by distraction and not reported, as described in the case study.

5. Conclusion

Foresight is the process of inferring new knowledge from pre-existing one. Enhancing the knowledge gathering process should be considered as a precondition to improve existing foresight methods. In this context we presented a novel framework with two objectives. The former is to increase engagement of sharp-end operators by means of a gamification approach and of the FRAM method. The latter is to use elicited knowledge and computational creativity methods to support safety analyst in thinking out of the box and in conceiving unimagined situations relevant to safety analysis.

The concrete example of application of this framework in the healthcare sector and a first positive feedback from safety analysts demonstrate, from one side, the need of novel more engaging approaches to collect expert knowledge and, from the other, the need to further increase the computational creativity support of our framework.

References

Borst, W. N. (1997). *Construction of engineering ontologies for knowledge sharing and reuse*. Universiteit Twente.

Coletti, A., De Nicola, A., & Villani, M. L. (2017). *Enhancing creativity in risk assessment of complex sociotechnical systems*. *Lecture Notes in Computer Science* (Vol. 10405 LNCS).

Colton, S., & Wiggins, G. A. (2012). Computational creativity: The final frontier? In *Proc. of the 20th European conference on artificial intelligence* (pp. 21–26).

De Nicola, A., & Missikoff, M. (2016). A lightweight methodology for rapid ontology engineering. *Communications of the ACM*, *59*(3).

Gangemi, A., Guarino, N., Masolo, C., Oltramari, A., & Schneider, L. (2002). Sweetening ontologies with DOLCE. *Lecture Notes in Computer Science, Vol. 2473*, 223–233.

Gruber, T. R. (1993). A translation approach to portable ontology specifications. *Knowledge Acquisition*, *5*(2), 199–220.

Hackos, J.T., Redish, J.C., 1998. Conducting the site visit - honing your interviewing skills. John Wiley & Sons, New York, NY.

Hernan, A.L., Giles, S.J., Fuller, J., Johnson, J.K., Walker, C., Dunbar, J.A., 2015. Patient and carer identified factors which contribute to safety incidents in primary care: a qualitative study. BMJ Qual. Saf. 24, 583–593.

Hollnagel, E., 2012. FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-technical Systems. Ashgate.

Niles, I., & Pease, A. (2001). Towards a Standard Upper Ontology. *The 2nd International Conference on Formal Ontology in Information Systems*, 2–9.

Patton, M.Q., 2002. Qualitative research and evaluation methods, 3rd edition. ed. Sage Publications, Thousand Oaks, CA.

Reeves, B., & Read, J. L. (2009). Total Engagement: How Games and Virtual Worlds Are Changing the Way People Work and Businesses Compete. Harvard Business Press.

Stanford. (2016). Protégé Ontology Management System, http://protege.stanford.edu/about.php.

Woods, D.D., Cook, R.I., 2002. Nine Steps to Move Forward from Error. Cogn. Technol. Work 4, 137–144. doi:10.1007/s101110200012

Session 6:
Foresight for safety management

Strategy and projects for a predictive safety regulation and safety management – Extended Abstract

Antonio D'Agostino, Marina Aguado

European Union Agency for Railways

120, Rue Marc Lefrancq

59300 Valenciennes, France

Extended Abstract

The European Union Agency for Railways is an Agency of the European Union, which roles and responsibilities have just been modified by the new Regulation (EU) 2016/796.

The Agency is moving from being essentially a technical body supporting the European Commission and, to a certain extent, the railway sector, to being an active player in the railway system dealing with certification and authorisation processes.

The Agency is in fact becoming an authority.

In the past years, the Agency developed several pieces of legislation aiming at harmonizing safety management in Europe and trying to support operators and countries in improving their safety performances. Those regulations were all supporting a proactive and predictive safety management combined with an approach based on learning on experience.

- *A specific regulation on risk evaluation and assessment;*
- *A specific regulation on monitoring safety management systems, requiring also the use of leading indicators;*

Today, carrying the responsibilities of its new tasks the Safety Unit of the Agency has invested human and financial resources in developing projects to push the railway industry towards a more proactive and predictive safety management by:

1. *Better understanding of the operational contributing factors:*
    a. *Deeper analysis of the causes of accidents and incidents, by analysing the work done by the National Investigation Bodies;*
    b. *More data/information sharing:*
        i. *Safety Alert IT tool*

   ii. *Safety Information System*

   iii. *Common Occurrence Reporting – Safety Management Data sharing*

   c. *Identification of performance shaping factors in accidents and incidents.*

2. *Better understanding on the decision making process at national level by monitoring the National Safety Authorities and supporting the peer review of the National Investigation Bodies;*
3. *Improving competence and ability in evaluating and assessing risks arising from organisational, operational and technical systems:*
   a. *Develop expertise in the field or railway risk assessment by starting a collaboration with universities and railway operators;*
   b. *Improving support for assessing and evaluating risks arising from the Transport of Dangerous Goods.*
4. *Creating a specific framework on Safety Culture and Human and Organisational Factors;*
5. *Investigate the use of data and analytics techniques in railways to support better management of the risk of accident (aka big-data study).*

The study mentioned at point 5 is still on-going and it is supposed to finish by the end of April 2018. Currently it is still too early to draw conclusions but, from the first results it is possible to state that a "silo approach" adopted in developing IT systems and platforms in the railway sector is limiting the possibility to combine data and to use it for an extensive automatic accidents modelling. The same issue is undermining a systemic use of data for risk profiling and prediction of accidents. The Agency is considering potential solutions to address the previously identified problems.

It is also possible to report that some big-data projects - promoted under the initiative of single companies- are being stopped/hold due to the insufficient critical data volume to provide reliable results. A possible solution to this issue is to improve data sharing. This approach is in line with what the Agency is trying to do.

For the future, the Agency will definitely try to support data sharing and harmonisation, including all data type which are not traditionally considered as "safety relevant" despite a difficult start we still believe that, with an appropriate support and cultural change, the railway industry can address a "foresight revolution" by "better using better data", all supported by a modern legal framework.

Justifying safety interventions based on uncertain foresight: empirical evidence

Eric Marsden

Foundation for an industrial safety culture (FonCSI)

6 allée Émile Monso, ZAC du Palays, BP 34038

31029 Toulouse Cedex 4 — France

Abstract

Safety interventions suggested as a result of a foresight process are more likely to be related to non-urgent issues, and be affected by a greater level of uncertainty, than interventions suggested by experience feedback or by regulatory changes. By analyzing a number of accident cases where proactive foresight-based suggestions were not implemented before the accident, we assess whether the uncertain and long-term nature of the predictions had a negative effect on the implementation of the interventions suggested.

Keywords: foresight, uncertainty, short-termism, justification, decision-making

1. Introduction

Classically, the prioritization of safety interventions (investment in new technical or organizational barriers, implementation of organizational or cross-organizational changes) is mainly driven by two processes:

- Risk analysis: risks are assessed, fed in part by operational experience feedback, the effectiveness and cost of possible safety barriers is estimated, and budgets are allocated, often with input from expert opinion and decision-support tools such as cost-benefit analysis.
- Updates to industry standards or obligations imposed by the regulator, possibly in reaction to recent accidents.

The implementation of foresight-based methods for safety analysis (which we will define for the purposes of this article as the proactive identification and assessment of medium-term threats, based on the idea of plausibility rather than that of probability) introduces a third source of safety interventions. The threats to safety identified using these methods are likely to be related to longer-term issues and their characterization is affected by a greater level of uncertainty.

Research hypothesis. The hypothesis examined in this paper is that safety interventions suggested via foresight processes will often be ignored, with decision-makers citing lack of evidence, or uncertainty concerning the effects, to justify the associated financial or organizational effort. Indeed, decision-makers are known to prioritize short-term issues over long-term threats, and managers in industry who regularly change job position are unlikely to be immune to this bias. Furthermore, the presence of uncertainty can be used as a justification for prioritizing short-term risks and operational performance over actions to reduce hypothetical medium-term risks.

Method. We analyze findings from past accident investigations to check for the presence of ignored safety foresight. We analyze who produces future-oriented safety concerns and how these concerns have been received in the cases studied.

From a methodological point of view, our case-based approach which focuses on accidents (inevitably introducing hindsight bias (Fischhoff 2003)) does not allow us to obtain a general picture of decision-making with respect to foresight-based interventions. By analyzing different cases where the argument put forward based on foresight analysis seems to have been strikingly strong, we hope to identify some common patterns that may also appear, though less vividly, in other decisions on safety management.

2. Theory

There are a variety of cognitive and motivational barriers to adopting a long-term perspective and to spending now on uncertain threats that may possibly occur many years from today:

- **short-termism**, or placing more weight on certain upfront costs than on uncertain and delayed benefits, even if the potential benefits are large. There is a well-known conflict between short-term and long-term decision-making, which leads decision-makers to sacrifice longer-term objectives through excessive focus on short-term goals. For instance, research shows that decision-makers find it difficult to take decisions with respect to long-term threats such as climate change. Part of the explanation is that decision-makers discount future benefits in a quasi-hyperbolic manner (Laibson 1997), so benefits in 10 years are perceived to have little value compared with benefits next week. A decision-maker who is a manager may also adopt a very limited time horizon, such as the number of years until they expect to change job position, when assessing future benefits, whereas significant organizational or technical safety interventions generally require a much longer time horizon to see a return on investment.
- **loss aversion** (Kahneman and Tversky 1979), the observation that people tend to be more averse to perceived costs (for example of safety investments) than to foregone benefits (such as averted accidents).
- **regret aversion**: decision-makers tend to avoid taking actions due to the fear that it may later turn out to have been the worse option (Bell 1982). This leads to a bias in favour of the status quo.
- **ambiguity-driven indecisiveness**: an individual may be indecisive between some options when she does not know the probability distributions over outcomes.

Recent research in experimental economics (Sautua 2017) suggests that regret aversion and ambiguity-driven indecisiveness are equally important (in a laboratory setting) in generating status quo bias in the presence of uncertainty.

- **dilution of responsibility** in case of major accidents: if a large accident does eventually appear, it is likely (in the generally safe systems we are familiar with today) to have resulted from a combination of unusual factors, so accountability for the accident is likely to be spread across multiple individuals. In contrast, the responsibility for defending an investment in equipment or the organizational effort involved in a change in the organization is focused on the person arguing in favour of the intervention.

We will analyze a number of cases where these characteristics of decision-makers appear to have been combined with multiple and partially inconsistent organizational goals and incomplete or ambiguous information, generating unfortunate outcomes.

3. Case studies

We have selected a number of accident cases which are well documented, and where decision-makers appear, with hindsight, to have been fairly well informed about the risks present in their system, on the basis of proactive foresight-based analyses. These analyses pointed to uncertain, medium-term threats to safety.

3.1 Fire at Grenfell Tower

In June 2017, a fire in the 24-storey Grenfell Tower block of flats killed approximately 80 people. The tower had been renovated in 2016, with the addition of thermal insulation on the outside of the concrete structure covered by aluminium composite cladding. The fire, which started due to a faulty fridge on one of the lower floors, spread very rapidly to the entire building via the external insulation and cladding. The material used for the cladding, which includes a polyethylene core, is very flammable, and is banned for use in high-rise buildings in many parts of the world. There is ongoing debate as to whether the insulation and cladding used on the tower are allowed by UK building regulations, which are somewhat ambiguous on the matter[16]. Fire protection in the building was also lower than in many similar buildings elsewhere in the world due to the lack of sprinkler systems and the single staircase.

A significant number of reports preceding the fire could have generated foresight on the risks posed by the building. After a 1999 fire in Irvine, Scotland, in which fire also spread via external cladding, a committee specialized in fire safety engineering had warned the UK Parliament that building regulations needed updating to deal with new flammable cladding materials. Similar fires in high-rise buildings with exterior

16 The regulations do not specifically ban the use of this material (which is cheaper than the fire-resistant alternative, and led to a 340k€ saving for this building) for high-rise buildings. Building regulations specify three routes to conformity concerning external insulation and cladding, the first being the use only of limited-combustibility materials, the second being a fire test on a mock-up of the proposed design in which the elements are assembled in the same manner as in the planned work, and the third a comparison with previous accepted designs. It appears that the two latter routes were not used for the refurbishment of Grenfell Tower, which was certified as "conforming to the relevant provisions" by the local government authority that owned the building.

cladding occurred in Shanghai in 2010, Melbourne in 2014, in Dubai on New Year's Eve 2015, with many fatalities (White and Delichatsios 2014). A parliamentary group[17] had sent letters to four ministers from the Department for Communities and Local Government recommending change[18] to building regulations. One of the ministers replied stating "*I have neither seen nor heard anything that would suggest that consideration of these specific potential changes is urgent and I am not willing to disrupt the work of this department by asking that these matters are brought forward.*" The parliamentary group responded "*As a consequence the group wishes to point out to you that should a major fire tragedy, with loss of life, occur between now and 2017 in, for example, a residential care facility or a purpose built block of flats, where the matters which had been raised here, were found to be contributory to the outcome, then the group would be bound to bring this to others' attention*".

In this case, the strongly-worded warnings from experts and the numerous accidents elsewhere in the world illustrating the reality of the hazard were not sufficient to push ministers to amend building regulations. They did not help the local government choose the safer, but more expensive, option for refurbishing the building, nor install sprinklers during the work on the building. They did not allow the building inspector to request stronger evidence that the cladding and insulation system was safe for a high-rise building.

3.2 Air France flight 447

Air France flight 447 was a scheduled passenger flight from Rio de Janeiro, Brazil to Paris, France, which crashed in 2009. The Airbus A330 entered an aerodynamic stall from which it did not recover, crashing into the Atlantic Ocean, killing all 228 passengers and crew aboard the aircraft.

The crew flew into a line of thunderstorms in the intertropical convergence zone north of Brazil, making little effort to deviate around it. The aircraft's three pitot tubes iced up in the thunderstorm, causing the loss of accurate airspeed indications. The atmospheric conditions exceeded the pitot tubes' capacity to deal with the obstruction for about 40 seconds. The loss of airspeed indications caused the autopilot, flight director, and autothrust to disconnect, as they require airspeed information to operate. The airplane's handling characteristics also changed, as the airplane's fly-by-wire flight controls degraded from its Normal to Alternate law. This led to the loss of many automatic protection mechanisms built into Normal law, including stall protection. The pilot operating the controls struggled to understand the situation and maintain aircraft control, in the process climbing nearly 3000 feet and losing critical airspeed. The airplane's stall warning (an audio alarm) went off for over 50 seconds, but the pilots were poorly trained on how to handle such an event at high altitude and seem not to have heard or interpreted this alarm correctly. They responded by applying full power, as their low-altitude stall training had taught them, but little additional power was available. The airplane became deeply stalled and descended at high speed into the

17 The All-Party Parliamentary Fire Safety and Rescue Group.

18 The group wrote in 2014 "*Surely however when you already have credible evidence in 2012 to justify updating a small but important part of the guidance in the Approved Document, which will lead to saving of lives, you don't need to wait another three years in addition to the two already spent since the research findings were updated, in order to take action?*".

ocean. The plane was fully functional as it was crashed into the ocean by pilots who did not understand how they had lost control so abruptly.

Significant media attention after the accident was paid to the faulty pitot tubes, whose icing triggered the accident. This issue had in fact been detected on previous flights, and analyzed by the aviation authorities (EASA in Europe), by the aircraft manufacturer and by the operating company. These pitot tubes were progressively being replaced across Air France's A330 fleet by an alternative model, but the change had not yet been made on this aircraft. It had not at the time been made mandatory by EASA (but did become an obligation after the accident). Less media attention has been paid to a more sensitive topic, the general airmanship skills of pilots and their training of pilots on upset recovery, including when the aircraft protection mechanisms are disabled. The pilots on this flight, despite significant number of flight hours on this type of aircraft, did not understand the situation that they encountered, and reacted very poorly to the situation. Whereas in past decades, most pilots had significant manual flying experience either due to their previous military experience or to personal experience flying small planes, newer generations of pilots of passenger jets tend to have little experience in manual flying. Increasingly sophisticated automation on modern aircraft have changed the nature of pilots' work, with many flight phases undertaken on autopilot. The automatic protection systems in Airbus aircraft prevent many pilot actions that could lead to loss of control, and pilot training includes little exposure to loss-of-control situations[19] (indeed, the reduced training costs for pilots due to the automation is a commercial argument for Airbus). Sessions on a simulator are fairly predictable for pilots, who are familiar with the list of events that may arise in training. Simulator training does not help prepare them for the "startle effect" triggered by a new and unusual situation for which they have not been previously trained[20].

The BEA report into the AF447 accident states "*The training regime for pilots is not designed to compensate for a lack of manual high-altitude flying skills, or for a lack of experience on conventional aircraft. It also limits the ability of pilots to acquire or maintain basic airmanship skills.*" (BEA 2012). The report includes a recommendation to increase the amount of manual flying in pilot training, to improve training on basic airmanship skills, to add simulator training on abnormal flight modes, and to develop training scenarios that expose pilots to the "startle effect" and to situations with a high emotional load[21].

Air France had identified in an internal report that the airmanship skills of some of its long-courier pilots were weak, and that there was a generalized loss of common sense and general flying knowledge among its pilots, and that pilots often had trouble in

19 In particular, the Airbus flight crew training manual indicates that it is not necessary to train pilots on recovery from stall at unusual attitudes, the hypothesis being that the aircraft protection mechanisms will prevent the entry of such states.

20 For instance, it seems that the pilots were not familiar with the aural stall warning alarm, which sounded more than 70 times in the minutes before the crash.

21 Recommendations numbered FRAN-2012-041, FRAN-2012-045 and FRAN-2012-046 in the BEA investigation report.

sensemaking after an equipment failure (identifying the fault, assessing its level of severity and possible consequences) (BEA 2012, p. 199).

The industry has made some limited changes to the training regime for pilots to increase their ability to respond appropriately in unusual situations. For instance, Air France has added specific training on stalls and upset recovery. EASA launched rulemaking tasks concerning pilot's theoretical airmanship skills[22] and the fidelity of aircraft simulators in non-nominal situations. The FAA has issued an advisory circular pointing out good practice on stall training[23], with some related improvements concerning the prevention, recognition and recovery from stalls. However, it is not evident that the associated actions are sufficiently far-reaching to make significant changes to a fairly deep-seated situation of poor basic airmanship skills, deskilling due to the increasing role of automation on the flight deck, and limited ability to recover from a loss of control.

This case illustrates both a classical risk analysis process which led to a good decision (experience feedback leading to the decision to change the pitot tubes, even if this change was not rolled out sufficiently quickly to prevent the accident) and apparent lack of foresight concerning the impact of automation on pilot skills.

3.3 Xynthia windstorm

In February 2010, a large windstorm named Xynthia struck the west coast of France during a high-tide period, killing 59 people and causing more than 2M€ in damage. The mayor of La Faute-sur-Mer, a small coastal town that saw the largest number of victims from the storm after a protective dike failed, was found guilty on appeal in 2016 of involuntary homicide and condemned to a suspended sentence of two years imprisonment[24].

Under French law, the mayor is responsible for informing the local population of flood risks, for preparing a local emergency plan, and for approving building permits which did not include obligatory protective measures for flood zones. The mayor of this locality was found guilty of approving numerous building permits in a flood zone and not establishing an emergency plan. Over a 12-year period, the mayor had received more than 40 different documents describing the flood risk and explaining the consequences in terms of urban development (Cour des comptes 2012). Some of these letters described precisely the scenario that played out during the storm, with high sea levels caused by low atmospheric pressure and wind leading to dike failure[25] and the flooding of areas behind the dike that lie below the sea level. Over the past 100 years,

22 EASA rulemaking tasks RMT.0581 & RMT.0582.

23 FAA Advisory Circular AC120-STALL. Advisory circulars are not binding regulatory texts.

24 The first trial in 2014 found him guilty of involuntary homicide and endangerment, with a sentence of 4 years' jail. The findings of the first trial were very severe, stating [author's translation] "*The tragic consequences of Xynthia are not the result of bad luck. [The accused] have intentionally concealed the risk in order to preserve the benefits of this small piece of heaven which provided them with power and money. They have lied to their constituents, have put their lives in danger, have considered them as negligible objects, stewing in their obsolete certainties. They have gambled that the known risk would not be realized, but the seed money for their gamble was the physical integrity of the inhabitants of La Faute-sur-Mer.*"

25 The dike that protected a part of the village was known to be weak, and several official reports since 2001 had warned of risks of submersion, internal and external erosion, and general instability.

5 storms had led to flooding in the area. The mayor had ignored several orders from the Préfet (a regional representative of the national government) to inform inhabitants of the risks they were exposed to. He did not distribute to inhabitants an information leaflet produced by the regional government describing the flooding risk. He also ignored alerts sent by the Préfet to his mobile phone and email in the hours before the storm, warning of severe flood risk.

A regional government official testified during the trial that in a meeting with the mayor concerning the establishment of a flood-prevention plan, he had explained the flooding risks again and stated, speaking as a former judge, that he hoped there was no major flooding in the future, as otherwise they would be called assassins.

The mayor's legal defense invoked the notion of *force majeure* related to the unpredictable nature of such a severe hazardous event. The judges stated that "*the exceptional intensity of Xynthia [...] does not change the predictability of a major accident hazard, whose potential contours were perfectly identified. The statistically low frequency of an extreme natural phenomenon does not imply that such an event will never occur.*"

It seems clear that the uncertainty concerning the likelihood of such an extreme flooding event occurring during his mandate played a significant role in the mayor's apparent decision to ignore this risk.

3.4 BP Texas City refinery explosion

In 2005, an explosion on the Texas City refinery in Texas killed 15 workers and injured more than 170 others. The explosion occurred when a hydrocarbon vapour cloud was released during startup the isomeration process unit. The level of liquid inside a splitter tower overflowed, due to an erroneous level transmitter, a defective high-level alarm in the tower and a faulty relief valve. BP had acquired the Texas City refinery, the third-largest in the USA, as part of its merger with Amoco in 1999.

The US CSB investigation into the accident identified a large number of safety management failings on the refinery. Process equipment was not compatible with current state of practice, due to long-term underinvestment (in particular, the use of blowdown drums for emergency discharges that vent directly to the atmosphere has long been replaced by discharge to a flare system). Several safety-critical instrumentation and control elements on the tower were faulty. Operators did not follow the official startup procedure for the unit, because they were under pressure to start the unit quickly to avoid production problems. A supervisor was not present during the startup operations, and during the preceding shift transfer communication between the two teams was poor. Finally, numerous portable sheds were in use by workers (many of whom were killed by the explosion) close to the process hazard, contrary to industry guidelines and to BP's own regulations[26].

26 To illustrate the level of non-conformity of the site, after the accident BP paid a fine of 21.3M USD to resolve more than 300 separate alleged violations of OSHA regulations and allocated 1 billion USD to upgrade the site equipment over 5 years.

A 2001 presentation titled "Texas City Refinery Safety Challenge" written by refinery managers stated that without a significant improvement in performance, a worker would be killed in the next three to four years (USCSB 2007, 154). A 2002 report requested by the regional BP manager stated that the Texas City refinery process units and infrastructure were vulnerable, with findings that were "*urgent and far-reaching with important implications for the site, including the integrity of on-going site operations*". It also stated that there were "*serious concerns about the potential for a major site incident due to the large number of hydrocarbon releases*" (USCSB 2007, 156). The leadership culture at the refinery was described as "*can't finish*" as regards the implementation of necessary changes, and the report recommended a "*major overhaul of the basics*" and increases in maintenance spending of 235M USD. A followup report later in the same year stated that "*the current integrity and reliability issues at [the refinery] are clearly linked to the reduction in maintenance spending over the last decade*" and noted that "*The prevailing culture at the Texas City refinery was to accept cost reductions without challenge and to raise concerns when operational integrity was compromised.*"

A BP group-level strategy document[27] explicitly aimed to "*limit the amount of capital allocated in the Refining SPU due to its volatility*". This budget restriction made it difficult for the Texas City refinery to obtain the investments necessary to upgrade its aging infrastructure. When considering the possibility of connecting the isomeration unit to the flare system of a newly built unit in 2002, the manager of the refinery chose to avoid the cost of connection, and "*bank the savings in 99.999 percent of the cases*" (USCSB 2007, 115). A 2003 BP report found that "*most action items were not implemented because of budget constraints*." (USCSB 2007, 160). A 2004 safety culture report made by external consultants found that "*The pressure for production, time pressure, and understaffing are the major causes of accidents at Texas City*" and "*There is an exceptional degree of fear of catastrophic incidents at Texas City*". The 2005 health and safety plan for the site warned that the refinery would "*kill someone in the next 12-18 months*".

All these observations, with many more reported in the CSB report into the accident, paint a picture of site-level and regional managers who were well aware of serious process safety deficiencies on the refinery, and of the detrimental impact of budget cuts on the mechanical integrity of their process equipment, who had action plans available for improving the situation, but who did not push back at the corporate cost-reduction targets that prevented them from implementing the plans. Corporate (board-level) directors had a "short-term focus"[28], lacked safety expertise, were poorly informed of the safety situation at Texas City[29] and did not appreciate the impact of their cost-cutting measures on safety.

27 The BP "Management Framework" describing the company's corporate governance system, dated 2003.

28 BP Baker Panel report, page xii.

29 Safety was monitored at the board level using the recordable injury rate, a metric which concerns (mostly low-severity) occupational accidents and which is notorious for not providing information on process safety. Furthermore, internal reports on risk at the refinery sent to the CEO did not mention accidents and fatalities that occurred on the site.

3.5 Ladbroke Grove train collision

A head-on collision between two passenger trains at Ladbroke Grove in London in 1999 killed 31 people and injured more than 400. One of the trains passed through a red "stop" signal, which was preceded by a yellow "prepare for red" signal. The red signal that was not respected by one of the trains was known to be dangerous due to its poor visibility, having been passed eight times in the previous six years; the inquiry into the accident found that the train driver, who was inexperienced, most likely had not seen or had misinterpreted the signal[30]. Factors that contributed to the accident include inadequate training for one of the train drivers, poor visibility of the signal compounded by blinding light from the sun at the time of the accident, and inadequate response from the railway control center. The accident could also have been prevented by the system-wide installation of an automatic train protection system. A cost-benefit analysis had concluded that the safety benefits of such a system did not justify its high cost (the cost per statistical life saved was estimated at 4M€, compared with the 1.4M€ threshold used at the time). A post-accident analysis confirmed the numbers used in the study[31].

The signal passed in the accident was known to be dangerous, and the rate of signals passed at danger in the area was known to be "*exceptionally high*"[32], but no work had been planned by the railway infrastructure company to improve its visibility. A report indicated that the signal was located in a curve, was partially obscured and intermittently visible to a driver. An HSE[33] report indicated that the signal was partially obscured by overhead power lines, that a nearby bridge could produce dazzle, and that the signal was *"susceptible to swamping from bright sunlight"*. An expert review of the visibility of signals had not been undertaken by the infrastructure company for several years in the area, despite several requests for such a risk assessment. The operations and safety director of one railway operating company, Ms Foster, wrote several letters to the railway infrastructure company concerning signaling in the Paddington area and the specific signal involved in the collision. One letter in 1998 stated "*I should be grateful if you would advise me, as a matter of urgency, what action you intend to take to mitigate against this high risk signal*". A subsequent letter in 1999 (which received no reply) stated "*This is clearly not the manner in which to manage risk and an approach to which I am strongly opposed. Therefore, I suggest that an holistic approach is taken to SPAD management in the Paddington area and all changes to infrastructure or methods of working are properly risk assessed.*" The inquiry into the accident found that the Paddington area was characterized by an "*endemic culture of complacency and inaction*" (Cullen 2001, 137).

The British railway system had seen large organizational changes in the past few years, following the privatization of British Rail and its separation into more than 100 separate

30 The area around Paddington where the collision occurred sees significant amounts of high speed and bidirectional rail traffic, and the signals are some of the most complicated in the UK. The signals were further obscured by a bridge and by recently installed overhead electrical systems (Cullen 2001). During the Cullen inquiry, a former operations manager with British Rail stated that *"In over 45 years in the industry, I have never seen such a confusing set of options to a driver"*.

31 However, a less expensive system called Train Protection & Warning System was implemented in the UK from 2000 onwards.

32 Report by the railway infrastructure company in 1993.

33 The UK Health and Safety Executive was at the time the safety authority for railways.

companies. The resulting inter-organizational complexity seems to have contributed to the accident. The infrastructure company, responsible for the design and visibility of signals, has an incentive to consider signals passed at danger as a driver error issue, rather than digging into contributing factors such as signal design. During the inquiry, the infrastructure company defended the design of the signal, indicating that though the approach was complex, its location should be known to all train drivers. The railway infrastructure company did not respond to urgent and repeated requests from a highly-ranked representative of an operating company to improve the safety of a dangerous signal. The accident, which occurred in close succession with two other railway accidents, led to major changes in the formal responsibilities for management and regulation of safety of UK rail transport.

4. Discussion

Going over the different cases described, we can identify a certain number of common features that seem to[34] have led to safety foresight being ignored:

- **Competing priorities**, such as production pressure and profit: organizations pursue multiple goals, and safety is never the primary reason for existence of industrial activity. The impact of goal conflicts is seen in the decision to use lower-cost cladding at Grenfell Tower, to allow building permits without flood mitigation measures at La Faute-sur-Mer, to fly through the thunderstorms on the Rio-Paris flight instead of avoiding them as most other flights did, and in BP's decision to cut maintenance spending without assessing the impact on safety. Rasmussen's migration model (Rasmussen 1997) provides some context for the effect of production pressure and cost-cutting on safety margins.
- **Lack of explicit decision-making** on the safety issue or proposed intervention. In some of the cases studied, a formal decision was made not to implement a proposed safety intervention: a formal decision was made not to install automatic train protection systems that would have prevented (at a high financial cost) the Ladbroke Grove accident, and a minister in the Grenfell Tower case explicitly decided not to request a reassessment of building regulations. Other cases in the safety literature of explicit decisions not to implement a safety mechanism (later highlighted by accidents) include the decision not to redesign the Ford Pinto gasoline reservoir (Birsch and Fielder 1994) and Boeing's decision not to redesign the central fuel tanks of the 747 prior to the crash of flight TWA 800 in 1996 (Negroni 2000). In the AF447 case, an explicit decision was made by Air France to progressively change the pitot tubes on their A330 aircraft, as parts became available, and EASA made an explicit decision not to make the change mandatory for airlines. In most of the cases we have described, however, no formal decision-making process is recorded as having taken place, with instead letters of concern not receiving any answer (Ladbroke Grove), or acceptance that no budget was available to address severely degraded equipment (Texas City), or repeated brushing away of concerns raised (La Faute-sur-Mer).

34 Our analysis is based only on the analysis of secondary sources, with no direct interviews of the people involved in the decisions, making it impossible to assert precisely which factors were most influential in the decisions or indecisions.

- **Status quo bias**, or inertia in individual decision-making, is a well documented phenomenon in experimental economics[35]. It seems to have contributed to the resistance to change and the lack of a sense of urgency seen in the Grenfell Tower case and Ladbroke Grove.
- Difficulty for decision-makers to understand the safety implications of their decisions, due to lack of knowledge or lack of information: this weakness was present at BP (board-level decision to reduce maintenance, misunderstanding of the relevance of occupational safety metrics).
- The effect of the **complexity of bureaucratic organisations** on safety management and decision-making (Vaughan 1999) seems to have played a role in the Ladbroke Grove accident, where recent privatization of the railway sector and separation of a previously integrated entity into multiple operating companies and an infrastructure operator had introduced numerous changes to the organization.

A number of factors frequently identified in the safety literature as contributing to poor decision-making do not appear to have played a role in the cases studied:

- Difficulty for safety professionals to communicate risk to decision-makers: the cases studied are perhaps most striking for the great clarity of the messages delivered to decision-makers on the importance of changing the status quo.
- The suppression of minority viewpoints, or lack of psychological safety.
- Group-think, in which a group of people arrives at a decision that would not have been reached by any member acting individually.

Our analysis of medium-term decisions focuses our attention on "blunt-end" decision-making (removed from the hazard source), rather than on sharp-end activity. A range of levels of authority of the decision-making actors can be observed, with regional-area managers (Ladbroke Grove), site-level and corporate-level managers (BP Texas City), local government officials (La Faute-sur-Mer), regulators and safety authorities (Grenfell Tower, EASA) and legislators (Grenfell Tower). Adopting a categorization suggested by (Rosness et al. 2010), the (in)decisions analyzed are political, managerial and analytical.

35 For example, the legal default in organ donation has a strong effect on people's decision (Johnson and Goldstein 2003), and the default level of savings proposed in retirement investment forms has a significant impact on their level of saving (Cronqvist and Thaler 2004).

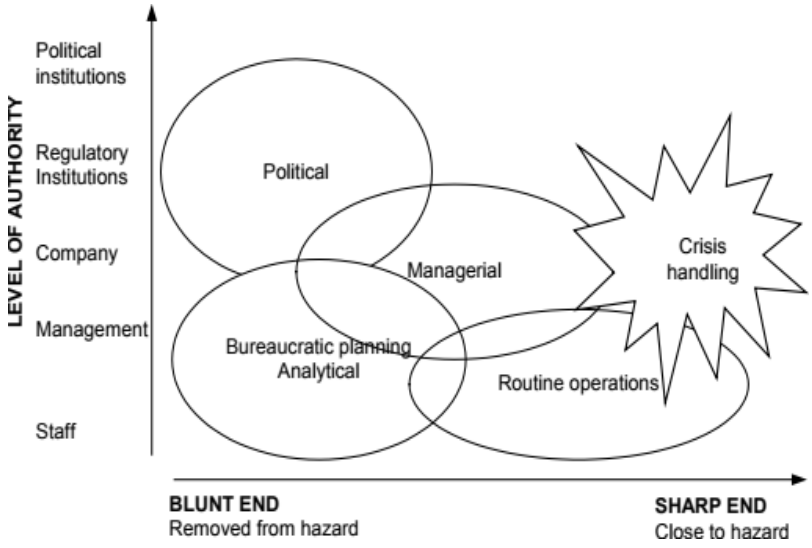


Figure 1. Classes of decision-processes, from (Rosness et al. 2010)

Our research hypothesis was that safety interventions suggested via foresight processes are often ignored, with decision-makers citing lack of evidence to justify the associated financial or organizational effort. Our first observation is that in many of the cases, we cannot identify a formal "decision" made not to adopt a specific safety intervention. Indeed, in most of the cases no safety intervention was developed because the risk was not taken on board, or put on the agenda, before this stage. In the cases where formal decisions were made, it does seem that lack of evidence of the immediate or certain nature of the hazard played a role in allowing the decision-makers not to implement risk treatment measures.

5. Conclusion

In the area of financial decision-making, researchers have suggested (Kunreuther and Weber 2014) the implementation of mechanisms that create short-term incentives for long-term thinking. For example, home-owners in flood-exposed areas could be provided with loans to help them implement flood-proofing measures, with the cost of the loan offset by reduced insurance premiums. The literature on the role of whistleblowers in raising safety concerns is also very relevant to situations where decision-makers refuse to put risks on the agenda or to allocate the monetary or organizational resources necessary for risk treatment.

References

BEA. 2012. "Rapport Final. Accident survenu le 1er Juin 2009 à l'Airbus A330-203 immatriculé F-GZCP exploité par Air France. Vol AF 447 Rio de Janeiro - Paris." https://www.bea.aero/docspa/2009/f-cp090601/pdf/f-cp090601.pdf.

Bell, David E. 1982. "Regret in Decision Making Under Uncertainty." Operations Research 30 (5): 961–81. doi: 10.1287/opre.30.5.961.

Birsch, Douglas, and John H. Fielder. 1994. The Ford Pinto Case: A Study in Applied Ethics, Business, and Technology. State University of New York Press.

Cour des comptes. 2012. "Les enseignements des inondations de 2010 sur le littoral Atlantique (Xynthia) et dans le Var." Cour des comptes, France. https://www.ccomptes.fr/sites/default/files/EzPublish/rapport_public_thematique_inondations_var_2010_xynthia%20_072012.pdf.

Cronqvist, Henrik, and Richard H. Thaler. 2004. "Design Choices in Privatized Social-Security Systems: Learning from the Swedish Experience." American Economic Review 94 (2): 424–28. doi: 10.1257/0002828041301632.

Cullen, Lord. 2001. The Ladbroke Grove Rail Inquiry: Part 1 Report. HSE Books. http://www.railwaysarchive.co.uk/documents/HSE_Lad_Cullen001.pdf.

Fischhoff, Baruch. 2003. "Hindsight ≠ Foresight: The Effect of Outcome Knowledge on Judgment Under Uncertainty." BMJ Quality & Safety 12 (4). doi: 10.1136/qhc.12.4.304.

Johnson, Eric J., and Daniel Goldstein. 2003. "Do Defaults Save Lives?" Science 302 (5649). American Association for the Advancement of Science: 1338–9. doi: 10.1126/science.1091721.

Kahneman, Daniel, and Amos Tversky. 1979. "Prospect Theory: An Analysis of Decision Under Risk." Econometrica 47 (2): 263–91. doi: 10.2307/1914185.

Kunreuther, Howard, and Elke U. Weber. 2014. "Aiding Decision Making to Reduce the Impacts of Climate Change." Journal of Consumer Policy 37 (3): 397–411. doi: 10.1007/s10603-013-9251-z.

Laibson, David. 1997. "Golden Eggs and Hyperbolic Discounting." Quarterly Journal of Economics 112 (2): 443–77. doi: 10.1162/003355397555253.

Negroni, Christine. 2000. Deadly Departure. Cliff Street Books.

Rasmussen, Jens. 1997. "Risk Management in a Dynamic Society: A Modelling Problem." Safety Science 27 (2): 183–213. doi: 10.1016/S0925-7535(97)00052-0.

Rosness, Ragnar, Tor Olav Grøtan, Geir Guttormsen, Ivonne Herrera, Trygve Steiro, Fred Størseth, Ranveig Kviseth Tinmannsvik, and Irene Wærø. 2010. "Organisational Accidents and Resilient Organisations: Six Perspectives."

Sautua, Santiago I. 2017. "Does Uncertainty Cause Inertia in Decision Making? An Experimental Study of the Role of Regret Aversion and Indecisiveness." Journal of Economic Behavior & Organization 136: 1–14. doi: 10.1016/j.jebo.2017.02.003.

USCSB. 2007. "Investigation into the Refinery Explosion and Fire at BP Texas City, March 2005." U.S. Chemical Safety; Hazard Investigation Board (CSB). http://www.csb.gov/assets/1/19/CSBFinalReportBP.pdf.

Vaughan, Diane. 1999. "The Dark Side of Organizations: Mistake, Misconduct and Disaster." Annual Review of Sociology 25: 271–305. doi: 10.1146/annurev.soc.25.1.271.

White, Nathan, and Michael Delichatsios. 2014. "Fire Hazards of Exterior Wall Assemblies Containing Combustible Components." Fire Protection Research Foundation. http://www.nfpa.org/~/media/files/news-and-research/resources/research-foundation/research-foundation-reports/building-and-life-safety/rffirehazardsofexteriorwallassembliescontainingcombustiblecomponents.pdf

Is whistleblowing a promising "tool" for event occurrence prevention?

Yves Dien

CHAOS,

6, rue Lucien Feuchot

92190 Meudon, France

Abstract

Some industrial accidents show that before their occurrence some persons, called whistle-blowers, raised concerns about the level of safety. Unfortunately they were not listened and even sometimes isolated or bullied. From analysis of cases of whistleblowing, we will figure out features of alerts and whistle-bowers and how to take them into account in safety prevention process.

Keywords: whistleblowing, Whistle-blowers, Process Safety Alerts, Warnings.

> "*O monstrous world! Take note, take note, o world*
> *to be direct and honest is not safe!"*
> Shakespeare, Othello, III, iii

1 Introduction

Current, relevant and interesting debates about (industrial) safety call into question the relevance of some concepts whose definitions and approaches have seemed, so far, to be widely shared. One such concept is that of safety. Does safety mean avoiding things that could go wrong or ensuring that things go right? Are causes of events to be found in failures, errors and malfunctions – the operational dark side – or should we consider that both expected and unwanted outcomes occur in the same way (Hollnagel, undated; Hollnagel, 2014)?

In many of these discussions, the focus of safety approaches is still mainly on the avoidance of adverse events. In spite of undeniable progress in recent decades, many experts share the view that safety has reached an asymptote (Frantzen, 2004). Facing this problem, practitioners are trying to find new ways in order to improve safety management.

In this article, we will analyse if taking account of whistleblowing could be one path for improvement. First, we will raise the issue and give a first definition of whistle blowers. Then, we will give a few examples of "whistle blowers". From the examples, we will draw up features of whistle blowers and see what is the attitude of their

organisations (companies) towards them. For concluding, we will see what is the added value of whistleblowing in terms of safety.

Because this article aims at the industrial sector, it will not address the societal domain which could have been exemplified whistleblowing cases such as the following:

- Edward Snowden, an American computer scientist who worked at the National Security Agency (NSA) and who disclosed in 2013 numerous classified documents which proved existence of programs for global (illegal) surveillance of people;
- Dr Irène Frachon, a French pulmonologist who warned in 2007 against a widely prescribed medicinal product which had side effects on cardiac valves. Thanks to her tough "struggle", especially with pharmaceutical company producing it, drug was withdrawn in France in November 2009[36].
- In April 2016, someone leaked the so-called Panama Papers, 11 million documents leaked from one law firm, Mossack Fonseca, which showed how some of the world's wealthiest individuals and businesses had been able to shelter their money away from the tax man.
- More recently, another whistle-blower, from Appleby, an offshore law firm based in Bermuda company, has leaked 13.4 million documents, the so-called Paradise Papers, to the German newspaper, Süddeutsche Zeitung, which, with the International Consortium of Investigative Journalists, is leading 95 newspapers in exposing how the rich have been hiding their money, with the consequence that tax burden falls on the rest of us.

Furthermore, the article will **not** tackle subject of whistle-blowers' legal and judicial protection.

2 The Issue

Current industrial safety approaches and practices mainly rely on two pillars: risk analysis and learning from experience.
Risk analysis can be broadly described as the process of risk identification and measurement. In that case, risk mitigation is a means to avoid unwanted events or to minimize the impacts of their occurrence. Quantitative risk analysis seeks answers to questions such as the following:

- What are the events, with negative safety impacts, that could occur?
- What are their likelihood?
- What would be consequences of their occurrence? [37]

Risk analysis allows us to define the "***notionally** normal starting points*" of the industrial process, meaning (i) "*initial culturally accepted **beliefs** about the world and its hazards*" and (ii) "*associated precautionary norms set out in laws, codes of practice,*

[36] In 2011, Irène Frachon received a "Citizens Whistle-Blower" award.

[37] Qualitative risk analysis uses words or colours to identify and evaluate risks or presents a written description of the risk.

mores and folkways"[38] (Turner and Pidgeon, 1997, p. 72). Because theoretical knowledge evolves with time, analysing risks is a continuous process.

In spite of substantial efforts in terms of methodology and successes in terms of results due to risk analysis, some events happen during production. These events are analysed in order to figure out causes of their occurrence and to determine and implement improvement(s). Industries, especially high-risk industries, have set up operating feedback systems for learning from experience. It is the second pillar of industrial safety approaches. Unfortunately, it seems that industries have reached a limit in terms of results. They hardly progress, they are ''*dancing a tango on asymptote*'' (Frantzen, 2004), meaning that, from year to year, numbers of safety records are more or less the same (either slightly higher or slightly lower). Does it mean that "learning from experience" is in a state of persistent deadlock?

Occurrence of an event can be described from two different points of view. On the one hand, the operating feedback system is **responsive** (the conventional approach):, that is, an event is seen as a surprise, as an "exceptional set of unfortunate circumstances" (Finn, 2002). Nowadays, safety is more foresight-oriented, considering a situation as "an accident waiting to happen", i.e., when we are living during the "incubation period"[39] of an event. Indeed, "[a]ny event is generated by direct or immediate causes (such as a technical failure or "human error"*). Nevertheless, its occurrence and/or its development is considered to be induced, facilitated or accelerated by underlying organizational conditions (complex factors) and some warning signals exist prior to the event*" (Dien, 2006, p. 148). So, goal becomes to assess degradation of the safety level in detecting the warning signals, near-misses, and **weak signals**… In that sense, our operating feedback systems need to become **proactive**.

The concept of weak signals exists in several areas such as history, geology, medicine, acoustics… It was more recently coined by Vaughan (1996) in the domain of industrial safety after the space shuttle *Challenger* disaster: *"A weak signal is one conveyed by information that is informal and/or ambiguous, so that its significance* […] *is not clear"* (Vaughan, 1996, p. 355). Essentially, a weak signal is a symptom of degradation of the production system.

Turner and Pidgeon (1997) describe these kinds of signals, "visible" during the incubation period, as a "set of events". They observed that these events go unnoticed. Indeed, unfortunately, even if detection and treatment of weak signals seems a promising way to go, it appears quite difficult to precisely define what a weak signal is. Its features are (Vaughan 1996):

- Qualitative (in contrast with quantitative);
- Subjective;
- Inconclusive;
- Giving partial information;

[38] Emphasis added.

[39] "Accumulation of an unnoticed set of events which are at odds with the accepted beliefs about hazards and the norms for their avoidance" (Turner and Pidgeon, 1997, p. 72).

- Ambiguous, meaning several interpretations are potentially possible.

Furthermore, weak signals could be repetitive. In that case, repeatability itself is the criterion for identification.

Detection of a weak signal relies on an engineer's feelings, intuition, perceptions rather than rational and scientific demonstration. In that sense, a weak signal is not in line with, *"the norms of quantitative, scientific positivism"*[40] (Vaughan, 1996, p. 355). Indeed, it may even be in conflict with such norms.

Furthermore, often, in terms of safety, a signal makes sense only after an event has occurred. In other words, the meaning of signs related to safety is not obvious, and organisations put in place systems for collecting and gathering signs that they do not really know what to do with except compiling statistics on accumulated data. Furthermore, companies have to cope with two concerns:

- Taking into account and treating a "wrong" signal (i.e., a signal that did not impact safety), which would lead to waste resources and time;
- Not detecting a relevant signal, which would be symptomatic of poor safety management and could lead to a major event.

So: here is a key question: Is it worth investing in the collection and treatment of weak signals, especially if we do not even recognise the weak signal? And here is another question: How should we define the relevant and accurate features of a weak signal? The analysis of major events often shows that, in many cases, they were preceded by alerts, warnings launched by persons close to (or knowing) how a system functions technically.

Organisations are generally not a monolithic whole, a homogenous entity. Sometimes, within the midst of the organisation, some dissident voices alert the powers about potential safety problems. Could these persons, whom we call "whistle-blowers", help to improve levels of safety? Could they help to meet the challenge of foresight for safety?

3 Definition of "Whistle-Blowers"

Before proceeding further, let's define the term "whistle-blower" (or whistleblowing). The implied definition mainly refers to the societal domain.

For Wikipedia, a "*whistle-blower (also written as whistle-blower or whistle blower) is a person who exposes any kind of information or activity that is deemed illegal, unethical, or not correct within an organization that is either private or public*".[41]

[40] Let's remember that when engineers of the space shuttle O ring manufacturer raised an alert concerning the performance of seals in cold temperatures, the NASA decision-makers challenged them to prove it by *quantifying their concerns*!! (Vaughan, 1996).

[41] https://en.wikipedia.org/wiki/Whistleblower.

The Council of Europe (2014) considers that a *whistle-blower* is "*any person who reports or discloses information on a threat or harm to the public interest in the context of their work-based relationship, whether it be in the public or private sector*".
ADIE (2008) added a notion explaining that a "whistle-blower is anyone who discloses or helps to disclose fraud, irregularities and similar problems". So a whistle-blower is not only the one who acts, but also the one who supports.
Chateauraynaud and Torny[42] (1999) make a distinction between "*prophets*" whose message is future dedicated and "*whistle-blowers"* (denouncers) who condemn past and ongoing events. Nevertheless, in both cases, the aim is to avoid occurrence of unwanted events and/or negative outcomes.

4 Some Whistle-Blowers

Whistleblowing is a quite recent concept. Nevertheless, if we immerse ourselves in mythology, we already may find, in tales of ancient Greece, persons who warned their compatriots. Perhaps the most famous was Cassandra, Princess of Troy, daughter of King Priam and Queen Hecuba, who spoke true prophecies. Unfortunately, a curse struck by Apollo had the consequence that her true prophetic statements would never be believed.

But she was not alone. Laocoön, a Trojan priest, was not convinced by the story told by Sinon, an undercover Achaean Greek soldier, about the great wooden horse left by the Achaean Greek soldiers after they lifted the siege. It was supposed to be an offering to Poseidon for safe sailing back home. Laocoön thought the horse was full of soldiers and cautioned against moving the horse into the city of Troy. He recommended burning the horse. Alas, no one followed his advice.

4.1 A Committed Nuclear Engineer

Let's return to our times, where I wish to draw your attention to a decision made in January 1996 by the US Nuclear Regulatory Commission (NRC)[43], to put the three units at the Millstone nuclear power plant (NPP) in Connecticut on the Watch List. This action allows the NRC to order the shutdown of a unit and to authorize its restart only under certain conditions.

This decision was motivated by serious unsafe practices in the operation of the plant (during the refuelling process). It was not the consequence of an incident nor did it result from an investigation or an audit carried out by the Safety Authority. It was the result of determined, voluntary and pugnacious action by a NPP senior engineer, named George Galatis. As early as 1992, he became concerned about the management of spent fuel that did not comply with regulatory safety requirements. He warned his hierarchy but they did not take his alert into account. In the next two years, nothing changed, except that Galatis was isolated and bullied within the plant. In 1994, he took the initiative to directly alert the NRC, knowing that the NRC had been aware of the plant practices for the previous 10 years and had not taken any corrective action. Faced with

[42] They were the first French scholars who tackled this issue. The French concept is "lanceur d'alerte" which means in a word-for-word translation "alert launcher"1

[43] American Nuclear Safety Authority.

the persistent apathy of the NRC, Galatis decided, in August 1995, and in connection with a NGO, to petition the NRC to suspend the Millstone I licence for 60 days and deny the company's request for an amendment of the regulatory requirements concerning fuel unloading. (Miller, 1995; Pooley, 1996). The pressure on Galatis redoubled, but the case became public, and the NRC was forced to react.

The "stubborn crusade" of this engineer earned him a long article and the cover of the American magazine TIME.

4.2 A Product Engineer Involved in Safety

On 3 March 1974, the Turkish Airlines Flight 981 crashed over the Ermenonville Forest, north of Paris, few minutes after its taking off from Orly airport. The 346 people on board of the DC-10 airplane died.

The direct cause of the accident an explosive decompression, due to a broken cargo door at the rear of the plane. It led to a collapse of the passenger compartment floor that cut all wires necessary to control the aircraft. The plane became uncontrollable and crashed to the ground.

A similar event had happened two years before. On 12 June 1972, the rear cargo door of American Airlines Flight 96 DC-10 blew off while flying over Windsor, Canada. Because they were fewer passengers (67 persons), decompression led to (only!) a partial collapse of the compartment floor with (only!) a partial restriction of the controls. In spite of the situation, the pilot was able to land safely.

Fifteen days after this event, Dan Applegate, Director of product engineering for Convair, a McDonnell Douglas subcontractor involved in the DC-10 design, wrote a document known as the "*Applegate Memorandum*". Applegate gave it to his immediate supervisor. In the memo, he mentioned some concerns. The long memo stated (among other things:

"*The potential for long term Convair liability has been causing me increasing concern for several reasons:*

1 The fundamental safety of the cargo door latching system has been progressively degraded since the program began in 1968.
2 The airplane demonstrated an inherent susceptibility to catastrophic failure when exposed to explosive decompression of the cargo compartment in 1970 ground tests.

[…]

"*Since Murphy's Law being what it is, cargo doors will come open sometime during the twenty-plus years of use ahead for the DC-10"*

[…]

I would expect this to usually result in the loss of the aircraft"

[…]

"***it seems to me inevitable that, in the twenty years ahead of us, DC-10 cargo doors will come open and I would expect this to usually result in the loss of the airplane***"[44] (Eddy et al., 1976, pp. 183-185)

Applegate's supervisor considered that it was needed to "*look the "other of the coin"*" (Eddy et al., 1976, p. 186).

Convair vice-president in charge of the DC-10 project convened a meeting to decide the company's policy regarding this issue. Convair management thought that changes requested from the memo would be costly and it was not sure which company would pay the bill (Convair or McDonnell Douglas). During this meeting, it was acknowledged that Applegate was closer than his supervisor to the engineering of the DC-10. Nevertheless, the reasoning of the supervisor was preferred and the "*"interesting legal and moral problem"*" was resolved "*by deciding that Convair must not risk an approach to Douglas*". […] *most of the statements made by Applegate were considered to be well-known to Douglas and there were nothing new that was not known to Douglas* (Eddy et al., 1976, p. 187). So Douglas was never officially informed about Applegate's concerns.

4.3 A Field Journalist

On the night of 2 - 3 December 1984, a toxic cloud of methyl isocyanate (MIC) spread over the city of Bhopal, Madhya Pradesh, 600 kilometres south of Delhi. The cloud made its way especially into and around the shanty towns located near the Union Carbide India Limited (UCIL) pesticide plant. The disaster eventually created about 600,000 victims, including more than 12,000 deaths.

The cause of the disaster is still under debate. Nevertheless, we could assume that slack management leading, among other things, to deferred maintenance created a situation where routine pipe maintenance caused a backflow of water into a MIC tank, triggering the accident[45]. Before the accident, the plant was idling with reduced staff (Shrivastava, 1992; Lapierre & Moro, 2001).

Several serious events preceded the catastrophe. On 23 December 1981, a phosgene (toxic gas) leak occurred during a maintenance shutdown and caused the death of Mohammed Ashraf, foreman of the plant. Union Carbide concluded that the causes of the accident were two human errors. However, the trade unions claimed that the accident resulted from a deterioration of the plant's safety levels since the rules of procedure prohibited the storage of phosgene when the treatment unit was out of service. On 10 February 1982, a new gas leak occurred on a phosgene pump: 25 people were intoxicated[46]. Factory workers launched a strike.

---

[44] Emphasis added by authors Eddy et al.

[45] Union Carbide Corporation, owner of the plant at the time of the accident, claimed it was due to sabotage.

[46] Six other serious incidents, which led to a dozen victims (dead and wounded), occurred before the disaster. Some of these events were in connection with the MIC.

Rajkumar Keswani, owner of and reporter for the local newspaper, the "Rapat Weekly", was an acquaintance of Mr. Ashraf. He wanted to know if his death was an accident or the consequence of internal failures at the pesticide plant. With the collaboration of plant workers, he was able to visit it illegally. After consulting scientific books, he came to the conclusion that "tragedy was only a matter of time" (Lapierre and Moro, 2001, p. 264). He also obtained results of an audit carried out in May 1982 by three engineers from the technical centre of the parent company in the United States. Its conclusions concerning safety of the plant were alarming. The audit report revealed hundreds of deviations from both operational and safety rules. He also underlined the high staff turnover, the lack of training and insufficient operating procedures.

With this information at the end of his investigation, Keswani tried to alert the public by writing a series of articles with prophetic titles:

- "Please, spare our city", on 17 September 1982. In this article, he warned: "*If one day misfortune happens, do not say you did not know*."
- "Bhopal: "*we are all sitting on the crater of a volcano*", on 30 September 1982.
- "*If you refuse to understand, you will be reduced to ashes*", on 7 October 1982.

Keswani became a modern-day Cassandra. His articles gave rise to indifference and at worst to denial. Thus, the Madhya Pradesh State Minister of Labour said: "*There is no reason to worry about the presence of Carbide because the phosgene it makes is not a toxic gas*" (Lapierre and Moro, 2001, p. 266-269).

Bored by the attitude of his fellow citizens, the journalist left Bhopal shortly after, but before the tragedy of December 1984.

4.4 A Conscientious Operations and Safety Director

On 5 October 1999, two trains on the same track collided head-on at the Ladbroke Grove Junction a few kilometres west of Paddington Station, London. The accident cost 31 lives and injured more than 400 people.

A Public Inquiry was launched after the accident and the Investigation Commission chaired by Lord Cullen conducted a detailed and thorough analysis of the event. The immediate and direct cause of the accident was a signal (SN 109) passed when it was red. It brought to light that beyond the direct cause, the accident was rooted in the shortcomings of organisation and poor management of safety in this railway sector (Cullen, 2000).
The investigation showed in particular that the SN 109 signal had been passed eight times when it was red in the six years preceding the accident[47]. During this same period, 46 cases of signal passed at red were recorded in the railway zone of the accident.

[47] It means that with this single signal, there is an annual risk of collision of 7.2%, that is to say, the risk of a collision every 14 years. It seems that, sometimes, even "scientific" data are not enough for an organisation to make the (right) decisions!

The Commission of Inquiry noted the existence of a whistle-blower in the person of Mrs. Forster. She was the Operations and Safety Director of the rail company operating at Paddington. In February 1998, a train of her company passed the SN 109 signal when it was red. She was informed that a train from another company had also passed the same red signal in early August.
This information worried her. So, she wrote at the end of August to the chairman of a working group in charge of proposals for improvements in signal safety. She shared her concerns about the SN 109 signal and she asked what action could be taken "to mitigate against this high-risk signal"? In view of the dilatory response[48] of the chairman and his move to another position, she wrote to his successor to reiterate her concerns about "*a serious problem with drivers misreading signals*" in the Ladbroke Grove zone. The new chairman promised her "*a full risk assessment*" through a future study that a consulting firm would have to carry out. No contract was ever signed on the subject and the "new" chairman of the working group left office. Mrs. Foster wrote again to the third chairman four months before the accident. Her letter remained unanswered, the addressee confessing after the accident that "he was not aware of the remit which had been given" to the working group (Cullen, 2000, p. 117-118).

4.5 A Seismologist Warning about Tsunami

On 11 March 2011, a powerful earthquake struck Japan, triggering a tsunami and a nuclear accident. It was an earthquake with a magnitude of 9.0 on the Richter scale. The tsunami, with waves more than 10 meters, impacted a wide area of the Japanese north-eastern coast. It caused huge damage to buildings and infrastructure. The earthquake and tsunami caused great loss of life and widespread devastation in Japan. More than 15,000 people were killed, more than 6,000 were injured and, at the time of writing of this report, about 2,500 people were still reported to be missing.

The tsunami specially impacted 3 NPPs: From north cost to south, it was Onagawa NPP (3 reactors), Fukushima Daini NPP (4 reactors) and Fukushima Daiichi NPP (6 reactors). The antitsunami seawall of Fukushima Daiichi NPP (called Fukushima in the rest of the section) was 10 meters high, with about 6 meters above the sea level. The 15 meters high waves of the tsunami submerged the seawall. Waves flooded and totally destroyed the emergency diesel generators and every other power generation systems of the plant. The loss of electricity led to an insufficient cooling of the reactors and nuclear meltdowns in Units 1, 2, and 3 (from 12 March to 15 March). Loss of cooling also caused the pool for storing spent fuel from Reactor 4 to overheat (15 March). It is difficult to assess consequences of the nuclear disaster. Indeed, ionizing radiations and life of radioactive elements are a continuous (endless) process.

In 2009, the NISA[49] hold meetings with panel of experts to discuss the safety needs of the Japanese NPPs. During the meetings, issue of tsunamis was never on the agenda. In 2007, an earthquake with a magnitude of 6.6 impacted the west cost of Japan. It caused radioactive leaks at Kashiwazaki-Kariwa NPP, owned and operated by

[48] "*I have commissioned a special study to determine what causes can be identified which contribute... I expect a report in the near future and this will ensure that effective solutions are identified for early implementation…"* However, no such report was ever produced.

[49] Nuclear and Industrial Safety Agency, the Japanese Safety Authorities.

TEPCO[50], as Fukushima, and water from a pool of nuclear wastes entered the Sea of Japan. When case of Fukushima NPP was addressed, the panel focused on earthquake. Dr Yukinobu Okamura, a respected seismologist, was invited to a meeting in order to present its findings. It was concerned because NISA did not see tsunamis as likely enough to be considered in the Fukushima area. Data used for preventing effect of earthquake were taken from the largest earthquake recorded in 1938 with a magnitude of 7.9. It caused a small tsunami and TEPCO had built a seawall able to stop this kind of tsunami. Okamura explained to the panel that this earthquake was no the biggest. An earthquake that occurred in year 869 was more important and Okamura did not understand why it was not mentioned. The TEPCO representative said that it did not cause much damage. Okamura disagreed and said that damage had been severe. Discussion were focus on earthquakes, not on tsunamis. Furthermore, for TEPCO the 869 earthquake was simply "historical" with not certified data. Eventually, the safety report for Fukushima was approved. It did not consider the 869 earthquake in model used for updating Fukushima safety guidelines (Clarke and Eddy, 2017).

We note that Okamura was not the only person raising concerns. For instance, a geologist, Masanobu Shishikura told the government before the Fukushima disaster, that north-eastern Japan was overdue for a huge wave (McKie, 2011).

4.6 Remarks about cases documentation

The role and importance of whistle-blowers in the domain of safety is not yet fully acknowledged[51]. For instance, Rajkumar Keswani (see §4.3) is not cited in the accident analysis seen as a reference by scholars (Shrivastava, 1992). His action is "only" described in a general audience book (Lapierre and Moro, 2001). You could not find the name of Dan Applegate (see §4.3) in the official accident report (Secrétariat d'État aux Transports, 1976): to know the existence of his warning, you must read a book written by journalists (Eddy et al., 1976). The same story has happened to the alert launched by Carlyle Michelson (see §5): it is expressed in a technical report drafted for the NRC (Rogovin and Frampton, 1980) and not in the "official" report of the President's Commission on the accident (Kemeny et al., 1979).

We have also to note that it is difficult to find documentation about cases for which a warning was successfully listened and treated.

Taking whistleblowing into account does not belong to a statistical or probabilistic paradigm. Event occurrence and whistle-blowers belong to the domain of "outliers of the curve" treatment. It takes effort to dig as deep as possible during an event analysis to highlight the existence of whistle-blower(s). We assume that the game is worth the candle because events would be analysed in a more systematic way and it would allow us to define more precisely features or alerts of whistle-blowers.

[50] Tokyo Electric Power COmpany.

[51] One reason could be because event reports are anonymous (people are not named), disembodied. It seems that no human being with flesh and blood were present at the time of the event!

5 Features of whistle-blowers and of whistleblowing

In the paper, we addressed only few cases.

We could have talked about Carlyle Michelson, a nuclear engineer who worked part-time for the NRC and who took, in 1977, the initiative to study behaviour of the process in case of a small break in a specific location of the reactor primary circuit (top of the pressurizer). Results were far beyond design (designers) assumptions, yet few people read about them. A reviewer in NRC prepared a memo based on Michelson's concerns and based on a previous incident that occurred at Davis Besse NPP (Ohio). Michelson's study and the memo did not circulate widely because the issue was not identified as a generic safety problem for operating plants. Eventually the memo was filed away (Rogovin, 1980). About one year later, a major accident occurred at the Three Mile Island NPP (Pennsylvania). The scenario was similar to that imagined by Michelson.

We could also have told about the story of Roger Boisjoly, one of the most well-known whistle-blowers in the "history" of industrial safety. He was a mechanical engineer at Morton Thiokol, the manufacturer of the solid rocket boosters for the Space Shuttle program. In July 1985, he wrote a first memo about their weaknesses, arguing that if, unfixed, it could lead to a catastrophe. He wrote several other memos on that matter, but no action was taken. On the eve of the launch of the 25th Space Shuttle flight, on 28 January 1986, he tried with some colleagues to convince the NASA management to postpone the flight because of the cold temperature. They felt that this would jeopardize the safety of the mission, and potentially lose the shuttle. No one listened to them. The Space Shuttle exploded 73 seconds after liftoff, killing the seven astronauts on board (Vaughan, 1996).

Even if the search for whistle-blowers is not yet a major concern of event analysists, we could still provide an outline of whistle-blowers and of whistleblowing features:

- Whistleblowing deals with degradation of safety and could prevent occurrence of some events;
- Duration of an alert is variable: It can last days, months or years;
- A whistle-blower is either inside or outside the organisation (company / plant), but he / she is always close to the technics;
- The position of a whistle-blower in the organisation could be from the bottom (e.g., a field operator) to the top (e.g., a manager) and expertise. The whistle-blower has the power of influence, but is not a decision-maker regarding the alert launched;
- For informing about the alert, the whistle-blower uses internal channels (within organisation), or (often then) the Safety Authorities, or the media, or NGOs;
- Alerts are technically oriented and safety oriented and they can be repeated, sometimes in different ways;

- Most of the time, alerts are issued by people close to the technical field, or having information from field personnel.

- We have to stress that alerts are **not** an "expert opinion", since a whistle-blower is personally involved and committed. Typically, an alert is not a simple denunciation since the alert is developing. This is not a prediction because an alert relates to the symptoms of deterioration of safety.

- This first set of features might help to make a difference between alerts and background noise, i.e., to figure out relevant safety alerts among the numerous alerts that are launched.

6 Position of the organisation

As we saw, very often, organisations do not listen to whistle-blowers[52]. The two reasons that lead to this result are on the one hand the inability to identify the relevance of alert, and on the other hand, the will *not* to detect or to identify the alert.
When an organisation is unable to identify or accept the alert, it will have an attitude of denial in claiming that whistle-blowers are dissatisfied or displeased. The organisation will deny the risk (e.g., Keswani, Okamura) or engage in delaying tactics (e.g., Forster).
When an organisation does not want to identify an alert, it becomes obstructive in isolating or bullying the whistle-blower (e.g. Galatis).

In every case, the implicit message is that organisation denies the expertise and competence of the whistle-blowers.

We also note that in some cases whistle-blowers are isolated by their colleagues who consider them as "traitors" (e.g. Galatis, Boisjoly).

7 Conclusion

It turns out that listening to whistle-blowers is a way to detect major degradation of safety level and, so, potentially to prevent major events. Nevertheless, to listen to whistle-blowers does not mean to agree with them. However, listening to them should lead to open debates about safety and its current and actual practices. Debates about safety could naturally, not to say mechanically, lead to an increase in safety because the organisation mindset would change.

Taking account of whistleblowing requires the adoption of a new paradigm: to see beyond quantitative approaches and to leave room for "alternative voices" and field expertise, which is one feature of highly reliable organisations[53] (Weick and Sutcliffe, 2001).

[52] Unfortunately, as we already said, we do not have enough data concerning alerts listened and treated.

[53] For differences between "reliability" and "safety", see Llory and Dien, 2006.

The solution goes through a bottom-up approach (i.e., decision-makers listening to the technical experts) to complement the top-down approach (i.e., decision-makers asking questions), recommended, for instance, by Conklin (2012).

Whistle-blowers cannot be an official position, a box of the organization chart. To be a whistle-blower is a specific moment in a professional career.

The entire safety burden cannot be carried by whistle-blowers. Listening to whistle-blowers seems a necessary but not sufficient condition for maintaining and increasing safety. Whistle-blowing must just be one (more) tool in the toolbox for prevention. Every sign or event, near-miss… must continue to be treated in order to increase safety. For instance, in the six months preceding the accident, 1,000 incidents related to the cargo door were reported (it means about 10 incidents by DC-10 aircraft in service in the USA). It seems to "sign" a poor safety culture and safety flawed approaches in the aviation domain at that time So, it is not a big surprise that warning of Dan Applegate was lost in an "ocean of indifference", not to say an "ocean of denial" to safety. The curse of Casandra lives on.

8 Acknowledgements

The author wishes to thank Dr J. Kingston and D. Wright and the ESReDA PG "Foresight for Safety" members for their help.

References

ADIE (2008) *Whistleblowing in Action in the EU Institutions*, RBEUC, Tallinn, https://www.whistleblower-net.de/pdf/ADIE_Whistleblowing_EU.pdf.

Chateauraynaud, F. and Torny, D. (1999) *Les sombres précurseurs - Une sociologie pragmatique de l'alerte et du risque*, Éditions de l'École des Hautes Études en Sciences Sociales.

Clarke, R.A. and Eddy, R.P. (2017) *Warnings – Finding Cassandras to Stop Catastrophes*, Harper Collins Pubishers.

Conklin, T. (2012) *Pre-Accident Investigations – An introduction to Organizational Safety*, CRC Press – Taylor & Francis Group.

Council of Europe (2014) *Protection of Whistleblowers - Recommendation CM/Rec(2014)7 and explanatory memorandum*, https://rm.coe.int/16807096c7.

Cullen, W. D. [Lord] (2000) *The Ladbroke Grove Rail Inquiry, Part 1 Report*, HSE Books, http://www.railwaysarchive.co.uk/docsummary.php?docID=38.

Dien, Y. (2006) Les facteurs organisationnels des accidents industriels, In : Magne, L. et Vasseur, D. (Coordonnateurs), *Risques industriels – Complexité, incertitude et décision : une approche interdisciplinaire*, pp. 133-174, Éditons TED & DOC, Lavoisier.

Eddy, P., Potter, E. and Page, B. (1976) *Destination Disaster – From the Tri Motor to the DC10: The Risk of Flying*, Quadrangle/The New York Times Book Co.

Finn, P. (2002) Crash Described as "Exceptionally Unlucky", *The Washington Post*, July, 3.

Frantzen, C. (2004) Tango on an Asymptote, *13th SRA Europe Annual Conference*, Paris, 15-17 November.

Hollnagel, E. (undated) *From Safety-I to Safety-II: A brief introduction to resilience engineering*, http://safetysynthesis.com/onewebmedia/Introduction%20to%20S-I%20and%20S-II.pdf.

Hollnagel, E. (2014) *Safety-I and Safety-II: The Past and Future of Safety Management*, CRC Press – Taylor & Francis Group.

Kemeny, J. G., Babbitt, B., Haggerty, P. E., Lewis, C. D., Marrett, C. B., Mc Bride, L., Mc Pherson Jr, H., Peterson, R., Pigford, T. H. and Trunk, A. (1979) *The Need For Change – The legacy of TMI, Report of the President's Commission On The Accident At Three-Mile Island*, Government Printing Office, Washington DC.

Lapierre, D. and Moro, J. (2001) *Il était minuit cinq à Bhopal*, Éditions Pocket Robert Laffont Pocket.

Llory, M. and Dien, Y. (2006) Les systèmes sociotechniques à risques : Une nécessaire distinction entre fiabilité et sécurité, Partie 1 : *Performances* n°30, septembre – octobre, pp. 20-26, Partie 2 : *Performances* n°31, novembre – décembre, pp. 9-13, Partie 3 : *Performances* n°32, janvier – février, pp. 20-26.

McKie, Robin (2011) Japan ministers ignored safety warnings over nuclear reactors, *The Guardian*, http://www.theguardian.com/world/2011/mar/12/japan-ministers-ignored-warnings-nuclear

Miller, J. (1995) Millstone's Neighbors in a Quandary, *The New York Times*, November 5.

Pooley, E. (1996) Nuclear Warriors, *Time Magazine*, vol. 147 n° 10, March 4.

Rogovin, M. and Frampton, G. T. (1980) *Three Mile Island - A Report to the Commissioners and to the Public, Vol I*, NRC Special Inquiry Group, NUREG/CR-1250, Washington DC.

Shrivastava, P. (1992) *Bhopal Anatomy of a Crisis*, 2nd edition, Paul Chapman Publishing.

Secrétariat d'État aux Transports (1976) *Rapport final de la Commission d'Enquête sur l'accident de l'avion D.C. 10 TC-JAV des Turkish Airlines survenu à ERMENONVILLE, le 3 mars 1974*, Journal Officiel de la République Française, Éditions des documents administratifs, N° 27 du 12 Mai.

Turner, B. and Pidgeon, N. (1997) *Man-Made Disasters*, 2nd edition, Butterworth Heinemann, Oxford [1rst edition: Turner, B. (1978), Wykeham Publications].

Vaughan, D. (1996) *The Challenger Launch Decision - Risky Technology, Culture, and Deviance at NASA*, The Chicago University Press.

Weick, K. and Sutcliffe, K. (2001) *Managing the Unexpected – Assuring High Performance in an Age of Complexity*, Jossey-Bass Publishers.

Session 7:
Early warning signs: understanding threats through monitoring

From maritime multi-sensorial data acquisition systems to the prevention of marine accidents

Lorenzo Fiamma

European Maritime Safety Agency

Praça Europa 4

Cais do Sodré, 1249-206 Lisbon, Portugal

Extended Abstract

Multi-sensor based ship tracking

EMSA operates, along with the Member States of the European Union, the SafeSeaNet, the vessel traffic monitoring and information system covering the waters in and around Europe. The platform enables for maritime data exchange across the Union's competent authorities. VHF radio signals are captured from Automatic Identification System (AIS) which are installed aboard the circa 17,000 vessels which operate in and around EU waters. By tracking ships using AIS signals, the system gathers also identity details, latest positions and other status information in near-real-time.

Data acquired through this channel are correlated and enriched with additional details, such as the presence of hazardous goods and the number of people aboard, or the ship track in a given timespan. It can also inform about estimated or actual arrival and departure times in ports, and to highlight ships with high risk profiles or those that were involved in accidents and incidents.

Long-Range Identification and Tracking (LRIT) and satellite-based AIS technologies are exploited to track vessels outside the range of AIS coastal networks. This extends the system to a worldwide coverage.

The European Marine Casualty Information Platform (EMCIP)

The European Marine Casualty Information Platform (EMCIP) is a database application that provides the means to store data and information related to marine casualties involving all types of ships and occupational accidents. It also enables the production of statistics and analysis of the technical, human, environmental and organisational factors involved in accidents at sea.

The database taxonomy has been developed by EMSA in consultation with the Member States, on the basis of European research and international recommended practice and procedures. EMSA and the national competent authorities operate the system within a culture of 'no blame, no liability' and personal data protection.

From reactive to preventive measures

In the course of a technical enquiry into a marine casualty, investigators need to reconstruct the events that led, or contributed to an occurrence. This often implies the need to know the whereabouts of the vessel that was involved in the casualty, or of other vessels that may hold important information about the occurrence. Vessels' position and voyage data have been already used to this end, and has enabled investigators to identify and understand the peculiar circumstances which very serious or catastrophic accidents have developed in.

Recent developments have brought to life additional services, like the vessels' behaviour monitoring tools or other automatic alerting features which may be the precursors of future intelligent and smart agents for the prevention of accidents, rather than for the mitigation of existing risky conditions or threats.

Kinematic data could be streamed directly form onboard sensors and crew's biological parameters captured from wearables devices. Big-data dynamic algorithms may be used to get the foresight of critical conditions and of dangerous situations and to warn users in real-time. Multidimensional and multisensorial dataacquisition is already a reality in the maritime safety sector and the situation is pregnant with new possibilities!

Keywords:

Evolution of remote performance monitoring in ship's safety decision making reinforced by Analytic Hierarchy Process

Ioannis Dagkinis, George Leventakis, Nikitas Nikitakos

Department of Shipping Trade and Transport, University of Aegean

Korai 2a

82132, Chios, Greece

Abstract

Among the objectives of shipping industry are to maintain safety. Also the measuring of safety in relation to the application of evolutions in operational management of ship's and developing strategies to avoid future accidents is crucial. So recognizing signals before an accident occurs and by enhancing with the right decisions any operational procedure is offered the possibility for improving safety.

In this paper, we address the challenge to evaluate the Remote Performance Monitoring by identify and scrutinize features which may affect the ships safety and must take into consideration of the decision makers during its implementation. The evaluation performed by using the Analytic Hierarchy Process and answers the question, how remote performance monitoring using internet of things and big data, leads in further improvement in terms of machines performance with safety. The implementation of method for ship's safety decision support will be presented and analysed with real world case studies.

Keywords: AHP, Remote Performance Monitoring, Threat Attack, Shipping Safety.

1. Introduction

The shipping industry is on the verge of a new frontier where innovative ideas, sophisticated approaches and technologies are emerging for ship's performance planning and verification methods. Also new challenges are faced such as the significant increase in transport volumes, the growing environmental requirements and a shortage of seafarers in the future. The continued high oil prices and the burden of increasing regulatory compliance make the development of energy management strategy crucial to fleet owners worldwide, with continued innovations and the sustainability to be at the heart of the new targets in the shipping industry. The new objectives focus on improving energy efficiency, reducing greenhouse gas emissions and other emissions as well as the safety which resulted as the aim of ship's new innovative operational modes.

The overall composition of a comprehensive maritime lane of the future includes ambitious plans to develop, refine and implement progressive policies in key areas of sustainable performance, such as environmental, social and economic.

Global shipping to become viable should organize ships and any other shipping sector in relation to effective management and operation principles. This will require the adoption of new techniques and conversions in companies, ships, systems and management practices. Overall, the ships quality will simultaneously focus on broad and profound developments such as:

- Efficiency of logistics and networks, optimizing networks, capacity and speed.
- Efficiency with optimized the vessel operations, like the performance tracking, economic speed etc.
- Jurisdiction and awareness.
- Technologies, with innovative components and systems that enhance ship's operation.
- Contracts and partnerships that representing NewBuilding, charter parties, innovation with suppliers etc.

So, the choice of marine equipment and the optimization of marine systems focus on factors such as the ship's control and continuous monitoring, low energy consumption, low pollution, high efficiency, e.g. when assessing the technical index of ships, a high emphasis should be placed on the ratio of the load factor of the main engine, generator, boiler etc. as well the effective control of harmful emissions, vibration and noise. Also, a full control of the ship can be reached from the bridge position, while the propulsion and auxiliary plants can run from the bridge, giving to the crew full picture of entire ship. This is consequence due development, because the coming age of ubiquitous computing promises to change allot of activities in significant ways. As we will see in near future everyday objects, cars, train tracks and traffic lights, homes (thermostats and voice activated appliances), and of course consumer goods such as phones, wearables, and more, will become “smart" and will contain embedded processors; they might monitor behaviour or operational conditions, react and adapt their functionality to the preferences of the user. The same happens in some cases today and will happen in more extent in the future on ships, where monitoring sensors adjust the machine and machinery condition in order to achieve its effective operation. These integrated automation systems could be managed far away from the ship with data transition through internet implementation, since future of technology lies in data transmission and its analysis.

But the data itself does not produce these objectives that needed for improve the performance. Solutions can arise from analyzing by combine Internet of Things (IoT) and the Big Data [1, 2]. The term IoT refers to the networked interconnection of everyday objects, which are often equipped with ubiquitous intelligence. This increase the ubiquity of the Internet by integrating every object for interaction via embedded systems, which leads to a highly distributed network of devices communicating with human beings as well as other devices. On the other hand, the term big data refers to extremely large data

sets that may be analyzed computationally to reveal patterns, trends, and associations, relating to human behaviour and interactions as well data that can be analyzed for insights that lead to better decisions and strategic business moves. So its combination will lead in integrated systems with ability in use for improve the effectiveness of vessels like SCADA [3].

In this paper, the challenge to evaluate the remote performance monitoring (RPM) is considered by identify and scrutinize features, which may affect the ships safety, and must take into consideration of the decision makers. The application of RPM is facilitated by recent technological improvements in big data and ship's connectivity. The evaluation performed by using the Analytic Hierarchy Process (AHP), a multi-criteria methodology which is used for a wide variety of decision and other applications. The AHP selected because the evaluation of remote performance monitoring characterized by structure complexity and the method is capable to handle measurements on a ratio scale. The evaluation answers the question, how remote performance monitoring using internet of things and big data, leads in further improvement in terms of machines performance, energy efficiency in ship operation, the environmental management of ships and all these with safety. The AHP implementation for ship's safety decision support will be presented and analyzed with real world case study based on experts' opinion.

2. Vessel's performance monitoring and maintenances

The IMO (International Maritime Organization), responsible for standardized regulations covering all aspects of marine safety, has Special classifications for providing information on whether the hull and technical equipment of a ship are perfectly seaworthy in all respects. These strict international guidelines refer to the construction and running of a ship – but also to its maintenance and the conditions that have to be met. Against this background the reliability of all systems onboard is gaining in importance, and makes it easy to see why intelligent automation solutions are indispensable aboard modern ships.

In respect to maintenance and performance monitoring model that shipping companies follow today for their ships and it is defined by international regulations, the engine components as well the machinery parts which have a certain operation life cycle, at least the critical based on manufactures' specifications, must be replaced after a specific period. This must be done irrespective from their actual condition and their ability for further usage. That means even if a specific part be in an acceptable condition and can be used without a failure risk of vessel's operations or affect the availability of machinery it must be replaced with a new one.

In accordance the previous model of inspection and information flow about ship's machinery, engines and other parts of the ship that inspected are followed maintenance models like preventive or condition based. On those models very considerable is the presence of human factor, since various reports based on data that the vessel crew recording. Also it is notable that the communication between the fleet manager and the engineers is not direct and presents problems. These problems can summarized at the scheduled inspections and the results which are not always accurate due to sensors fault or false measurements by the crew. Hence, the fleet manager has periodical indirect communication with the captain and the description of each case may lack in accuracy because it depended on captain's approach. That results that the decisions to be taken for

determination of repair actions and maintenance by the engineering team on the ship and the suggestions of engineer's department in the company office are not based on actual and real-time data, but on incomplete and unreliable data. Moreover, this communication and correction mode creates confusion because is difficult to measure the effect of implementation of various actions.

The consequence of the maintenance models mentioned above are disadvantages like high cost of spare parts and sometimes incorrect maintenance procedures as well incomplete technical reports, which offer limited or unreliable data and cause difficulties in decision making. Moreover, in most vessel's that sails today, except the very synchronous, the monitoring of engine performance either the fuel and oil consumption compared to the vessel instantaneous performance are absented or it depends on human observation, something that in many occasions is dubious. So a common policy to manage the ship and monitoring the performance in order to make the correct decision is difficult to be determined. Furthermore, the absence of a prognosis system causes difficulties to prevention of breakdowns and provokes high cost and time-consuming repair procedures. Hence the research experience and operation analysis of maritime companies indicates problematic issues due the absence of a complete remote monitoring system of the fleets, which additionally affects the environmental consequences of vessels operation.

Hence as the maritime industry in our days faces the limited crews number, low technical quality of the crew due the rapidly innovation which grows by technologies, the big competition in rates, along with the increasing limitations from regulations, in order to operate safely the vessels, the necessity of integrated systems is obvious. Moreover, it is needed to enhance the reliability through right monitoring of vessel performance and reduce the environmental impact that a vessel creates due to its inherent operation. These are the basic reasons for adopt monitoring systems, capable of improving decision-making based on integrated information resulting from automated systems and that are met by new technological applications.

These applications arise from the advances in wireless communications, digital electronics, MEMS (microelectromechanical) technology, miniaturization, low power circuit design and computing enhanced the effort of developing sensor nodes that are small size, lightweight, compact, autonomous, rather cheap, have low power needs, communicate wirelessly and can process and store the sensor data locally [4, 5]. Those systems inherent compactness, that can operate efficiently, with low power consumption, and ability to big data processing and adequate storing capability, which can communicating by wiring and wireless on board and out of board, provide a great leap to shipping industry for an effective monitoring operation of vessels.

Such system implementation of open architecture for ship's control, alarm and performance monitoring is the Supervisory Control and Data Acquisition (SCADA). It is met in modern ships and is an automatic system control that includes control, alarm and monitoring system that have access to all process, control stations and can monitoring them.

3. Typical SCADA system and its benefit

Supervisory Control and Data Acquisition (SCADA) systems are used to monitor and control plants or equipments in industries such as energy, oil, telecommunications, gas refining and transportation.

In the environment of a marine plant many parameters need to be controlled or monitored that includes temperatures, speed, torque control, voltage, current, machinery status (if it is on or off), equipment status (open or closed), pressure, level, flow control, and fuels viscosity. The control of these parameters on ships in the past was responsibility of the watch keeping engineers which observe and control the machinery plant. This was achieved by periodically controls in the engine room and manually inspection of the condition each running machinery. Often the engineers were totally dependent of their natural senses and frequently supported by distributed simple monitoring devices [6, 7, 8].

Today, with SCADA implementation ship engineers and operators be able to use different number of screens, with different types of man machine interface such that it can display and control different sensor or system status. These sensors can be voyage data recorder, wind speed, direction GPS, hull opening, hull stress, radar, ship speed, tank fuel level, fuel and machinery temperature, consumption of engines, propulsion engine condition and performance, fire doors control station, etc.

This is achieved because a typical SCADA system consists of one field data interface devices usually RTUs (Remote Terminal Units) and/or PLCs (Programmable Logic Controllers) which interfaces to field sensing devices, local control switch boxes and valve actuators. Moreover, a communication system is used to transfer the data among field data interface devices the control units and computers in the SCADA central host which is a host server or more servers [9]. A collection of standard and/or custom software, sometimes called HMI (Human Machine Interface) software, is used to provide the SCADA central host and operator terminal application, supporting the communication system, monitor and control remotely located field data interface devices. Devices such as temperature transmitters, power consumption meters, pressure gauges, level meters, flow meters, and valve position transmitters, provide all necessary information's that can inform an experienced operator how effective the system is performed.

The benefits of SCADA systems provide immediate knowledge of system performance, improvement on system efficiency and performance, operational cost reduction, increase equipment operational life, reduction of repair cost, reduction of man-hours required for troubleshooting or maintenances, expediting compliance with regulatory requirements through automated report generating.

Taking into account the structure of the system that transmit the data which will enhance the effective management of the ship, typical systems that provide connectivity to the respective corporate IT and SCADA systems onboard vessels are satellite networks, onboard Wi-Fi and Internet access (which can be used by crew), Radar, Simplex Teletype Over Radio (SITOR), NAVTEX, satellite telephones and other ship-to-shore telecommunications systems and voice over Internet Protocol (VoIP) telephony.

SCADA systems have been engineered for monitoring performance, enhance reliability, flexibility and safety, but due to the structure of data transfer of the system as mentioned above, security of the ship must be considered, since may disrupted against most advanced and persistent threats which take place at corporate and industrial networks. Security threat of any suspicious act or circumstance that could threats the security of the vessel, marine facility, port administration or interfaces between vessels or between a vessel and the marine facility.

4. Scenario of cyber attack and evaluation methodology

The importance of SCADA systems as mentioned is the automation. This allows to the vessel managers a carefully study and anticipate the optimal response to measured conditions and execute those responses automatically every time. Relying on precise machine control for monitoring equipment and processes virtually eliminates human error. More importantly, it automates common, tedious, routine tasks once performed by human, which further increases productivity, improves management of critical machine failure in real-time, and minimizes the possibility of failures. In addition, SCADA systems monitor and control a large number of parameters where a vessel may not have enough manpower to cover. Thus, reliable communication and operability of all aspects is critical to safety and profitability.

Hence, a virtual failure caused by cyber attack on vessel performance monitoring system SCADA is a serious situation that must be considered since affects the safety of the vessel the crew and the environment.

The scenario that is presented in this paper is related to a failure alarm for high lube oil temperature of propulsion engine, which affects the propulsion engine operation and its availability. So the actions that must be taken include the stopping of propulsion engine, the reduction of speed or to maintain a constant/full speed. These could be the major alternatives that can a decision maker take in order to avoid unwanted consequences. In addition, the ship might sail in a restricted area, e.g. a Traffic Separation Scheme where the ship must keep its operability or in an area where high risk may occur due to pirate activity or a combination of this two. So, each one of decisions affect in different way the overall attitude against the risk and the safety of the ship. If this risk includes the safety of the crew, the ship's machinery operability since such failure may cause further damages, and the cargo safety.

Further definitions about lube oil high temperature failure alarm is that it relates and affects the operation of the engine and its occurrence is liable to cause serious damage and shut down the propulsion engine operation. The extent of the damage can lead the ship to a shipyard for further repairs, which means expenses for ship owners as well as losses of profits. Moreover, taking into account the area where the ship is sailing, the vessel meet risks associated with maritime safety and the likelihood that the ship and cargo will captured by pirates with all the unpleasant consequences. So, in any case, technicians of technical department and managers of the shipping company in cooperation with the ship's crew will have to decide on actions that must be taken in accordance with several parameters. One of these parameters is the possibility of the recorded failure to be result of malfunctioning of the automated SCADA control system due a cyber attack.

In order to evaluate and enhance the decision makers in the possibility of a threat attack during data transition of vessel's monitoring performance, which relates to the SCADA system operation, a comprehensive support tool is presented. This tool is the multi-criteria method AHP and was implemented to evaluate different alternatives with specific criteria in a scenario with a ship which sails in restricted sea and face a possible cyber attack in monitoring performance transition system, where the lube oil high temperature failure alarm belonging.

In accordance with the previous paragraphs scenario presented, briefly, the three alternatives for decisions against threat attack on SCADA system data transmission evaluated by AHP in this study are the following:

- stopping the engine and patching the SCADA system in order to fix any threat. In a landmark study of the Patching for post-release bugs in software, [10] showed that between 14.8% and 24.4% of all fixes are incorrect and directly impact the end user. And if that's not bad enough, 43% of these faulty 'fixes' resulted in crashes, hangs, data corruption or additional security problems. Furthermore, patches don't always solve the security issues they were designed to address. Also the patching in SCADA must be performed by an authorized person and a stopped vessel is sensitive in weather contrition's, piracy threats.

- reduction the vessel speed with slowing the engine till it reaches a safe area. This alternative may set the ship in danger in relation to pirate actions or potential create dangerous operating conditions in relation to other ships sailing in the area but allows the crew without stopping completely the propulsion engine maintain the ship's control and further investigate the cause of failure alarm.

- constant/full speed till the vessel reaches an safe area. This alternative eliminates the piracy actions threat and weather condition undesirable situations but endangers the ship and its machinery in case the failure alarm is real.

5. The Analytic Hierarchy Process

The AHP was developed at the Wharton School of Business by Thomas Saaty. It's a powerful and flexible multi-criteria decision-making tool and allows decision makers to model complex problems where both qualitative and quantitative aspects need to be considered [11, 12]. The AHP helps the decision makers to organize the critical aspects of a problem into a hierarchical structure similar to a chart of components depicted in boxes. The top box of chart represents the goal of the decision problem, and then is splitting in lower levels boxes which represent an objective contributing to the goal. Each box can then be further decomposed into lower level boxes, which represent sub-objectives, and so on. Finally, boxes corresponding to the lowest level sub-objectives are broken down into alternative boxes, where each alternative box represents how much the alternative contributes to that sub-objective. By reducing complex decisions to a series of simple comparisons and rankings, then synthesising the results, the AHP not only helps the decision makers to achieve the best decision, but provides also a clear rational for the choices made.

Step-by-step the use of AHP procedure is the following: First the decision criteria in a form of objectives hierarchy are defined. The hierarchy structured on different levels from the top (i.e. the goal) down to intermediate levels (criteria and sub-criteria on which subsequent levels depend) and then to the lowest level (i.e. the alternatives).

Then criteria, sub-criteria and alternatives weighted as a function of their importance for the corresponding element of the higher level. For this purpose, AHP use simple pairwise comparisons to determine weights and ratings, so that the analyst can concentrate on just two factors at one time. One of the questions which arise when using a pairwise comparison in this paper is: how important is the "Ship's Safety" factor with respect to the "decision against threat attack applicability" attribute, in terms of the "decision selection against threat attack" (i.e. the problem goal)? The answer may be "equally important", "weakly more important", etc. The verbal responses are then quantified and translated into a score via the use of discrete 9-point scales (with 1 ranking when a criterion i and criterion j are of equal importance, and 9 when criterion i is absolutely more important than criterion j). After a judgement matrix has been developed, a priority vector to weight the elements of the matrix is calculated. This is the normalised eigenvector of the matrix.

Since the priorities of the Criteria with respect to the Goal and the priorities of the Alternatives with respect to the Criteria are known, we can calculate the priorities of Alternatives with respect to the Goal and finally synthesize the final priorities. This is a straightforward matter of multiplying and adding, carried out over the whole of the hierarchy and the results give to us the overall priorities and the solution for making the decision.

6. Hierarchical Decision Model Development

When the AHP hierarchical boxes chart develops, the aim is to develop a general framework that satisfies the needs of the decision makers to solve the selection problem of the best decision against threat attack during data transmission of SCADA system. The AHP as described above starts by breaking down a complex multi-criteria problem into a hierarchy, where each level comprises a few manageable elements which then analyzed in another set of elements (Fig. 1). Considering the critical aspect of this step for AHP, the structure has been created by experts' suggestions in relevant strategies followed by working staff in shipping companies. Then to studied the problem in this case the AHP hierarchy is developed in three levels. The first level represents the main goal of best decision against threat attack selection and the lowest level comprises the alternatives against threat attack. The evaluation criteria that influence the primary goal are included at the second level and are related to four different risk aspects: Ship's Safety, Operational conditions, Weather conditions, and the Type of Ship (Fig. 1). These criteria then could break down into several sub-criteria.

The circumscription of the hierarchy methodology that is described above has been developed using a brainstorming process [13] with expert's support. Also the judgements of all the people concerned with failure alarms on board and onshore are included. In particular, in this study we include the opinions of maintenance engineering personnel, On Ship and On Shore who perform the analyses of monitoring performance and develop the strategies to improve procedures against failures, the operation personnel who

manages the failures in order to improve the ship operations and the safety personnel who performs the analysis of factors related to safety.

The relevant factors defining the Ship's Safety and Weather conditions criteria are identified as the loss of propulsion power, the possibility of pirates to attack and the unexpected consequences of bad weather conditions. These are related to the operational reliability of the ship, the damage to environment due to collision etc, the influence to personnel safety, and to the company's reputation. The Operational conditions are linked to the ship's availability downtime derived from a failure, the time required for detection, repair or restoration to operating condition and re-starting. The risk concerning the type of ship factor, relate to the age of the ship, its size, the hazards of cargo, parameters which need special handling.

7. AHP implementation

Once the hierarchy structure of the most preferred strategy against threat attack problem is defined, every available data is imported. Then the analytic hierarchy process (AHP) mathematical solver runs to synthesize the results and normalize the values. The priorities for the alternatives specified in respect to each of the decision criteria, and priorities for each of the criteria with respect to their importance to reaching the goal calculated by use pairwise comparisons.

Then the transfer of the experts' judgments in Table I (one example of alternatives) to an AHP matrix, and the processing with software yields the result for the Alternatives with respect to ships safety and the priority results shown in Table II.

Table I: Alternatives compared with respect to Ship's Safety.

Stop the Ship	1	Speed Reduction	7	Speed Reduction is very strongly important than criterion to Stop the Ship. Weight: 7
Stop the Ship	1	Keeping constant/full speed	4	Stop the Ship is weakly more important to Keeping constant/full speed. Weight: 4
Speed Reduction	9	Keeping constant/full speed	1	Speed Reduction is absolutely more important to Keeping constant/full speed. Weight: 9

Table II: The transfer of weights to the matrix.

Safety of the Ship	**Stop the Ship**	**Speed Reduction**	**Keeping constant/full speed**	**Priority**
Stop the Ship	1	1/7	1/4	0.0649
Speed Reduction	7	1	9	0.7846
Keeping constant/full speed	4	1/9	1	0.1505

The next steps are the pairs' comparison of alternatives with respect to ship operational conditions, Weather conditions and Type of Ship. The weights transferred into the matrixes and solve the AHP. Then the criteria compared with respect to reaching the goal and with pairwise comparisons take the higher-ranking criterion to achieving the goal.

Table III: Results for choose the best alternative.

Best decision against threat Attack in SCADA system	**Safety of the Ship**	**Operational conditions**	**Weather conditions**	**Type of Ship**	**Goal**
Stop the Ship	0.0390	0.0100	0.0245	0.0089	0.0824
Speed Reduction	0.4711	0.1429	0.0117	0.0609	0.6866
Keeping constant/full speed	0.0904	0.0252	0.0895	0.0260	0.2320
Totals	0.6005	0.17811	0.1256	0.0958	1.0000

In Table III shows the final ranking in decisions rank for lube oil high temperature failure alarm in SCADA monitoring system.

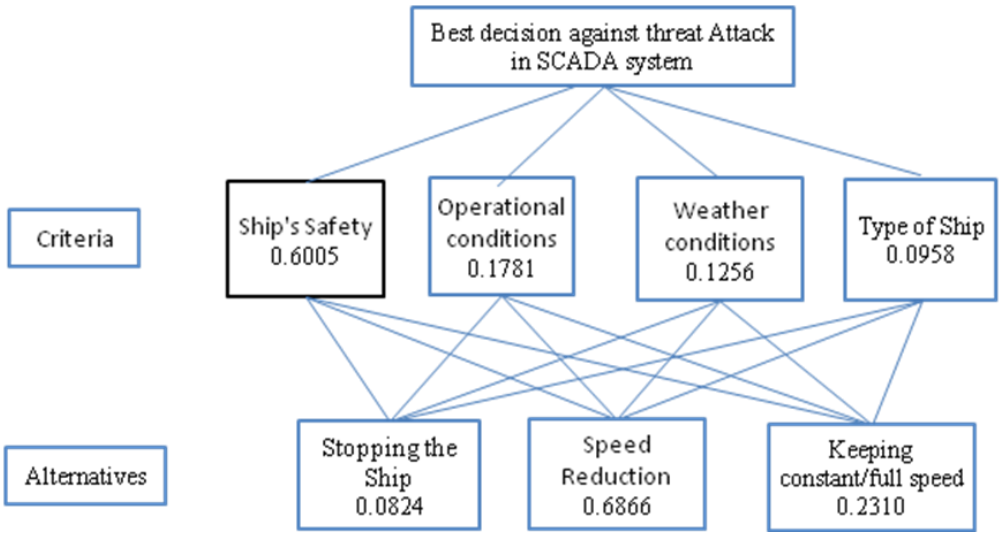


Figure 1. The AHP development and the global priority indices

.

Based on the expert's choice of decision criteria, on their judgments about the relative importance of each one and on their judgments about best decision against threat attack in data transmission with respect to each of the criteria, Speed Reduction, with a priority of 0.6866, is by far the most preferable strategy against threat attack in performance monitoring SCADA system. The decision to Keeping constant/full speed with 0.2311 priority is second in decision and finally the Stop of the Ship at 0.0824 is that with lowest rank.

8. Conclusions

This paper describes one approach for Risk Evaluation during data transmission in SCADA system due a cyber attack in seagoing ships. The application of the AHP method has enabled modelling of various risk aspects that influence total risk of a ship that faces a threat attack. In the model, each risk criterion had weighting based on experts' opinion and introduced in a matrix where calculated and synthesized with pairwise comparisons. The results of ranking of risk elements provides support to making decisions in order to prevent the influence of an improper decision during a possible cyber attack of a certain risk during vessel's voyage.

The results and satisfaction from choosing a decision against threat attack in SCADA system derived by using the AHP method and confirms that it can improved and represents an effective approach to arrive at making decisions. Through the method implementation the decision maker could found a tool to enhancing their decisions in order to be able to eliminate the impact of a possible attack on a monitoring control system as their implementation is expected to spread in the coming years with the implementation of smart systems.

References

Atzori, L., Iera, A., & Morabito, G. (2010). *The internet of things: A survey*. Computer networks, 54(15), 2787-2805.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013*). Internet of Things (IoT)*: A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.

Cagalaban, G., Kim, T., & Kim, S. (2010, May). *Improving SCADA control systems security with software vulnerability analysis*. In Proceedings of the 12th WSEAS international conference on Automatic control, modelling & (Vol. 38, pp. 409-414).

Kopke, A., Willig, A., & Karl, H. (2003, March). *Chaotic maps as parsimonious bit error models of wireless channels.* In INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies (Vol. 1, pp. 513-523). IEEE.

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). *Wireless sensor networks: a survey*. Computer networks, 38(4), 393-422.

Sitao, W., & Qingquan, Q. (2000). *Using device driver software in SCADA systems*. In Power Engineering Society Winter Meeting, 2000. IEEE (Vol. 3, pp. 2046-2049). IEEE .

Hahn, A., Kregel, B., Govindarasu, M., Fitzpatrick, J., Adnan, R., Sridhar, S., & Higdon, M. (2010, April). *Development of the PowerCyber SCADA security testbed.* In Proceedings of the sixth annual workshop on cyber security and information intelligence research (p. 21). ACM.

Katsikas, S., Dimas, D., Defigos, A., Routzomanis, A., & Mermikli, K. (2014). *Wireless Modular System for Vessel Engines Monitoring, Condition Based Maintenance and Vessel's Performance Analysis*. In Proc. of the 2nd European Conference of the Prognostics and Health Management Society (PHME'14) (pp. 1-10).

Zaghloul, M. S. (2014). *Online Ship Control System Using Supervisory Control and Data Acquisition (SCADA).*International Journal of Computer Science and Application.

Yin, Z., Yuan, D., Zhou, Y., Pasupathy, S., & Bairavasundaram, L. (2011). *How do fixes become bugs?*. In Proceedings of the 19th ACM SIGSOFT symposium and the 13th European conference on Foundations of software engineering (pp. 26-36).

Saaty, T.L. (1980). *The analytic hierarchy process*. New York: McGraw-Hill International.

Saaty, T.L. (2008). *Relative Measurement and Its Generalization in Decision Making Why Pairwise Comparisons are Central in Mathematics for the Measurement of Intangible Factors The Analytic Hierarchy/Network Process*. Rev. R. Acad. Cien. Serie A. Mat. VOL. 102 (2), pp. 251–318.Almeida AT, Bohoris GA. (1995). *Decision theory in maintenance decision making*.Journal of Quality in Maintenance Engineering;1 (1):39–45.

Almeida AT, Bohoris GA. (1995). *Decision theory in maintenance decision making.* Journal of Quality in Maintenance Engineering;1 (1):39–45.

Increased forced unavailability of power plants due to economical conditions

H.C. Wels, DEKRA Material Testing & Inspection

Meander 1051, 6825 MJ ARNHEM , the Netherlands

T. Slot, DNV GL Netherlands B.V.

Utrechtseweg 310, 6800 ET ARNHEM , the Netherlands

Abstract

Electrical production must be equal to electrical demand in order to maintain a precise frequency. When a power plant fails unexpectedly, other plants take up the load as normally there is reserve power available to counteract forced unavailability of plants. Insufficient reserve leads to potential overload of generators which is prevented by shutting down load to areas, if not a blackout on the electrical grid may occur. Forced unavailability of power plants may increase due to the present low electricity prices which are especially low when large wind and sun generation is input in the grid. Such economical conditions result in minimal maintenance of fossil plants as well as a potential increase in failures due to changing operating conditions. The increase is expected to be especially present at vintage coal fired plant that was not designed for cycling but it can also be present in other types of plants. Minimal maintenance is expected for every plant at too low electricity prices. Numerical data in the Netherlands as well as from the VGB's KISSY database show the presence of such effects, however the effect of changing operating conditions is not so clear as plants operate less (reduced exposure to for instance creep) but start more often (increased exposure to low cycle fatigue). These effects are not taken into account when assessing the probability of grid blackouts by authorities and grid operators, as well as possible effects due to imperfect mothballing causing teething problems when de-mothballing,

Keywords: Reliability, Security of supply, Power failure

1. Introduction

Reserve power that can instantly be delivered to the grid, for example reserve power plants in operation ("operating reserve") for which the power can be increased some 10 %, must be present to keep the frequency precisely at the defined value (50 Hz or 60 Hz). If an incident occurs that causes forced unavailability of a plant in the system and such reserve is not present, electrical load must be reduced by curtailing the demand of customers. If not, generators will shutdown (trip) because of their protection systems and cascade

effects may cause a blackout. While forced unavailability of a plant is a daily occurrence in a moderate to large system, the probability of a demand curtailment is much lower and a curtailment when it occurs is generally not noticeable to the general public. It is known that parties have contracts allowing such curtailment (as they have own production facilities for which production may be more costly than the grid) have experienced such events. The general public in the Netherlands probably does not remember the blackout event of 23-6-1997. A cascade effect caused forced outage of several power plants that resulted in having the province of Utrecht without electrical power. Prolonged blackouts may result in unwanted social behaviour (plundering) and causes financial losses the least. This event happened at a total installed power to peak demand factor of about 1.3 and can be regarded as an incident.

Market liberalization in the Netherlands has led to major overcapacity with many old and new combined cycle plants and new coal fired power installed, therefore the probability of such events in the past has been low. However, due to the so called Energie Akkoord (Energy Agreement) for climate reasons, old coal power has been decommissioned recently, discussion on mid-life and new coal power is ongoing and many combined cycles have been mothballed for economic reasons. The market is assumed to solve any future shortages in capacity. If due to a low electricity production market price (even so-called negative prices have occurred with much wind and fossil power unable to stop production delivering steam to industry, district heating, contract obligations), costs must be cut further. Maintenance costs are a prime target for cost reduction as there is no directly felt effect of maintenance cost reduction to operations. Machines will react later on in time (in the order of months to years). We have found in the Netherlands that in the last years of operation of plants, forced unavailability of such to-be-decommissioned plants increased to 20 – 30 % of time due to cuts on maintenance.

Now, if the forced unavailability of power plants rises due to cycling and economic conditions, with plants that are still mothballed because of prices, and renewables such as sun and wind are missing (at night, prolonged high pressure zone in Europe), curtailing of demand becomes probable.

The paper is set up as follows. At first the signal is given that forced unavailability rises abroad. It is probable that this may also be the case for the Netherlands as the reasons are the same. The amount of rise might be different though as the production plant types differ from abroad. Reasons for forced unavailability are given, one of which is a change in operating conditions in combination with minimal maintenance. These influence factors are benign yet as the fraction of renewables in the Dutch grid is relatively small (it is much smaller than in Germany). It is clear the even new combined cycles will be forced to start and stop every day. In principle this causes additional stress to its components. From the point of security of electrical supply it is unwanted that combined cycles will stay mothballed with old coal power decommissioned due to the Energie Akkoord causing less reserve. The effect of the different influence factors is quantified using simple models and compared with Tennet's Monitoring Report and calculations with the extensive DNV-GL European PLEXOS model.

2. Forced power unavailable before liberalization

From 1976 up to 1996 all forced unavailability data from practically every plant delivering power to the grid were sent both to Sep[54] and KEMA[55] in a long-duration project to lower forced unavailability. By simple addition of these data the total forced unavailable power can be calculated. An example is given in figure 1.

The figure shows that in the years before liberalization, total unavailable power varied between 500 MW and 2500 MW on a system peak demand of about 13000 MW with about 50 power plants present. On average, about 1600 MW was forced unavailable which is 12 % of peak demand. This fraction is somewhat high compared with the forced unavailability of a plant which normally is less than 10 %. However, cycling and reserve plants are not needed all the time and therefore repair time outside the window of need should not be regarded. Therefore the order of magnitude is comparable. The percentages indicate that with a reserve factor lower than 10% – 12% measures are necessary in order to prevent load curtailment.

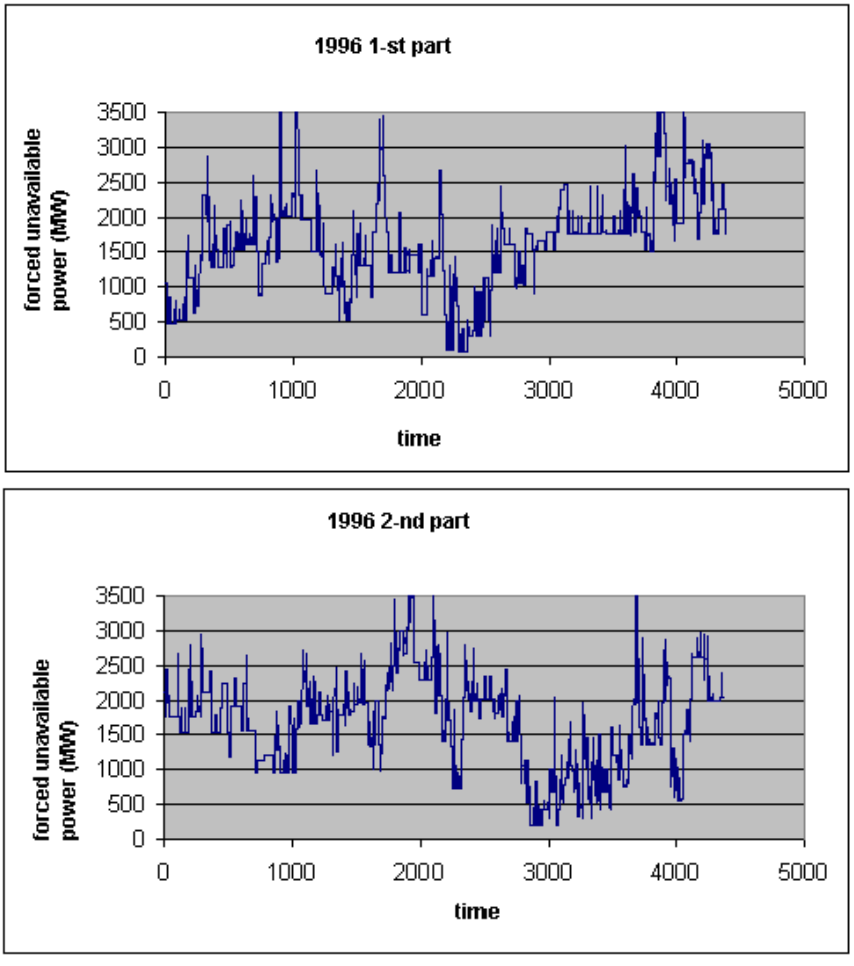


Figure 1. Total power in the Netherland being forced unavailable

[54] Sep = Joint Electricity Producers

[55] KEMA = research institute for Electricity, with electricity production and distribution companies as its shareholders

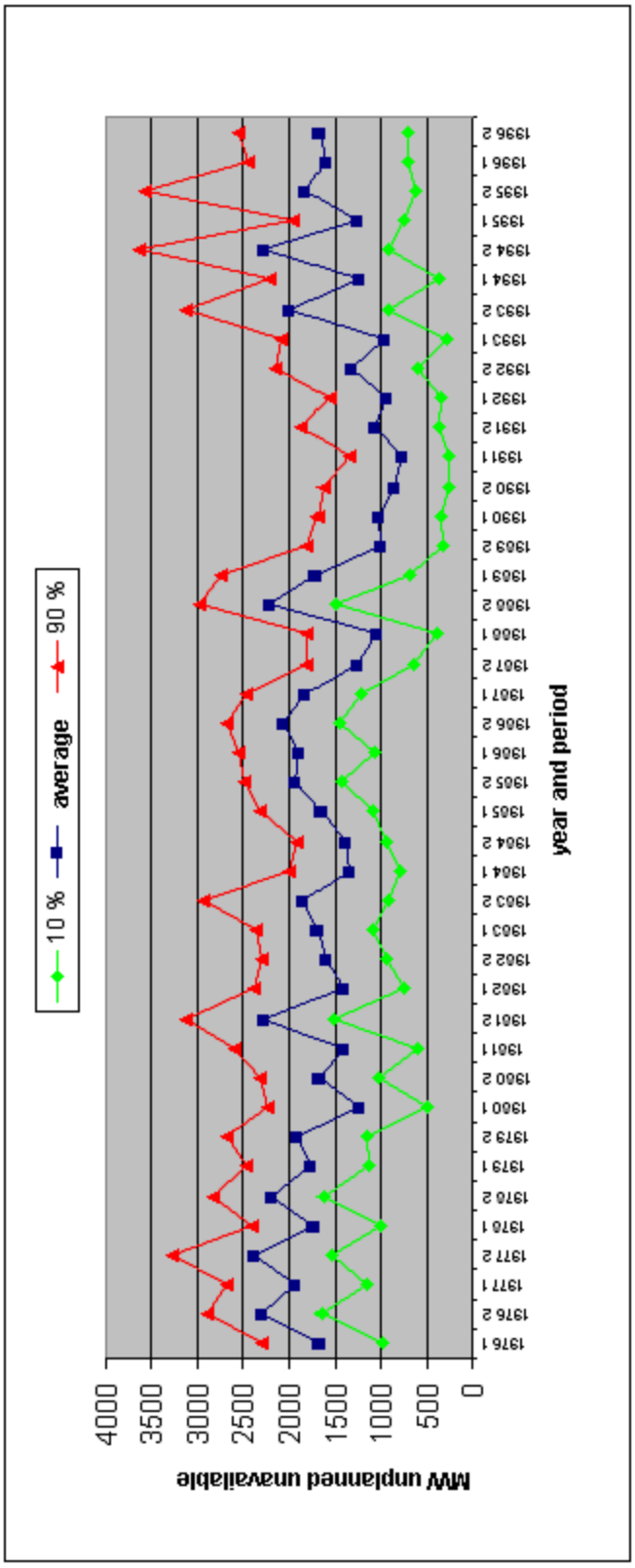


Figure 2. Total forced power unavailable from 1976 – 1996

Figure 2 shows the trend in total forced power unavailable up to 1996. The decrease after 1988 possibly is due to the benign effects of the Sep and KEMA R&D project to

systematically gather and analyze failure data at plants. The increase after 1991 possibly is the effect of taking over of companies and a change in mind set from a public utility to a commercial production company. Since, large amounts of data were made available to the general public (the so-called Transparency Data) but it can be shown that data quality has decreased with the amount of data increasing.

3. Development of demand

Any analysis of the security of supply must regard demand. The Dutch have up to 1998 presented the demand predictions in the so called Electricity Plan. Until liberalization the total installed power was coordinated by Sep. In the early days a yearly increase in % was assumed that resulted in very high (exponentially rising) demand curves as shown in figure 3. The figure shows that factual demand always has been lower the prognosticated central or total demand. This appears to be a general tendency also for many projects today. During liberalization installed power increased appreciably due to large coal fired plants. However, the economical crisis has led to stabilization of the peak demand at about 15.000 MW. Furthermore, due to the increase in wind and solar power in Germany being supplied to neighbouring countries over the grid, and the low coal price because of the US shale gas, overcapacity led electricity producing companies to mothballing of Dutch plants, even for district heating plants nowadays supplying their customers with auxiliary boiler heat only. It is to be expected that the peak demand will not be much higher in the near future unless the demand from electrical automobiles or other new users will substantially contribute to the peak demand.

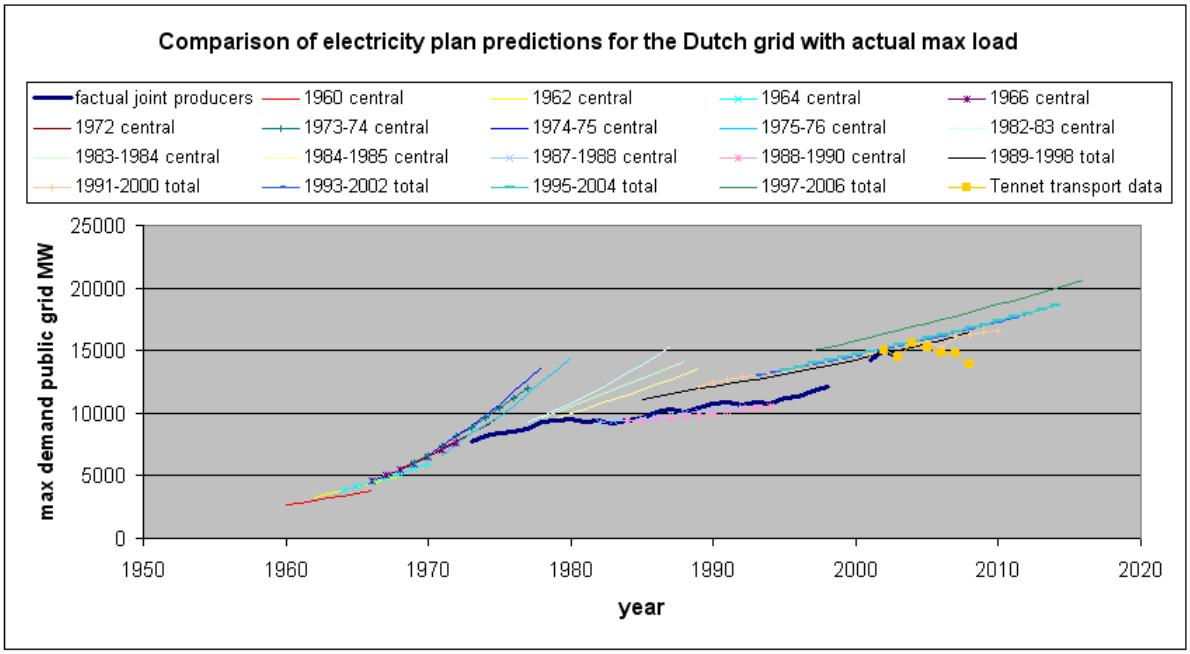


Figure 3. Historical peak demand prediction

4. Present production situation

In 2012 the Dutch "Energie Akkoord" between a large number of parties was ratified. Amongst the measures to take it was decided to decommissioning older coal fired power plants. In accordance with the "Akkoord" the units BS12 (392 MW), G-13(603 MW), A-81 (645 MW) and MV-1 and MV-2 (each 520 MW) were decommissioned. Targets for renewable energy and consumption reduction have not been met yet[56] .

The present generation situation as per Tennet publicly available files is shown in figure 4. In the Netherlands a system exists in which producers and grid operators sent the day-ahead power to Tennet in the so called Tprog with Tennet further scheduling generation and balancing the grid. Figure 4 shows the load duration curve for 2015. Peak demand is about 18000 MW. Small producers (say less than 50 MW) are not included as they are present on lower (< 110 kV) voltage grids. Base load, the minimum demand that is always to be produced centrally, is about 4000 MW. Evidently, there is a difference between scheduled and realized (actual) generation. Also, as figures 5 and 6 show, the difference between scheduled and Tprog becomes higher at low demands (for reasons unknown to the authors) and the difference between realized and scheduled ranges between -30 % and + 30 % (thought to be the effects of unavailability of plants, balancing, etc.)

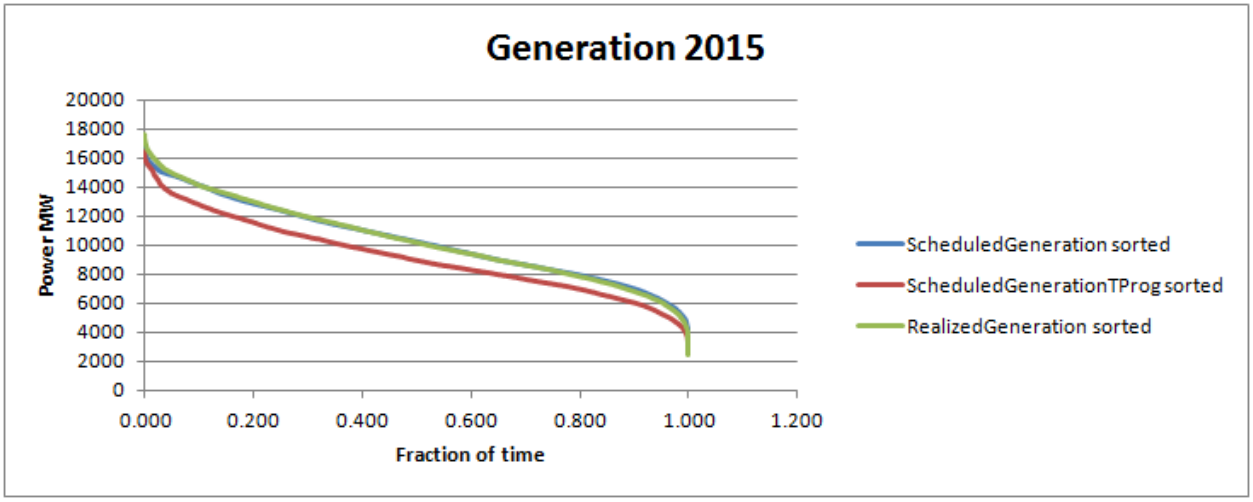


Figure 4. Load duration curve

[56] Progress report 2016

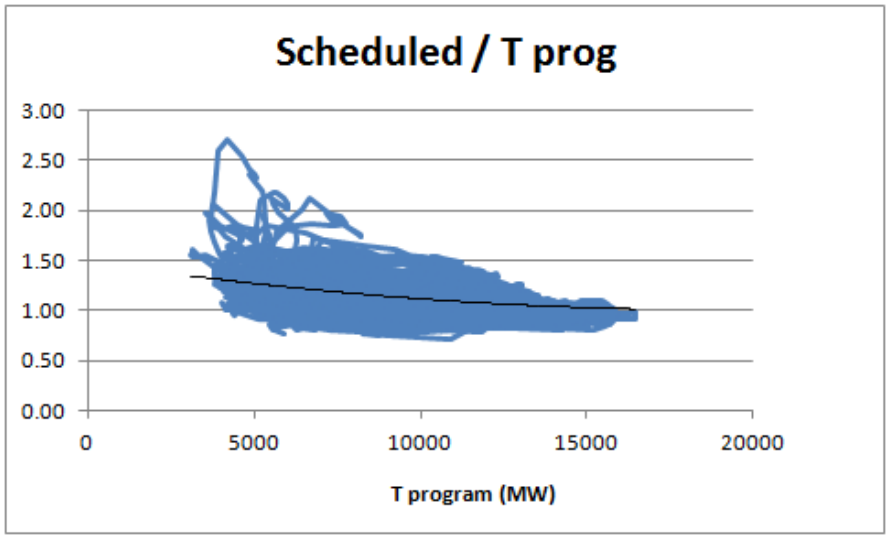


Figure 5. Difference scheduled generation and day-ahead production needs

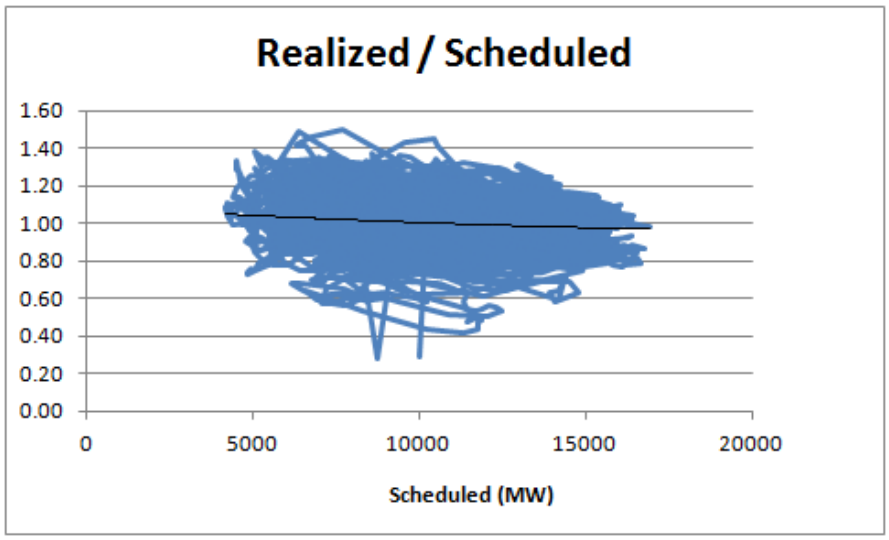


Figure 6. Difference realized and scheduled generation

By estimating a merit order for the generation of power based on expected variable production cost and projecting the cumulative power on the load duration curve, the fraction of time that a plant will be operating is derived. Coal power and gas from steel factories[57] have the lowest cost per MJ despite the lower efficiencies of these plants compared to modern combined cycles (< 40 % for midlife plants compared to >60 % for new combined cycles). In the Netherlands there is only one nuclear power plant that is expected to continue operation in base load. Implicit in this model is that when a plant operates, it operates at more or less constant name plate power. Nowadays even for base load this is not really the case and average power is significantly less than name plate. Also, maintenance costs may be larger for new gas turbine types having exotic materials

[57] Fired at a low cost price as flaring is on the only other option

compared to older gas turbines, gas contracts may result in gas prices different from market conditions[58] , etc.

If we look at operating time derived from the merit order in 2015 with old coal power still in operation, figure 7 shows that much gas power is in reserve and therefore was logically mothballed. With ageing coal out of operation and gas power mothballed according to figure 8 there appears to be a shortage of supply. With large gas power de-mothballed in figure 9, gas power will be in weekend stop (especially plant supplying district heating), cycling and in reserve. For the future, large wind parks will aid in installed power however it is well known that for each MW installed, on average only 30 % – 40 % is available as generated power is a function of wind speed to the power of 3 and wind speed is not a constant. Now, many smaller district heating combined cycle plants are expected not be started again being mothballed with none to minor conservation measures. Larger combined cycle plants were mothballed with optimized conservation measures for a long time. One wonders if strategic decision making to increase price may be applicable, however it takes time to de-mothball also (up to a year for deep mothballing) and prices are volatile.

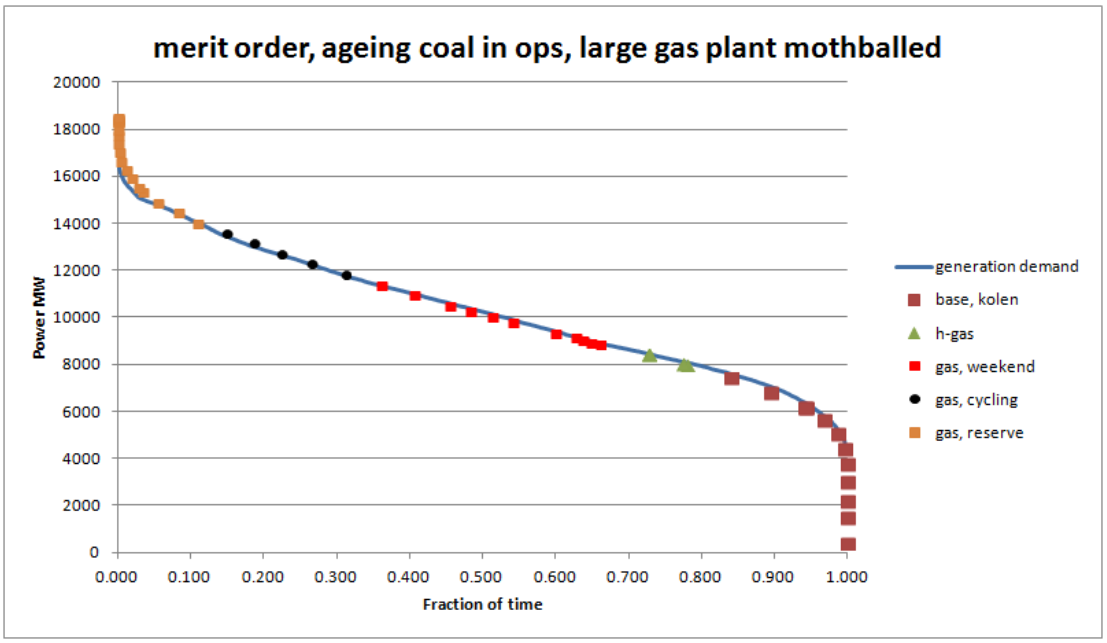


Figure 7. Fraction of time operating with ageing and new coal in operation, major gas plants mothballed

[58] For the Eems EC3-7 combined cycles a 1995 Sep-Statoil take-or-pay gas contract ("gas for the price of coal") was signed for a 20 year duration

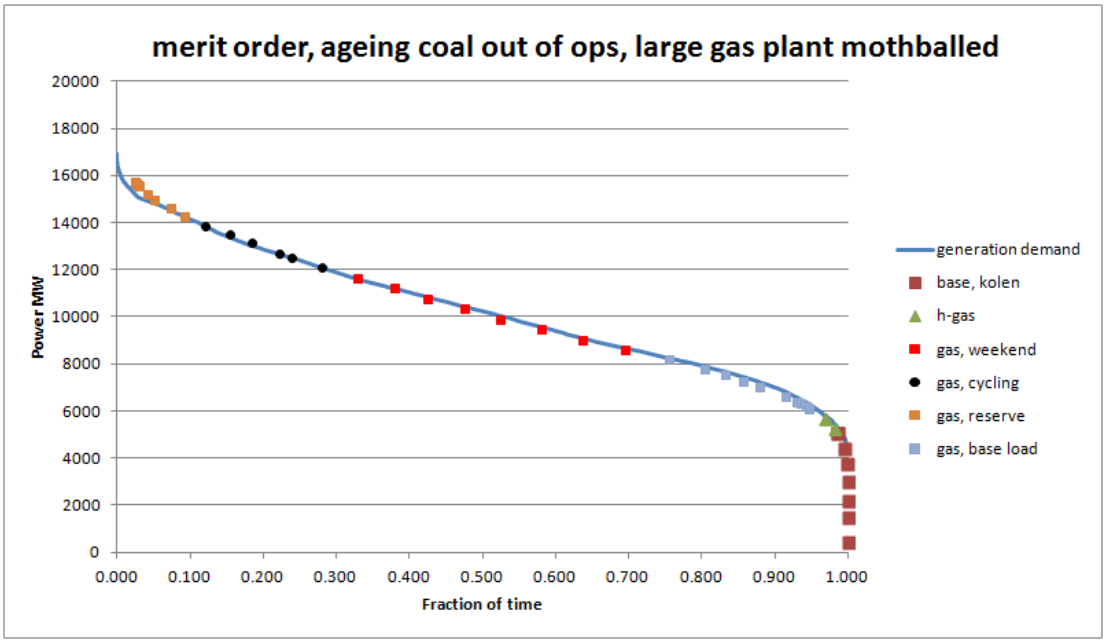


Figure 8. Fraction of time operating with ageing coal phased out, gas plant mothballed

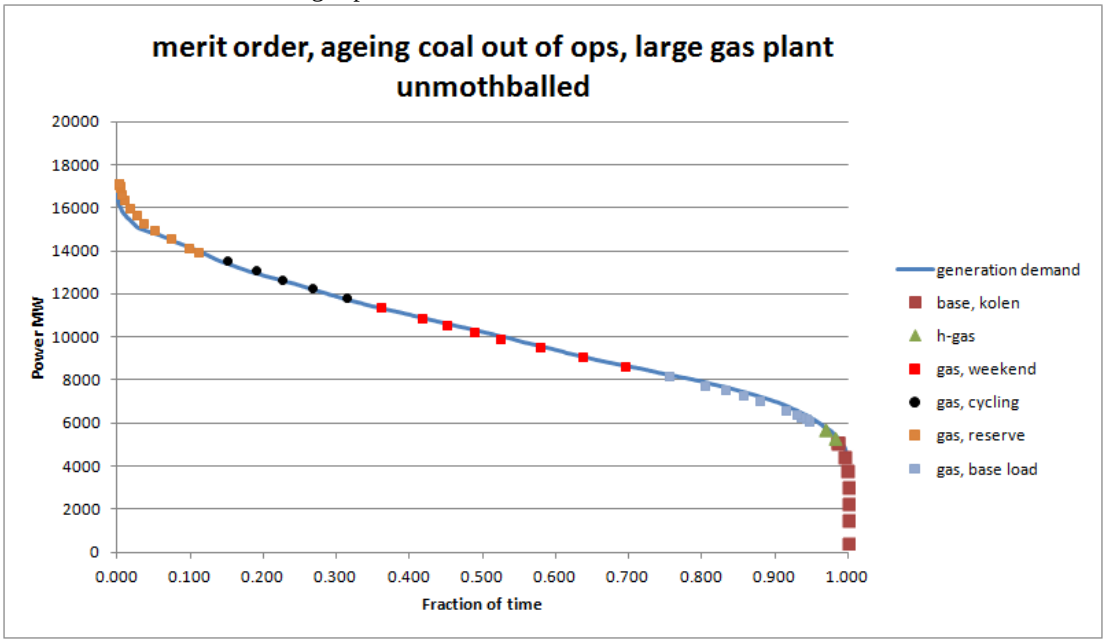


Figure 9. Fraction of time operating with ageing coal phased out, gas plant de-mothballed

5. Emergency power called for

Potential shortages have led to a market for emergency power. Figure 10 shows the development in the application of such power, generally for 1 – 2 hours per event at an average size of 80 – 150 MW. With sufficient installed power, the companies of plants having forced outages are able to buy replacement power limiting the duration of them having to pay for unbalance in the grid requiring Tennet to schedule and operate reserve power. In past times, during such periods prices increased to over 1000 EUR/MWhr, however over the years markets have become more stable. It is thought that this is also the

effect of grid connections with abroad. Figure 10 shows an increase in the application of emergency power as a function of time. According to Energia, for 2014 and 2015 Tennet explained this by the commissioning of new large coal fired power (Uniper, Engie, RWE) during which teething problems occurred. Yet, a light increase since 2008 seems to be present.

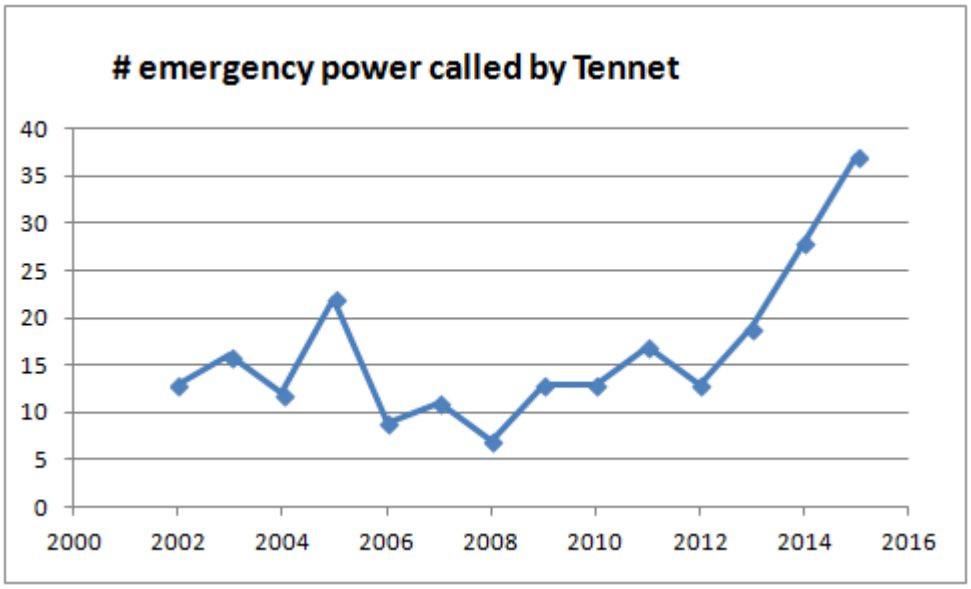


Figure 10. Application of emergency power per year

6. General model for forced unavailability of power units

Forced unavailability is partly caused by technical factors and partly by human factors. Examples of technical factors are teething problems with new types of equipment, cycling operation causing high stress on components and worsening of the condition of components by the processes that are inside (for example failures of GT coating, thick steam chests). Examples of human factors are management decisions with regard to minimal maintenance and cost reduction, effects of operator experience, etc.

If one looks at FOR as a time series, the series can be divided into so called High Impact Low Probability (HILP) failures and "normal" failures.

HILP failures are failures with duration of over a month, sometimes in the order of half a year. Such long duration failures occur once or twice over the life of a production unit. A description based on an average value per year is therefore not optimum, HILPs can result in sudden increases in the yearly average FOR of a power unit. HILP failures can occur at many components of a production unit, are difficult to predict and are therefore difficult to fight. HILP failures can be managed up to some extend by carrying out a Failure Mode Effect & Criticality Analysis (FMECA) and making sure that the actions in this FMECA to counteract the HILPs are taken. HILPs cannot be totally prevented however.

"Normal" failures for a power production unit show a typical bathtub curve as a function of time. After a period with teething troubles, the bottom of the bathtub should be in the order of less than 10 failures on a yearly basis and less than 10 % FOR at well performing

plant. Not all failures are full outages. Average repair times are in the order of 40 hrs. Now, while these values are averages, one strives for 0 failures and, without massive financial investments in the technical and human area, power plants in base load have shown 0 failures for 1 or 2 years in a row. It takes however human investments to arrive at such low values! Forced unavailability FOR of less than 5 % is considered a "good" value for coal fired plant, for combined cycles this should be even lower. Generally, the number of failures per year stays constant or is getting lower each year even up to 25 years of operation due to betterment projects, operator and maintenance actions unless minimum maintenance is applied or the way of operating is changed.

When one studies the pattern of failures, one finds that a fraction of the failures is of a repetitive nature. For some components, it can be shown that 30 % of the failures, with per definition moderate outage times, is on average repeated within 1 week.

Large differences in mean time between failures can occur between units that are contributable to differences in geometry and systems (older types of combustion chambers, teething problems with advanced Low Nox burners, etc.).

These influence factors are detailed in the next chapters. International as well as plant specific failure data allow modelling the patterns developing in the generation portfolio both from teething problems as well as ageing.

7. Planned unavailability

Maintenance costs, planned unavailability and forced unavailability (FOR) are not independent. Planned unavailability (overhauls, inspections) is carried out in order to limit and, if possible, eliminate FOR. It is possible to reduce both and find a cost minimum. Several sources of information show a (irregular) picture of both lower forced unavailability and lower planned unavailability (as a proxy for maintenance costs). Examples are shown in Figure 11.

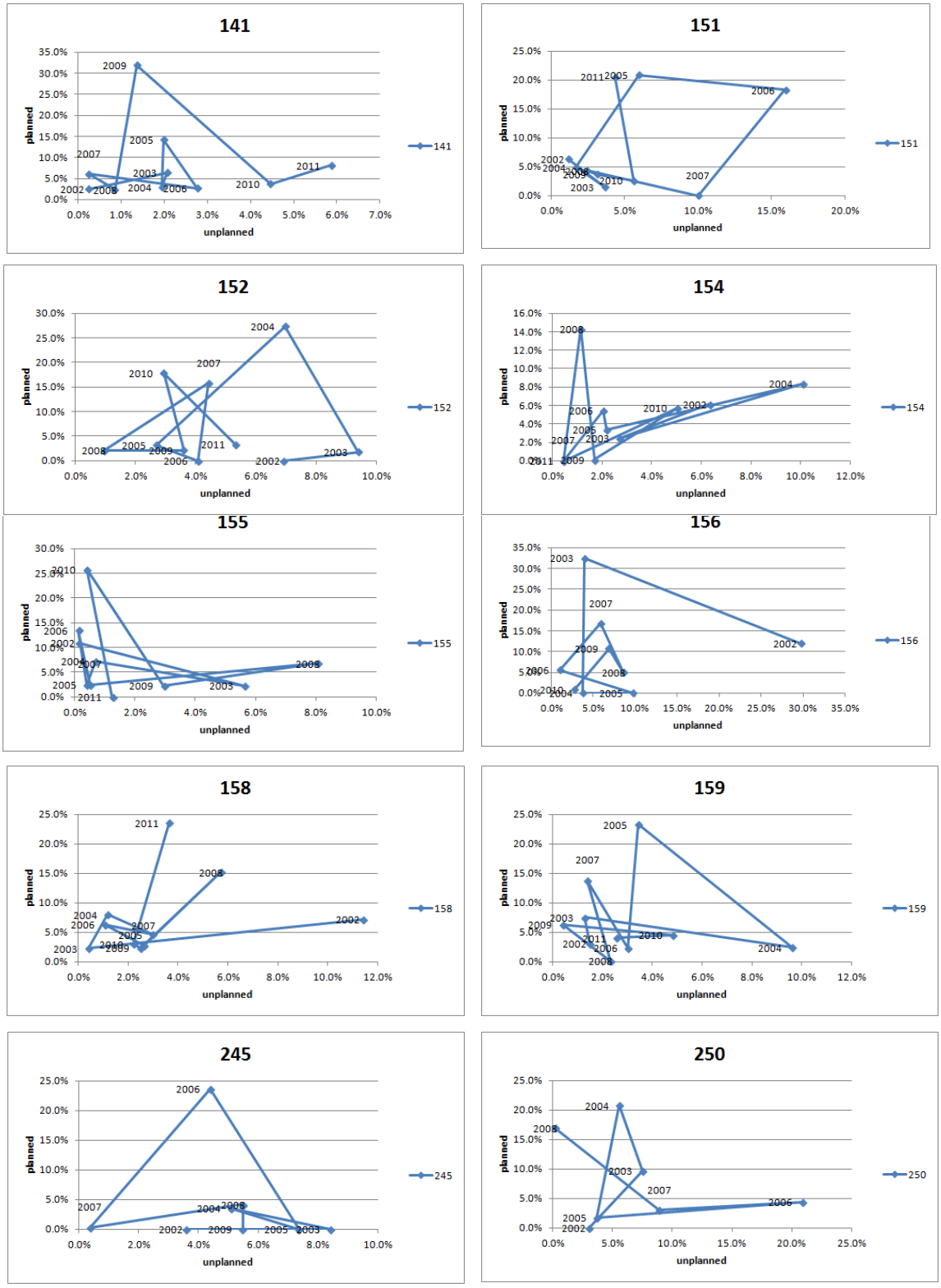


Figure 11. Semi-random walk for planned versus unplanned unavailability

The classical relation "less planned maintenance (planned unavailability) results in more unplanned maintenance (forced unavailability)" appears to be a generalization only. It is known however that without or with minimum maintenance in 3 – 5 years the forced unavailability will easily reach 20 – 30 %.

In the Sep period planned unavailability was scheduled in the summer window in such a way that LOLE[59] did not vary too much over the year. It is not known whether Tennet still coordinates in such a way. The author understands from German colleagues as well as from a Tennet meeting that a plan is to be submitted against which the grid operator may object.

In the simple load duration curve used to assess the fraction of time plants are operating it is assumed that planned unavailability should be taken into account for base load only, as cycling plants should be able to shift operation to periods with lower demand. Also for LOLE calculations based on simple modelling for weekend stop and cycling, planned unavailability can be shifted to favourable periods and is therefore not taken into account.

8. Modelling FOR to take account of differences in plant type

On the level of components given by 3 letters KKS-code (let's call this a super-component) the forced unavailability FOR can be described by a bathtub curve for the expected number of failures per operating hr together with an average downtime. The FOR will be different per phase (teething troubles, bottom of the curve, ageing period), as conceptually shown in figure 12. Super-components result in an effective description given the differences in failure characteristics:

1. The boiler especially that of a coal fired unit, especially when fans & auxiliaries are included, causes normally a significant number of failures for a production unit. However, not all failures are full outages. The heat recovery boiler of a STAG[60] plant normally has fewer failures than a conventional boiler.

2. A steam turbine normally has significantly less failures than a boiler, while planned maintenance is carried out at larger intervals. The failure parameters of a generator are similar to that of a steam turbine, but a generator failure compared to a steam turbine failure is expected to show a more gradual degradation behaviour before occurrence of the failure.

3. A gas turbine normally has the largest number of failures per unit operating time for a production unit. Especially for gas turbines, teething troubles in a new design may be present.

4. Steam turbines, generators and gas turbines (blade failures) are susceptible to HILP type of failures.

[59] LOLE: Loss of Load Expectation in hrs / year

[60] A STAG plant is built from one or more gas turbines, heat recovery boilers, a steam turbine and one or more generators. A conventional gas or coal fired plant is not equipped with a gas turbine except in a few cases for feedwater heating. The boiler is much larger and of other construction than that of a STAG

Super-component characteristics can be inserted into more detailed reliability analysis taking redundancy, common cause failures and failure mechanisms in account in order to model a power plant as precisely as possible. Reliability block diagrams as shown in figure 13 allow modelling for example differences in feedwater pump configuration, gas turbine configurations (1 GT, 2 GTs, effect of # of generators, etc.).

For (large) STAG plants the failure characteristics of a steam turbine and generator are not different from coal fired plants, however the boiler is certainly different. Therefore, if one notes an increased FOR for coal fired plants this certainly cannot be directly copied to STAG plants. As stated before, the majority of the portfolio in the Netherlands is STAG with aged coal plant phased out.

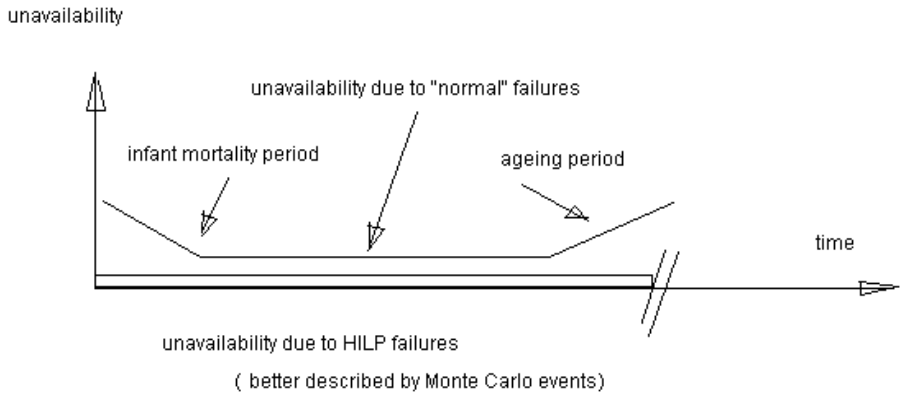


Figure 12. Bathtub curve for super-components

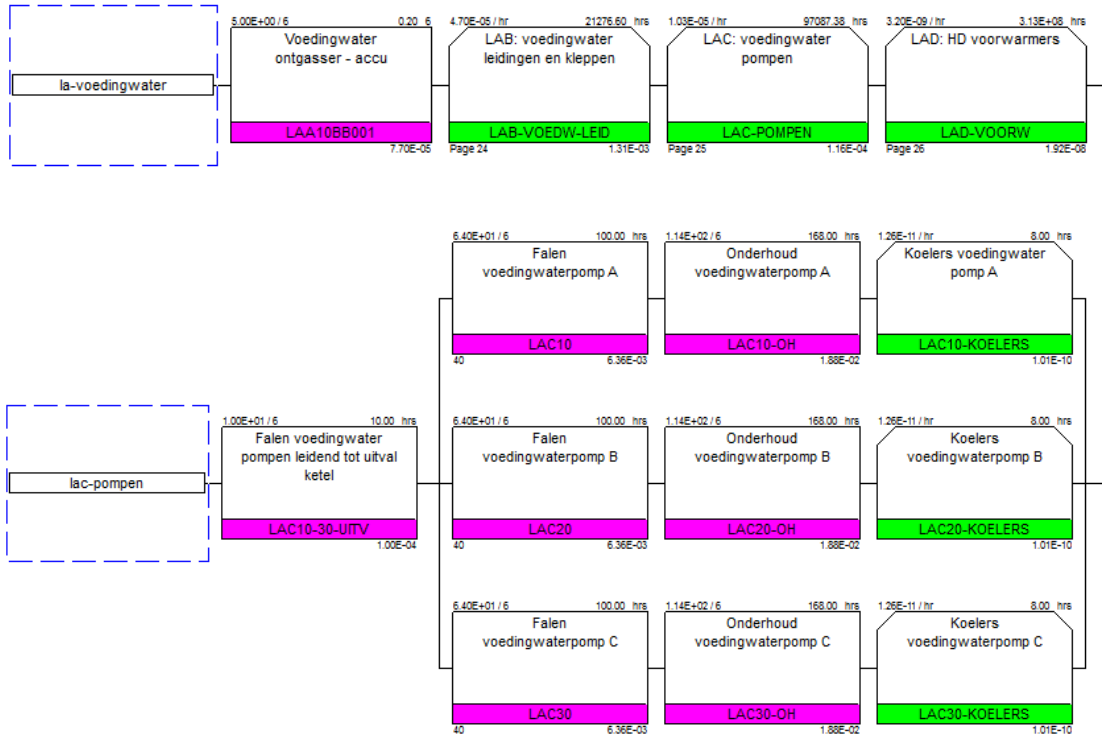


Figure 13. Part of detailed reliability block diagram for a power plant (feedwater system)

9. Operating conditions

A base-load unit is most easy to describe: operating hours are all calendar hours in which no planned availability or FOR as a result of full forced outages is present. The FOR description for non-base load plants is preferably extended by assessing the postponement of repairs to periods with lower unavailability costs, for instance the weekend or the night and not counting any repair hours outside the window of need of the plant. Postponement of repairs is especially applicable for cycling units although especially for new plant postponement is less than for old plant due to automatic tripping. However, cycling induces additional loads on components (for instance thermal fatigue) causing a higher number of failures per operating hour. Also, a failure probability per start should be included, the effect of which for a base load unit on a yearly basis is negligible since base-load plant only starts after an overhaul or after a FOR event. For cycling units with sufficient operating hours, the effect of calendar time (for instance due to corrosion) on failures is expected to be minor compared to the effect of operating time (for instance due to high temperature creep). However, it has already been found that there is a change in components that are dominant in FOR (for instance dominancy of LP preheaters was found for one plant operating as a reserve plant, which is somewhat unusual).

Forced unavailability can be split into FOR during which the unit is necessary and FOR during which the unit is not necessary given its windows of opportunity. Billington and Allan (1984) already presented the IEEE 4 state analytical model on the basis of Markov analysis. One is inclined to use Monte Carlo simulation given the ease in modeling and

the ability to see the spread in values next to the average. However an analytical model is decidedly faster than Monte Carlo although it usually only shows averages. Using the IEEE 4 state model as per chapter 14, the modelling parameters are extended with operating hours per year, starts per year and only a fraction of repair time which results in unavailability costs. By assuming the different failure mechanisms to be dominantly dependant either on starts, operating time, calendar time or combinations, one arrives at FOR as a function of operating conditions.

10. Life extension

It has become customary to operate old plants longer than say 25 years as there is margin in the technical life of components and because power companies try to avoid large investments due to uncertain market circumstances. Experience has shown that with modest investments one can operate such plants longer without excessive rise of neither unavailability nor safety consequences. Failure data analysis shows which components to investigate when intending to operate a power plant longer than say 25 years.

On the basis of Reliability Block diagrams (RBD), the failure rate, average repair time and forced unavailability was calculated for sister plants A1 and A2 for a set of Life Extension investment scenarios. The RBD's were based on P&I diagrams, interviews and failure data gathered since the start of operation of these plants. A reference model for the 'bottom of the bathtub curve" with historic failure data resembled realized forced unavailability well, with a low 2.5 % equivalent forced unavailability (EFOR)[61]. A model with historical failures extrapolated to the future without investment indicated EFOR in the range of 24 %. The reference model EFOR as well as historic EFOR is shown in figure 14. Please note the appearance of High Impact Low Probability (HILP) failures with the reference model only showing the average expected EFOR. Over the years before the investment scenarios, FOR increased due to minimal maintenance in combination with changed operation (cycling not designed for) indicating the importance of these influence factors.

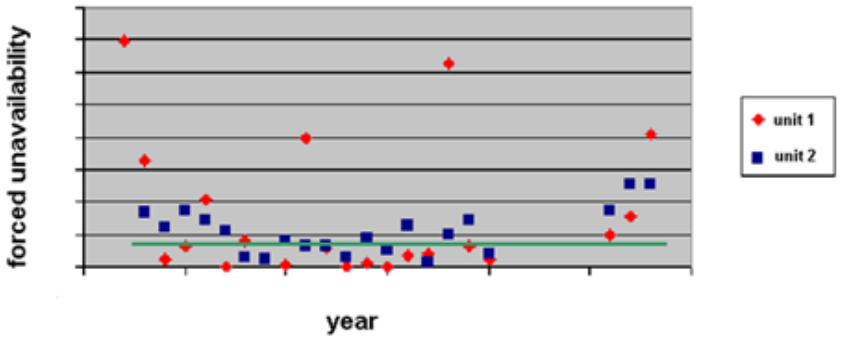


Figure 14. Reference model compared with Unit A1 and A2 historic realization

Failure data were derived from plant records over a period of 23 years as well as from the VGB KISSY database and discussed with plant experts. Components not present in either

[61] The gap in the data in figure 14 is caused by a management decision for this plant to no longer to gather data as end-of-life appeared imminent

database were estimated using DEKRA databases. Trend analysis of G1 and G2 unavailability records showed that for these plants only for a few components ageing in terms of an increase in the number of failures per unit time was present. Minimal maintenance was, despite the age of the plant, certainly no applied due to the need for the DH grid.

The unplanned forced unavailability FOR as a function of time was forecasted for the scenarios 1) DO NOTHING on LTE but continue with maintenance as usual and 2) carry out LTE as per planned measures. The result is shown in figure 15, clearly showing the time behaviour both in the historical data as well in the modelling.

The results show that ageing can be efficiently counteracted by investment in certain components. It was however assumed that such investment leaves only 10 % remaining failures for these components.

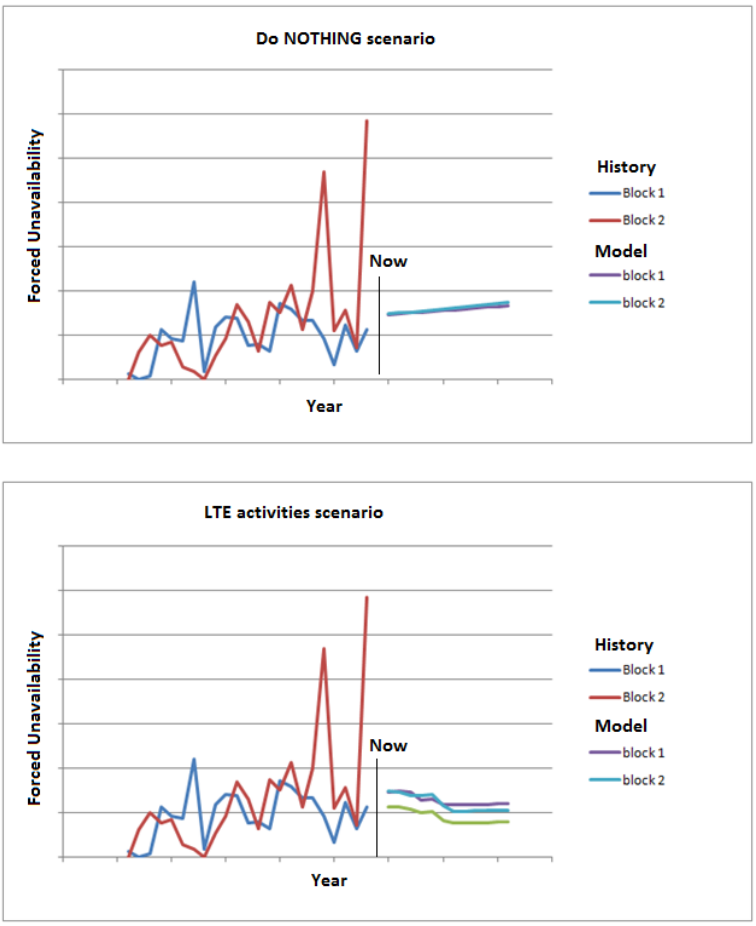


Figure 16. Result for yearly expected forced unavailability as a function of time

11. Failure patterns in practice

Finally, to make clear that during the life phase of plants typical patterns are existing in practice, figures 16-21 show some theses failure patterns for 3 power plants as a function

of time from the start of operating in the 70-ties until decommissioning. It is thought that such patterns will also exist today. All plants are combined cycles (hot windbox repowering) from the same company with well known historical information. Units Y1 and Y2 are identical with 2 Frame Type gas turbines each. Unit X has 1 larger Frame Type gas turbine. The figures show clearly:

a) teething problems for all plants after newbuilding (figure 16)

b) teething problems for all plants after the hot windbox repowering (figure 17)

c) High Impact Low Probability problems HILP after a design error (figure 18)

d) High Impact Low Probability problems HILP also without this error, for example due to GT blade problems (figure 19)

e) The effects of cycling unit X, units Y1 and Y2 are not cycling. Unit X is also subject to minimal maintenance (figure 20)

f) All units have less operating hours per year and show less failures because of the low hours (figure 21)

It would be interesting to see if teething problems are present after (long duration) mothballing. Reasons could be corrosion at unexpected places or difficulties finding an experienced crew.

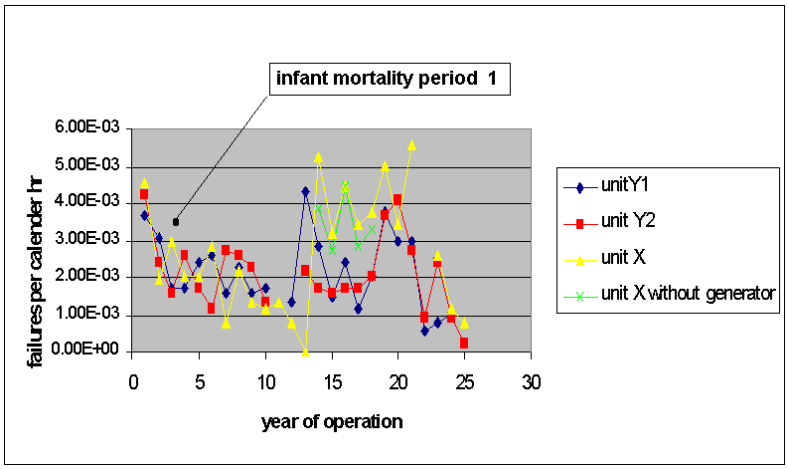


Figure 16. Unavailability of units: teething problems

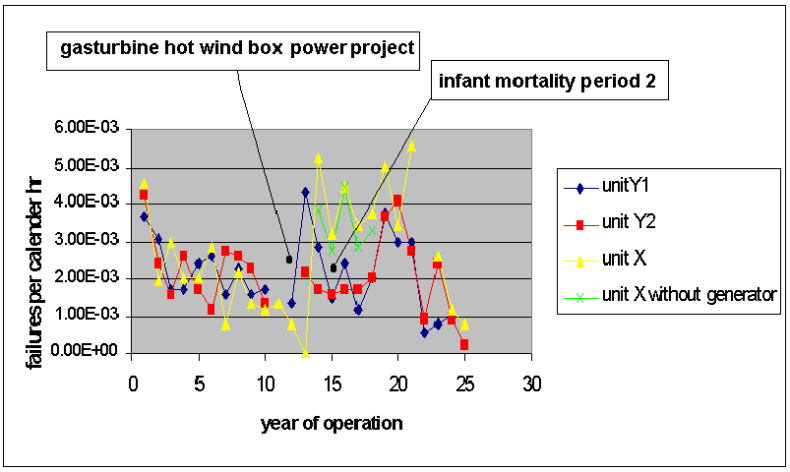


Figure 17. Unavailability of units: teething problems

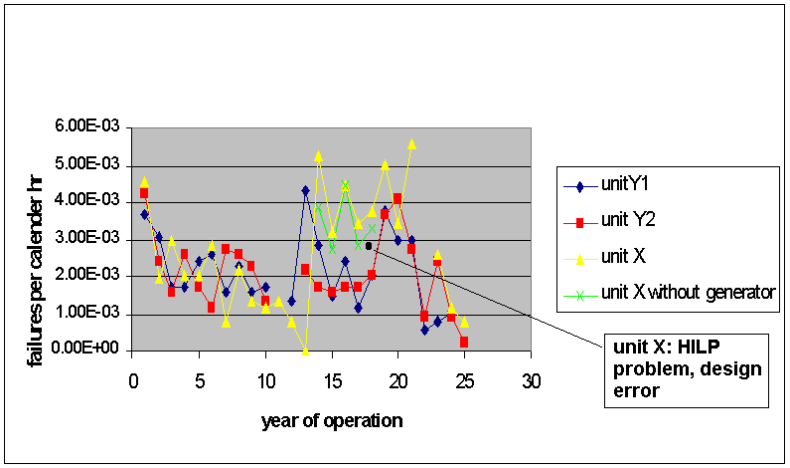


Figure 18. Unavailability of units: HILP design error

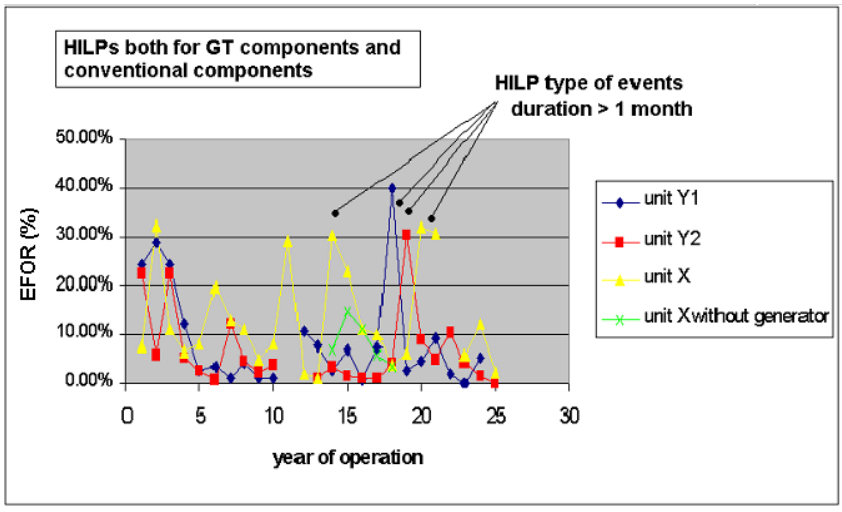


Figure 19. Unavailability of units: HILP failures

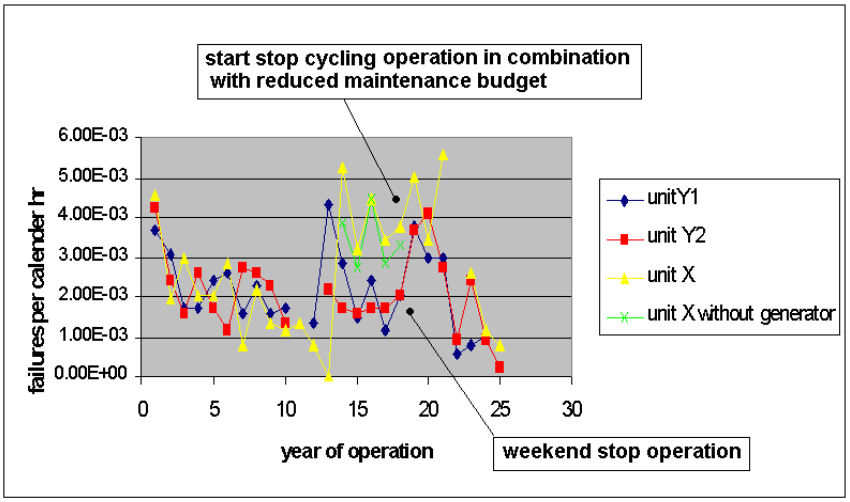


Figure 20. Unavailability of units: cycling operation and minimal maintenance

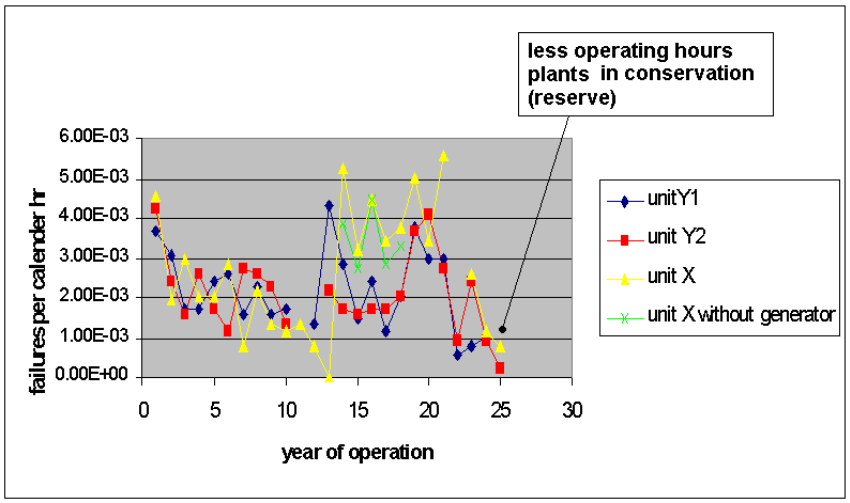


Figure 21. Unavailability of units: reserve

12. VGB KISSY database availability module

VGB operates 2 databases to gather the unavailabilities of power plants, known as KISSY = Kraftwerksinformationssystem. Part A, the so-called Availability module contains the planned and unplanned unavailabilities, fraction of the time operating, etc. for a large number of plants on a yearly basis. In the last decade many international plants entered the module therefore it should not be regarded as German only. Part B, the so-called Unavailability module contains the planned and unplanned unavailability as events with KKS = Kraftwerk-Kennzeichensystem component coding. Evidently for the plants in module B total unavailability can be calculated and compared with module A if present there also. As not every plant due to age or because of internal company coding uses KKS, module B contains fewer plants and relatively has a larger number of German plants. Both modules are operated with stringent coding instructions for example to define planned versus unplanned (planned if known 4 weeks before the outage). The different plants in

different countries involved can lead to different failure patterns and may explain that the A module clearly shows a systematic increase in forced unavailability in time while the B module does not show such systematic increase clearly.

For the paper we have used the most recent (2016) type A data from the yearly report that is available from VGB. Figure 22 shows clearly that on average the forced unavailability, especially the non-postponable part, has risen from an all-time low in 1996-1997 of 3 % to values above 10 % in 2015-2016.

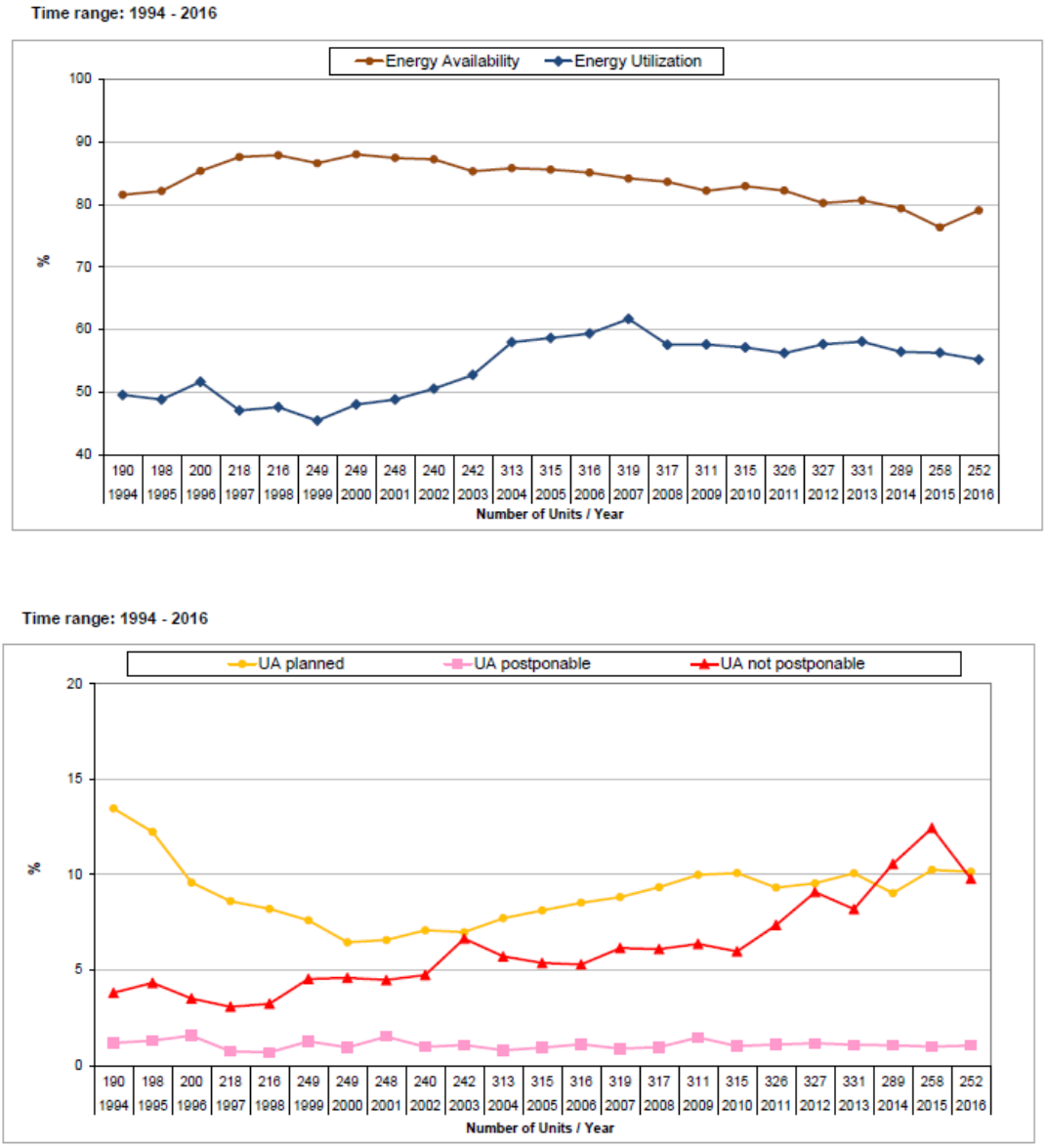


Figure 22. VGB KISSY availability data

The same pattern appears to be present for other subsets of the database, especially for the coal fired plant "workhorses " in the 200 – 600 MW size. However, for the Dutch portfolio, combined cycles are important as they supply mid—merit order power. The

KISSY availability data are given in figure 23 also for combined cycles. The forced unavailability rises from about 2 % in 2013 to about 7 % in 2015. The value of 9 % in 2009 is caused by some outage extensions, which under the VGB KISSY definitions are unplanned (if known less than 4 weeks before the actual outage). The problem here is that the number of plants in the category combined cycle is international and diverse[62], therefore the agregate data should not be used without care.

13. VGB KISSY database unavailability module

Using data from the part B unavailability module, a Research Project[63] was carried out in 2014 to directly arrive at reliability indicators using the layout of every plant in the database as for instance the failure rate = failures per operating hour for generators should be corrected for the number of generators in the plant, which is not necessarily 1 in a Combined cycle plant. The data from this Research Project were used to assess ageing in the components of STAGs based on KKS-coding (Kraftwerk- Kennzeichensystem). The level of detail shown in figure 24 is 2 letters KKS pinpointing major systems[64]. Each data point in figure 24 generally is representing 10 years of operation. The figure shows:

MB = gas turbine. Trend shows ageing, however it is known that the plants that were over 20 years had difficulty in acquiring the spare parts for the aero-derivative gas turbines. From other projects it is known that given spare parts and proper maintenance, no ageing should be visible in the data

MK= generator. Trend shows ageing however this is fully caused by a HILP type failure at one of the plants (2100 hrs outage).

HA = heat recovery boiler. Trend shows ageing with an appreciable amount of spread.

MA = steam turbine including condenser. Trend shows ageing, again with an appreciable amount of spread.

[62] Plants that have a gas turbine in the feedwater system, hot windbox repowerings and STAG plants all are called combined cycles

[63] Reliability Indicators with KISSY – VGB Research Project 361, ISBN 978-3-86875-751-4

[64] We are able to calculate failure rate, average repair time, unavailability, postponement, trips, etc. to a level of 3 letters KKS which is sufficient to consistently model differences between plants

B.1.1.5 Combined cycle units, 200 MW ≤ nominal capacity < 600 MW
(47 units, AT, DE, FR, LV, NL, PT)

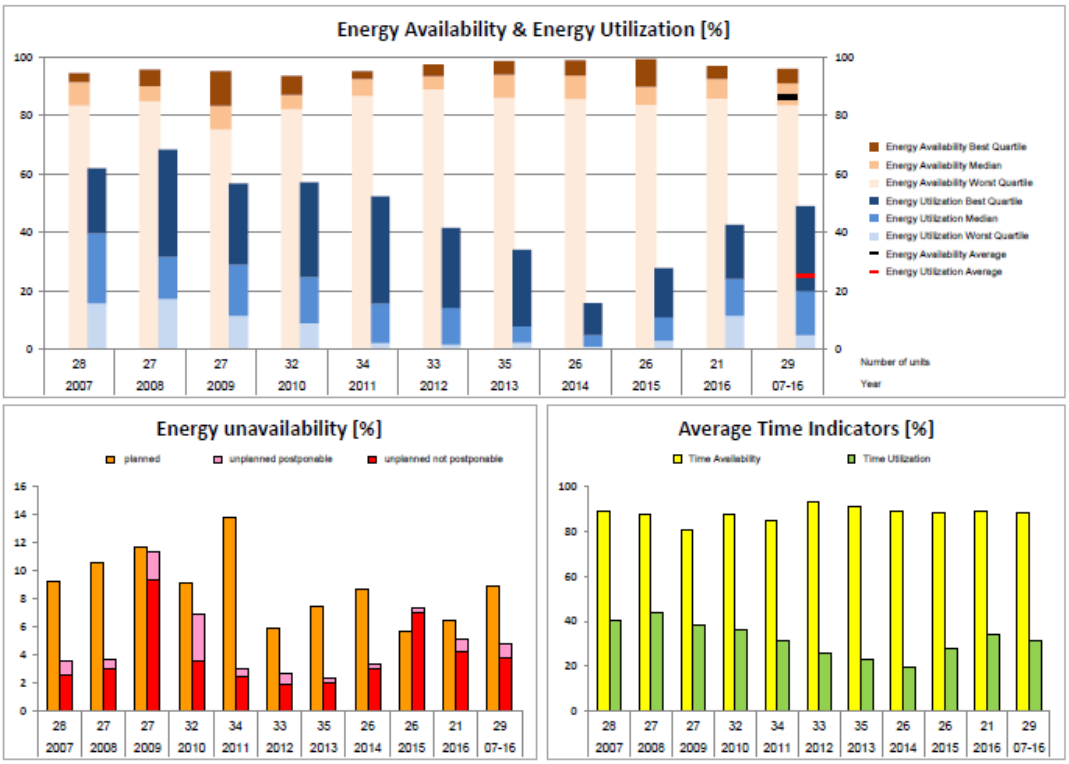


Figure 23. KISSY Combined cycle data

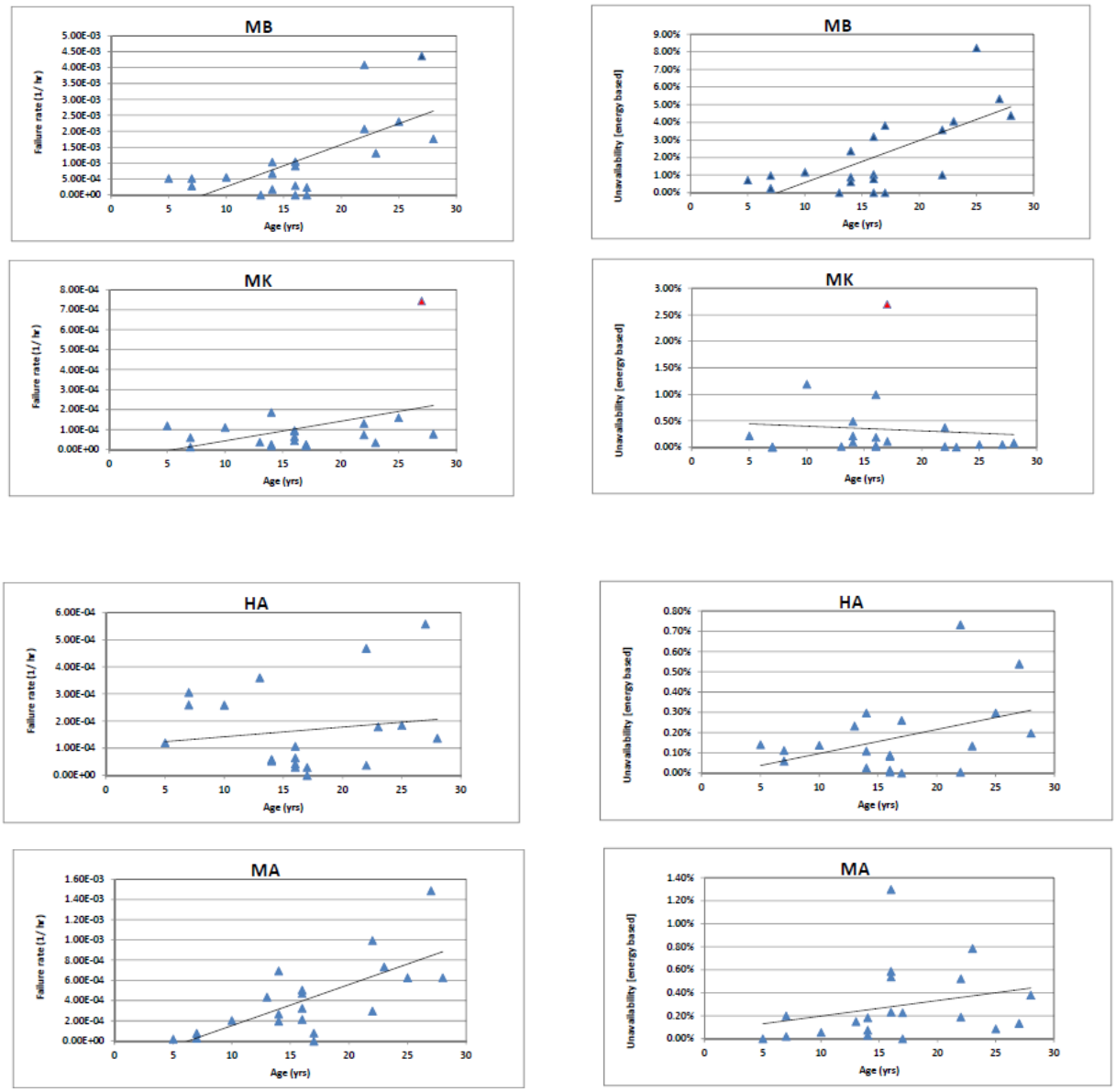


Figure24. Failure rate (per operating hour) and forced unavailability (calendar hours)

14. IEEE 4-state model

It is customary to present forced unavailability on the basis of calendar hours. However forced unavailability should be defined in such a way that it is the probability that the plant is not there when needed. A first approximation is a simple 2-state model (the plant is either operating or unavailable) however for plants in reserve this is too conservative. The IEEE 4-state model already given in Billington and Allan (1984) [65] is more

[65] Reliability Evaluation of Power Systems, Billington & Allan, 1984

appropriate however it needs as additional parameters the frequency per hr that the plant is needed and average duration of that need in order to assess the fraction of repair time that is outside the period of need.

2 - state model

FOR $= \lambda * \theta / (1 + \lambda * \theta)$

λ = failure rate (/ operating hr)

MTBF $= 1/\lambda$ = mean time between failures

θ = average repair duration (calendar hr)

4 - state model

FOR = f * FOT / (ST + f * FOT)

f $= (1/\theta + 1/T) / (1/D + 1/\theta + 1/T)$

θ = average repair duration (calendar hr)

D = average demand duration (calender hr)

T = average reserve shutdown between demands (calender hr)

FOT = total forced outage time (calender hr)

ST = operating time (calender hr)

A series of test calculations was carried out with the KISSY plants present in the VGB Research Project 361 data to estimate the effect. The results show that the difference between forced unavailability on a calendar time basis and on operating time basis in either the 2 or 4 state model is important for Combi plants. The STAGs within the total subset of Combi plants are comparable to the STAGs in the Dutch portfolio that will operate in cycling mode more and more as the result of renewable generation in the grid. It was proposed to VGB to further analyse the 4-state model for the large number of plants in the KISSY Availability database (type A), a decision on this proposal is pending. As shown in figure 25, evidently the difference between the models disappears for base load and is the most important for reserve type single cycle gas turbines.

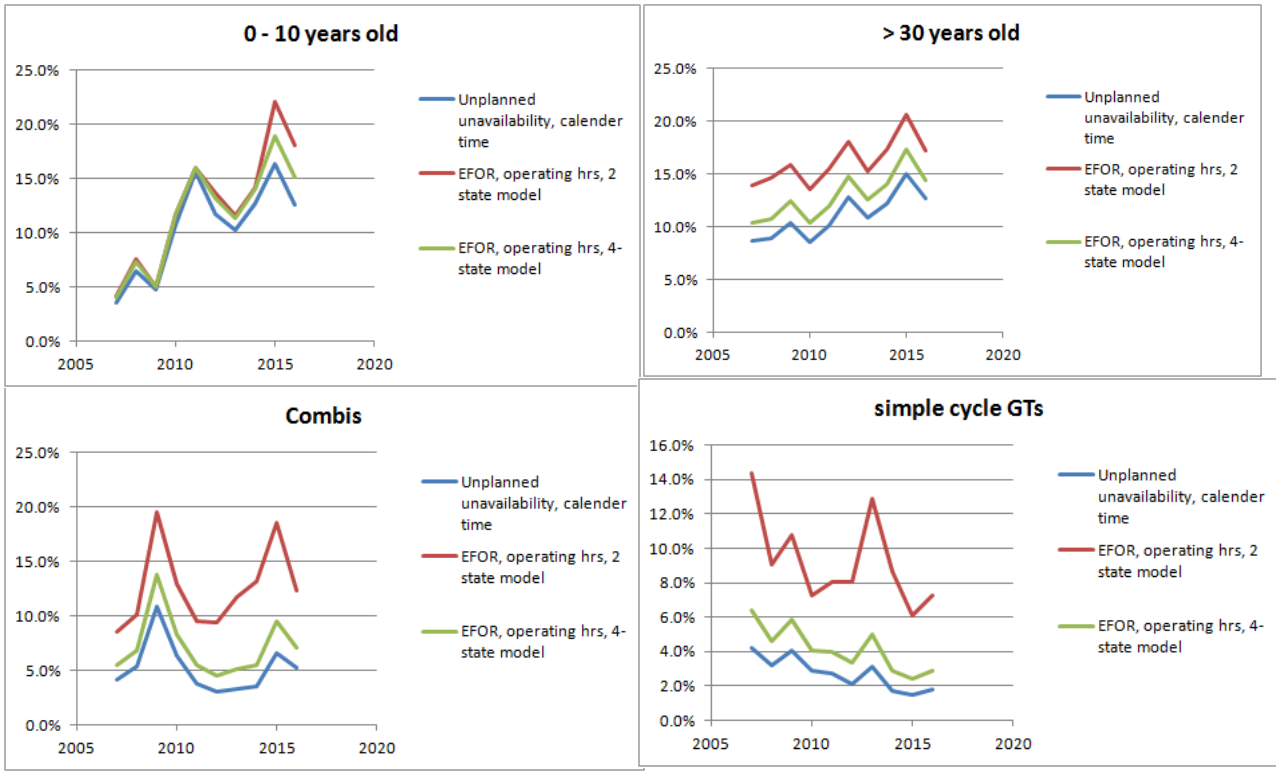


Figure 25. Four state versus two state model

15. Loss of load expectation

Again, when too many power plants are forced unavailable, load has to be reduced. If not, cascade effects may result in blackouts.

In Billington and Allan (1984) a method (originally from Schenk and Rau) is given based on a Fourier transform method to calculate the loss of load expectation (LOLE). This method appears to be valid when the distribution of capacity outages can be approximated by a normal distribution. For the Dutch system with 50 + production units over the period 1978 -1986 this appeared to be the case despite varying sizes of production units between about 15 MW and about 700 MW. The distribution of power plant size however is not a normal distribution, with average size about 240 MW but with some large units > 600 MW. It is quite common that both average size and size of largest power plants increases over time therefore it is expected that the normality requirement is still met today.

	B	C	D	E
90			LOLE	
91	**Situation**	**reserve factor**	include planned unavailable for base load	forced unavailability only
92	aged coal fred units IN, large combined cycle IN, typical forced unavailability	1.26	0.005	neglectable
93	aged coal fred units IN, large combined cycle MOTHBALLED, LARGE forced unavailability	1.17	182	121
94	aged coal fred units IN, large combined cycle MOTHBALLED, typical forced unavailability	1.17	1.5	neglectable
95	aged coal fred units OUT, large combined cycle IN, typical forced unavailability	1.09	2.8	neglectable
96	aged coal fred units OUT, large combined cycle IN, LARGE forced unavailability	1.09	229	38
97	aged coal fred units OUT, large combined cycle MOTHBALLED, typical forced unavailability	1.00	60	1.8

Figure 26. Results of simple LOLE calculations

The results of the LOLE calculations are shown in figure 26. The relevant results are given in column E of figure 26 with only forced unavailability taken into account. The results indicate that as long as the forced unavailability of the power plants stays as per typical historical values, LOLE is less than the 4 hrs per hr that has been defined as acceptable by Tennet. However, when large forced unavailability occurs (for example due to economic conditions as per figure 27), the LOLE rises appreciably. The results in column D indicate that it is really necessary to centrally coordinate planned outages in order to keep LOLE to acceptable values.

What does a LOLE of 4 hrs per year really mean? Essentially it is a probability having both a frequency component as well as a duration component. An average frequency of once per 10 years with an average duration of 40 hrs leads to the same LOLE as a each year on average 4 yrs or 4 times per year 1 hr. Evidently the last LOLE is less acceptable. However, the frequency is not defined by Tennet. When such an acceptable frequency would be defined we would like to refer to the age-old "100 year wave" that the old shipbuilders used as input to define the strength of their ships on. The expected frequency of blackouts should be such that during a professional career one should at maximum have had this experience once. Please note that a nuclear incident target frequency is defined as once per hundred thousand years up to once in a million years per plant operating year which is much lower.

16. PLEXOS calculations

As suggested by DEKRA, DNV GL has tentatively investigated the impact of increased forced outage rate on the generation adequacy of the Netherlands using its PLEXOS model for the European electricity market model for single deterministic simulation runs of 2018.

The European market model contains detailed representation of the generation, transmission, demand and reserves. Generation capacities in the core countries are modelled on individual basis with detailed techno-economic characteristics (e.g. flexibility parameters, combined heat and power characteristics, bid curves, renewable availability profiles). Renewable generation takes volatility into account through the use of historical or re-analysed time-series of e.g. wind-speeds and solar-irradiation data for different locations. It contains a flexible division of detailed core countries and an aggregated representation of remaining European countries.

Two market simulations have been performed: one with the traditional forced outage fraction assumptions and one with higher forced outage fractions. The combined cycles already mothballed in 2017, based on the so-called "Transparancy" data, were kept mothballed. All aged coal fired plants in the Netherlands are out of operation in 2018. Based on these two simulations, a comparison is made between the hourly reserve margins. The forced outage fractions used are given in figure 27.

	Traditional forced outage rate	High forced outage rate
Old coal (from before 1995)	7%	16%
New coal	7%	13%
Lignite	7%	7.5%
Nuclear	1%	10%
CCGT	2%	8%
GT	2%	4%

Figure 27. Force outage fractions used in the PLEXOS runs

The hourly reserve margin is defined as the total hourly available generation capacity minus the hourly electricity demand. The total hourly available generation capacity includes wind and solar-PV that is adjusted for their availability, but excludes generation capacity that is in maintenance or in forced outage event. The available generation capacity does not distinguish between dispatched capacity and not-dispatched capacity. The results for the hourly reserve margin are given in figure 28.

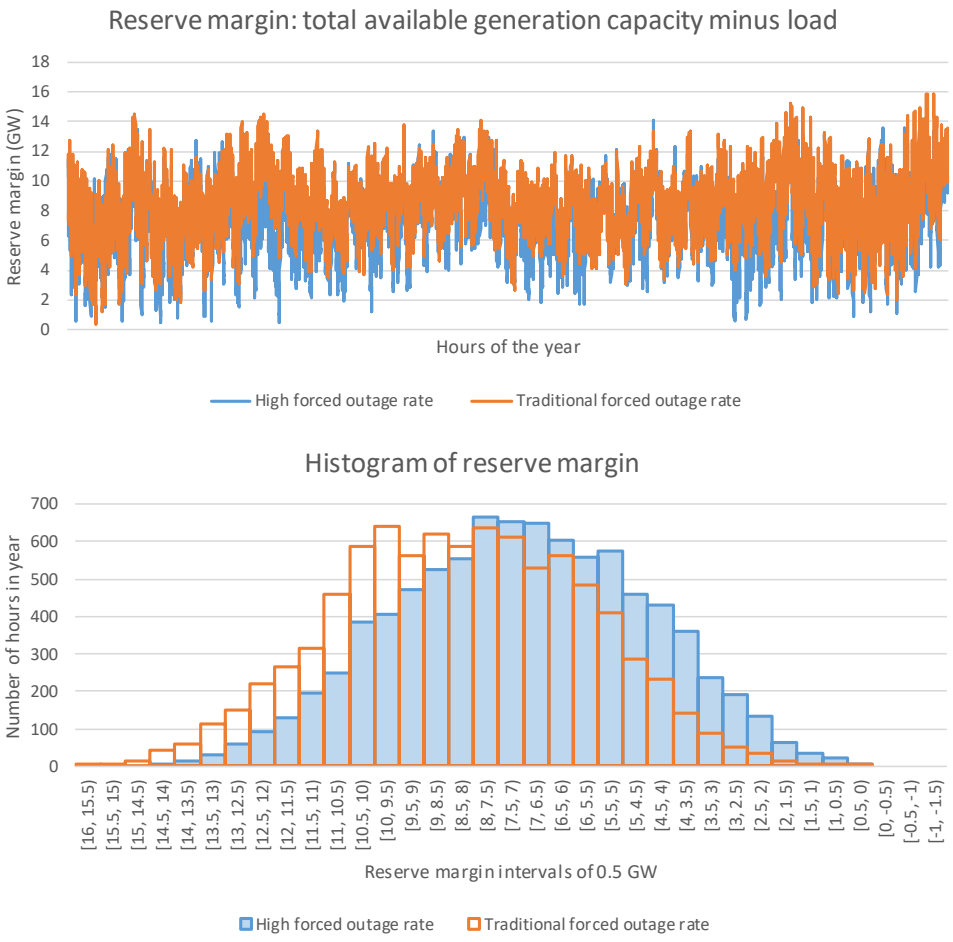


Figure 28. Hourly reserve margin in PLEXOS runs

In addition, the impact on the import-export balance of the Netherlands and the amount of hours with unserved energy is assessed.

Taking into account the higher forced outage rate[66], reduces the total available capacity by on average 800 MW. This lower total available capacity reduces the hourly reserve margin. In the case of higher forced outage rates, the number of hours with 1GW or less increased from 2 hours to 26 hours. Note that in both cases of traditional and higher forced outage rates, there occurred no hours with unserved energy in the Netherlands in the single deterministic run. Incorporating a higher forced outage rate Europe-wide, reduces the net import position of the Netherlands by 7 TWh (30%), that is: the Dutch are more dependent on the grid connection to abroad that however that is able to deliver less.

The exact number of hours depends on the maintenance schedules, timing of forced outage events and renewable patterns. Forced outage events preferably are calculated using a

[66] Forced outage rate actually is not a rate (frequency) but the equivalent fraction of time a plant is unavailable weighing deratings with the power not available

large number of Monte Carlo runs, however as a single deterministic run for the European model already takes about 4 hrs, for the present modelling this was not feasible.

.

17. Comparison with Tennet's Monitoring report

Each year since 2006 Tennet presents the so called monitoring report that shows the risk on insufficient power to meet demand. The report available for the paper is the 2016 report with 2017 in the making but not yet available.

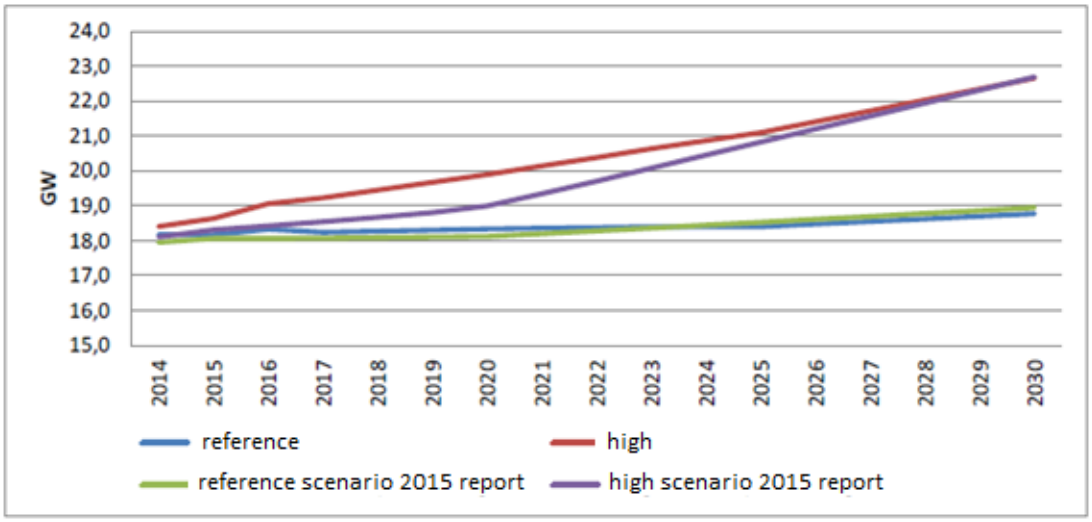


Figure 29. Peak demand in Tennet's 2016 monitoring report

The reference peak demand scenario for 2017 or 2018 in the report is about 18 GW with a more or less linear increase of 1.8 % on a yearly basis. The calculations in chapter 15 are in accordance with this peak demand.

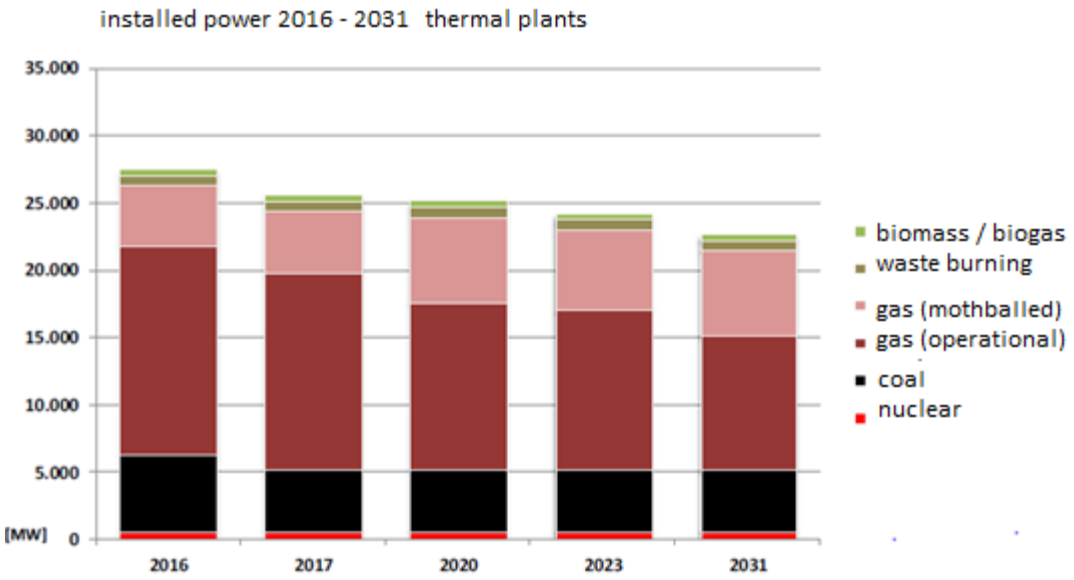


Figure 30. Installed power in Tennet's 2016 Monitoring report

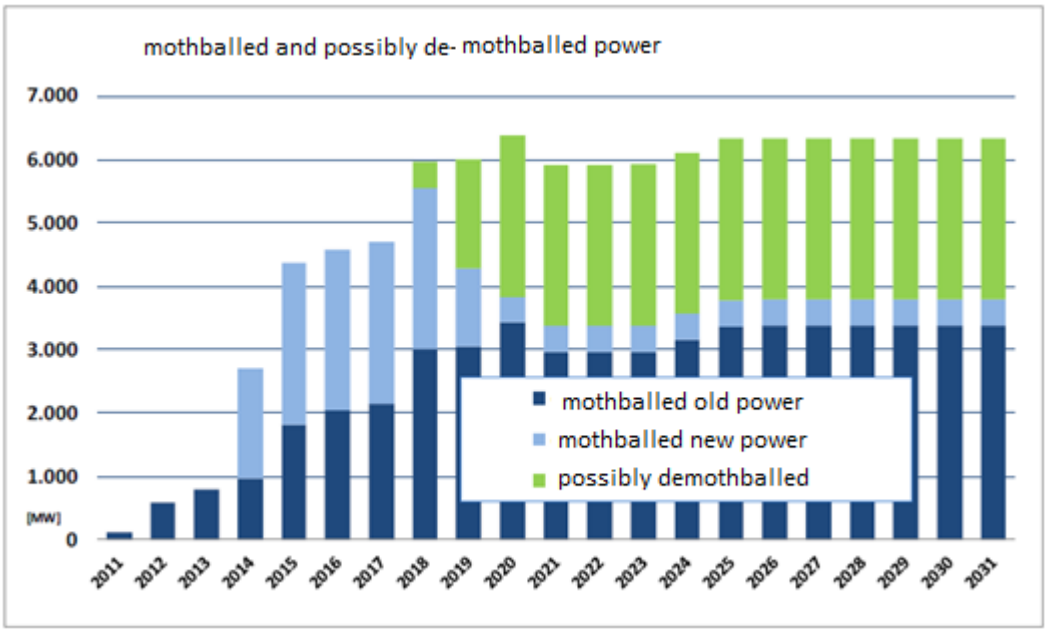


Figure 31. Mothballed power in Tennet's 2016 Monitoring report

Evidently the installed power is important. Figure 30 (figure 3.7 from the 2016 report) shows the large contribution of gas power (Combined Cycles) together with coal supplying between 7000 MW and 5000 MW. The figure also shows that a large fraction of gas is mothballed. This in more detail given in figure 31 (figure 3.8 from the 2016 report) which shows that on a demand of about 15000 MW market overcapacity has resulted in 4500 MW conserved = mothballed power. Even new power has been conserved. About 3000 MW is thought to be feasible for de-mothballing, evidently only when economical conditions are favourable. As yet there is no capacity market in the Netherlands that pays for keeping power in reserve. Furthermore it shows that some 7000

MW are "missing" in the calculations in chapter 15. A meeting with Tennet has made it clear that this is industrial power, not incorporated in the large traditional utility power that is listed on Tennet's site. Evidently the Dutch security of supply situation is dependent on the behaviour of a large number of smaller producers, making their own financial trade-offs for generation (either produce it yourself or depend on the grid).

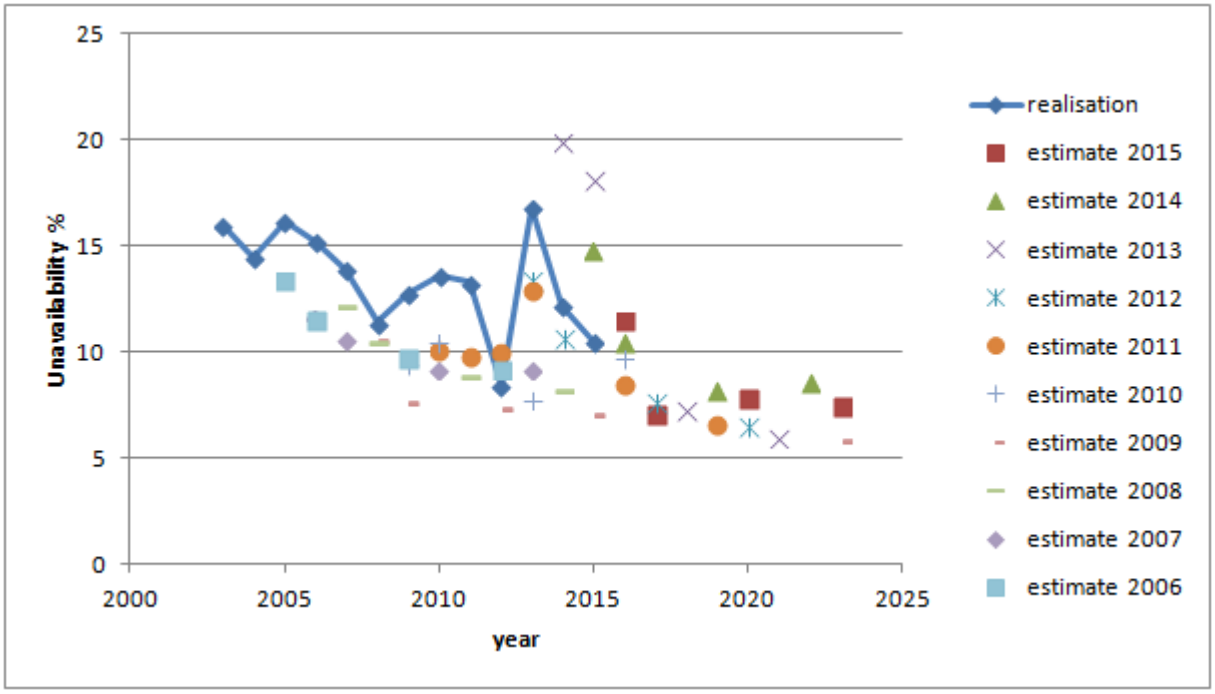


Figure 32. Availability prediction and realisation in Tennet's Monitoring reports

Evidently the unavailability of plants is input in Tennet's Monitoring Report. Figure 32, based on figure 4.2 of the 2016 report and its earlier versions shows over the early periods a systematic underestimation by electricity production companies of the unavailability of their plants of about 2.1%. The companies have been too optimistic. In recent years (2013, 2014, etc.) the forecast of companies for unavailability appears to be more random with less underestimation and even overestimation.

Finally the basic result of Tennets monitoring report is shown in figure 33 (figure 4.3 from the 2016 report). This figure shows that from 2017 on the Dutch are depending on import from abroad. The formal Tennet LOLE allowable is defined as 4 hrs per year. The dependency increases when realized unavailability is considered instead of the predicted unavailability by the companies involved.

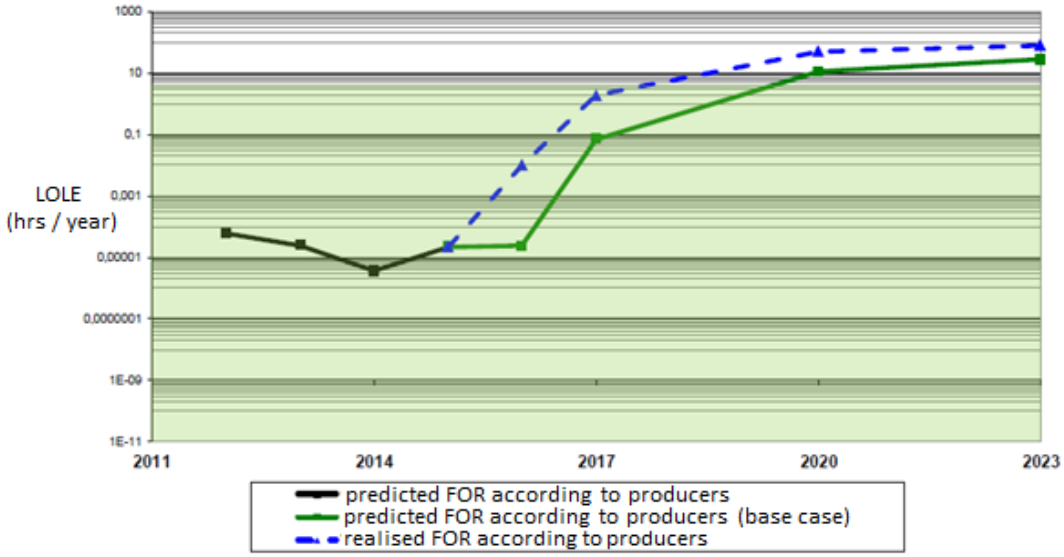


Figure 33. Results for LOLE in Tennet's Monitoring report

It appears that for electricity there is no independent checking of both realized and predicted unavailability while for distribution there is independent checking by certified auditors. It is recommended to carry out such checking, which was disbanded with the introduction of liberalization. Before liberalization Sep and KEMA were working together collecting data from plants, discussing the data at plants, etc. By showing the interest of decision makers into (forced) unavailability it appeared that the forced unavailability was decreasing!

The authors had a meeting with Tennet discussing trends for confirmation purposes. It is hoped to continue discussion with Tennet to have power plants modelled as realistically as possible and in order to improve data quality for unavailability data. The VGB KISSY database can be used as a tool, however inputting data is by VGB members only and no obligation exists to do so.

The simple Billington model is consistent with Tennet's Monitoring report in that for typical forced unavailability not taking an increase for economic reasons into account, it shows that LOLE is negligible. However if a fraction of large combined cycles continue to be mothballed in the situation that the aged coal fired plants (A-81, MV-1-2, G-13, BS12) are out of operation as per the Energie Akkoord, large forced unavailability for economic reasons leads to an unacceptable LOLE in the Billington model. Connections to abroad will dampen this effect however abroad similar conditions may exist. Also increased wind power will only dampen this effect as out of every MW installed only 30 – 40 % is available on a yearly basis as windpower is a function of windspeed to the third power and conditions without much wind may occur over Central Europe for a week or more.

The detailed PLEXOS model is consistent with Tennet's Monitoring report in that it shows the increased dependency on the grid connections with abroad. However it also shows that blackouts occurring say next year are unrealistic. It is recommended however

to repeat the calculations over a larger time horizon and somehow incorporate the statistical uncertainty of both forced outages as well as wind conditions.

18. Conclusions

Minimal maintenance is thought likely to occur in the Dutch production situation when prices are low due to overcapacity in combination with more renewables in the grid. As yet, there is no reserve market in the Netherlands that pays for the costs of keeping power plants in reserve. As a consequence, the forced unavailability of plants will increase which is not desirable as fossil power is the replacement of renewable power when this is not present (no sun or no wind) as long as there is no storage.

The security of supply and the acceptable Loss of Low Probability LOLE appears to be not immediately at risk. However, the Dutch will be more depending on abroad precisely when the grid connections with abroad are less dependent as the same economic situation for fossil power plants is present abroad as well.

It is recommended to improve the quality of availability data from power plants by applying stringent definitions as per the VGB KISSY database, visiting the plants to discuss and validate the data and model the plants taking teething problems for new plants, ageing for old plants and High Impact Low Probability HILP problems into account.

Forced unavailability should be defined on an as-need basis rather than on the basis of calendar time. Simple models on this basis are in existence for decades.

References

Flyvbjerg, B. (2009) *Optimism and Misrepresentation in Early Project Development.* Making Essential Choices with Scant Information, Palgrave Macmillan, ISBN 978-0-230-20586-4

Billington & Allan (1984) *Reliability Evaluation of Power Systems,* PITMAM Publishing, ISBN 0-273-08485-2

VGB PowerTech Service GmbH (2017) *Availability of Power Plants 2007-2016*, ISBN 978-3-86875-983-9

Session 8:
Learning through experience to improve foresight in safety

The Learning Review: Adding to the accident investigation toolbox

Ivan Pupulidy

US Forest Service, Innovation and Organizational Learning

Crista Vesel

Dynamic Inquiry LLC

Abstract

Accident investigation techniques have remained essentially the same for many decades, yet the recognition that complexity is increasing in most organizations demands an added form of inquiry. The Learning Review, first adopted by the U.S. Forest Service, explores the human contribution to accidents, safety, and normal work. It is specifically designed to facilitate the understanding of the factors and conditions that influence human actions and decisions by encouraging individual and group sensemaking at all levels of the organization. The Learning Review introduces the need to create a narrative inclusive of multiple perspectives from which a network of influences map can be created. This map depicts the factors that influence behaviors and can aid the organizational leadership to effect meaningful changes to the conditions while simultaneously helping field personnel to understand and manage system pressures.

Keywords: Accident investigation, complex systems, investigation models organizational learning, sensemaking.

1. Introduction

The Learning Review[67] emerged from organizational necessity, as the prescriptive model of accident investigation used by the U.S. Forest Service was unable to effect positive change to its most important element: the human. From 1995 to 2015 the Forest Service lost over 400 wildland firefighters in active fire operations. These line-of-duty deaths affected our community and our organization emotionally, yet no substantive changes in operation or policy resulted from the investigations that followed these accidents. The investigative model in use was delineated by the Serious Accident Investigation Guide (SAIG), which was formalized in 2001 (Whitlock, 2001). The SAIG was an amalgamation

[67] The Learning Review is the process that formally replaced the Serious Accident Investigation Guide in 2014. It is the outgrowth of seven years of experimentation and research in alternative methodologies.

of the most common investigative tools in use; however, it did not provide wildland firefighting operations with the information needed to prevent accidents. Forest Service investigations often pointed to the failure of people, without understanding why they failed or what failure really meant to the system. In addition, the accident rates were trending upward.

The need for a new approach was also deeply felt at the field level. The results of investigations, called 'factual reports,' chronicled accidents from the often-biased perspective of the investigation team. Secrecy surrounded the process as the team collected 'evidence' and treated the incident like a criminal event, even if there were no criminal implications. Lurking beneath the surface of each causal statement was a sense that the firefighters *intended* to err, as almost all the listed causes in reports were counterfactual and did not provide the 'hard data' that the investigators claimed to have uncovered. Distrust brewed in the wildland firefighting ranks following the release of these reports, and people became less willing to share information or take positions of risk in the agency.

The SAIG was revised in 2005 with the best intent; however, it was an adaptation of several tools designed for the analysis of linear events that displayed straightforward cause-and-effect relationships, such as those developed in machines. These analytical methods of investigation are referred to as linear because they follow a straight path from problem detection to problem solution. The model can be useful when dealing with strict mechanical problems; however, it is not useful in human-centered work environments. People do not handle problems in a linear fashion—in fact, their solutions are often the antithesis of linear. The tools described in the SAIG worked well for the analysis of mechanical failures, but it did not help us to make sense of the complex human interactions that make up wildland fire operations.

The SAIG's approach is not uncommon in modern investigations. The approach does not consider that workers are balancing conflicting goals, messages, rules, regulations, direction, and even laws in their everyday encounters with complex work environments. In contrast to the SAIG instruction to create a timeline-centric narrative, we recognized the importance of building context around decisions and actions. This approach focuses on the correlation between the behaviors and the influencing conditions while avoiding any unintentional implication that workers intended to do harm, which is rarely the case. English is a particularly agentive language; this means that by language alone we can inadvertently name a person as the agent of an action, even if that was not our primary intention. The words that people use to describe everyday actions can carry with them powerful implications that can lead to causal explanation of the event(s) (Vesel, 2012). Thus, accident investigators must be mindful of language throughout the process of gathering information and creating a report.

The SAIG process is designed to measure performance against an unreasonable expectation that work as designed fully represents the work required by the operational environment. Compare and contrast some of the expectations we have of our experts with those of novice workers (See Table I). We expect our novices to have knowledge of and to follow prescriptive policies, yet we expect our experts to adapt policies and direction to meet the challenges they face. We expect our novices to comply with instruction, direction, and procedures, yet we expect experts to improvise solutions. We expect

novices to use knowledge of basic rules, regulations, policies, and procedures to navigate all work situations, yet we expect our experts to use complex adaptive problem solving and critical thinking skills to achieve results.

Table I: Comparison of Expectations, Novice to Expert (adapted from Pupulidy, 2005).

We expect our novices to:	**We expect our experts to:**
Have knowledge of prescriptive policy.	Apply rules to situations and adapt rules as needed.
Comply with instruction.	Know how to improvise to meet operational goals.
Know basic rules, regulations, policy, and procedures.	Use complex adaptive problem solving or critical thinking skills to achieve results.
Know and follow the plan.	Use intuition to know when to change the plan.
The basic goal is to "control" actions and limit decisions.	The basic goal is to facilitate "empowerment."

The fundamental difference is we expect to control the behavior of our novices while simultaneously facilitating the empowerment of our experts. When the expert is successful, we reward the innovation (rule bending, outside the box thinking, risk taking, etc.). However, when the outcome is adverse or negative, the tendency is to hold the expert to the expectations of the novice.

2. Designing the Learning Review

We (Pupulidy, 2015) identified the need to recognize the differences between key system types and the corresponding need to review accidents through the lenses provided by each of these systems. Three systems were identified: simple, complicated, and complex (See Table II). This classification helped us to shape an understanding of the origin and application of traditional methods of investigation. The identification and mapping of these three systems also helped us to understand the limitations of the traditional methods of investigation and forced the development of an additional set of tools.[68] Wildland firefighting is a unique laboratory, as the work is largely conducted in the absence of simple and complicated components. Simply put, wildland firefighting takes place almost entirely in the realm of complex system operation, and as a result, traditional tools were stretched to the breaking point and a new set of tools had to be developed.

The first step was to understand that simple and complicated systems had some fundamental commonalities. Simple systems are made up of parts that are *interconnected* and *interactive*. Each part has a unique and specific role to play in the functionality of the machine. Think of a simple mechanical wristwatch in which each part, spring, or gear interacts in a specific and predictable way with its counterpart—this is required for time

[68] See the US Forest Service "2017 Learning Review Guide." https://www.wildfirelessons.net/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=be30b128-0565-c151-2c68-cbe70dae0b85&forceDialog=0.

to be accurately captured and depicted. If a part breaks, the system fails in a very predictable way. Parts can be inspected, deficiencies found, and the part(s) can be replaced in a very procedural way. In a simple system, the cause and effect relationship is direct—for every cause there is a single effect. Trending failures can result in processes that can reduce the likelihood of failures at unwanted periods of operations. This has resulted in increased safety margins for a number of industrial applications.

Table II: Simple, Complicated and Complex Systems (Components list adapted from Page, 2011).

System Name	Components	Frame	Pathway	Characteristic
Complex	The parts are interconnected, interactive, diverse, and adaptive (they adapt, often predictably).	Organic – These systems cannot be broken down without losing the ability to understand interactions.	Sensemaking, improvisation, and learning—developing adaptations in real time.	Unlimited number of questions with an equally unlimited number of answers. Requires sensemaking.
Complicated	The parts are interconnected, interactive, and diverse,	Systemic – These systems are composed of nested sub-systems.	Directional flow relationships—cause and effect connections exist with a limited set of outcomes.	Each question has a limited number of discrete answers. Reacts well to analysis.
Simple	The parts are interconnected and interactive.	Mechanical.	Cause and effect connections are strong—problems can be solved.	Each question has one discrete answer. Reacts well to analysis.

Complicated systems share some commonalities with simple systems; the parts are interactive and interconnected—however, we can add diverse to this list. In this case, diversity represents the system design quality of multiple defenses in depth and/or the inclusion of redundant systems. This type of diversity strengthens the reliability of the system because in situations where there is a component failure, other parts of the system can compensate, allowing for continued operations. Processes of this type are often depicted as flow diagrams where a malfunction can be identified, isolated, and bypassed, allowing other parts of the system to take the place of the failed component. This design generally allows for failures to occur gracefully (without major consequence) and catastrophic failure to be avoided.

Complicated systems exhibit cause and effect relationships that are as diverse as the system being analysed. For every cause, there can be a limited number of effects. The number of effects is limited to the number of system permutations (normal system variability). This type of system drove the development of many of the current models of accident investigation, such as the Swiss-Cheese, Fishbone, and the SHELL models. Analysis of complicated systems is often effectively conducted using these and other engineering analytical models.

Complex systems share the first three components (interactive, interconnected, and diverse); however, there is a very dynamic addition—adaptation (Page, 2011). Complex systems exhibit qualities of adaptation and can opportunistically change based on innumerable variables, or they can intrinsically change based on conditions, perceptions, and perceived stimuli. These systems are often *learning systems*. Complex systems defy full prediction or control (Morin, 2008). More data can help to refine predictions; however, these predictions are always fraught with some uncertainty. Human interaction with a complicated or simple system often evolves into a complex system. In these cases, it is challenging to avoid being seduced into mechanical or engineering models of accident analysis, which can only describe simple or complicated systems.

Adaptation is demanded by the uncertainty inherent in complex systems. Cause and effect relationships are non-linear—for every cause there can be an unlimited number of effects. This quality directly affects prediction and places the organizational ability to both control the system and control reactions to the system, out of reach. In the case of complex system interaction, the expectation on workers should be that they recognize when the system is delivering the 'unexpected.' In *novel* situations, experts recognize the need to perform outside routine, exemplifying an understanding of complexity—that no one can write a rule or process to fit every situation. The requirement on workers is to create safety in these situations. Professor Reuben McDaniel provides a doctrinal approach: "Workers are expected to make sense of the situation, learn in the moment, and improvise solutions, much like a jazz musician during improv sessions" (Author's personal conversation, 27 November 2015).

The need for workers to improvise actions when faced with novel situations places the investigator in a very difficult situation. Judging actions as right or wrong can only be accomplished when the outcome of the situation is known. This information is not accessible to workers—workers do not know the outcome of their innovation.

Pupulidy (2015) recognized that complex systems need a unique framework for post-accident learning, which we refer to as sensemaking. The actions of people are often, if not always, complex. People do not perform precisely the same way in all situations. This is the result of individual heuristics, unique learning, and biases. As no two humans will perform in exactly the same way when placed in identical situations, system analytics that rely on trending frequently fail. Our research shows the use of system mapping can be more useful to the sensemaking process.

3. Human Actions in Complex Systems

The way that people react to situations is influenced by many factors or conditions. If they are familiar with the work and the system is delivering the expected conditions, then routine responses are appropriate and will often work. In these cases, the routine response is also usually the most effective and efficient response (Klein, 1999). When the system delivers the unexpected and the worker follows a routine, success is not guaranteed. In this case, the routine or procedure is being applied to a situation that is outside the original intent or design. Routine processes, when applied to unpredicted or unexpected conditions, might work if the worker is lucky. Our research has shown that routine actions applied in novel situations can make the worker more vulnerable, as the routine response can result in increased risk exposure (Saddleback Fire Fatality Learning Review, 2013).

When the system is delivering the unexpected, the situation will require that the workers make sense of the conditions, learn in the moment, and innovate actions (McDaniel, 2007). With practice, this skill can be improved through coordination with others and is referred to as "Group Sensemaking" (Weick, 1995; Jordan et al., 2009; Maitlis, 2014). In time-critical situations, sensemaking is often overlooked, and people tend to "Satisfice" (Gigerenzer, 2010; Simon, 1956). This means that workers often find solutions that meet the minimum needs of the conditions they perceive in the moment; workers will act based on the limited information they have at hand. Satisficing is efficient; however, it represents actions driven by the need for efficiency, which can result in a loss of thoroughness (Hollnagel, 2009).

Satisficing can also be seen as a blend of action (intuitive response) and deliberate decisions. Our research indicates that this is common in wildland firefighting operations and is supported by Professor Gary Klein's work with structural firefighters. Acting/deciding is a natural human endeavour, and it takes place in a non-linear way. Every person tends to process information in his or her own way. The resulting responses, or action/decisions, are related to the perceived conditions or stimulus, and these can vary considerably from one person to the next (Panther Fire Fatality Report, 2008).

Work systems are becoming more complex daily, and this complexity brings a level of uncertainty. This uncertainty equates to greater risk in the system. If workers can equate uncertainty to risk, Professor John Adams suggests they will naturally react to create safety in the work system. This is something we see every time we do not experience an accident in the workplace (what we will call 'normal work'). With this in mind, we have to not only expect workers to create safety; we have to learn how to encourage it. Our research demonstrates the importance of recognizing the role of the worker in the creation of safety and the corresponding need for the worker to innovate solutions in complex situations.

4. Action/Decision – It's More Than a Choice

"To err or not to err is not a choice" (Dekker, 2006).

Following an accident, it can seem that some of the actions of workers were careless or even negligent. In fact, discussions with investigators reveal that the term "stupid" is often casually used to describe these actions. These labels are common to events where the outcome is known. Leaders express this form of hindsight bias when they ask questions such as, "Why didn't they stop?" or "Why didn't the workers follow the rules?" The easiest way to respond to this line of inquiry is to point out, "Had they known that there was going to be an accident, they would have stopped or followed the rule." This line of questioning, quite unfairly, asks the investigator to explain something that did not happen. The Learning Review process recognizes the shortcomings of this approach and directs energy toward understanding what actually happened by asking, "Why did it make sense for the worker to do what he/she did?" (Dekker, 2006) This same line of reasoning is also applied to the leadership of the organization in order to begin to understand their motivations.

5. The Learning Review

The Learning Review is not designed to replace traditional accident investigation tools; rather it is a fully developed process designed to explore the social contribution to accidents and to relate the resulting learning products to normal work operations. The process, while designed to review negative outcome events, has been used to understand the pressures and conditions in work that resulted in a desired outcome or what we call *normal work*.

The fundamental goal in producing a learning product is to move the reader from judgment of action to understanding the conditions that influenced people during the mission/operation. The foundation for understanding an event emerges from the recognition of these conditions. Leadership is asked to manage conditions in order to create a workplace where workers can be effective (Reason, 1990). Scenarios can be presented to workers under the premise that they explore the ways conditions can influence decision and actions in normal work environments.

5.1 The Learning Review began with operating principles:

- Forest Service employees are well intentioned and work within organizational systems to meet the expectations of leadership and the system.

- Accidents and incidents can be a by-product of the uncertainty inherent in complex systems.

- Enhanced accountability:
  - Prior to incidents, leaders and managers are responsible for knowing how the organization functions. At this point, traditional forms of accountability can be valuable.
  - After the incident, prevention is based on learning. The organization becomes accountable to learn all it can from the event.

- Actions and decisions are consequences, not causes. Following an event where the outcome was a surprise, the goal is to understand why the action or decision made sense to those involved at the time. This is based on the premise that, "If it did not make sense to them at the time, they would not have done it."

- Conditions shape decisions and actions; revealing these conditions will aid the agency and personnel in understanding how to recognize, change, and react to conditional pressures.

These principles led to the development of tools and techniques specifically designed for the Learning Review. One tool is the complex narrative, which includes a deliberate emphasis on reducing the inadvertent bias of language. We realized that human recollection is fundamentally inaccurate, no matter when the story is gathered. This knowledge allows us to approach interviews in a different way. The stories shared by participants are captured and recorded as perspectives—we don't attempt to create a factual account from the narratives or a plausible single view of the incident—which is

what most investigative processes demand. Instead, we recognize witness accounts as perspectives, and we try to capture each as accurately as possible, but with the understanding that these accounts may be in conflict with one another. This conflict is an important part of the narrative, as it may lead to different questions. For example, "Did the participants recognize their differences in perspective?" And if so, "How did they communicate that understanding?"

The complex narrative is paired with a network of influences map, which is a representation of the conditions that influenced decisions/actions. It is similar to Rasmussen's Acci-map with some striking differences. For example, it is based on *influence*, rather than cause. Searching for causes restricted our teams from exploring some very critical aspects of our organizational culture and prevented us from asking hard questions regarding the perverse nature of some of the influences we discovered. For example, we had trouble making the case for the influence of overtime pay on the behavior of our crews. We had recorded admissions of workers indicating that overtime played a role in decision-making and risk acceptance, but we could not prove a causal link. Simply shifting the conversation to 'influence' was enough of a softening of language to allow a dialogue to begin that could explore the possible ways that overtime nudged decisions.

The initial network of influences map represents the interaction between the conditions as they were perceived during the incident; however, our goal is to move quickly into the normal work environment. Prevention is forward looking, and our processes were all retrospective. Our traditional techniques kept us rooted in findings that led to causes and then to recommendations, with each needing a direct tie to the accident. This method prevented us from examining the influences in normal work operations, which is where safety really starts. We now present the complex narrative and the network of influences map to focus groups, which helps us understand how the conditions noted during the accident are perceived in normal work environments. If the focus groups indicate that the conditions are common in normal work, we focus attention there. If the conditions are unique to the incidents, we place them in another category.

Conditions are a currency for change. We have found it best to divide the conditions into four categories to facilitate organizational acceptance and learning:

1. Conditions that are outside the control of the agency leadership.
2 Conditions that will have meaningful impact but will take time to change (these are usually cultural issues).
3. Conditions that will have meaningful impact on the operations and can be changed quickly.
4. Conditions that, if changed, would likely have a negligible impact.

It is a fallacy that simply attending an accident investigation course suddenly imbues the investigator with the ability to directly create social corrections to the system. We used to develop recommendations that were meaningless or impossible to put into action. Instead, the Learning Review Team humbly engages those closest to the work to help craft recommendations. Recommendations are now a collaborative effort with field personnel who provide input through focus groups.

6. Conclusion

The Learning Review was specifically designed for complex systems, particularly those involving people. The Learning Review is fundamentally a social sensemaking activity that reviews an accident, incident, or even normal work for clues as to where workers contribute to the safety of operations or where the system inhibits this capacity.

This approach describes a new way to view the human contribution to work and safety, one that strives to understand the context of action. This context is converted into dialogues that serve as opportunities to share stories that challenge deeply held assumptions about the way things are supposed to be done. The goal is to place learning above correcting and fixing. This moves us from judging actions as right or wrong, and inadvertently, people as good or bad, to a forward looking exploration of our system.

References

Adams, J. (1995). *Risk*. Oxen, England: Routledge.

Dekker, S. (2006). *The field guide to understanding human error*. Burlington, Vermont: Ashgate Publishing Company.

Gigerenzer, G. (2010). "Moral Satisficing: Rethinking Moral Behaviour as Bounded Rationality." *Topics in Cognitive Science*, 2, pp. 528-554.

Hollnagel, E. (2009). *The ETTO principle: efficiency-thoroughness trade-off; why things that go right sometimes go wrong*. Burlington, Vermont: Ashgate Publishing Company.

Jordan, M. E., Lanham, H. J., Crabtree, B. F., Nutting, P. A., Miller, W. L., Stange, K. C., & McDaniel, R. R., Jr. (2009). "The role of conversation in health care interventions: enabling sensemaking and learning." *Implementation Science*: IS, 4.

Klein, G. (1999). *Sources of Power: How People Make Decisions:* MIT Press.

McDaniel Jr., R. R. (2007). "Management Strategies for Complex Adaptive Systems." *Performance Improvement Quarterly*, pp. 20, 21.

Morin, E. (2008). *On Complexity*. Cresskill, NJ: Hampton Press, Inc.

Page, S. E. (2011). *Diversity and complexity*. Princeton, NJ: Princeton University Press.

"Panther Fire Fatality Report." (2008). Wildland Fire Lessons Learned Web site. https://www.wildandfirelessons.net.

Pupulidy, I. (2015). *The transformation of accident investigation: From finding cause to sensemaking*. Tilburg University, Tilburg, The Netherlands

Reason, J. (1990). *Human Error*. New York: Cambridge University Press.

"Saddleback Fire Fatality Review." (2013). Wildland Fire Lessons Learned Web site. https://www.wildandfirelessons.net.

Simon, H. A. (1956). "Rational Choice and the Structure of the Environment." Psychological Review. 63 (2): pp. 129–138.

Vesel, C. (2012). *Language bias in accident investigation*. Master of Science Degree Dissertation. Sweden: Lund University.

Weick, K. E. (1995). *Sensemaking in organizations*. Thousand Oaks, CA: Sage Publications.

Whitlock, C. (2001). Accident Investigation Guide: 2001 ed. Missoula, Montana: Forest Service, United States Department of Agriculture, Missoula Technology and Development Program.

A model for analyzing near-miss events by adopting system safety principles

Maria Grazia Gnoni

Department of Innovation Engineering, University of salento

Campus Ecotekene, Via per Monteroni

73100, Lecce, Italy

Silvia Ansaldi, Paolo A. Bragatto

Inail, Centro Ricerca

Via Fontana Candida 1

00078, Monteporzio Catone (RM), Italy

Abstract

This study aims to point out potential contribution of system safety principles adopted in risk management for supporting the prioritization and cause analysis phase, which usually characterize near-miss management systems at hazardous establishments. System safety principles are domain-independent and technologically agnostic; they are based on a small set of general rules from which many safety measures – usually adopted in the design and management phase of a plant - derive. The most relevant are the Fail-safe, the Safety margins, the Defense-in-Depth and the Observability-in-Depth principles. Usually, system safety principles can be translated and adopted in many different ways as safety measures to deal with a broad range of hazards in different contexts. The idea is that safety principles shall offer a new lens by which to analyse and prioritize near-miss events: thus, one important result is that near-miss data can be classified and interpreted in light of safety principles violated, and that safety interventions can be particularly effective when organized around such findings. The model proposes to analyse near-miss events – but also minor accidents – by measuring quantitatively how much one (or more) safety principles were be violated for each near-miss events. This model could be adopted to support the prioritization process of near-miss data and the causal analysis by underlying the generating mechanism of a given precursor or near-miss, not just its immediate cause or symptom.

The model has been validated by using data about near-miss events and minor accidents recorded in a hundred of chemical companies working under the Seveso directive in Italy and collected by the Italian National Institute for Insurance against Accidents at Work. Data regards both process plants and storage facilities, characterized by different dimensions and organizational models.

Keywords: Near-miss priorization, system safety principles, Seveso Inspections.

1. Background

The background of the work is described at first aiming to outline the main scope of the proposed research. The work rises from an operational experience developed by INAIL, which participates the inspection activities at Seveso plants. After the implementation of Seveso II Directive for the control of Major Accident Hazard in 1999, the Italian Competent Authority adopted a guide for the inspections at Seveso establishments. It was based on a detailed check list, with about 150 points. Before scrutinizing those points, the inspectors were required to discuss the operating experience, including near misses NMs, in order to prioritize the points in the check list. The guideline was revised in 2008 and in 2015, due to the implementation of Seveso III Directive in the Italian Legislation. The last release of the Inspection Guide is more flexible than the first check list, as it recognizes the importance of discussing the operating experience and comparing it with the preventive and protective safety barriers, as identified in the risk assessment. Thus, in recent inspections, the focus is often on the study of accidents and near-miss events. The approach based on near-miss discussion, compared with safety barriers is usually considered more "risk based" as it is able to single out the critical issues of the safety system. In Italy, the practice of exploiting near-miss events for assessing the global efficiency of a safety management systems, presented years ago by few pioneers [1], is becoming more and more common today. The 2016 campaign of Seveso Inspections developed by the Ministry of the Environment has been the first after the Seveso III implementation and the new guideline has been applied for the first time by the inspection teams participated by INAIL, Environmental Agencies, and Fire-fighters representatives. In many case the approach "risk based" has been preferred and the near-misses management has been, consequently, stressed indeed. According the inspection guideline near misses and accidents recorded in the previous five years must be discussed, at the beginning of the inspection. For each event, a form must be filled in by the operator and provided to the inspectors. The 2016 campaign involved 150 of the over 450 upper tier establishments; about 900 records of operating experience have been gathered. Accuracy of the documents is not homogenous and interpretation of an event as a near- miss varies from one establishment to another (which is also a typical problem in near-miss identification). On the other hand, near-miss events collected by inspectors during the annual campaign include anomalies, unsafe situations, failures and trivial errors. This sample has been used to develop the study activity. These records, even heterogeneous, are important, as they are providing researchers as well as regulators with a realistic picture about the actual management level of safety in Seveso establishments located in Italy.

The goal of the present paper is to understand how to exploit in a more formal way this valuable information treasure, in order to get knowledge and address, consequently, the safety of the Italian Process industries. The aim is to provide to the Italian Seveso sector, a fast but effective methodology to manage near-misses gathered during the annual inspection campaign. The present paper is the first step in this directions. Its objectives paper are:

- identifying a method for near-miss management, suitable for higher hazard industries, falling under Seveso legislation;
- demonstrating the suitability of the method by experiencing it on a subset of data extracted from the 2016 campaign.

Obtained results will be used by inspectors to better address the issue of near-misses in the annual inspection campaign.

2. State of the art about NMS

Near-miss Management Systems (NMSs) have been demonstrated as important safety tools for addressing, in a more effective way, safety interventions. This tool could contribute to the application of a new approach for safety management, which aims to support high-hazard organizations in managing efficiently system safety [2]: the so-called High Reliability Organization (HRO) paradigm [3]. The HRO paradigm outlined the importance of integrating a prevention with a resilient approach for an effective safety management in complex organizations [4]. Two main pillars characterize HROs [5]: prevention and resilience. Firstly, preventing accidents by anticipating the cause analysis of potential negative events - i.e. accident precursors - will provide a more effective prevention strategy. In addition, the second basic pillar of an HRO is its capability to speed up the recovery process through a more resilient organization. In order to provide high reliability, the organization has to maintain or recover a dynamically stable state, which allows it to continue operations in the presence of a continuous stress and/or after a major mishap [6]. By focusing on the prevention strategy in the HRO paradigm, NMSs represent a valuable tool to support it. One critical process is to design the NMS aiming to maximize its effectiveness. This work aims to evaluate the potential contribution of system safety principles in designing effective NMSs. These concepts integrate traditional risk analysis methods in providing design or operational guidelines and principles for eliminating or mitigating risks. System safety principles are domain-independent and technologically agnostic, and from which many safety measures derive. A small set of general safety principles can be translated and adopted in many different ways as safety measures to deal with a broad range of hazards in different contexts. It has to be noted that safety interventions - especially when unsafe acts or behaviours are targeted - can be particularly effective when organized around safety principles.

2.1 NMS: levels of adoption in the process industry

NMS are concerned with the broadest definition of near-misses and include adverse conditions (defined also as accident pathogens), unsafe acts and procedures, and adverse events or sequences of events “that precede and [can] lead up to an accident”. All these

aspects constitute an important source of knowledge when their safety implications are properly understood [7]. Learning from near-misses is less costly than learning from their fully developed more destructive similar events, i.e. accidents [8], [9]. The inherent value of a NMS is in the learning loops it provides within and across organizations, in improving accident prevention and sustainment of safety [10] [11], [12], [13]. NMS consist in an organizational structure and function with people, processes, and IT support or infrastructure, and whose objective is to collect and prioritize anomaly and precursor data, to interpret and assess their risk implications, and to transform this data into risk-informed interventions and safety improvements and awareness [14]. Its end objective is to help improve accident prevention and sustain safety from different (technical, operational, and organizational) point of views. The system teases out the failure generating mechanisms in and the risk implications of, anomaly and precursor data and reflects them back to the organization in a variety of ways to have them addressed. The design and operation of NMS varies across industries [15] - e.g., for a manufacturing company or an airline operator- , and depending on whether it is implemented within a company or at the regulatory level overseeing an entire industry. Thus, designing a NMS usually involves several factors, such as industrial context, firm organization, in order to manage correctly information from the field and spreading knowledge to prevent accidents. No reference guideline has been defined as a standardized approach could not effectively work in different contexts. Several studies had faced with this problem. [16] proposes an interesting analysis of near-miss reporting system for the chemical sector. [17] described a research project in the marine oil transportation industry for optimizing near-miss data management: the focus is to reduce human and organizational errors due to oil spills during tanker loading and discharge operations. [15] proposed an approach based on a set of indicators for identifying and checking near-miss events: the aim is to recovery critical information derived from operational field.

2.2 Basic elements of a NMS

Main processes usually characterizing a NMS [16] are:

- *Event identification and reporting*: first activity is usually developed by workers which highlight an event as an accident precursor (near-miss, unsafe act, or unsafe condition). A brief analysis about the event dynamics could developed directly by the signaller, who represents "the knowledge source", or by safety analysts. Main information and data about the event are usually reported in a predefined form;

- *Event assessment*: next, event information are usually transferred to analysts - e.g. from the Health and Safety Department (H&S) - which have to carry out cause and consequence analyses. If the number of reported events is higher, a prioritization activity is essential in order to support an efficient planning of urgent measures at the workplace. Root cause analysis will be also developed to deeply analyzed main factors contributing to the event occurrence;

- *Prevention measure identification and application*: corrective and preventive actions are the main output of the event assessment phase. Thus, a program of interventions is developed for supporting their application;

- *Follow-up actions*: finally, an ex-post analysis is carried out after the intervention application phase aiming to both verify their effectiveness and to propose guidelines to avoid in the future the occurrence of similar events.

The focus of the paper is to develop an efficient methodology to support the event assessment phase: the idea is to evaluate, in a quick way, main elements, which have led to the near-miss events thus allowing a priorization of events.

3. System safety principles: a brief introduction

Detailed guidelines are defined for each industry and for dealing with different hazards (e.g. electrocution, fire). In contrast with this proliferation of safety measures, there exist a small set of safety principles, which are domain-independent and technologically agnostic, and from which many safety measures derive. A small set of general safety principles can be translated and adopted in many different ways as safety measures to deal with a broad range of hazards in different contexts. Basically, the system safety principles are built on the notion of hazard level (and escalation) and accident sequence. Although these safety principles are not meant to be exhaustive, they cover a broad range of safety considerations, and many detailed safety measures derive from or can be traced back to them. The analyzed system safety principles will be derived from (Saleh et al, 2014): the Fail-safe, the Safety margins, the Defense-in-Depth (DiD) and the Observability-in-Depth principles (OiD). The *Fail-safe principle* requires design features such that the failure of a component in a system will result in operational conditions that preventing potential harm or damage by blocking an accident sequence from further advancing, and/or freezing the dynamics of hazard escalation in the system. As an example, if the principle has been adopted for designing a critical device in an industrial plant, when a failure does occur, the device will tend to fail in a predictable manner to a safe state. Thus, the *Fail-safe principle* represents a particular form of robustness and failure tolerance. On the contrary, if the *Fail-safe principle* is not implemented, a component's failure would aggravate a situation by further escalating the system hazard level, thus initiating an accident sequence or leading to an accident. The adoption of safety margins originates from the civil engineering sector, where structures are designed with a safety factor to account for larger loads than what they are expected to sustain, or weaker structural strength than usual due to various uncertainties. The *Safety margin principle* extends beyond civil engineering and is more diverse in its implementation than the particular form it takes for structures. It requires a preliminary estimation of a critical hazard threshold for accident occurrence, and an understanding of the dynamics of hazard escalation in a particular situation. The *Safety Margin principle* requires that systems adopted to maintain the operational conditions and the associated hazard level at some "distance" away from the estimated critical hazard threshold or accident-triggering threshold. Safety margins are one way for coping with uncertainties in both the critical hazard threshold (a random variable) and in our ability to estimate and manage the actual operational conditions in a system, such that their associated hazard level does not intersect with the real critical hazard threshold. The *Defense-in-Depth principle* derives from a long tradition in warfare by virtue of which important positions were protected by multiple lines of defences. The principle has several pillars and requires that (i) multiple lines of defences or safety barriers be placed along potential accident sequences; (ii) safety should not rely on a single defensive element

(hence the "depth" qualifier in DiD); (iii) the successive barriers should be diverse in nature and include technical, operational, and organizational safety barriers. The various safety barriers have different objectives and perform different functions. The first set of barriers, or line of defense, is meant to prevent an accident sequence from initiating.

Should this first line of defense fail in its prevention function, a second set of safety defenses should be in place to block the accident sequence from further escalating. Finally, should the first and second lines of defense fail, a third set of safety defenses should be in place to contain the accident and mitigate its consequences. This third line of defense is designed and put in place based on the assumption that the accident will occur, but its potential adverse consequences should be minimized. These three lines of defenses constitute defense-in-depth and its three functions, namely prevention, blocking further hazardous escalation, and containing the damage or mitigating the potential consequences. The *Observability-in-Depth safety principle* constitutes an important complement to DiD, without which the latter (DiD) can devolve into a defense-blind safety strategy. OiD requires and is characterized by the set of provisions, technical, operational, and organizational de-signed to enable the monitoring and identification of emerging hazardous conditions, accident pathogens, and adverse events in a system to eliminate safety blind spots that might be introduced in the system because of DiD or other hazard concealing mechanisms. It requires that all safety-degrading events or states that safety barriers are meant to protect against be observable. This implies that various tools have to be adopted to observe and monitor the system state and breaches of any safety barrier, and reliably provide this feedback to the proper stakeholders (operators, users, engineers, managers, etc.). OiD seeks to: (i) minimize the gap between the actual and the assumed hazard levels, and (ii) ensure that at the hazard levels associated with the breaching of any safety barrier, these two quantities coincide. The "depth" qualifier in OiD has both a causal and a temporal dimension, and it characterizes the ability to identify adverse states and conditions far upstream (early) in an accident sequence. It reflects the ability to observe emerging accident pathogens and latent failures before their effect becomes manifest on the system's output or behaviour, or before a more hazardous transition occurs in an accident sequence.

4. Contributions of system safety principles

4.1 Assessing the potential contribution of system safety principles

The safety principles discussed in the previous section could be effectively adopted to design the NMS; they can help to inform and guide the two central phases in these systems, i.e. the event assessment and the prevention measure identification and application phases although a contribution could be also outlined for the two other phases. Following, a critical analysis about the contribution of applying system safety principles in the two central phase characterizing NMSs. The basic issue of the fail-safe principle is to define systems (e.g. physical devices, procedures, etc.) to block the accident chain. Thus, its main contribution could be oriented to prioritize precursor events that are more critical as they are closest to an accident or they are the blocking line for an accident occurrence. A similar contribution could be outlined for the safety margins principle: its main aim is to "dismiss" the accident by adopting organizational as well as technical "spacers". By evaluating the DiD principle, the potential contribution to the event assessment phase in NMS could be also to prioritize events, but it could also contribute to

define the consequences due to the event occurrence, thus outlining if such defense lines have blocked or not the accident chain. By analyzing the OiD principle, it has wider impact comparing the other three principles as it integrates a strategy for designing safety systems with tools for controlling their performance. Although they operate on different levels of abstractions, it can be said that NMS is one of the pillars of the implementation of OiD. The two other pillars are "fault diagnosis systems and online monitoring", and "periodic inspections". These approaches are information-centric and meant to scan for, detect, and assess adverse conditions and hazardous occurrences in a system before they escalate into full blown accidents. They operate though by different means and over different time scales as we discuss next.

4.2 The adopted approach for priorizating near-miss events

Near-miss are unexpected hazardous events with no consequences for workers as well as plants. Knowledge derived from their analysis regards only causes: usually, accidents and near-miss have common causes, thus, outlining near-miss causes shall be effective for preventing accidents. The basic idea is that if a near-miss is occurred, a "fault" in the system has occurred. Based on a simplified hypothesis that adopting safety principles could prevent accidents, the fault shall originate from three different cause categories:

- Case 1: No safety principle has been adopted in the safety design process: several reasons could lead to this occurrence such as an underestimation of the criticality level of the equipment and/or the procedure;

- Case 2: A safety principle had been adopted, but the system introduced (e.g. a redundancy, or a new procedure) has not already worked thus causing hazardous conditions out of normal control;

- Case 3: A safety principle had been adopted and the system introduced has worked, thus "confining" hazardous event and, reducing the impact of near-miss on plant operations.

Based on these assumptions, each near-miss event cause could be analysed to prioritize most critical events: if case 1 is highlighted for an event (or a a set of events), the highest priority is assigned; if case 2 or 3 are pointed out, a medium or low priority is assigned respectively. The flow diagram of the proposed procedure is in Figure 1.

The proposed procedure aims to support a quick but effective assessment of near-miss events based on "simple" rules: as near-miss events are precursor of an accident, the absence of adopting a safety principle outlines a high proximity to an accident. Otherwise, if a safety principle has been applied aiming to turn away a potential accident, a fault in the equipment and/or procedure outlines a less but still critical condition to be analyzed.

Finally, if no fault occurred, the event has been stopped by the adoption of a safety principle; thus, it could provide feedback for continuous improvement rather than for urgent interventions. In the next section, the proposed methodology has been tested using a real dataset of near-miss events collected during Seveso inspections in Italian process plants.

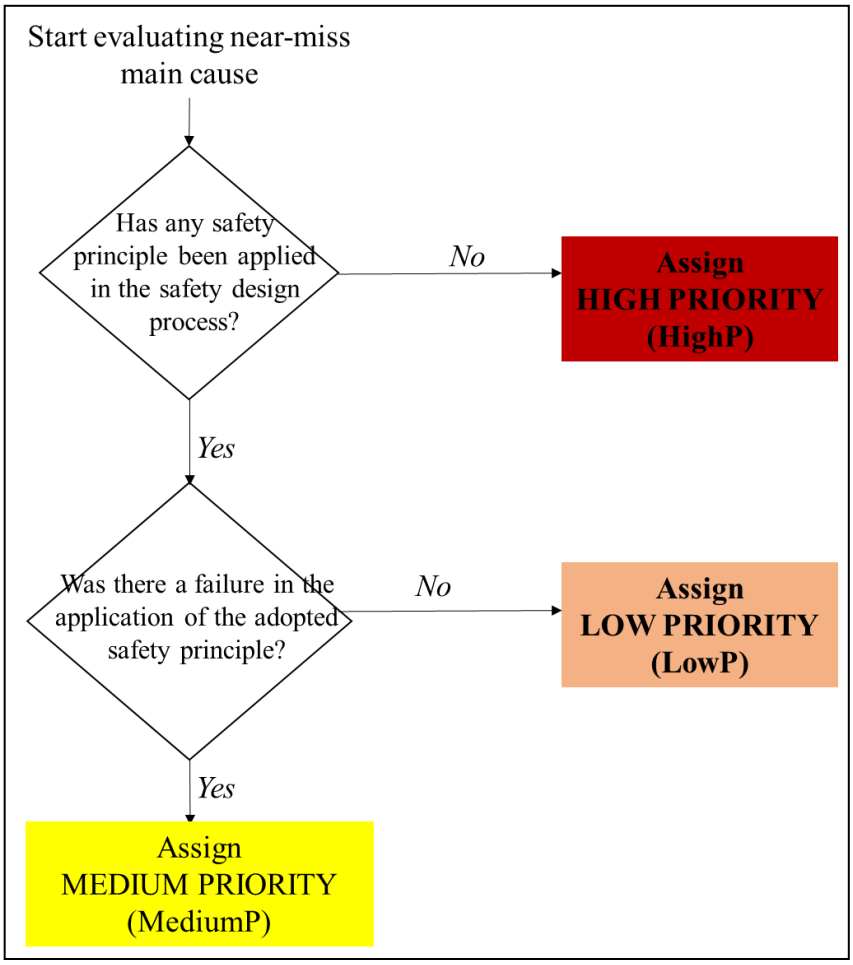


Figure 1. The flow process for analysing near-miss event causes

5. The testing case

5.1 The dataset in analysis

The analysis has been developed through a random extraction of near-miss documents gathered during the 2016 inspection campaign, described in the first part of this work. The data regard both process plants and storage facilities. The dataset includes about seventy reports of near-misses or minor accidents, shared between process industry and storage facilities in the chemical sector. Companies operate in different industrial sectors, including chemical, pharmaceutical, and metallurgical fields. The chemical process plants provide basic products for industrial purposes. The storage facilities considered refer to chemical, toxic, petroleum products, and liquefied gasses. Near-miss events have been collected by using a similar form, containing the following information: a description of the event and the conditions under which it occurred, the actions undertaken and those planned. Although the form is the same, the level of detail adopted by each Seveso company could be different. The dataset is a consistent sample, since the main industrial sectors under Seveso legislation have been evaluated, and refers to a large variety of industrial activities and situations from industrial depots to more complex plants. The

most frequent occurrences deal with the failure or rupture of an equipment or its component (34%) and during the transfer and the load/unload activities (21%). A 14% of the dataset refers to near-misses detected during daily controls or safety walks, while 11% during planned inspections or technical tests. Other near misses refer to activities involving transport vehicles or handling hazardous substances (9%), or maintenance activities (8%). The dataset reports also a few cases concerned to adverse climatic conditions (3%).

5.2 Results discussion

A sample of events has been extracted from a dataset of events collected in the annual (i.e. 2016) inspection campaign developed by the Italian Authority. The analysed sample includes data collected for different establishments in the process industry sector: event information belong to storage facilities (chemical depots, oil terminal, toxic depot) and process plants (from chemical plant, metallurgical and pharmaceutical ones).

Next, after the sample definition – composed by 55 events- each near-miss event has been analysed based on the methodology proposed in section 4.2: results for storage facilities and plants are reported in Table 1 and 2 respectively.

By analysing data for storage facilities, data shows a low presence of most critical events: about 17% of events have been classified under the highest hazardous category (defined as HighP). The largest group (about 74%) refers to events where a safety principle has been adopted in the design phase and it was revealed effective during operations, thus reducing consequence of the event at the low level, i.e. usually the event has caused no consequence for safety at the Seveso establishment where it has been collected. Similar trends is outlined for the process plants: the HighP category is the largest one together with MediumP category; it is confirmed the lowest value for events without adoption of safety principle (HighP).

Table 1: Event classification reported based on plant type and safety principles for analysed storage facilities.

	Chemical depot	**LPG depot**	**Oil terminal**	**Toxic Depot**	
Event Type	#	#	#	#	**Total**
HighP	4	1	0	2	7
MediumP	1	1	1	0	3
LowP	5	8	8	8	29
Safety Principle	#	#	#	#	**Total**
Fail-safe	2	1	1	2	6
Safety-margins	2	2	5	0	9
DiD	2	6	0	5	13
OiD	0	0	0	1	1

For storage facility clusters, the Fail-safe principle has been outlined for all events under the MediumP cluster; in 29 events under the LowP group, DiD represents the largest category (with 37%) and the Safety margins principles represents the second one. Differently for process plants, the largest category (about 76%) of safety principle under the MediumP group is defined by the Fail-safe principle; Safety margins and DiD are the following two groups respectively.

Table 2: Event classification reported based on plant type and safety principles for analysed process plants.

	Chemical plant	**Metallurgical Plant**	**Pharmaceutical Plant**	
Event Type	**#**	**#**	**#**	**Total**
HighP	3	0	0	3
MediumP	4	5	4	13
LowP	3	5	5	13
Safety Principle	**#**	**#**	**#**	**Total**
Fail-safe	2	4	4	10
Safety-margins	2	0	0	2
DiD	3	5	2	10
OiD	0	1	3	4

Finally, by evaluating the LowP cluster, most of events (about 92%) have applied DiD principle n safety design process.

Finally, the proposed methodology has provided a quantitative priorization of events, grouped in clusters: this classification could allow safety managers as well as inspectors to analyse firstly most hazardous precursor events (i.e. ones included in HighP groups), thus allowing to concentrate efforts on analysing most critical events and defining quick resolutions for them.

6. Conclusions

Near-miss events represent an important source of information for both companies about and competent authority to increase knowledge about actual safety levels at workplaces. One of the main problems in near-miss management system design is to define an efficient method to "extract" knowledge to eliminate main causes lead to the event. The study proposes a simple methodology to point out near-miss events that are more "critical". The criticality level has been estimated using system safety principles: if the main condition that has lead to the event is the absence of adopting a safety principle at the design phase, the event is classified under the most critical category; otherwise, if a safety principle has been applied but the system adopted has not worked, the criticality decreases. The methodology proposed has been validated based on a dataset regarding near-miss events collected during annual inspection at Seveso process plants in Italy. The methodology could also be adopted to support inspectors during their campaign to support companies in analysing near-miss and defining more effective prevention activities.

References

Agnello, P., Ansaldi, S.M., Bragatto, P.A. (2012). Plugging the gap between safety documents and workers perception, to prevent accidents at Seveso establishments Chemical Engineering Transactions, 26, 291-296.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2008). Organizing for high reliability: Processes of collective mindfulness. Crisis management, 3(1), 81-123.

Hopkins, A. (2009). The Problem of Defining High Reliablity Organisations. CCH Australia Ltd.

Schulman, P. R. (2004). General attributes of safe organisations. Quality and Safety in Health Care, 13 (suppl 2), ii39-ii44.

Saleh, J. H., Marais, K. B., Bakolas, E., & Cowlagi, R. V. (2010). Highlights from the literature on accident causation and system safety: Review of major ideas, recent contributions, and challenges. Reliability Engineering & System Safety, 95(11), 1105-1116.

Sutcliffe, K.M & Vogus, T. (2003). Organizing for resilience. In Cameron KS, Dutton JE & Quinn RE (eds.). Positive organizational scholarship. San Francisco: Berrett Koehler, 94–110.

Saleh, J. H., Saltmarsh, E. A., Favarò, F. M., & Brevault, L. (2013). Accident precursors, near misses, and warning signs: critical review and formal definitions within the framework of Discrete Event Systems. Reliability Engineering & System Safety, 114, 148-154.

Nielsen K.J., Carstensen O., Rasmussen K., 2006. The prevention of occupational injuries in two industrial plants using an incident reporting scheme. Journal of Safety Research, 37, 479–486.

Sepeda, A.L., 2006. Lessons learned from process incident databases and the process safety incident database (PSID) approach sponsored by the Center for Chemical Process Safety. Journal of Hazardous Materials, 130, 9–14.

Bier, V. M., & Mosleh, A. (1990). The analysis of accident precursors and near misses: implications for risk assessment and risk management. Reliability Engineering & System Safety, 27(1), 91-101.

Wu W., Gibb A.G.F., Li Q., (2010). Accident precursors and near-misses on construction sites: An investigative tool to derive information from accident databases. Safety Science, Vol. 48, 845–858.

Andriulo, S., & Gnoni, M. G. (2014). Measuring the effectiveness of a near-miss management system: An applica-tion in an automotive firm supplier. Reliability Engineering & System Safety, 132, 154-162.

Hodges, M. S., & Sanders, C. E. (2014). Nuclear criticality accident safety, near misses and classification. Progress in Nuclear Energy, 76, 88-99.

Teizer, J., & Cheng, T. (2015). Proximity hazard indicator for workers-on-foot near miss interactions with construction equipment and geo-referenced hazard areas. Automation in Construction, 60, 58-73.

Phimister J.R., Oktem U., Kleindorfer, Kunreuther H., (2003). Near-miss incident management in the chemical process industry, Risk analysis, 23, 445-459.

Van de Schaarf T. W., (1992). Near-miss reporting in the Chemical Process industry, Phd Thesis, Eindhoven University.

Mason E., Roberts K., Bea R., 1995, Reduction of Tanker Oil and Chemical Spills: Development of Accident and Near-Miss Databases, Available at http://nsgd.gso.uri.edu/cuimr/cuimrt95003.pdf (Accessed 2017-9-10).

Session 9:
From database management to foresight

Use of Event and Causal Factor Short Chart Reports to Assess and Simplify Accident Reports

Miodrag Stručić

European Commission, DG Joint Research Centre – JRC

Directorate G – Nuclear Safety & Security,

Unit G.I.4 Nuclear Reactor Safety and Emergency Preparedness

Westerduinweg 3, 1755 LE Petten, The Netherlands

Abstract

This paper concentrates on assessing events described in hazardous industry's incident/accident reports using the Event and Causal Factor Charting technique. Event and Casual Factor Charting (ECFC) is a process that first identifies a sequence of events and aligns the events with the conditions that caused them. It is used to visually give better insights and emphasize important points.

Events and respective conditions are aligned along a time line. After the representation of the problem is complete, an assessment is made by "walking" the chart and asking if the problem would be different if the events or conditions were changed asking the questions: What went wrong, how and why? Which deviation occurred? Which rules were transgressed? This leads to identifying causal factors which are evaluated. This approach provides basics for brief risk assessment and can reveal some hidden warning signs in related event reports.

The use of ECFC has proven to be a valuable tool for accident investigators and a clear and concise aid to understanding of accident causation for the report readers and stakeholders. This paper also suggests using a more standardised approach in presenting events by graphical tools for greater effectiveness in accident investigating and reporting.

Keywords: foresight, safety, investigation, weak signals, risk assessment, incident/accident report

1. Introduction

The key evidence in the most of incident/accident investigation is collected early in investigation phase [1]. Beside collection and preservation of physical evidence, it is equally important to collect all actors' statements, i.e. their perception of the event or parts in which they were involved [2]. Unfortunately, the most of operational event safety

assessments experts are not present on the site and not in contact with the actors involved in incident or accident. Therefore, written statements and preserved evidence should be used for assessment. Final reports should provide all findings, analysis and recommendations, but, depending on the authority's requirements [3], which are usually legally defined, reports could cover only part of the whole event.

From other side, the authority, interested in the event (internal or from other similar organisation), may miss important information that could be used for concrete definition of actions. Fortunately, some weak signs, often presented in reports, could trigger additional investigation on their existence and result in measures for their elimination. Therefore, helping stakeholders to find these signs is of high importance in incident/accident prevention.

For the purpose of detecting weak signals, visualisation of event evolution could be used. Using Event and Causal Factor Charting (ECFC) technique [4] can help in detection and amplification of these signals, and consequently give appropriate level of attention.

ECFC technique is used in event investigation. The process first identifies a sequence of events and aligns the events with the conditions that caused them. It is used to visually give better insights and emphasize important points. Events and respective conditions are aligned along a time line. After the representation of the problem is complete, an assessment is made by use of other investigation tools, such as Cause and effect analysis, Interviewing, Task analysis, Change analysis, Barrier analysis etc. [4]. The main purpose is to understand accident causation and reveal causal factors that can be eliminated to prevent occurrence of similar events.

Use ECFC diagram in presenting event provides basics for brief risk assessment and can emphasizes some hidden warning signs in related event reports. By this paper, author will try to justify usefulness of ECFC in detection, amplification and elimination of latent weaknesses by two concrete examples from Nuclear Power Plant (NPP) event reports.

2. Warning Signs in ECFC

Due to strict reporting criteria, the original incident/accident report (e.g. Licensee Event Report) has to provide relevant information to regulatory body or other authority, but does not need to explicitly address all Causal Factors that could be found in thorough event analysis. Event and Causal Factor Chart (ECFC) can be of practical use to show the other possible Causal Factors. These factors could be latent weaknesses of the reporting organisation, but because of weak transparency, some of them present Weak Signs of decreased safety.

2.1 Example 1

Often, Operating Experience Feedback (OEF) process efficiency is not explicitly addressed in event report's action plans, although deficient use of OEF could contribute or result in decreased safety of the operating plant [5]. The US Nuclear Regulatory Commission Licensee Event Report [6] "Loss of Cooling to the Unit 1 and Unit 2 Shutdown Board Rooms due to Faulted Chiller Coils" (highlighted part on Figure 1) can be used as example, because it does not transparently address OEF process weakness as

contributor to the event, but suggests that the affected NPP had similar problems in the past which resulted in unsuccessful actions ("lack of existing actions to address natural phenomena affecting plant equipment").

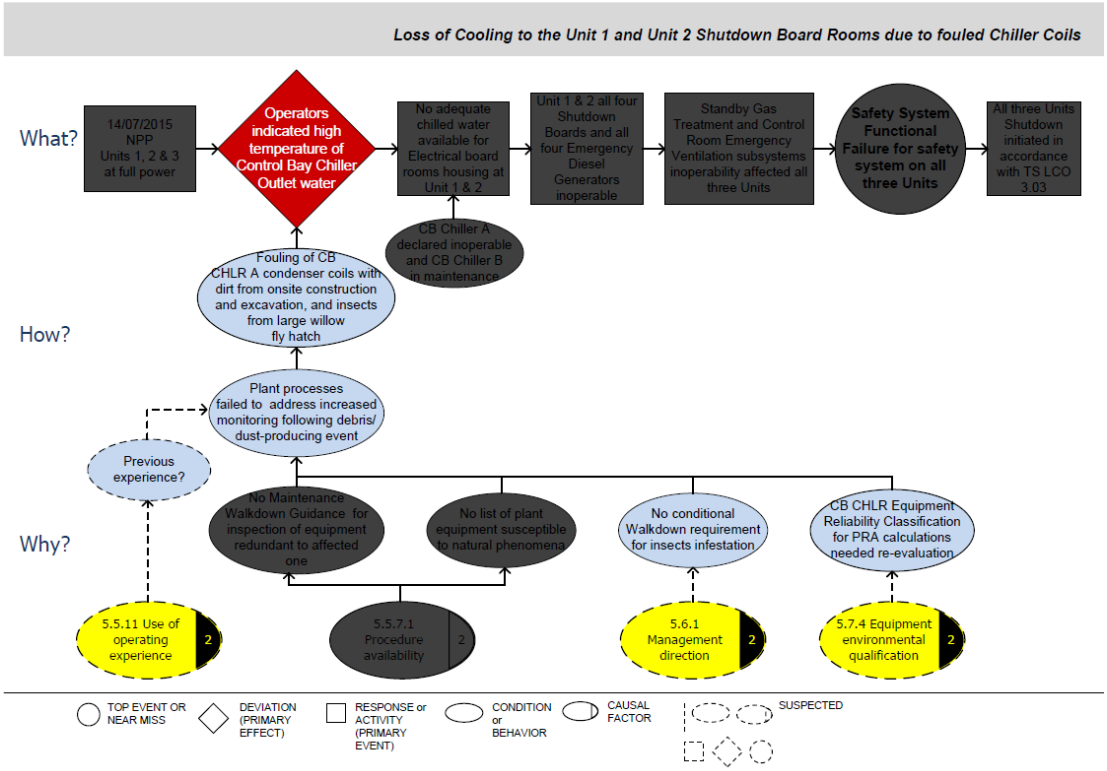


Figure 1: 1st case

The additional causes, "No conditional walkdown requirement for insect's infestation" and "CB CHLR Equipment Reliability Classification for PRA calculations needed re-evaluation" (Control Building Chiller Equipment Reliability Classification for Probabilistic Risk Assessment…), could give a sign that some weaknesses exist in the area of Management Directions and/or Equipment Environmental Qualification process.

2.2 Example 2

The ECFC of second example "Unit 1 'B' Inboard Main Steam Isolation Valve, HV141F022B closed during surveillance test which caused a SCRAM on Unit 1"

(highlighted part on Figure 2), shows with more credibility, that in reporting organisation, management deficiencies may exist.

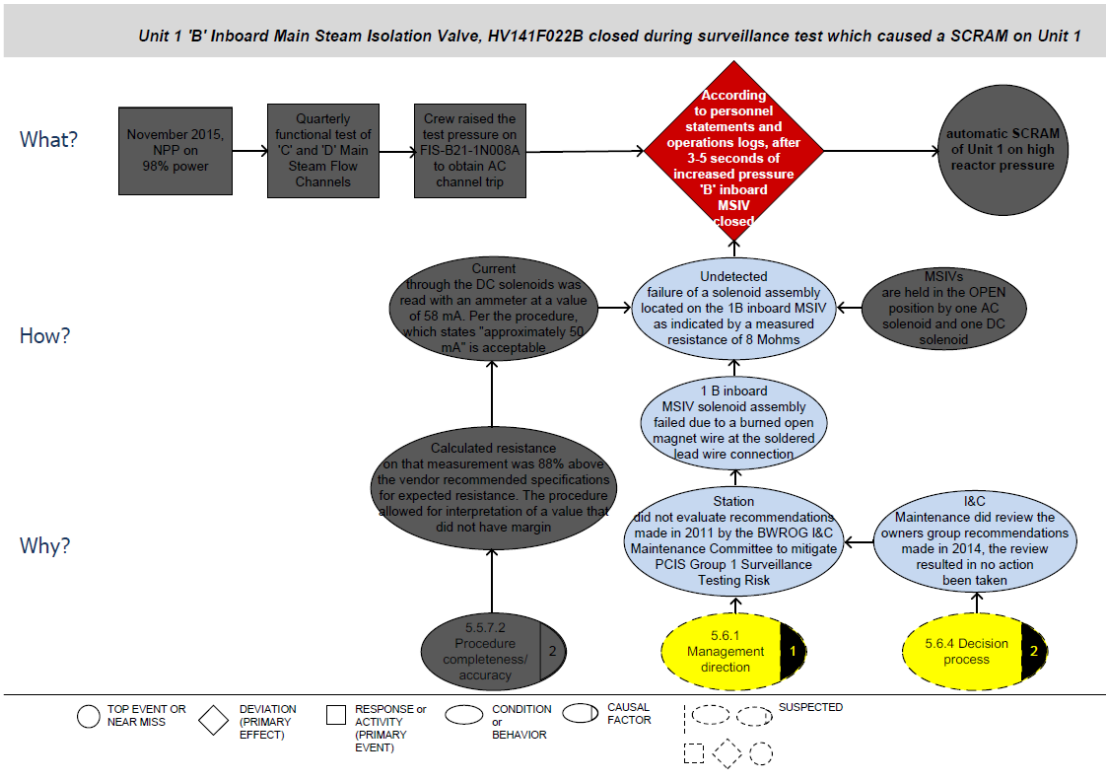


Figure 2: 2nd case

In both ECFC examples (Figure 1, Figure 2), it is easy to address suspicious deficiencies (dot line in the diagrams) and point to area where additional investigation may take a place. In both examples, many reasons for these weaknesses may exist, and they should be additionally investigated.

It is expected that reporting site provides adequate explanations or taken measures to requesting authority, but if not, then it is the authority's duty to raise the safety question about findings.

3. Qualification of the Risk

For efficient accident prevention, decision makers of the organisation dealing with hazard should base action plans on risk assessment results. To estimate the risk of potential accident, it is necessary to assess possible consequences and probability of occurrence [7]. By use only Short ECFC, it is obvious that quantification of risk is not possible, but for the most of decisions on internal Minor Event or external Operational Experience (OE) reports, precise calculations are not necessary. Therefore, qualitative approach is very welcome.

The following two subchapters, Potential consequences and Probability of similar event simplify risk assessment [8] by qualifying these two parameters which define the risk.

3.1 Potential consequences

To assess possible consequences of event described in event report (e.g. external OE report), it is important to be familiar with own operating organisation and understand its design and safety features. Skilful, knowledgeable and experienced decision makers can foresee potential consequences on safety if the similar even occurs in their organisation. In Short ECFC, it is easy for them to determine main safety aspects by assessing the primary event line in ECFC.

In the example on Figure 3: Primary event line - Case 1, it is visible that Main Steam Isolation Valve (MSIV) of the affected NPP inadvertently closed and produced shutdown signal. Reader should be able to envisage this event in the organisation under his/her responsibility and foresee possible specific safety consequences. There are different designs of NPP, so the potential consequences for them could easily differ. E.g. in Pressurised Water Reactor NPP type, this event would be considered as design bases event that triggers only protective system and not safety. However, closing function of MSIV is of highest importance for safety and wider perspective could be applied.

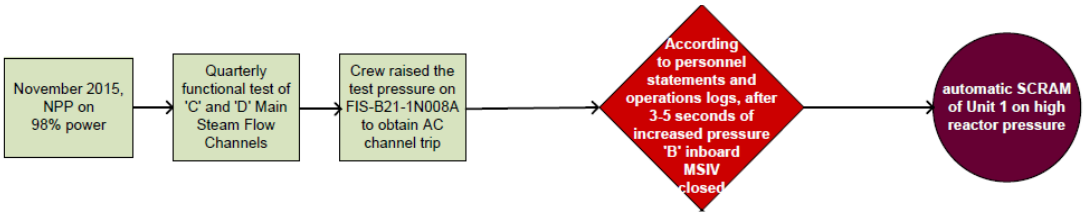


Figure 3: Primary event line - Case 1

In the second example on Figure 4: Primary event line - Case 2, there is a chain of happenings that produced inoperability of several safety systems and affected more units. In this NPP, the design is very specific and, comparing to other designs, consequences could significantly differ. Safety degradation assessment, in this case, is more concentrated on specific scenarios to stakeholder's NPP in the case of similar initiating event – Loss of Chilled Water system.

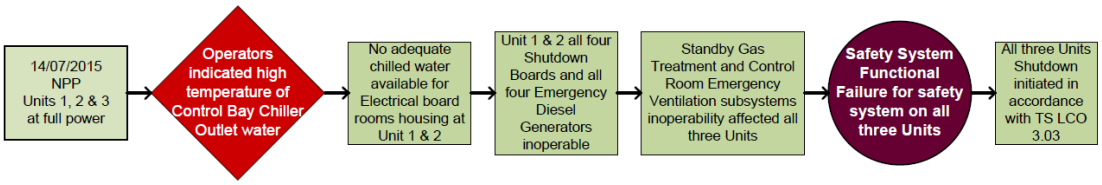


Figure 4: Primary event line - Case 2

3.2 Probability of similar event

Other important element of risk assessment is probability of similar event. Again, decision maker should be capable to estimate probability of similar event to occur in his/her NPP.

In first example on Figure 5: Causal sequence – Case 1, it may be estimated on many sites that insect's invasion is not probable but construction and excavation work could produce

similar effects. Consultation with operator could be the first step before making any decisions.

In second example on Figure 6: Causal sequence – Case 2, it should be necessary first to find faulted solenoid assembly model and manufacturer, and then set some action plans. These details are important part of report, so it shouldn't be problem to find them there.

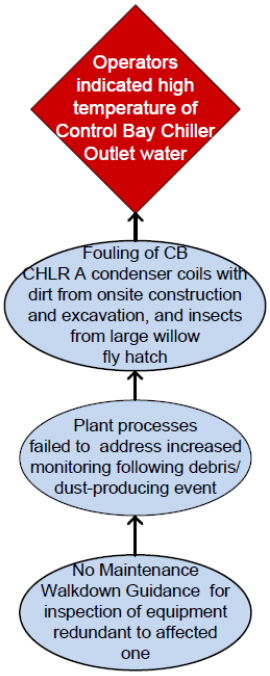


Figure 5: Causal sequence – Case 1

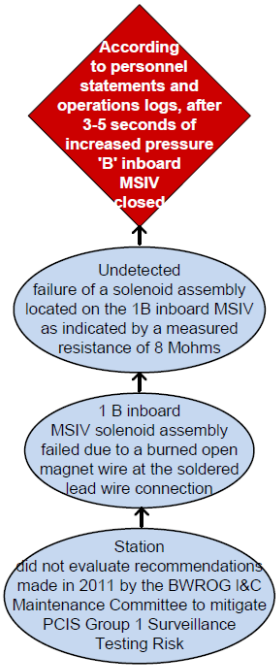


Figure 6: Causal sequence – Case 2

4. Benefits from use of Short ECFC diagrams

Through these two examples, it is shown that events can be efficiently presented in the simple form. For the most of NPP event reports, the important parts of report are clearly visible, but those "hidden" should be visible too. The Short ECFC diagram used for that purpose would enable reader to quickly understand the event evolution and causation.

The Short ECFC diagram presents not only course and causation of event, but also significantly helps in highlighting weak signs of degraded safety. These signs can be easily noticed by decision makers, and push them to foresee possible consequences that are not explicitly presented in original report.

Furthermore, dotted-line figures, although just assumptions, are based on the facts which causes may need additional investigation. Usually they didn't result in described event(s), but they are weaknesses that may evolve in significant event if adequate attention is not paid.

The technical part of original event report is usually very specific and many readers or stakeholders don't really need to understand all specificities of affected technological process or equipment. It is important that decision makers possess adequate experience

and knowledge of safety aspects of design and operation. The Short ECFC diagram can also help them to estimate the risk of leaving deficiencies unsolved. This means that they should understand causality i.e. be able to estimate probability of reoccurrence, and potential safety consequences, which gives them idea of risk and possible decisions.

Although Short ECFC is the best if drawn by expert from affected organisation, it is important to note that author of Short ECFC could also be from external organisation. Furthermore, Short ECFC can be used for internal as well as external OE event, i.e. other similar organisation event.

It is also very important to standardise approach in presenting events by graphical tools for greater effectiveness in accident investigating and reporting. ECFC technique has being used for a long time in many areas for analysing problems [9]. Therefore, it is somehow natural to use this type of diagram for presenting the events. According to this paper author's experience in use of presented form, it looks that readers can be familiarized with this approach very quickly. It is advisable to keep the standardised, user-friendly visual appearance in every Short ECFC report.

References

[1] IAEA-TECDOC-1600. Best Practices in the Organisation, Management and Conduct of an Effective Investigation of Events at Nuclear Power Plants. IAEA, Vienna, 2008. ISBN 978–92–0– 109308–0.

[2] Human Performance Enhancement System, INPO 90-005, Atlanta: Institute of Nuclear Power Operations, (1990).

[3] Guidelines for Safety Investigation of Accidents. ESReDA, Working Group on Accident Investigation (Eds.). Oslo, 2009.

[4] Ziedelis s., Noel M. Comparative Analysis of Nuclear Event Investigation Methods, Tools and Techniques, EUR 24757 EN, ISBN 978-92-79-19712-3, European Commission 2011.

[5] SF-1. Fundamental safety principles: safety fundamentals. IAEA, Vienna, 2006. ISBN 92–0–110706–4.

[6] US Nuclear Regulatory Commission, Licensee Event Report Search: https://lersearch.inl.gov/Entry.aspx .

[7] IAEA safety glossary: terminology used in nuclear safety and radiation protection: 2007 edition, IAEA, Vienna, 2007. ISBN 92–0–100707–8.

[8] Wikipedia: https://en.wikipedia.org/wiki/Risk_assessment .

[9] Events and Causal Factors Analysis. Technical Research and Analysis Center SCIENTECH, Inc. Idaho Falls, August 1995. SCIE-DOE-01-TRAC-14-95.

HIAD - Hydrogen Incident and Accident Database

Daniele Melideo, Eveline Weidner, Francesco Dolci, Pietro Moretto

European Commission, Joint Research Centre - Directorate for Energy, Transport and Climate

Westerduinweg 3

1755 LE Petten, The Netherlands

Abstract

The Hydrogen Incident and Accident Database (HIAD) has been designed to hold high quality information on accidents and incidents related to hydrogen production, transport (road/rail/pipeline), supply and commercial use. The database is updated with the latest information concerning each event in order to take advantage of the most recent outcomes of accident investigations. The database has been set up to improve the understanding of hydrogen unintended events, to identify preventive measures and strategies, to avoid incidents/accidents and to reduce the consequence if an accident occurs. The experience of the past years has revealed some shortcomings and generated improvement needs for HIAD. Some of the original goals related to risk assessment had to be abandoned, due to the limited amount of statistics available on faults and failure modes. A major overhaul of the database structure and interface was undertaken. The new version is mainly focused on facilitating the sharing of lessons learned and other relevant information related to the safety of hydrogen technologies. The database will contribute to improve safety awareness, enabling the users to benefit from the experiences of others as well as to share information from their own experiences. The main challenge at present is to attain a clear commitment of the fuel cells and hydrogen technology community to provide sufficient information on safety relevant events.

Keywords: Hydrogen database safety lesson learned

1. Introduction

Current trends in energy supply and use are economically, environmentally and socially unsustainable. Without decisive action, energy-related emissions of carbon dioxide (CO2) will more than double by 2050 and increased fossil energy demand will heighten concerns over the security of supplies. Within this scenario, low-carbon energy technologies will have a crucial role to play. In order to achieve reductions in greenhouse gas emissions,

increased energy efficiency, renewable energy sources, carbon capture and storage and new transport technologies will all require widespread deployment.

Hydrogen and fuel cell technologies can support climate change and energy security goals in several sectors of the energy system, such as transport, industry, residential and power generation sector. Hydrogen has the potential to connect different energy sectors and energy transmission and distribution networks, and thus increase the operational flexibility of future low-carbon energy systems [1-3].

Hydrogen technologies and applications should provide the same level of safety, reliability and comfort currently experienced by consumers for established technologies. Compared to the fossil energy carriers used at present, hydrogen introduces different safety and regulatory issues which need to be understood and tackled. Hydrogen has already been used and safely handled for many years in several application areas (e.g. in aerospace technology, chemical processing, food and electronic industries). Information related to hydrogen incidents and accidents is available on the internet and in literature, but the scientific community identified a gap due to the fragmented experience and knowledge on hydrogen safety. The Hydrogen Incident and Accident Database (HIAD) has been created as a repository for data describing undesired hydrogen-related events (incidents or accidents). HIAD had originally been developed in the frame of the HySafe EC co-funded Network of Excellence (NoE).The main purpose behind the creation of HIAD was to be an international hydrogen accident and incident reporting platform and to assist all stakeholders in better understanding hydrogen-related undesired events.

2. The Hydrogen Incident and Accident Database (HIAD)

The Hydrogen Incident and Accident Database (HIAD) has been designed to hold high quality information on accidents and incidents related to hydrogen production, transport (road/rail/pipeline), supply and commercial use. The database is updated with the latest information concerning each event in order to take advantage of the most recent outcomes of accident investigations.

HIAD had originally been developed in the frame of the HySafe EC co-funded Network of Excellence (NoE), which aimed at filling the lack of structured information clearly identified by the scientific community [4]. HySafe NoE (2004-2009) aimed at facilitating the safe introduction of hydrogen as an energy carrier, contributing to the safe transition to a more sustainable development in Europe [5]. The HySafe NoE network brought together competencies and experience of 24 partners from 12 European countries and one partner from Canada, representing private industries (automotive, gas and oil, chemical and nuclear), universities and research institutions; more than 100 scientists performed integrated research activities related to hydrogen safety issues. The main objective of the HySafe NoE network was to strengthen, integrate and focus fragmented research efforts to provide a basis allowing the removal of safety-related barriers to the deployment of hydrogen as an energy carrier. Synthesis, integration and harmonization of these efforts aimed at breaking new ground in the field of hydrogen safety and at contributing to the increase of public acceptability of hydrogen technologies within Europe by providing a basis for communicating the risks associated with hydrogen. One of the means to achieve those objectives was the development and establishment of the Hydrogen Incident and Accident Database, HIAD. After the end of HySafe NoE in 2009, a new legal entity was

founded to continue the activities such as HIAD and the biannual International Conference on Hydrogen Safety. The new legal entity is a non-profit organization, the International Association for Hydrogen Safety (IA HySafe), whose mission is to facilitate the international coordination, development and dissemination of hydrogen safety knowledge

The Hydrogen Incidents and Accidents Database HIAD had originally been designed as a multi-tasking tool: a communication platform suitable for risk and safety lessons as well as a potential data source for risk assessment [6]. The tool had the ambition to promote both the safety performance of existing hydrogen technologies and safety actions after events involving hydrogen.

Specifically, HIAD was originally intended to:

- contribute to the integration and harmonization of fragmented experience and knowledge on hydrogen safety;
- contribute to the progress in common understanding of hydrogen hazards and risks;
- constitute a reliable tool that provides inputs for safety and risk assessment [7];
- enable generation of common generic accident and incident statistics;
- serve as a common reference database for ongoing data collection and storage;
- keep the industry updated with recent hydrogen events, along with trend analyses;
- represent a reference source for the understanding and experience transfer of hydrogen accident phenomena, scenarios and hazard potential.

In order to achieve those objectives, HIAD data collection was and still is characterized by a significant degree of detailed information about recorded events (e.g. causes, releases, fires, explosions, consequences). The data are related not only to real incident and accidents but also to hazardous situations and false positive events.

The partners in the NoE HySafe collected and entered a considerable amount of data into HIAD. A quality assurance plan was developed to ensure a sufficient level of quality for all entered data. Each event submitted by a provider to HIAD was therefore subjected to a quality assurance process managed by a group of experts. This process was in place till the end of the HySafe project (2009).

The experience of the past years has revealed some shortcomings and generated improvement needs for HIAD. The goal of HIAD to become a tool for quantitative risk assessment was too ambitious, due to the limited number of events made available by a technology which has not yet attained full market maturity and is not yet deployed extensively. Available statistics on failures and failure modes of individual components belonging to the hydrogen technology chain are still not enough to allow for reliable quantitative analysis. This is the reason why activities on Quantitative Risk Assessment (QRA) of hydrogen technologies still now make use of failure statistics from different,

though partially equivalent, technologies such as off-shore gas industry data. Finally, another identified issue was that after the end of NoE HySafe the database has not been supported financially by the community of hydrogen stakeholders. This had as a consequence that the pool of international experts which were providing quality assurance was not available anymore and that the communication channels linking potential event providers with the database had disappeared together with the network. After the end of the project, JRC became the only data provider, only publicly reported events have been collected and the quality assurance process had to be organised relying only on internal expertise. [8].

Based on the experience gained from HIAD operation of the previous years, JRC performed in 2016 a thorough analysis of the database functions, from a strategic as well as operative point of view. As a consequence, it was found that a complete overhaul of the database was required, addressing shortcomings in several areas.

The usefulness of the database as a tool providing information to the hydrogen and fuel cell community was also identified as an area for improvement. Among the various objectives of the database, the one related to making HIAD an input tool for QRA was far from being achieved, for the reason mentioned above. To maximise the impact of the database it was necessary to focus on what could be learned from events. These lessons learned could result from the analysis of each individual event and/or from summarising conclusions from a cluster of similar events specific to each sub-technology. The dissemination of these lessons to the whole hydrogen technology Community had to become the overarching goal of the tool; as a matter of fact, the analyses of the incidents and accidents recorded in the database will help to identify lessons learned, which then can be disseminated throughout the Community to prevent a recurrence of similar accidents. The detailed assessment will be of high value in terms of establishing improvement needs in safety, health and environmental protection. This shift in focus is very similar to the one experienced by a comparable database developed by the US Department of Energy [9]. To allow for this strategic re-focussing, the structure of HIAD had to be reviewed. The need of providing a tool for QRA required an extremely high level of detail for the description of events. The thorough analysis mentioned above identified a considerable number of fields which had remained empty for all the events. The re-structuring of HIAD started with the simplification of the events descriptors by merging several fields and reducing the level of detail for fields in which data were non-existent. In addition a qualitative description of the event is now encouraged, rather than the previously compulsory quantitative data entries which are now optional.

The need for improvement of the data collection process is another of the strategic aspects emerging from the mentioned analysis. Getting access to information on safety related events is a challenge, as facility owners or project coordinators, with some exceptions, do not have any obligation to provide data to HIAD. Several publically funded projects are mandated to report any incidents to HIAD, but this does not apply for all European and nationally funded projects. Establishing a requirement for any publically funded project to report any incident to HIAD would improve the data collection process considerably. Another option to get better access to safety related information is to have a commitment to report to HIAD as a requirement by permitting authorities. These measures would ensure a robust and distributed, European-wide network of data providers.

As to the event data itself, the attainability of accurate event reports is also a concern. The providers of an event description tend to give only a minimal amount of information, which limit any further analysis and lessons learned from the event. Relying on publically available information is not an option, as public press journal articles almost never provide data with the required quality and resolution. HIAD would profit from full accident reports made available by internal investigators, local authorities and/or first responders. Contacts with associations of first responders are on-going.

Finally, the interface of HIAD for entering event data was not easy to use as it had been developed for expert operators, not for end users. As mentioned above, the ambitious goal to serve as quantitative risk assessment tool had as a consequence that the level of details for a full event description was rather daunting and involuntarily encouraged misreporting and incomplete event description. Experience showed that the amount of detailed data required must be balanced with the average availability of information provided for a typical event. Therefore a simplification of HIAD users' interface was deemed critical, from event input to data selection and retrieval.

3. The new version of HIAD

The upgrade work on HIAD was started by the JRC with close collaboration of the Fuel Cells and Hydrogen Joint Undertaking (FCH JU). The development of a new version of the database in order to specifically collect incidents from FCH JU projects (namely FCHJU-HIAD) began in 2016. The new database has a significantly simplified structure: based on an in-depth analysis of the data quality collected in the previous years, entry fields were redefined and reduced, resulting in a more streamlined user interface compared to the older HIAD version. The front-end and back-end of the database were completely redesigned: a new database structure and a new user interface has been redesigned. In addition, a template for data collection was developed; it includes explanations for each entry field and guides the reporting activities. The access to the FCHJU-HIAD database is limited only to staff of the FCHJU and to the HIAD team.

At the same time JRC will maintain a public database which will be further developed in the future (namely HIAD 2.0)[10]. This database will only contain publically available reports on events and incidents. The FCHJU-HIAD database and HIAD 2.0 will be completely independent from each other. Both databases will share the same graphical front-end user interface (see Figure 1).

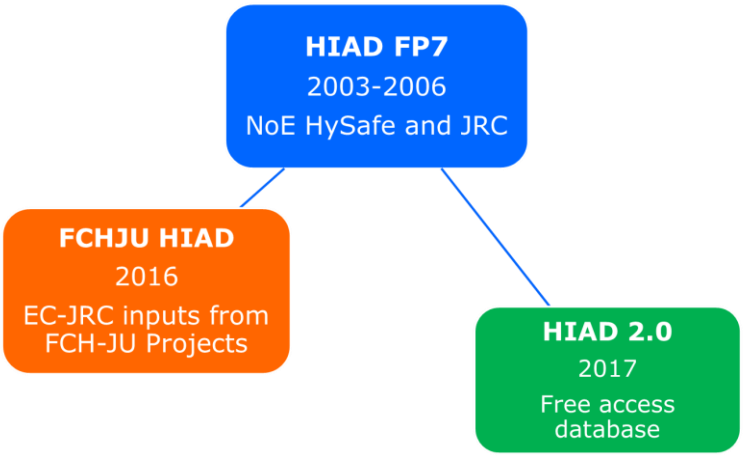


Figure 1. New databases and their relation with HIAD.

4. The structure of the new databases

The events inserted into the new databases are divided into three main categories, giving the first quick piece of information about the full event scenario: "Event classification", "Physical consequences" and "Application" (see Figure 2). The "Event classification" is grouped in the following sub-categories:

- Hydrogen system initiating event: event not directly caused by the hydrogen system (e.g. sudden, unintended damage to hydrogen vehicles, installations or plants caused by impact, high voltage, failure of conventional components, etc.)

- Non-hydrogen system initiating event: event triggered directly by system containing hydrogen (e.g. rupture of hydrogen pipe, valve, tank)

- False positive: emergency alarm or procedure triggered in the absence of any actual problem; a hydrogen sensor giving a false alarm, for instance, falls in this category.

- The "Physical consequences" category is sub-divided in jet fire and explosions, no hydrogen release and unignited hydrogen release; while the "Application" category has several subcategories such as hydrogen production, hydrogen transport and distribution, hydrogen refuelling station, road vehicles, etc.

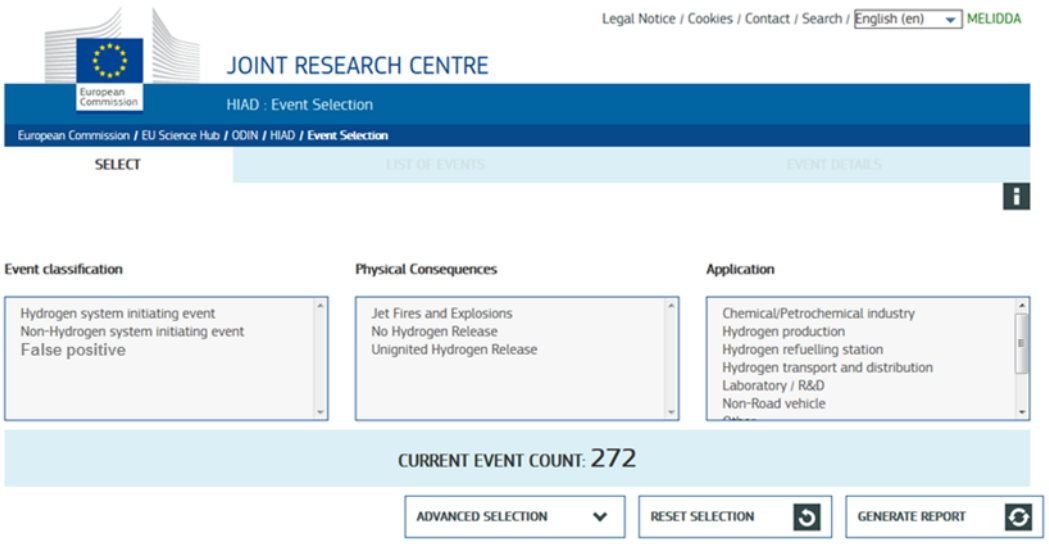


Figure 2. The front-end retrieval page.

- An advanced selection process allows the possibility to filter the event search results using additional fields such as year of the event, cause, etc. (see Figure 3)

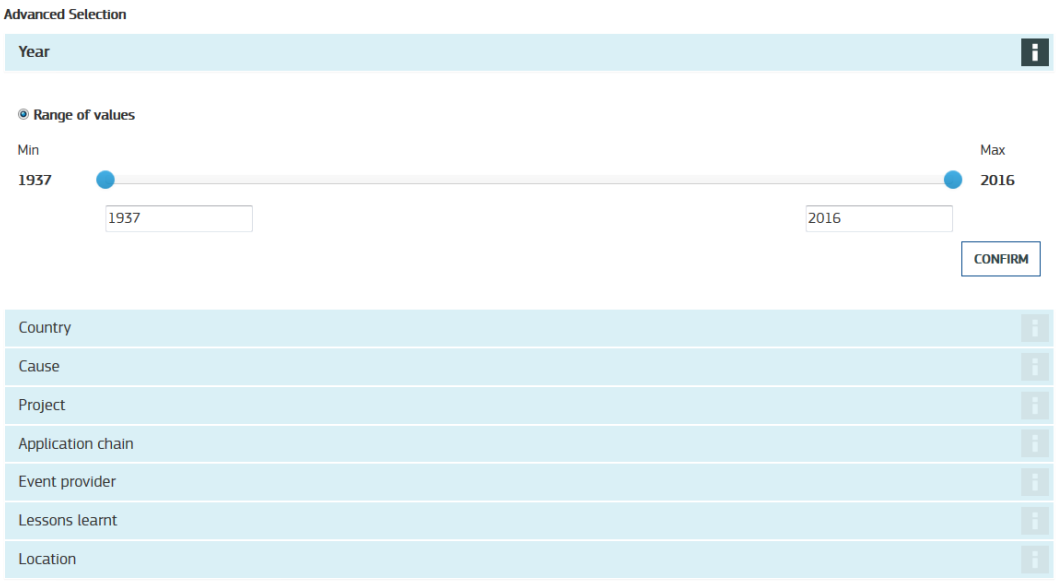


Figure 3. Advanced selection criteria page.

5. Data collection

A dedicated on-line form will be used for reporting any safety-related event. The on-line form welcome page is shown inFigure 4; the form is divided into sub-sections (some of which are mandatory):

- Provider information: the contact information will only be used by the JRC for requesting clarifications on information provided, but will not be disclosed any further and will not be entered in HIAD.

- General information: together with the event category (i.e. "Non-Hydrogen system initiated event", "Hydrogen system initiated event" and "False positive") a summary of the key aspects of the event has to be reported. This summary should specify the causes of the event and the context, the event dynamics, the technical details of the accident and a quantitative description of the effects.

- Initial situation (pre-event): it is a description of conditions prior to the event; it should be mentioned if the event occurred during planned or routine operation; there is also the possibility to specify information on the weather conditions, if considered important for understanding the event

- Application: it is the category related to the type of operation during which the event occurred (such as hydrogen production, hydrogen transport and distribution, hydrogen refuelling station, road vehicle, non-road vehicle, stationary fuel cell, portable fuel cell, laboratory / R&D and chemical/petrochemical industry). By selecting one category, relevant sub-category will appear allowing further specification of the type of application.

- Consequences: it is the description of the physical consequence (i.e. no hydrogen release, unignited hydrogen release and hydrogen release with jet fires and explosions) after the event; it is optionally possible to specify which part failed or was most affected in the event (e.g.: tank of a road vehicle, compressor of a hydrogen refuelling station, etc.); in addition a describe of the consequences to people, equipment and environment (e.g.: which kind of injury, damage, etc.) is request.

- Cause of the event: it is a description of which causes were identified or are deemed most likely (e.g.: human error, lack of maintenance, untrained personnel, etc.)

- Corrective actions taken (if any): the description of the corrective actions already taken to avoid recurrence of the event and if the event required further investigation (for instance official investigation) has to be reported.

- Lessons learned: it is related to any lessons learned from the event; this could consist in improved procedures, new preventive and/or mitigating measures, better training, etc.

- Reference: it is also possible to upload reference documents or pictures of the event, if available.

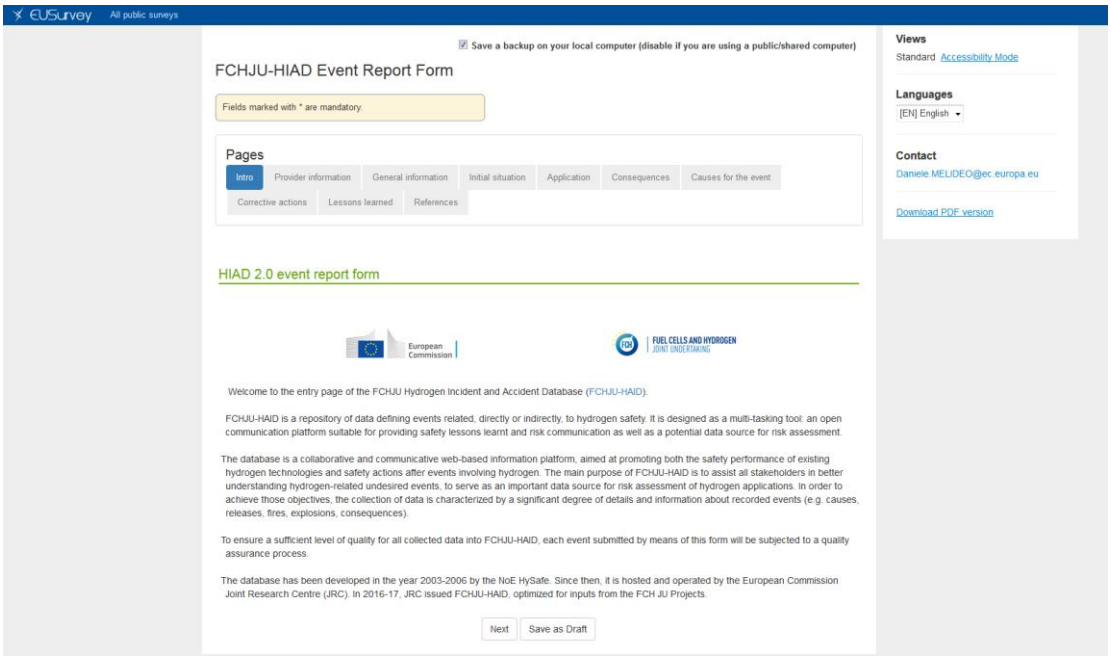


Figure 4. Event report form: first page overview

Previous experience has shown that in some cases the information given in a report form is not sufficiently detailed or that clarifications are necessary. Therefore a direct contact with the event provider is crucial, to prevent misunderstandings and to ensure that a complete picture of the event is available. This will be also necessary in the case of a complex accident, where the description may need further details to enable understanding of the event circumstances and consequences. Once the additional needed information is received, the event will be formatted, entered in HIAD and validated by the HIAD team.

In the specific case of the FCHJU-HIAD, if needed, the acquired information will be processed, analysed and reported with the external support of selected FCHJU Hydrogen Safety Panel (HSP) members (see Figure 5), consisting of a group of recognized hydrogen safety experts. In this case, the experts of the HSP will have access to individual events within FCHJU-HIAD for further analysis and for obtaining the lessons learned together with the JRC HIAD team. This will take place under a confidentiality agreement with the selected HSP experts.

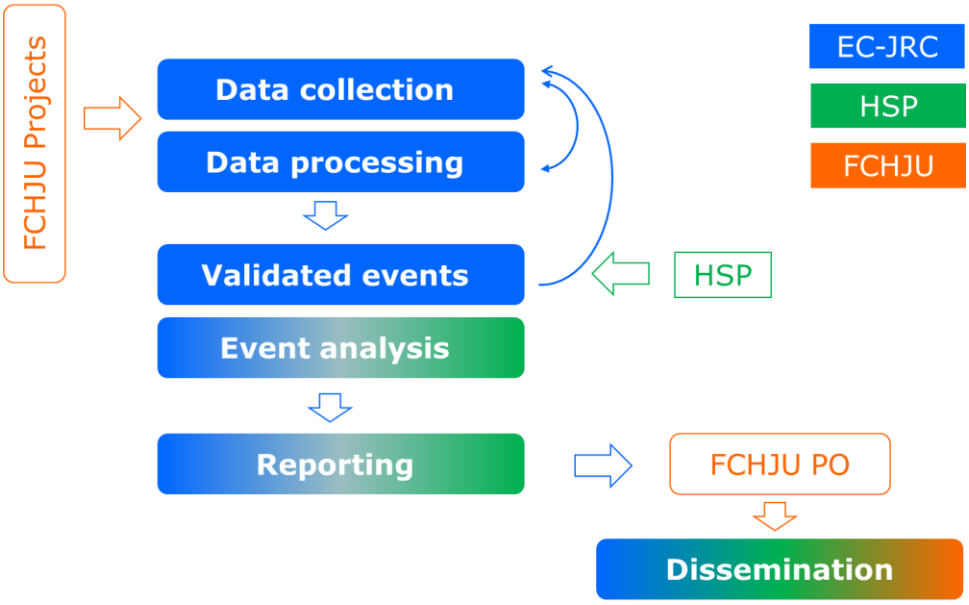


Figure 5. Data collection, analysis and reporting process.

6. Current status and outlook

Based on the experience gained from HIAD operation of the previous years, JRC has performed a thorough overhaul of the HIAD database. A strategic re-focussing was undertaken, to facilitate the sharing of lessons learned rather than providing a tool for QRA. The original goal of providing input to QRA could possibly be revisited in case the knowledge on failure modes and statistics advances to a sufficient degree. The simplification of the user interface will enable a more effective event reporting and subsequent analysis. The database is now separated into a public (HIAD 2.0) and a limited access (FCHJU-HIAD) section. All reported incidents will be analysed by safety experts and the lessons learned from events will be made available to the FCH community.

The data entered into FCHJU-HIAD from FCHJU Projects will be owned by the FCHJU, whereas the database itself is property of the JRC. The events already entered in HIAD during the FP6 and FP7, before the start of the collaboration with the FCH2JU are belonging to the broader technology and scientific community and have been transferred to the HIAD 2.0.

Initial contact with the FCHJU Projects required to report to FCHJU-HIAD has been established. Future efforts by the JRC, assisted by the safety community, will be to encourage other funded projects to report into HIAD 2.0, and in general increase the awareness of this tool for the hydrogen and fuel cells community.

References

[1] Rifkin J, Carvalho M, Consoli A, Bonifacio M. *Leading the way to the third industrial revolution*. Eur Energy Rev December 2008;1:4-18 [Special edition].

[2] Nakata T, Silva D, Rodionov M. *Application of energy system models for designing a low-carbon society*. Prog Energy Combust Sci 2010;37:462-502.

[3] Carvalho M, Bonifacio M, Dechamps P. *Building a low carbon society*. Energy 2010;36:1842e7.

[4] Funnemark E, Eldor JE, Haugom GP. *Identification and review of database for reliability data*. HyApproval; Deliverable 4.4; 2006.

[5] Jordan T. *HySafe - the network of excellence for hydrogen safety*. In: Proceedings of the Sixteenth World Hydrogen Energy Conference; 2006.

[6] M. Cristina Galassi, Efthymia Papanikolaou, Daniele Baraldi, Espen Funnemark, Erling Haland, Angunn Engebø, Gerd Petra Haugom b, Thomas Jordan c,d, Andrei V. Tchouvelev. *HIAD e hydrogen incident and accident database*. International Journal of Hydrogen Energy Volume 37, Issue 22, November 2012, Pages 17351-17357

[7] Funnemark E, Engebø A. *Development of tools for risk assessment and risk communication for hydrogen applications*. In: Proceedings of the First International Conference on Hydrogen Safety; 2005.

[8] Kirchsteiger C, Vetere Arellano AL, Funnemark E. *Towards establishing an international incidents and accidents database (HIAD)*. J Loss Prevent Proc 2007;20:98e107

[9] https://h2tools.org/lessons

[10] https://odin.jrc.ec.europa.eu/odin/index.jsp

Cognitive Inhibitors for Threat Assessment and Automated Risk Management

Jochen L. Leidner[1, 2] and Tim Nugent[1]

[1] Thomson Reuters, Research & Development,

The Reuters Building, 30 South Colonnade,

London E14 5EP, England, United Kingdom.

[2] University of Sheffield, Department of Computer Science,

211 Portobello, Sheffield S1 4DP, England, United Kingdom.

Abstract

The analysis of risks and threats, whether it is on the macro level (geopolitical security) or micro-level (personal well-being or enterprise risk management) suffers from issues resulting from human limitations: it is ultimately humans that operate their own lives, run companies and governments. Unfortunately, humans suffer from cognitive limitations that have an adversarial impact on their ability to manage risks and threats: they create static authority-based organizations instead of empowering agile teams; they compartmentalize to manage complexity, which leads to blind spots (e.g. the 2008 financial crisis) and inconsistent behaviour (we have all seen smoking medical doctors); and they lack the ability to globally evaluate quantitatively complex systems, tending to forget or under-rate activities that are further removed from their personal "centre of gravity" as the saying "out of sight, out of mind" suggests. In this paper, we demonstrate how some of these human and organizational limitations can prevent us from conducting effective risk and threat management by giving examples from geopolitical and natural disaster risk, environmental risk, people risk, company risk, supply chain risk, and technology risk. By focusing on the risk identification stage, we show how software tools can be used to make the risk management process more objective, in the sense of inter-personally verifiable and consistent. We conclude that risk and threat management should attempt to overcome cognitive limitations by installing an auditable process that uses a human-machine collaborative approach.

***Keywords**: risk mining, computer-supported risk identification, risk analysis, natural language processing, machine learning.*

1. Introduction

Foresight is a field that can aid public policy: to anticipate possible futures as they are influenced by current and likely future advances in the sciences and technology are at its core, and it *"explores the future of scientific and technological achievements and their potential impacts on society. It aims to identify the areas of scientific research and technological development most likely to bring about change and drive economic, environmental and social benefits for the future*." (European Commission, 2017). The anticipation of future trends includes both the positive implications (opportunities) and negative implications (risks) associated with companies, people, topics/themes, countries, movements. Risk identification is the creation of a risk register or inventory of identified risks or threats. Threat assessment is a structured group process used to evaluate the risk posed by something or someone.

The analysis of risks and threats and their subsequent assessment, whether it is on the macro level (geo-political security) or micro-level (personal well-being or enterprise risk management) suffers from issues that are a result of human limitations: it is ultimately humans that operate their own lives, run companies and governments. Unfortunately, humans suffer from cognitive limitations that have an adversarial impact on their ability to manage risks and threats: they create static authority-based organizations instead of empowering agile teams; they compartmentalize to manage complexity, which can lead to blind spots (e.g. the 2008 financial crisis) and inconsistent behaviour (we have all seen smoking medical doctors); and they lack the ability to globally evaluate quantitatively complex systems, tending to forget or under-rate activities that are further removed from their personal "centre of gravity" (centre of attention, personal geographic centre, as captured by the saying "out of sight, out of mind").

In this paper, we will focus on the negative risk, and on those cases of risk surrounding companies, people and topics in particular, how human cognitive imperfections can lead to oversights, and how technology can usefully supplement human cognitive imperfections for better risk management. We demonstrate how some of these human and organizational limitations can prevent us from conducting effective risk and threat management by giving examples from geopolitical and natural disaster risk (Leidner and Schilder, 2010) people risk (Leidner and Nugent, 2017), company risk (Nugent and Leidner, 2016), supply chain risk (Carstens et al., 2017) and technology risk. By focusing on the risk identification stage, we show how software tools can be used to make the risk management process more objective, in the sense of inter-personally verifiable and consistent). We conclude that risk and threat management should attempt to overcome cognitive limitations by installing an audit-able process that uses a human-machine collaborative approach.

Our main contributions are: 1. a discussion of the effect on cognitive inhibitors and cognitive dissonance on an organization's ability to detect risks early, and to deal with them effectively; and 2. a demonstration how software tools can help with a more responsive and consistent approach that overcome some of these issues.

2. Humans: Cognitive Inhibitors and Cognitive Dissonance

2.1 Cognitive Inhibitors

Humans have many shortcomings when dealing with risk. Taleb (2007) pointed out at length how humans struggle to deal with probabilities, and how that adversely affects the area of finance. Humans are not just limited with respect to assessing probabilities, they also are slow at processing data, and poor at handling it consistently. For example, 10 analysts tasked with the job of tracking fires in the same daily newspapers will almost always come up with disparate results based on humans' limited ability to concentrate on quasi-mechanical tasks.

At a higher level, we observed that in many organisations such as governments and corporations, risk analysis is highly specialised and compartmentalised; in other words, while there may be many roles, each of which are concerned with particular types of risk (e.g. a bank's CRO may focus only on financial risk), there is typically no function that deals with the "other" risk types not covered by anyone else. This may also be true in other organizations, such as governments or NGOs. Generally, an organisation can suffer from such a "tunnel view" of risk, which can be seen as a form of selection bias. These and other human and organisational limitations motivated our research into computer supported approaches to risk identification.

2.2 Cognitive Dissonance

Dealing with risks and the impacts of them once they materialise can work out quite differently based on an organization's culture.

Syed (2015: 3-40) contrasts a non-learning system and a *learning system* based on two case studies, one from the medical domain and one from the air transportation domain. In the former, errors are often not admitted because there is a lack of openness, learning, feedback and continuous improvement, whereas in the latter, open information sharing across organisation and national borders promotes self-improvement, which means that at least the same types of error become less likely to re-occur.

In psychology, *cognitive dissonance* (Festinger (1957); Syed (2015: 69-116)) is the notion that any group or individual will attempt to reconcile their beliefs. Festinger's (1957) cognitive dissonance theory suggests that we have an inner drive to reconcile all our attitudes and beliefs to make them harmonic (and to avoid disharmony or dissonance). In a situation of conflicting beliefs a feeling of discomfort or friction is felt, which leads to a change of one's beliefs to reduce this discomfort. Importantly, this mechanism, which is useful as such, as it aims to avoid or reduce inconsistency ("principle of cognitive consistency"), can actually lead to irrational behavior.

Our conjecture here is that any external tool that provides an explicit documentation of identified risks (including the automatic production of tentative risks for review) could help reduce the effects of cognitive dissonance, since deriving risks from external sources in a transparent, objective and automatic way should make the process more immune to "group think". In the next section, we describe one such technology that could serve such a purpose.

3. Machines: Computer-Supported Risk Identification

Many organisations have long had news analytics functions (also known as *content analysis* or *news analytics*) to track topics of significance, either automatically (typically based on news keyword alerts) or manually (newspaper clippings).

The attempt to create a holistic risk and threat management by applying tools, e.g. for computer-supported risk identification, is relatively new (Leidner and Schilder, 2010; Leidner 2015; Nugent and Leidner, 2016; Leidner and Nugent 2017). In this section, we argue that tool support by computational tools can supplement human skills so that together, more consistent risk management can be accomplished.

We developed an approach (ibd.) that frames the problem as a binary relation extraction task between an entity (e.g. a person, a company, a topic) and a risk type (Table I). We built a semi-automated system for inducing a risk taxonomy of 4,000+ risk types, arranged in a graph (Leidner and Schilder, 2010). This permits us to use a risk type taxonomy, which is both detailed in granularity, data-driven/empirical (it is acquired from the World Wide Web), and up to date. As technologies emerge and geo-political situations change, risks change, and so do their names. But with our taxonomy learning approach, risk terms like "Brexit" (Britain's risk pertaining to existing the European Union) or "DDoS" (Distributed Denial of Service Attack) are coined, and can be identified by our risk taxonomy learning procedure.

Table I: Example Risk Tuples and Potential Application Domains.

Example Risk Tuples	**Application Domains**
Kodak — bankruptcy risk ‹*COMPANY-NAME*› IS-EXPOSED-TO ‹*RISK-TYPE*›	Foresight: Finance (investing)
BP — oil spill risk ‹*COMPANY-NAME*› IS-EXPOSED-TO ‹*RISK-TYPE*›	Foresight: Environment (preservation)
John Doe 1[69] *(name of the head of government procurement)* — corruption risk ‹*PERSON-NAME*› IS-EXPOSED-TO ‹*RISK-TYPE*›	Foresight: Anti-Money Laundering Rules (compliance)
John Doe 2 *(government employee)* — radicalisation risk ‹*PERSON-NAME*› IS-EXPOSED-TO ‹*RISK-TYPE*›	Foresight: Law Enforcement (counter-terrorism)
fracking (*hydraulic fracturing*) — skin burn risk ‹*TOPIC*› IS-LINKED-TO ‹*RISK-TYPE*›	Foresight: Health & Safety (medical accident prevention)
oil — geo-political risk ‹*TOPIC*› IS-LINKED-TO ‹*RISK-TYPE*›	Foresight: Political/Global Security (war risk)
uranium — nuclear proliferation risk ‹*TOPIC*› IS-LINKED-TO ‹*RISK-TYPE*›	Foresight: Political/Global Security (war risk)

These terms and phrases from the risk type taxonomy are then looked up in sentences in the vicinity of named entity mentions of companies or persons (and can likewise be

applied to country names, or any topic noun phrase, using the same method). A syntactic analysis of the sentential structure using a dependency parser followed by a supervised machine learning classifier (Nugent and Leidner, 2016) extracts likely pairs of risk-exposed entity (e.g. BP) and type of risk that characterises the kind of exposure in more detail (e.g. oil spill), together with a confidence value between zero (near-certainty that there conjecturing a risk relationship is not warranted by the evidence in a sentence) and one (near-certainty that the sentence supports postulating the given risk type). Figure 1 shows an interactive interface that permits any user to engage in risk profiles based on a drop-down menu for choosing a company, for which all found risks (shown here: for a year's worth of Reuters News 2016-2017) are extracted and displayed. Note that in a sense, journalists are used as social sensors by exploiting stated risks in recent or older news articles, so the quality of the extraction relies both on the quality of our model as well as the reliability of the journalistic reporting.

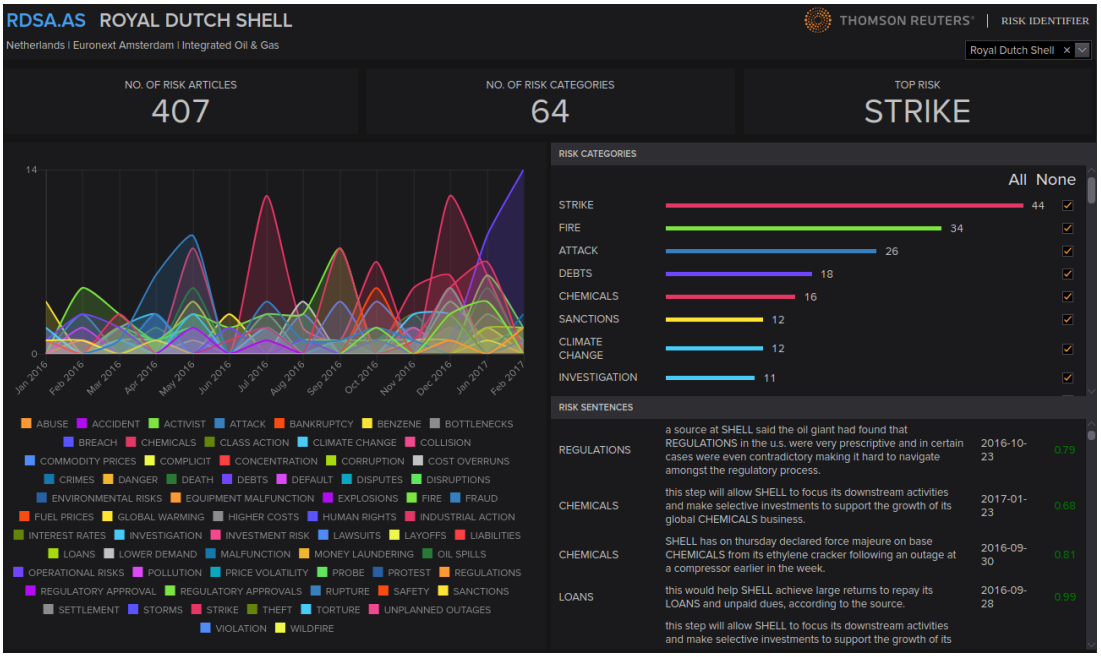


Figure 1. Output from Thomson Reuters Risk Identifier™. Shown is a visualization of risk mentions associated with a sample company; we processed one year of news and extracted risks from it.

Note that peaks in the diagram on the left does not indicate "high risk" as such, but high frequency of mention of a risk type. That is because we are conducting risk identification (including risk type identification), but not estimating the likelihood nor the impact associated with the stipulated risk (these two problems are harder, and are left for future work).

Nevertheless, our risk profiles computed by combining machine learning with fine-grained natural language processing provide a 360 degree "risk radar". While past work has been conducted in document classification, we believe that sentence-level processing is more appropriate in the context of automated risk analysis; imagine an article about a

football club, in which corruption issues linked to one coach are mentioned in passing – a document-level text classification approach would likely tag the whole story as "SPORTS", not "CRIME", missing a vital piece of information.

Returning back to our initial investigation of the shortcomings of human cognition adversely affecting risk analysis, we are now able to argue that computational support improves risk analysis effectiveness more convincingly due to the existence of our capability for mining risk relations: (1) it is computational, so it is resistant to fatigue, which leads to improved consistency. (2) Because it is processed by a computer, it can rapidly analyse thousands of news sources – a modern compute server can easily process 12,000 English news sources without creating a back-log. (3) because the risks are extracted (and thus stipulated) by a machine, the ensuing risk registers are objective, transparent, and not subject to "group think" effects.

4. Related Work

Many computational tools exist for manually constructing models of risk likelihood and impact (Garvey, 2008); as far as we aware, they all require manual entry (directly or indirectly) of their parameters, and none of them provide automation support for the first step of any risk management process, *risk identification*.

Automatic *sentiment analysis* (Liu, 2015) is similar to our presented risk analysis in that negative sentiment could point to a risk, and sentiment is also a relationship (between a holder who has the sentiment and a target that the sentiment is about). However, sentiment is defined as affective state (in psychology/linguistics), like/dislike of a product or feature (in marketing) or bearish-ness/bullish-ness of financial markets (in finance), respectively, and is more subjective in nature (does the holder believe it?), whereas risk exposure, as expressed in a news article, is something that can be reasonably reliably determined by humans.

5. Humans & Machines: Summary & Conclusions

We have discussed the topic of human cognitive shortcomings in the context of risk and foresight. We described a computer-supported risk identification capability (Leidner and Schilder, 2010; Leidner, 2015; Nugent and Leidner, 2016; Leidner and Nugent, 2017) that uses a combination of natural language processing and machine learning to compute an open-ended risk register (threat radar, risk profile) for an entity or topic from trusted textual sources. This capability is very applicable to foresight related topics, from environmental issues over global pandemics to the topic of nuclear proliferation. Its main strength is that it does not rely on a fixed list of keywords, and uses machine learning to induce a risk taxonomy from the World Wide Web (Leidner and Schilder, 2010). We then described how the combination of human analyst and automated risk analysis can overcome some of the described human limitations.

In future work, the correlation of risk types across classes of entities sharing a property should be explored (e.g. all retail companies, all company directors). Processing multiple languages and integrating extracted risk in a unified format, and data mining of risk causality graphs would also be very desirable directions for further research.

Acknowledgements

The authors would like to acknowledge the support of Khalid Al-Kofahi and Mona Vernon. We would also like to thank the contributors to previous research in this space that we built on: Artsiom Matronkin, Frank Schilder, and Steve Pommerville. Finally, thanks to Zdenko Šimić for discussions.

References

Berg, Heinz-Peter (2010), Risk Management: Procedures, Method and Experiences, Reliability: Theory & Applications, vol. **5**, no. #2(17), pp. 62-78.

Budzier, Alexander (2011) "The risk of risk registers – managing risk is managing discourse not tools", *Journal of Information Technology* vol. **26**, 274-276, doi:10.1057/jit.2011.13

Carstens, L., Leidner J. L., Szymanski K., Howald B. (2017), "Modeling Company Risk and Importance in Supply Graphs" In: Blomqvist E., Maynard D., Gangemi A., Hoekstra R., Hitzler P., Hartig O. (eds.) *Proc. ESWC*, LNCS vol. **10250**.

Douglas, Mary (1992), *Risk and Blame Essays in Cultural Theory.*

Elahi, Ehsan (2013), "Risk management: the next source of competitive advantage", *Foresight*, vol. **15**, no. 2, pp. 117-131, https://doi.org/10.1108/14636681311321121

European Commission (2017), "Foresight", https://ec.europa.eu/research/foresight/index.cfm, (online, cited 2017-09-30).

Festinger, Leon (1957), *A Theory of cognitive dissonance.* Stanford, CA, USA: Stanford University Press.

Garvey, P. R. (2008), *Analytical Methods for Risk Management: A Systems Engineering Perspective*, Boca Raton, FL, USA: Chapman-Hall/CRC-Press.

ISO (ed.) (2009), *ISO 31000:2009, Risk management – Principles and guidelines*, Geneva, Switzerland: International Organization for Standardisation (ISO).

Leidner, Jochen L. and Frank Schilder (2010), Hunting for the Black Swan: Risk Mining from Text. *Proceedings of ACL*, Uppsala, Sweden.

Leidner, Jochen L. (2015), *Computer-Supported Risk Identification for the Holistic Management of Risk*. Technical Report, ArXiv Pre-Print Archive, arXiv:1510.08285 [q-fin.GN], 19 pp., https://arxiv.org/abs/1510.08285 (online, cited 2017-09-30)

Leidner, Jochen L. and Tim Nugent (2017), "Towards Automating People and Company Risk Extraction for Extended Due Diligence Support", *26th SRA-Europe Annual Meeting of the Society of Risk Analysis (Europe), Lisbon, Portugal (SRA-E 2017).*

Liu, Bing (2015), *Sentiment Analysis: Mining Sentiments, Opinions, and Emotions*, New York, NY, USA: Cambridge: Cambridge University Press.

Nugent, Tim and Jochen L. Leidner (2016), "Company Risk Identification from Unstructured Sources" *Proceedings of ICDM*, Barcelona, Spain.

Syed, Matthew (2015), Black Box Thinking: Marginal Gains and the Secrets of High Performance. London: John Murray.

Taleb, Nassim N. (2007), *The Black Swan*: *The Impact of the Highly Improbable.*

Voros, Joseph (2003), "A generic foresight process framework", *Foresight*, vol. **5**, no. 3, pp. 10-21, 2003. ISSN: 1463-6689, doi:10.1108/14636680310698379

BIOGRAPHIES

SEMINAR OPENING

Luìs ANDRADE FERREIRA
ESReDA Chairman
Associate Professor
University of Porto,
faculty of Engineering
Porto,
PORTUGAL

Biography

Luis Andrade Ferreira (Associate Professor, Department of Mechanical Engineering, Faculty of Engineering, University of Porto - FEUP) has a degree in Mechanical Eng. (FEUP, 1980), PhD in Mechanical Eng. (INSA Lyon, 1985) and "Agregação" (equivalent to DSc.) by FEUP (2005). Vice-Dean of FEUP (2010 – 2014).

Member of Board of Directors of APMI - Portuguese Association of Industrial Maintenance. Editor of Maintenance magazine. APMI representative in EFNMS - European Federation of National Maintenance Societies.
Chairman of the Board of Directors of ESReDA - European Safety, Reliability & Data Association.
He has published over one hundred and fifty papers in the fields of Tribology, Reliability and Maintenance. He is the author of two books on Tribology and Maintenance.
lferreir@fe.up.pt

SEMINAR OPENING

Georg PETER
Head of Unit
Technology Innovation in Security
European Commission
Joint Research Centre
Ispra,
ITALY

Biography

Dr.-Ing. Georg Peter, born in 1959 in Frankfurt, Germany, holds a degree as Mechanical Engineer and a Ph.D. in nuclear safety. He joined the European Commission in 1989 as a research engineer in the Joint Research Center in Ispra analysing accident scenarios in nuclear power plants and in hydrocarbon facilities by developing and applying complex computer simulation models.

After having been responsible for the Safety & Security Unit of the JRC Ispra site, he was appointed as Head of the Unit "Technology Innovation in Security" in the Directorate "Space, Security and Migration" of the Joint Research Center of the European Commission.

His team is dealing with innovative solutions for the protection and resilience of critical infrastructures in Europe, advanced radio signal processing such as 5G, spectrum sharing and interference studies, scientific support to the European Global Navigation Satellite System Galileo, hazards in chemical industry and consequences of natural hazards to technological installations as well as possible policy aspects of future quantum technologies.

georg.peter@ec.europa.eu

SEMINAR OPENING

Ana Lisa VETERE ARELLANO
Scientific Officer
Technology Innovation in Security Unit[70]
European Commission
Joint Research Centre
Ispra,
ITALY

Biography

She graduated from University of Pavia as a geologist studying rock slides. As Marie Curie Fellow, she studied floods at University of Birmingham. She has worked at the European Commission Joint Research Centre since 2001, in different research areas: natural, environmental & technological risks, energy and information technology. Her expertise lies in risk management, working together with Competent Authorities, research centres, industry and international organisations and participated in several European research projects. She currently leads an IT team underpinning activity on accident analysis, lessons learned, and knowledge management. She has worked with ESReDA since 2005.

ana.vetere@ec.europa.eu

[70] At the time of this publication, Ana Lisa VETERE ARELLANO has moved to the Knowledge for Security & Migration Unit.

SEMINAR OPENING

Zdenko ŠIMIĆ
Scientific Officer
Knowledge for Nuclear Safety, Security & Safeguards Unit
Joint Research Centre
European Commission
Petten,
The NETHERLANDS

Biography

Zdenko Šimić is working as scientist at the EC JRC in the area of nuclear operating experience and safety. He has worked as a professor at the Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia, where he was teaching courses in the field of energy technology and risk and reliability in power systems. He has received his Ph.D. in 2001 from the same University. His research and expertise is especially related to nuclear power safety assessment and renewable energy source's characterization and utilization. In his career, he has twice stayed in the USA for several years - long expert work and research, and recently he has finished a two-year position as a visiting scientist at the European Commission Joint Research Centre - Institute for Energy and Transport in the Netherlands, all related to nuclear power risk and reliability. He has published more than a hundred scientific papers and expert study reports. He is active as a distinguished lecturer for the IEEE Power and Energy Society and he was Chair of the Croatian IEEE Power and Energy Society Chapter. He was also president of the Croatian Nuclear Society. Currently he is working in the EC JRC on nuclear energy operating experience feedback and safety.

zdenko.simic@ec.europa.eu

SEMINAR CLOSING

Franck WASTIN
Head of Unit
Knowledge for Nuclear Safety, Security & Safeguards
European Commission
Joint Research Centre
Petten,
The NETHERLANDS

Biography

Franck Wastin holds a PhD in Chemistry-Nuclear Chemistry from Liège University, Belgium and has developed, during almost 30 years research experience in nuclear fields, a broad expertise in condensed matter physics and chemistry of Actinides, nuclear fuel cycle and reactor safety. He has contributed to more than 170 scientific peer reviewed publications and to more than 200 conferences, He is currently the Head of the Knowledge for Nuclear Safety, Security and Safeguards Unit (JRC.G.10) at the European Commission, Joint Research Centre, Directorate G-Nuclear Safety and Security, which is one of the ten Directorates of the EC's Joint Research Centre. Previously, he was heading the Nuclear Reactor Safety Assessment Unit (F05) at the JRC-Institute for Energy and Transport, Petten, The Netherlands, and from 2007 to 2015, the Director's Office of the JRC-Institute for Transuranium Elements in Karlsruhe, Germany.

He is the EC representative at the Steering Committee of the IAEA Technical Support Organisation Forum (TSO-Forum) and at the NEA's Committee on Nuclear Regulatory Activities (CNRA).

franck.wastin@ec.europa.eu

SESSION 1 - TRANSFERRING FORESIGHT APPROACHES TO THE SAFETY DOMAIN

Fabiana SCAPOLO
KEYNOTE
Deputy Head of Unit
Foresight, Behavioural Insight & Design for Policy
European Commission
Joint Research Centre
Brussels,
BELGIUM

Biography

Fabiana Scapolo works at the European Commission Directorate General Joint Research Centre (JRC) in Brussels. She is Deputy Head of Unit for the Foresight, Behavioural Insights and Design for Policy. The Unit is responsible for the EU Policy Lab that aims at combining foresight, behavioural insights, design for policy and science and technologies studies to bring innovation and improve policymaking at European level. The EU Policy Lab combines the methods and tools of these disciplines to explore, connect and find solutions for better policies by making sense of emerging trends and envisaging alternative futures.

Fabiana's current duties are related to the general management of the unit. She is also coordinating the foresight and horizon scanning activities and she is very active in strengthening the JRC capacity and position as a key actor on Foresight and Horizon scanning at European and international level. She has more than 15-years of working experience on foresight both in terms of applying foresight to specific context and topics as well as advancing on the application of Foresight methods and tools in support to policy-making formulation at European level.

In the past she was involved in exercises on strategy formulation for the JRC and on the monitoring and implementation of the work programme of the JRC.

Fabiana's background is in Political Sciences (University of Milan) and she has a PhD on foresight methodologies (University of Manchester).
fabiana.scapolo@ec.europa.eu

Invited Lecture I

Foresight as tool to support policymaking and some reflection on how it can be applied to safety management

Abstract

The presentation will start with a brief introduction on why thinking about the future is becoming more and more a necessary activity for many organisations and domains. From there, definition and key characteristics of foresight will be provided together with an overview on what Foresight is and how and when it should be applied to policy making. An illustration on features, requirements and capabilities needed for foresight in a policymaking context to deliver will be delivered.

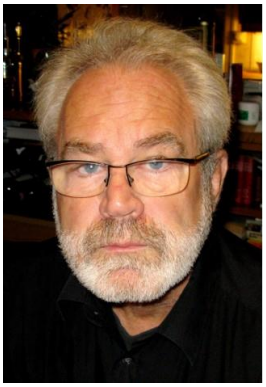
The presentation will also illustrate a number of possible foresight activities and methods. These include horizon scanning, trend analysis, visions, scenarios, technology assessment. Some examples on how these methods are applied will be provided.

The presentation aims also at reflecting on how foresight could be applied to safety management and risks assessment. It will suggest some practical ways of implementation.

fabiana.scapolo@ec.europa.eu

SESSION 1 - TRANSFERRING FORESIGHT APPROACHES TO THE SAFETY DOMAIN

Sverre RØED-LARSEN
Project Manager
SRL HSE Consulting
Oslo,
NORWAY



Biography

Sverre Røed-Larsen, sociologist (Mag.art. from the University of Oslo 1973), has more than thirty years of experience from consumer and product safety work in Norwegian public authorities, from the Norwegian State Railways and from work in Work Research Institute Norway (AFI-WRI); most of the time in leadership positions in different ministries and directorates. He has participated in different ESReDA project groups since 2000.

He was in 20 years a board member of the Norwegian Safety Forum (SF), was awarded the Safety Prize in 2010, and is now a board member of the Norwegian Society of Safety & Security (Nosif). He has in many years been teaching subjects related to Health, Safety and Environment at universities and university colleges in the Nordic countries. He has run his own self-employed business enterprise – SRL HSE Consulting – since 2000.

sverre.rl@getmail.no

John STOOP
Managing Director
Kindunos Safety Consultancy Ltd
Gorinchen,
The NETHERLANDS

Biography

John Stoop is an aerospace engineer, specialised in safety investigations and forensic engineering. He has been a guest professor at Lund University in Sweden, Delft University and the Amsterdam University of Applied Sciences. He is the managing director of Kindunos Safety Consultancy in the Netherlands. He is a member of the International Society of Air Safety Investigators, the Board of Directors of ESReDA and has been active in a variety of ESReDA Project Groups. He has been the secretary of ITSA, the international association of independent transport safety boards.

stoop@kindunos.nl

Uncertain future. Unsafe future? Or foresight in safety - theories, traditions and the ESReDA safety approach

Abstract

Foresight is a relatively new research discipline, established in the 1960s especially in Japan and United States, and later further developed in many research environments in other countries. The purpose of the use of foresight techniques is to employ a participant-based process for the systematic collection of forward-thinking knowledge and develop visions and future perspectives in a medium and in a long-term perspective. Based on a holistic approach and making use of knowledge of former events - such as results from the investigations of accidents and near misses and knowledge of the present situation - one can improve the current decisions and promote better prevention and harm reduction measures. Unfortunately, foresight methodology has so far been used only to a small degree in a safety context.

The paper will briefly review the evolution of foresight-theories and outline its historical background. It will describe the characteristic elements in foresight and give an overview of the most important methods used. In this context, the basic comprehension forms within the safety thinking are analysed, and it will be argued for changes in the moral and ethical values within safety for technological changes and improvements, as well as for the developing safety as a societal value. It is emphasized that the recognition of a necessary system shift must take place on two levels: as an incremental shift with derivative solutions for known problems, and as a substantial change with disruptive solutions for new problems. In addition to comparative examples of release of energy during aviation and railway accidents, and nuclear disasters, also the characteristics of so-called "weak signals" are discussed. The necessity of a paradigm shift is underlined. The paper ends with a brief description of the ESReDA PGs approach to foresight methodology within the safety area, and examples of challenges are given, and recommendations proposed for a new holistic safety management based on feed forward as well as on feedback information and insights.

SESSION 2 - FORESIGHT CHALLENGES IN SAFETY MANAGEMENT

John STOOP
Managing Director
Kindunos Safety Consultancy Ltd
Gorinchen,
The NETHERLANDS

How did aviation become so safe, and beyond?

Biography
See p. 302

Abstract
Aviation has been recognized as one of the ultimate safe socio-technical systems. This contribution discusses the conditions and context that moulded the system safety to its present level by applying integral safety, a sectoral approach and safety as a strategic value. At present the aviation system consists of institutional arrangements at the global level, a shared repository of knowledge and operational experiences, feedback from reality, the notion of Good Airmanship, together with the choice of technology as the flywheel for progress. This architecture made aviation a Non-Plus Ultra-Safe system characterized by a safety performance level of beyond 10^{-7} accident rate. To cross this mythical boundary in legacy systems like aviation, it is imperative to apply game changers such as socio-technical systems engineering, disruptive technologies and innovation transition management. In such a transition, a shift in focus occurs from performance to properties, from hindsight to foresight, highlighted by the case study of the stall recovery device, the Kestrel concept.

SESSION 2 - FORESIGHT CHALLENGES IN SAFETY MANAGEMENT

Dan SERBANESCU
Nuclear Safety Expert
Societatea Nationala Nuclearelectrica S.A.
Bucharest,
ROMANIA
***For participation in ESReDA actions he represents the* Division of Logic and Models – DLMFS / CRIFST of the Romanian Academy**

Biography

Graduated Moscow Power Institute. PhD thesis on risk of CANDU fuel failures. Training in IAEA, Canada, Korea. 38 years of work in nuclear and risk analyses, of which: 25 in Romanian national nuclear safety and nuclear engineering program – safety design, manufacturing, construction, licensing of commissioning and operation of CANDU 6 units, safety report chapters and risk analyses, corporate safety independent review, at working and management levels. 13 years in international projects (4 project manager risk study PBMR; 6 years in EC - 3 risk analyses, 3 project manager decommissioning of Kozloduy). One risk book, coauthor of 2, about 50 papers. Member of a committee under Romanian Academy.

office: dserbanescu@nuclearelectrica.ro
private: dan.serbanescu1953@yahoo.com

On some issues related to the safety margin and the process of safety foresight for the nuclear power plants

Abstract

The paper presents some insights from the author's research results on reviewed issues related to the level of Risk and Safety Margins (SM) for Nuclear Power Plants, regarded as complex systems. The overarching approach to safety review is presented and some practical real cases are illustrated. The focus is on aspects such as specifics of the SM evaluations for various lifecycle periods, iterative process of such evaluations, and consideration of human factors, which are part of the model itself. It is also illustrated, that for real cases, this approach was (for several decades of the author's experience) the basis for foresight in safety in various projects of nuclear installations in various lifecycle phases.

SESSION 2 - FORESIGHT CHALLENGES IN SAFETY MANAGEMENT

John KINGSTON
Board Member
Noorwijk Risk Initiative Foundation
Maasdijk,
THE NETHERLANDS

Biography

Dr. John Kingston is a board member of the Noordwijk Risk Initiative Foundation—a not-for-profit organisation that exists to build capacity in safety risk management. His interest in safety began as an accident investigator with the London Fire Brigade. After studying Psychology, and then Ergonomics, in 1996 he gained his PhD for research into the evolution and regulation of safety management systems. Through NRI and independently, Dr. Kingston works in aviation, aerospace and the emergency service sectors. His work focuses on monitoring, accident investigation and organisational design.

J.Kingston@nri.eu.com

Yves DIEN
Researcher
Club Heuristique pour l'Analyse Organisationnelle de Sécurité (CHAOS)
Meudon,
FRANCE

Biography

Born in 1955

Academic background: Social Sciences (postgraduate certificate)

Professional career:

Currently: pensioner;

From 2002 to 2015: EDF R&D Centre; researcher, leading a project dealing with "Organizational Factors of industrial accidents, incidents and crises";

From 1995 to 2002: EDF International Division; advisor for nuclear affairs in Central and Eastern Europe

From 1982 to 1995: EDF R&D Centre; ; researcher involved in design and evaluation of a computerized control room and of emergency operating procedures(both for NPPs);

From 1979 to 1982: Renault Cars Company; ergonomist involved in projects dealing with

introduction of new technologies (automation, computerization …).
yves.dien@hotmail.fr

The McNamara Fallacy Blocks Foresight for Safety

Abstract

Famously, 'what gets measured gets done', but the sociology behind the measurements, particularly those used to manage organisations, are little studied in the field of safety. Yankelovich described a pattern dealing with traps of quantification that he called the "McNamara fallacy" and which has four steps.

Process safety might be particularly vulnerable to the McNamara fallacy because the paradigm of reliance on numbers is very strong in engineering culture. However, as we argue, the McNamara fallacy is less a failing of individuals, than it is an outcome of the forces that produce order in organisations. In this paper after an explanation of the four steps of the "fallacy", we will argue how some failures of foresight are connected to poorly managed quantification, which is, according to Woods (2009), a basic form of organization failure.

SESSION 2 - FORESIGHT CHALLENGES IN SAFETY MANAGEMENT

Nicolas DECHY
Specialist in human and organizational factors
IRSN (French National Institute for nuclear safety and radiation protection)
Fontenay-aux-Roses,
FRANCE

Biography

Graduated as a generalist engineer from Ecole des Mines de Douai, he works at the organizational and human factors and learning from experience department at Institut de radioprotection et de sûreté nucléaire (IRSN) which provides expertise to the French nuclear safety authority. He worked as a consultant and expert at INERIS. His expertise experiences and research areas are on investigating and learning from events and accidents from technical aspects to human and organizational factors (e.g. Fukushima, Toulouse), emergency response and crisis management (staffing, stress), risk analysis, safety and subcontracting management in maintenance in nuclear and petrochemical industrial sectors. He was chair of the ESReDA project group on "accident investigation" and currently co-chairs the PG on "Foresight in Safety". He is a member of ESReDA Board of Directors.

nicolas.dechy@irsn.fr

Myriam MERAD
Research Director
CNRS, UMR ESPACE,
Nice Sophia Antipolis University - UMR LAMSADE,
PSL*, CNRS, Université Paris Dauphine
Paris,
FRANCE

Biography

Dr Myriam Merad serves as research director at CNRS (France) UMR ESPACE Nice University since October 1st, 2016. She is an associate member at UMR LAMSADE (Dauphine University). She passed her tenure in 2011 and holds a MBA. She leads research in Risk governance, land use planning and Decisions in safety, security and Health and Environment. She headed societal risk management and human and organisational factors and governance teams at INERIS.

Myriam.MERAD@unice.fr

Laura PETERSEN
Environment, Resilience and Risk Engineer
European-Mediterranean Seismological Centre,
Bruyères-le-Châtel,
FRANCE

Biography

Laura Petersen is an Environment, Resilience and Risk Engineer at the European-Mediterranean Seismological Centre (EMSC) where she focuses on social resilience and the use of new technologies in crisis communication. Currently in charge of managing the EU IMPROVER project for EMSC, she also has previous experience working on European projects related to sustainable development. She has a Master's degree in Engineering and Management of the Environment and Sustainable Development from the University of Technology in Troyes (UTT).
petersen@emsc-csem.org

Maria Luisa Pestana
Business Continuity, Crisis Management and Critical Infrastructures Expert
EDP DISTRIBUIÇÃO - Energia, S.A.,
Lisbon,
PORTUGAL

Biography

Maria Luisa Pestana graduated as Electrical Engineer. She is holding responsibilities in Business Continuity, Crisis Management and Critical Infrastructures in EDP Group Risk Management Department; was part of the team that started the Business Continuity Department in EDP's Portuguese DSO, that implemented the Business Continuity Management System, certified against the international standard ISO 22301 in 2015. Has been involved in European projects related to resilience, RESILENS and RESCCUE, and coordinates a "Resilience of Distribution Grids" working group within the framework of CIRED (INTERNATIONAL CONFERENCE ON ELECTRICITY DISTRIBUTION).
marialuisa.pestana@edp.pt

Biography

Dr. Igor Linkov is Risk and Decision Science Focus Area Lead with the US Army Engineer Research and Development Center and an Adjunct Professor of Engineering and Public Policy at Carnegie Mellon University. Dr. Linkov has managed multiple risk assessments and risk management projects in the areas of environmental health, climate change, homeland security, energy, infrastructure, emerging materials, Cybersecurity and systems vulnerability.

Igor LINKOV
Risk and Decision Science Expert
US Army Corps of Engineers, Concord, MA,
USA

Biography

See p. 306

Yves DIEN
Researcher
Club Heuristique pour l'Analyse Organisationnelle de Sécurité (CHAOS)
Meudon,
FRANCE

Foresight for Risk Prevention and Resilience: to what extent do they overlap?

Abstract

For several years now, resilience concepts appear to challenge traditional risk approaches. One of the key difference suggested is the way foresight is tackled in both. This paper discusses commonalities, differences and any overlaps in the use of foresight between these two approaches. Several lessons learned from historical cases are used for this purpose (before and after Toulouse chemical disaster, Fukushima nuclear accident, business continuity and crisis management for critical infrastructure). Both approaches are in fact rather complementary in fulfilling certain critical functions, and are less opposed than as claimed by resilience promotors. While the expectations and foresight differ, recovery is included in risk approaches as well as in resilience approaches. Furthermore, risk approaches also deal with unexpected events. The paper concludes with an analysis of the knowns, unknowns and awareness that enables one to distinguish different foresight categories in risk (defensive, reactive, ethical, proactive) and in resilience.

SESSION 3 - FORESIGHT AND TECHNOLOGY

Zdenko ŠIMIĆ
Scientific Officer
Knowledge for Nuclear Safety, Security & Safeguards Unit
Joint Research Centre
European Commission
Petten,
The NETHERLANDS

Biography
See p. 298

Potentials, limitations and problems of technologies for enhancing safety and foresight

Abstract
Technological advances potentially impact all stages of the life cycle of safety related systems. This is increasingly so with advanced sensors, as well as the exponential increase of computing power, communication bandwidth and storage capacity. The design and operation of safety related systems can benefit significantly with potential to continually reduce risk through the application of advanced software and hardware solutions including artificial intelligence (AI). The question is which kind of technological advances are in use and being developed and how they can potentially improve safety?
This paper aims at identifying major existing and emerging technologies with tangible potential safety benefits applicable to different life cycle phases of concerned systems (i.e., design, verification, validation, production, testing, commissioning, operation, maintenance, emergency response and decommissioning). These technologies generally comprise a combination of hardware and software used for e.g.: development, training, operation, monitoring, diagnoses and predictions. Examples are computer aided hybrid development, real time modelling analysis and various artificial intelligence applications. In this preliminary review the aim is to identify potentials, limitations and difficulties associated with the application of these advanced technologies for the enhancement of safety and foresight.

Some of the problems associated with the use of advanced technologies are related to the increased technical complexity that they may bring to the design (e.g., software and digital instrumentation and control validation and verification). In addition, other issues related to the need for connectivity like cyber security and privacy are becoming even more worrying. The open question is what are the limitations or ultimate potential benefits which can be gained by using advanced technology to enhance safety and foresight (considering challenges and benefits)?

SESSION 3 - FORESIGHT AND TECHNOLOGY

Tomasz JACKOWSKI
Coordinator for Nuclear Energy
National Centre for Nuclear Research
Otwock-Świerk,
POLAND

Biography

Electronics Engineer graduated in 1975 from Warsaw Technical University. Since 2010 Coordinator for Nuclear Energy in the National Centre for Nuclear Research. Since 2016 Expert in Early Stage Sp. z o.o., Sp. Kom. 40 year experience in the area of nuclear safety – long time expert of IAEA. Director, safety assessments of NPPs in many countries, construction of severe accident simulators, training of IAEA fellows; 2002-2007 Manager of health services; 2007-2010 Chief expert on nuclear energy in the Ministry of Economy. Member of the Boards of Polish Nuclear Society, Zygmunt Zaleski Stichting, European Safety, Reliability and Data Association; Member of the Executive Committee of Sustainable Nuclear Energy Technology Platform, Member of the Steering Committee of TSO Forum, Coordinator of the NC2I-R FP7 Program. Member of the Gemini + H2020 Program, Member of the Program Committee of the HTR 2018 and of the TSO 2018 Conferences.

Karol KOWAL
Assistant Professor
National Centre for Nuclear Research
Otwock,
POLAND

Biography

Karol Kowal holds a Master's Degree in Nuclear Physics, PhD in Electrical Engineering and Post-graduate Diploma in Business Management. He held an internship in General Electric Hitachi Nuclear Energy (Willington, USA) and worked as a Specialist for External Hazards Analysis in PGE – the largest power producing company in Poland, designated as the investor for the first Polish Nuclear Power Plant. Currently at the position of Assistant Professor in Polish National Centre for Nuclear Research. Co-author of several scientific papers and professional reports on Probabilistic Safety Assessment.

Karol.Kowal@ncbj.gov.pl

Sławomir POTEMPSKI
Head of the Centre of Excellence MANHAZ (Management of Health and Environmental Hazards)
National Centre for Nuclear Research
Otwock,
POLAND

Biography

Dr Slawomir Potempski is the researcher at the National Centre for Nuclear Research and the Head of the Centre of Excellence MANHAZ (Management of Health and Environmental Hazards). He obtained his doctorate at the Warsaw University in the field of applied mathematics. His main fields of interest are: risk analysis for chemical and nuclear installations, consequence analysis after the releases of dangerous substances to environment, emergency preparedness and response, numerical methods for high performance computing, advanced software technologies for distributed and parallel computations.

slawomir.potempski@ncbj.gov.pl

Cogeneration: technologies, possibilities, challenges

Abstract

Newly designed nuclear reactors can be applicable not only for the generation of electricity, but also for the production of process heat, hydrogen or hydrazine, which is of great importance for chemical industry. In the presentation entitled „Cogeneration: technologies, possibilities, challenges" a summary of the problems related to the licensing process of such reactors, safety and reliability issues of the whole processing combined chemical-nuclear installation and the challenges for needed research program will be given.

SESSION 4 - RISK ANALYSIS AS INPUT TO FORESIGHT

Ana AFONSO
KEYNOTE
Team leader Emerging Risks
Scientific Committee and Emerging Risks Unit
European Food Safety Authority
Parma,
ITALY

Biography

Ana Afonso, is the team leader of the Emerging Risks team at the European Food Safety Authority. Objectives of the Emerging Risks team are to: (i) to carry out activities aiming at identifying, assessing and disseminating information on emerging issues; (ii) ensure coordination with EFSA units, Panels other relevant EU institutions, MS and international organizations (iii) promote the identification of data sources and data collection and /or data generation in prioritized emerging issues and (iv) evaluate the collected information to identify emerging risks in the area of food and feed, animal and plant health. The team is also contact point for the Rapid Alert system for Food and Feed providing scientific and technical assistance and coordinates EFSA urgent response procedures and crisis preparedness.

She is a veterinarian specialized in Aquatic Veterinary studies and joined EFSA in 2006 as a scientific officer for the Animal Health and Welfare Unit. Prior to that she worked as a Veterinary official responsible for approval and inspection of food establishments, as a Veterinary assistant for hygiene and animal health issues on fish farming and as a Research / Lecturer assistant at the Portuguese Veterinary Faculty of Lisbon and Vila Real.

Ana.AFONSO@efsa.europa.eu

Kenisha Garnett
Cranfield Institute for Resilient Futures (CIRF)
School of Water, Energy and Environment
Cranfield University
Cranfield, Bedfordshire,

Biography

Dr Kenisha Garnett is a Lecturer in Decision Science at Cranfield Institute for Resilient Futures (CIRF) at Cranfield University. Kenisha has expertise in strategic foresight. Her current research is developing underpinning robust foresight methodologies that link evidence-based strategic

UNITED KINGDOM

risk with value judgements to assess system resilience and the robustness of policies, strategies and delivery mechanisms for the green economy. Kenisha has led the development of medium and large scenarios projects and delivered a strategic foresight programme, focused on the long-term sustainability of environment and food systems, primarily through a £1.8M pan-government futures partnership led by the Department of Environment, Food and Rural Affairs (Defra) and including 9 other government agencies across the UK.

k.garnett@cranfield.ac.uk

Hub Noteborn
Program Manager of Risk-ranking and Data Intelligence
Netherlands Food and Consumer Product Safety Authority
Utrecht,
THE NETHERLANDS

Biography

Hub Noteborn holds the position of program manager Risk-ranking and Data Intelligence in the Netherlands Food and Consumer Product Safety Authority (NVWA). There,fore he was head of Integrated Risk Assessment department and deputy Director of the Office for Risk Assessment and Research (BuRO), which is a governmental independent body to advice on animal and plant health, animal welfare, food and consumer product safety threats. Prior to his appointment at NVWA (2002) he was head of the GMO and novel food safety testing program in RIKILT-Institute of Food Safety at Wageningen University and Research Centre (WUR).

h.p.j.m.noteborn@nvwa.nl

Petros MARAGKOUDAKIS
Scientific officer
European Commission in the Joint Research Centre,
Directorate F – Health, Consumer Protection and Reference Materials
Ispra,

Biography

Petros A. Maragkoudakis holds degrees in microbial biotechnology and medical microbiology. His PhD and post-doctoral research focused on probiotics, health and food microbiology, technology and safety. Since 2010 he has been working mainly for the European Commission in the Joint Research Centre, providing scientific

ITALY

support in the area of food and nutrition policies and public health. He was a key participant in two recent major JRC food-system related foresight studies, one on research priorities for food and health and one on the resilience of the EU food safety and nutrition legislative/policy framework. He has contributed in various future and food system-oriented workshops, activities and fora inside and outside the JRC, and has a keen interest in the subject. Currently he is co-ordinating a joint JRC/SANTE project that maps scientific evidence, recommendation and policies in the broader field of nutrition and food. Petros has also worked as a free-lance consultant, a project manager for a company providing IT solutions in food legislation/compliance, as well as a lecturer in food microbiology.
Petros.MARAGKOUDAKIS@ec.europa.eu

Invited Lecture II

Emerging Risks in food and feed, the importance of foresight

Abstract

Food is produced, distributed and sold on a global scale. The interconnectivity of the market simultaneously builds resilience in supply chains but magnifies vulnerabilities, so it is more important than ever to have the best possible understanding of the world around us, and how it is changing. Reflection is required on how new technologies transform our global supply chains, trade policies, and future food production. The identification and prioritization of emerging risks is a complex process involving the gathering and evaluation of large amounts of information from different sources and the biggest challenge is to make sense of the complex interactions of different factors and actors in the food system to predict and possibly prevent future risks.

Forward-looking exercises have been employed by organisations, institutions, authorities or governments to enhance policy preparedness and promote prevention-based policy approaches. Foresight employs methods to explore change in the mid-to-long-term future based on the assumption that developments outside the food supply chain and even outside the food system are either directly or indirectly related to the

development of a particular food-borne hazard. Typical outputs from foresight studies, specifically scenario planning, are multiple scenarios that model systemic change in the food system in order to reveal potential unknown patterns of food-related challenges. This paper briefly describes the development and use of scenario planning as a foresight methodology, presents specific case studies applied in the area of food safety, and discusses the challenges and opportunities linked to this approach for identification of emerging risks and policy preparedness.

SESSION 4 - RISK ANALYSIS AS INPUT TO FORESIGHT

Milos FERJENCIK
Associate Professor
University of Pardubice
Pardubice,
CZECH REPUBLIC

Biography

Milos Ferjencik graduated in nuclear engineering at Prague Technical University in 1981. Between 1981 and 1992 he worked in the Nuclear Research Institute, and in Temelin NPP. Since 1992 he concentrated on chemical risk analysis. In 1995 he started his own consultancy profession. In 2004 he started to work as a full-time assistant professor of safety engineering at the University of Pardubice. In 2015 he was habilitated as an associate professor. Since 2015 he is a head of Institute of Energetic Materials. In his research work, he focuses on risk analysis and accident investigations.

milos.ferjencik@upce.cz

Biography

The article is focused on visibility of early warning signs. It describes how the incident scenarios can be used as a supporting tool for foresight. Possible appearance of the incident scenarios represents a starting point. The use of scenarios for the identification of early warning signs and for the prioritization of early warning signs is shown. Uses of both predictive and retrospective scenarios are analysed and common features of both the types are identified. Ways of the use of scenarios are illustrated by examples. According to the article, visualisation of hazard realizations represents the common principal purpose of the use of scenarios. Relation of the visibility of hazard realizations to the visibility of early warning signs is discussed and demonstrated. Methods of hazard identification and risk analysis and methods of incident cause analysis are brought to mind in the article.

Abstract

The article is focused on visibility of early warning signs. It describes how the incident scenarios can be used as a supporting tool for foresight. Possible appearance of the incident scenarios represents a

Roles of Incident Scenarios in Foresight

starting point. The use of scenarios for the identification of early warning signs and for the prioritization of early warning signs is shown. Uses of both predictive and retrospective scenarios are analysed and common features of both the types are identified. Ways of the use of scenarios are illustrated by examples. According to the article, visualisation of hazard realizations represents the common principal purpose of the use of scenarios. Relation of the visibility of hazard realizations to the visibility of early warning signs is discussed and demonstrated. Methods of hazard identification and risk analysis and methods of incident cause analysis are brought to mind in the article.

SESSION 4 - RISK ANALYSIS AS INPUT TO FORESIGHT

Nicola PALTRINIERI

Associate Professor
Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology – NTNU
Trondheim,
NORWAY

Foresight in process industry through dynamic risk assessment: implications and open questions

Biography

Nicola Paltrinieri is an associate professor in risk assessment at the department of Mechanical and Industrial Engineering of the Norwegian University of Science and Technology (NTNU). His position is sponsored by the "Onsager Fellowship Programme" rewarding high academic merit. He received his Ph.D. in Safety Engineering from the University of Bologna (Italy). He is associate editor for the journal Safety Science and the Norwegian Delegate at the EFCE (European Federation of Chemical Engineering) Working Party on Loss Prevention and Safety Promotion.
nicola.paltrinieri@ntnu.no

Abstract

Risk analysis is about to enter an era of larger and more complex data sets (big data), where the main challenges are represented by the ability to provide continuous acquisition, effective process and meaningful communication of information. However, most of the methods for quantitative risk assessment allow for static evaluations of risk in a frozen instant of the system life. Research on how to dynamically assess risk in process industry has been carried out, but no real implementation has been attempted. Some open questions are still undermining this approach and should be directly addressed to provide reliable models and exploit new technology opportunities. i) Which strategy should be adopted? ii) How early warnings and past events should be assessed and connected to the overall risk? This contribution aims to give an overview on preliminary answers and highlight possible uncertainties of future developments.

SESSION 4 - RISK ANALYSIS AS INPUT TO FORESIGHT

Eivind H. OKSTAD
Senior Research Scientist
SINTEF Technology and Society
Trondheim,
NORWAY

Biography

Eivind Okstad is a Senior Research Scientist in SINTEF Technology and Society. Okstad has an MSc degree in mechanical engineering from NTNU, and holds a PhD in petroleum production from NTNU. Before his research career, Okstad worked as a consultant in DNV GL within the field of reliability- and risk management. His main area of interest is risk- and safety management approaches at both operational, tactical and strategic levels. Okstad has years of experience from projects within offshore petroleum industry, land-based industry and transportation. At present, he is involved in research projects dealing with societal safety and protection of critical infrastructures.

Eivind.h.okstad@sintef.no

Øyvind DAHL
Senior Research Scientist
SINTEF Technology and Society
Trondheim,
NORWAY

Biography

Øyvind Dahl is senior researcher at SINTEF. He holds a PhD in organizational sociology from NTNU. Dahl has long experience from research within the field of organizational safety, practical frontline experience in safety work within the oil and gas industry and experience in governmental regulation of HSE.

oyvind.dahl@sintef.no

Horizon scanning approaches for early sensing of cyber-physical threats to water utilities

Abstract

The presentation is about horizon-scanning, which is a collective term of approaches capturing weak or early warning signals for use in political discourse and decision-making. The authors

would like to demonstrate whether horizon scanning methods fit in sensing emerging cyber-physical threats to water-supply and waste water systems. Could such methods enforce early warning capabilities, increase awareness and cooperation in the water sector aiming for policy- and strategic decision-making processes?

SESSION 5 - TOOLS AND METHODOLOGIES

Michela DEMICHELA
Assistant Professor
DISAT, Politecnico di Torino
ITALY

Analysis and management of accident precursors in manufacturing industry

Biography

Micaela Demichela is an Assistant Professor at the Applied Science and Technology Department of Politecnico di Torino in Italy. Her research field is related to process safety and operator safety in the work environment, with a glance to both technical and human and organisational factors. She is a member of the Board of Directors of the ESReDa Association.

micaela.demiche@polito.it

Abstract

The present work deals with the development of a new Accident Precursors Management System, starting from the HFACS taxonomy and the Fuzzy Application Procedure – FAP, already devised for the industrial risk analysis. The methodology proposed is composed by a data collection procedure, carried out in situ and that requires a short interview to the personnel involved in the observed events. Afterward, a data analysis tool, based on the Fuzzy Logic Approach, allows to obtain the preventive measures suitable to cope with the accident precursors analysed. The methodology described is generic and it does not depend on the working site type. It has been tested in a real industrial workplace and the results obtained are shown.

SESSION 5 - TOOLS AND METHODOLOGIES

Biography

Antonio De Nicola is a staff scientist at ENEA. He is member of the DTE-SEN-APIC Lab. He holds a master degree in Physics from Sapienza University of Rome and a PhD in Computer Science from University of Rome Tor Vergata. His research activity includes emergency management, semantic technologies, trusted information sharing, social networks, cybersecurity, and decision support systems. He has been working in more than 15 projects related to the above-mentioned topics. He is the author of around 50 papers published in journals and conference or workshop proceedings. He acts as expert reviewer for Horizon 2020 EU projects, for the Cost EU programme, and for relevant scientific journals.

antonio.denicola@enea.it

Antonio DE NICOLA
Researcher, PhD
Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile (ENEA)
Rome,
ITALY

Biography

Giordano Vicoli graduated in Electronic Engineering with computer science specialization. He has been working since 1988 for ENEA in the field of design and development of decision support systems for training and/or managing emergency in high risk industrial plants or critical infrastructures making use of expert systems, soft computing techniques and discrete simulation. He extended his research in the field of Critical Infrastructure Protection with particular emphasis on energy infrastructure and electrical SCADA protection. For this last topic he developed, during the European SAFEGUARD Project, a SCADA emulator where it is possible to simulate middle attacks in order to test algorithms to prevent and/or to detect cyber attacks. He also participated in several national and European projects like SAFEGUARD, IRRIIS, CRESCO, ESTEC and ASTROM. Furthermore he is interested in ICT technologies and has developed competences in object oriented

Giordano VICOLI
Department of Mechanical and Aerospace Engineering "Sapienza" University of Rome,
ITALY

programming, UML, JSE, JEE, JME, Web Services, Semantic Web, agile programming, discrete simulation, Mobile Development (iOS and Android).
giordano.vicoli@enea.it

Biography

She holds a PhD in Mathematics from the University of Warwick (UK) and a Master degree in Software technology from the University of Sannio (IT). Her current research activity includes: ICT methods and modeling tools for emergency scenarios and for risk/safety analysis of complex socio-technical systems; formal analysis techniques and discrete-event simulation; domain specific information gathering and knowledge representation through semantics-based techniques, and decision support systems for low carbon society. She is author of several scientific publications on these topics.
marialuisa.villani@enea.it

Maria Luisa VILLANI
Researcher
Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile (ENEA)
Rome,
ITALY

Biography

Andrea Falegnami is PHD student in Industrial and Management Engineering at Sapienza University of Rome. He is member of “Ordine degli Ingegneri di Roma” (National Engineer's Register – section of Rome). He holds a master degree in Mechanical Engineering from Sapienza University of Rome. His research activity is mainly focused on resilience engineering in health care.
andrea.falegnami@uniroma1.it

Andrea FALEGNAMI
PhD Student
Department of Industrial and Management Engineering
“Sapienza” University of Rome,
ITALY

Biography

Riccardo Patriarca holds a Bsc in Aerospace Engineering and an MSc in Aeronautical Engineering both at Sapienza University of Rome (Italy). He currently is a PhD Candidate and works as researcher and assistant lecturer at the Deptartment of Mechanical and Aerospace Engineering of Sapienza. His research interests focus on risk management and resilience engineering for complex socio-technical systems. He is author of research papers focused on innovative methodological approaches to risk and safety management, airline inventory management and airport operations.

riccardo.patriarca@uniroma1.it

Riccardo PATRIARCA
Researcher
Department of Mechanical and Aerospace Engineering
"Sapienza" University of Rome,
ITALY

Abstract

We present a novel framework to enhance safety imagination in socio-technical systems with gamification and computational creativity. This relies on the usage of the Functional Resonance Analysis Method (FRAM) for systemic analysis of socio-technical system. Information on the system structure and organization is elicited from sharp-end operators by means of a gamified and participatory approach. Then such knowledge is organized as a domain ontology compliant with FRAM and is used to feed a computational creativity system and to support the analyst in conceiving FRAM models. The case study concerns healthcare and, in particular, an accident happened during an abdominal surgery.

Enhancement of Safety Imagination in Socio-Technical Systems with Gamification and Computational Creativity

SESSION 6 - FORESIGHT FOR SAFETY MANAGEMENT

Antonio D'AGOSTINO
KEYNOTE
Head of Sector (interim)
Safety Unit
European Union Agency for Railways
Valenciennes, FRANCE

Biography

Antonio D'AGOSTINO works, since October 2012, as Project Officer at the European Union Agency for Railways where he is working on:

- Training and workshops on:
  - EU Railway Safety regulatory framework;
  - Safety Management Systems;
- Research on big data analytics;
- Development of a new safety performance reporting and analytics scheme.

Antonio is a Mechanical engineer and has 8-years of operational experience. He worked for several years in Competence Management, Railway Safety and Rolling Stock. He also gained experience as train driver.

Safety Certification and Safety Management Systems are his main areas of expertise.
antonio.dagostino@era.europa.eu

Marina AGUADO
Project Officer
Safety Unit
European Union Agency for Railways
Valenciennes, FRANCE

Biography

PhD in Telecommunications Engineering (UPV/EHU), MSc in Management of Manufacturing Systems at Cranfield University (UK) and BSc in Telecom Engineering – Radiocommunication (UPV/EHU). More than 10 years professional experience in the railway industry. Her expertise is focused on train control systems and communication technologies for transport systems. Currently, she manages the European Railway Agency Study on Big Data in the railway safety context.
marina.aguado@era.europa.eu

Strategy and projects for a predictive safety regulation and safety management

Abstract

The presentation is about the European Union Agency for Railways and the pieces of legislation it has developed aiming at harmonizing safety management in Europe and trying to support operators and countries in improving their safety performances. It also describes its tasks and projects that have been designed to push the railway industry towards a more proactive and predictive safety management.

The European Union Agency for Railways is moving from being essentially a technical body supporting the European Commission and, to a certain extent, the railway sector, to being an active player in the railway system dealing with certification and authorisation processes.

SESSION 6 - FORESIGHT FOR SAFETY MANAGEMENT

Eric MARSDEN
Programme manager
Foundation for an industrial safety culture (FonCSI)
Toulouse,
FRANCE

Biography

Eric Marsden manages research projects at FonCSI (Foundation for an Industrial Safety Culture), a French public-interest research foundation. He works on organizational aspects of safety in high-hazard industries, including experience feedback procedures, benefit-cost analysis for risk-related decision-making and risk regulation.

eric.marsden@foncsi.org

Justifying safety interventions based on uncertain foresight: empirical evidence

Abstract

Safety interventions suggested as a result of a foresight process are more likely to be related to non-urgent issues, and be affected by a greater level of uncertainty, than interventions suggested by experience feedback or by regulatory changes. By analyzing a number of accident cases where proactive foresight-based suggestions were not implemented before the accident, we assess whether the uncertain and long-term nature of the predictions had a negative effect on the implementation of the interventions suggested.

SESSION 6 - FORESIGHT FOR SAFETY MANAGEMENT

Yves DIEN
Researcher
Club Heuristique pour l'Analyse Organisationnelle de Sécurité (CHAOS)
Meudon,
FRANCE

Is whistleblowing a promising "tool" for event occurrence prevention?

Biography
See p. 306

Abstract
Due to several reasons, challenge of managing warning signs is hardly taken up by companies. Indeed, very often, a sign makes sense in terms of safety after the event. In other words, meaning of signs related to safety is not obvious, and companies put in place system for collecting and gathering signs that they do not know what to do except compiling statistics on data "accumulated". Furthermore, companies have to cope with two concerns:

• Taking into account and treating a "wrong" sign (i.e. sign which did not impact safety) which would lead to waste of resources and time;
• Not detecting a relevant sign which would be symptomatic of poor safety management.
Major events (accidents) analysis show that, in many cases, that they have been preceded by alerts, warnings launched by persons close to (or knowing) system technical functioning.
In the paper, we will define features of whistleblowing and whistle-blowers. We will also analyse how companies face whistleblowing.

An investigation is made on whether if there are lessons to be learned from civil society whistleblowing (e.g. protection of whistle-blowers). The paper will argue about interest of considering whistleblowing in the frame of safety prevention and will indicate directions on manners to deal with whistle-blowers for maintaining process safety.

SESSION 7 - EARLY WARNING SIGNS: UNDERSTANDING THREATS THROUGH MONITORING

Lorenzo FIAMMA
KEYNOTE
Project Officer for Marine Accident Investigation
European Maritime Safety Agency
Lisbon,
PORTUGAL

Biography

Lorenzo is a former Chief Petty Officer of the Italian Coast Guard. After serving as a safety and security inspector for almost fifteen years, he joined the European Maritime Safety Agency in 2008. He has cooperated in many international projects since, including the development of SafeSeaNet, the implementation of Integrated Maritime Services and more recently, the development of the European Marine Casualty Information Platform (EMCIP). Lorenzo holds a BS in Public Administration and is completing an MSc in Digital Education at the University of Edinburgh.
lorenzo.fiamma@emsa.europa.eu

From maritime multi-sensorial data acquisition systems to the prevention of marine accidents

Abstract
EMSA operates, along with the Member States of the European Union, the SafeSeaNet, the vessel traffic monitoring and information system covering the waters in and around Europe. The platform enables for maritime data exchange across the Union's competent authorities. VHF radio signals are captured from Automatic Identification System (AIS) which are installed aboard the circa 17,000 vessels which operate in and around EU waters. By tracking ships using AIS signals, the system gathers also identity details, latest positions and other status information in near-real-time. In the course of a technical enquiry into a marine casualty, investigators need to reconstruct the events that led, or contributed to an occurrence. This often implies the need to know the whereabouts of the vessel that was involved in the casualty, or of other vessels that may hold important information about the occurrence. Vessels' position and voyage data have

been already used to this end, and has enabled investigators to identify and understand the peculiar circumstances in which very serious or catastrophic accidents have developed.

Recent developments have brought to life additional services, like the vessels' behaviour monitoring tools or other automatic alerting features which may be the precursors of future intelligent and smart agents for the prevention of accidents, rather than for the mitigation of existing risky conditions or threats.

Kinematic data could be streamed directly form onboard sensors and crew's biological parameters captured from wearables devices. Big-data dynamic algorithms may be used to get the foresight of critical conditions and of dangerous situations and to warn users in real-time. Multidimensional and multisensorial data-acquisition is already a reality in the maritime safety sector and the situation is pregnant with new possibilities!

SESSION 7 - EARLY WARNING SIGNS: UNDERSTANDING THREATS THROUGH MONITORING

Ioannis DAGKINIS
Specialized Educational Personnel
University of Aegean
Chios,
GREECE

Biography

Mr. Ioannis Dagkinis K. is a graduate of Merchant Marine Engineering Academy (1990), and is Chief Engineer in merchant marine vessels. He is Specialized Educational Personnel and Chief Engineer in merchant marine vessels. From 2004 till now he works at University of the Aegean in Department of Shipping, Trade and Transport as Specialized Educational Personnel at courses of the undergraduate and postgraduate programs. He is holder of postgraduate degree from the University of the Aegean which deals with "Intermodal Transport and New Technologies" and he is PhD candidate at the University of the Aegean. He has participated in research programs such as floating desalination unit in the program "ΕΠΑΝ - ΦΠ 46", participated in designing the program I-PORTS, in SLIM-VRT program for maritime distance education and other projects. He has certified courses in maritime issues, courses in Evaluation and Risk Assessment and computer skills. Research focuses on international projects on renewable energies at sea and European educational projects. He has published books, articles in international referred journals and conferences.
idag@aegean.gr

George LEVENTAKIS
Senior Research Advisor
Dept. of Shipping Trade and Transport
University of the Aegean
Chios,
GREECE

Biography

Dr. Georgios Leventakis (PhD), is a qualified Security Expert. He holds a PhD in the area of Risk Assessment Models in Critical Infrastructure (CI) Protection. He has 22 years of professional experience in the public sector, of which 16 years are in Security Management. He has participated in several National, European and International projects and initiatives

regarding Physical Security of Critical Infrastructures, Border Management, Civil Protection/Homeland Security technology & operations. As of 2006, he is scientific coordinator for KEMEA's participation in the various European Programmes, funded by the E.C. as Senior Researcher in more than 45 EU security research projects.

gleventakis@kemea.gr

Nikitas NIKITAKOS
Professor
Dept. of Shipping Trade and Transport
University of the Aegean
Chios,
GREECE

Biography

Prof. N. Nikitakos is a graduate of Hellenic Naval Academy (1980) and holds a B.Sc. in Economics (University of Piraeus 1986) and 2 M.Sc. from Naval Postgraduate School, Monterey, CA, USA (M.Sc. Electrical .Engineering. and M.Sc. in Appl. Mathematics). He spent 25 years as Naval Officer (Captain H.N. ret.) when he participated in several NATO and EU committees He received a Ph.D. in Electrical and Computer Engineering from National Technical University of Athens (1996). He is Professor of Shipping Informatics and Communications and was Head of the Dept. of Shipping Trade and Transport in the University of the Aegean (2005-2009). He was AMMITEC's (Association of Maritime Managers Information Technology Electronics and Communication) president from 2006-2010. He holds 3 international patents on renewable energies at sea and he was awarded from Lloyd's List on Maritime Technological Innovation in 2006. He has published 5 books and many articles in international referred journals and conferences. Since 2009 he is a senior research fellow at the Center for Security Studies - KEMEA of the Hellenic Ministry of Public Order and Citizen Protection He holds ISPS, PMP and PMI-RPM certifications.

nnik@aegean.gr

Evolution of remote performance monitoring in ship's safety decision making reinforced by Analytic Hierarchy Process

Abstract

Among the objectives of shipping industry are to maintain safety. Also the measuring of safety in relation to the application of evolutions in operational management of ship's and developing strategies to avoid future accidents is crucial. So recognizing signals before an accident occurs and by enhancing with the right decisions any operational procedure is offered the possibility for improving safety.

In this paper, we address the challenge to evaluate the Remote Performance Monitoring by identify and scrutinize features which may affect the ships safety and must take into consideration of the decision makers during its implementation. The evaluation performed by using the Analytic Hierarchy Process and answers the question, how remote performance monitoring using internet of things and big data, leads in further improvement in terms of machines performance with safety. The implementation of method for ship's safety decision support will be presented and analysed with real world case studies.

SESSION 7 - EARLY WARNING SIGNS: UNDERSTANDING THREATS THROUGH MONITORING

Henk WELS
Engineer in Risk Management & Decision Analysis
Material Testing & Inspection
DEKRA
Arnhem,
THE NETHERLANDS

Biography

Henk Wels is a senior consultant with about 30 years' experience in assessing and quantification of the reliability, availability, maintainability and safety of mechanical and electrical systems. His fields of play include power plants, marine engineering, railways and waterways. His relation with power plants started in 1988 when a project was initiated to gather failure data of Dutch power plants in order to further improve their forced unavailability. The direct application of these data for betterment of power plants, the discussions with operators, maintenance personnel and management has led him to believe that failure data are a reflection of the asset management of a plant. Benchmarking the performance of power plants and their components against other plants, application of FMECA and RCM and the modeling of power plants and their crew are his core business.

henk.wels@dekra.com

Increased forced unavailability of power plants due to economical conditions

Abstract

Electrical production must be equal to electrical demand in order to maintain a precise frequency. When a power plant fails unexpectedly, other plants take up the load as normally there is reserve power available to counteract forced unavailability of plants. Insufficient reserve leads to potential overload of generators which is prevented by shutting down load to areas, if not a blackout on the electrical grid may occur. Forced unavailability of power plants may increase due to the present low electricity prices which are especially low when large wind and sun generation is input in the grid. Such economical conditions result in minimal maintenance of fossil plants as well as a potential increase in failures due to changing operating conditions. The increase is expected to be especially present at vintage coal fired

plant that was not designed for cycling but it can also be present in other types of plants. Minimal maintenance is expected for every plant at too low electricity prices. Numerical data in the Netherlands as well as from the VGB's KISSY database show the presence of such effects, however the effect of changing operating conditions is not so clear as plants operate less (reduced exposure to for instance creep) but start more often (increased exposure to low cycle fatigue). These effects are not taken into account when assessing the probability of grid blackouts by authorities and grid operators, as well as possible effects due to imperfect mothballing causing teething problems when de-mothballing, etc.

SESSION 8 - LEARNING FROM EXPERIENCE TO IMPROVE FORESIGHT IN SAFETY

Ivan PUPULIDY
Innovation and Organizational Learning
US Forest Service
Albuquerque, New Mexico
USA

Biography

Dr. Ivan Pupulidy applies dynamic perspectives to complex systems and high-risk environments, such as wildland firefighting, aviation, military and medicine. His approach to human factors includes the social aspects of human interaction and sensemaking, which are essential components of a learning organization. As a U.S. Forest Service Director, Ivan replaced the traditional accident investigation model with the Learning Review, which embraces complex events by looking at conditions and networks of influence; this approach helps organizations develop learning and cultural change.

Ivan's ability to integrate academic research with real world application comes from his varied life experiences, which have included work as a mine geologist, exploration geophysicist, and a U.S. Coast Guard pilot for rescue and law enforcement missions. Ivan served in the U.S. Air Guard and Air Force Reserves, where he flew the C-130 Hercules, including missions as a MAFFS tanker pilot on wildland fires. He also served on active military operations for combat and humanitarian support in Iraq, Afghanistan and Central Africa.

Ivan earned a Master's of Science degree in Human Factors and Systems Safety at Lund University, Sweden, under Professor Sidney Dekker. He completed his PhD in Social Science at Tilburg University, Netherlands, under Professor Kenneth Gergen.

Ivan is an international consultant and organizational coach who focuses on topics related to human factors, the "New View" of human error, real-time risk perspectives, holistic safety, learning from events, organizational dialogue, development of high-leverage learning products, and the

connection between resilience & high reliability organizing.
Pupulidy@me.com
ipupulidy@fs.fed.us

Crista VESEL
Manager
Dynamic Inquiry LLC
Santa Fe, New Mexico, USA

Biography

Crista Vesel holds a B.A. in Communication and Philosophy from the University of New Mexico and a Masters of Science in Human Factors and Systems Safety from Lund University, Sweden. Her focus on language in accident investigation was an important element in the development of the Learning Review process. She has been a principle contributor for fatality investigations in US Federal agencies and international organizations. Ms. Vesel manages Dynamic Inquiry LLC, which offers worldwide consulting services and language analysis for organizations looking to increase the capacity to learn from events, while simultaneously reducing bias.
DynamicInquiry@hotmail.com

The Learning Review: Adding to the accident investigation toolbox

Abstract

Accident investigation techniques have remained essentially the same for many decades, yet the recognition that complexity is increasing in most organizations demands an added form of inquiry. The Learning Review, first adopted by the U.S. Forest Service, explores the human contribution to accidents, safety, and normal work. It is specifically designed to facilitate the understanding of the factors and conditions that influence human actions and decisions by encouraging individual and group sensemaking at all levels of the organization. The Learning Review introduces the need to create a narrative inclusive of multiple perspectives from which a network of influences map can be created. This map depicts the factors that influence behaviors and can aid the organizational leadership to effect meaningful changes to the conditions while simultaneously helping field personnel to understand and manage system pressures.

SESSION 8 - LEARNING FROM EXPERIENCE TO IMPROVE FORESIGHT IN SAFETY

Maria Grazia GNONI
Professor
Department of Innovation Engineering
University of Salento
Lecce,
ITALY

Biography

Maria Grazia Gnoni is currently an Associate Professor of Industrial Systems Management at the Engineering Faculty of the University of Salento (Italy). Her research activity focused on operations management and safety management in hazardous industries as wells as SMEs. Research fields include near-miss data analysis, developing multi-criteria model for risk analysis, and designing IOT-based systems for preventing accident at workplace. She is author of more than 60 papers and reviewers for Safety Science, International Journal of Loss prevention and Expert systems with application.
mariagrazia.gnoni@unisalento.it

Silvia Maria ANSALDI
Researcher
Inail
Department for Technological Innovation and Safety Centro Ricerca Monteporzio Catone (RM),
ITALY

Biography

Degree in Mathematics. She has over 20 years of industrial experience in problem analysis and software solutions development, operating in several industrial fields, including mechanical and civil design, manufacturing sectors, environmental assessment. For 10 years, she has been working in the field of occupational safety, especially in major accident hazards topics. Her expertise concerns the conceptual model design, knowledge management, information retrieval methodologies, besides more technical competence, from analysis to software design and development.
s.ansaldi@inail.it

Paolo A. BRAGATTO
Scientist and Research Leader
Inail
Department for Technological Innovation and Safety Centro Ricerca Monteporzio Catone (RM),
ITALY

Biography

Dr. Bragatto, graduated in Physics in 1980, after 12 years of industrial experience, he entered, as a scientist, the National Institute for Prevention and Safety at Work, merged in INAIL in 2010. His main scientific interest is in the prevention of major industrial accidents. In particular, he has investigated the methods for Risk Analysis, the Human and Organizational Factors, the Safe Aging of Process Plants and, in the last years, the Smart Systems for Safety. He has a long experience as inspector of Seveso establishments and often transfer his experience to the research. He has leaded a number of national and international research projects and he is the Italian representative in the Saf€ra research consortium for Industrial Safety.

p.bragatto@inail.it

A model for analyzing near-miss events by adopting system safety principles

Abstract

The investigation of near misses is a pillar of major accident prevention at Seveso establishments. The improvement of classification and understanding is needed to exploit near misses for an effective safety foresight. For this purpose, the paper aims at investigating the contribution of the "Safety Principles". They are domain-independent and technologically agnostic; they are based on a small set of general rules from which many safety measures derive. Safety principles include "Fail-Safe", "Safety Margins", "Defense-in-Depth". The idea is to have a new lens to analyse them. The near misses can be classified and interpreted in light of violated principles, to make more effective forecasts and interventions. A sample of near misses, recorded at some Seveso sites, has been used as case study.

SESSION 9 - FROM DATABASE MANAGEMENT TO FORESIGHT

Miodrag STRUCIC
Scientific Officer
Nuclear Safety & Security Unit
Joint Research Centre
European Commission
Petten,
The NETHERLANDS

Use of event and casual Factor Short Chart reports to access and simplify accident reports

Biography

In 1989, Miodrag Stručić concluded Nuclear Energy study at Electrical Department of University of Zagreb in Croatia and earned his Master degree.

For more than twenty years, he worked in Nuclear Power Plant (NPP) Krško, where he accomplished different tasks from position of Reactor Operator to Independent Safety Engineering Group (ISEG) engineer. He was mainly involved in NPP Operations, Corrective Action Program, Event Investigation and Root Cause Analysis activities.

For last seven years Miodrag Stručić is working in European Commission, Joint Research Centre (EC JRC). The most of the time, he was engaged in Clearinghouse for European NPPs Operational Experience team activities. Recently, in EC JRC Directorate G – Nuclear Safety & Security, in Nuclear Reactor Safety and Emergency Preparedness unit, his job is mostly oriented to development of Emergency Preparedness and Response project for the case of accident in NPP.

Abstract

This paper concentrates on assessing events described in hazardous industry's incident/accident reports using the Event and Causal Factor Charting technique. Event and Casual Factor Charting (ECFC) is a process that first identifies a sequence of events and aligns the events with the conditions that caused them. It is used to visually give better insights and emphasize important points.

Events and respective conditions are aligned along a time line. After the representation of the problem is complete, an assessment is

made by "walking" the chart and asking if the problem would be different if the events or conditions were changed asking the questions: What went wrong, how and why? Which deviation occurred? Which rules were transgressed? This leads to identifying causal factors which are evaluated. This approach provides basics for brief risk assessment and can reveal some hidden warning signs in related event reports.

The use of ECFC has proven to be a valuable tool for accident investigators and a clear and concise aid to understanding of accident causation for the report readers and stakeholders. This paper also suggests using a more standardised approach in presenting events by graphical tools for greater effectiveness in accident investigating and reporting.

SESSION 9 - FROM DATABASE MANAGEMENT TO FORESIGHT

Biography
-
daniele.melideo@ec.europa.eu

Daniele MELIDEO
Energy Storage Unit
Joint Research Centre
European Commission
Petten,
The NETHERLANDS

Biography
-
eveline.weidner@ec.europa.eu

Eveline WEIDNER
Energy Storage Unit
Joint Research Centre
European Commission
Petten,
The NETHERLANDS

Biography

pietro.moretto@ec.europa.eu

Pietro MORETTO
Energy Storage Unit
Joint Research Centre
European Commission
Petten,
The NETHERLANDS

Biography
-
francesco.dolci@ec.europa.eu

Francesco DOLCI
Energy Storage Unit
Joint Research Centre
European Commission
Petten,
The NETHERLANDS

Abstract

HIAD - Hydrogen Incident and Accident Database

The Hydrogen Incident and Accident Database (HIAD) has been designed to hold high quality information on accidents and incidents related to hydrogen production, transport (road/rail/pipeline), supply and

commercial use. The database is updated with the latest information concerning each event in order to take advantage of the most recent outcomes of accident investigations. The database has been set up to improve the understanding of hydrogen unintended events, to identify preventive measures and strategies, to avoid incidents/accidents and to reduce the consequence if an accident occurs. The experience of the past years has revealed some shortcomings and generated improvement needs for HIAD. Some of the original goals related to risk assessment had to be abandoned, due to the limited amount of statistics available on faults and failure modes. A major overhaul of the database structure and interface was undertaken. The new version is mainly focused on facilitating the sharing of lessons learned and other relevant information related to the safety of hydrogen technologies. The database will contribute to improve safety awareness, enabling the users to benefit from the experiences of others as well as to share information from their own experiences. The main challenge at present is to attain a clear commitment of the fuel cells and hydrogen technology community to provide sufficient information on safety relevant events.

SESSION 9 - FROM DATABASE MANAGEMENT TO FORESIGHT

Jochen L. LEIDNER
Royal Academy of Engineering Visiting Professor of Data Analytics
Department of Computer Science
University of Sheffield
Sheffield,
UNITED KINGDOM

Biography

Director of Research, Thomson Reuters Corporation, Research & Development
leidner@acm.org

Timothy NUGENT
Research & Development
Thomson Reuters
London,
UNITED KINGDOM

Biography

-
eveline.weidner@ec.europa.eu

Cognitive Inhibitors for Threat Assessment and Automated Risk Management

SESSION 9 - FROM DATABASE MANAGEMENT TO FORESIGHT

Biography
Director of Research, Thomson Reuters Corporation, Research & Development
leidner@acm.org

Jochen L. LEIDNER
Royal Academy of Engineering Visiting Professor of Data Analytics
Department of Computer Science
University of Sheffield
Sheffield,
UNITED KINGDOM

Biography
-
Tim.Nugent@thomsonreuters.com

Timothy NUGENT
Research & Development
Thomson Reuters
London,
UNITED KINGDOM

Cognitive Inhibitors for Threat Assessment and Automated Risk Management

Abstract
The analysis of risks and threats, whether it is on the macro level (geopolitical security) or micro-level (personal well-being or enterprise risk management) suffers from issues resulting from human limitations: it is ultimately humans that operate their own lives, run companies and governments. Unfortunately, humans suffer from cognitive limitations that have an adversarial impact on their ability to manage risks and threats: they create static authority-based organizations instead of empowering agile teams; they compartmentalize to manage complexity, which leads to blind spots (e.g. the 2008 financial crisis) and inconsistent behaviour (we have all seen smoking medical doctors); and they lack the ability to globally evaluate quantitatively complex systems, tending to forget or under-rate activities that are further removed from their personal "centre of gravity" as the saying "out of sight, out of mind" suggests. In this paper, we demonstrate how some of these human and organizational

limitations can prevent us from conducting effective risk and threat management by giving examples from geopolitical and natural disaster risk, environmental risk, people risk, company risk, supply chain risk, and technology risk. By focusing on the risk identification stage, we show how software tools can be used to make the risk management process more objective, in the sense of inter-personally verifiable and consistent. We conclude that risk and threat management should attempt to overcome cognitive limitations by installing an auditable process that uses a human-machine collaborative approach.

SESSION CHAIRS

SESSION 1

Ana Lisa VETERE ARELLANO
Scientific Officer
Technology Innovation in Security Unit[71]
European Commission
Joint Research Centre
Ispra,
ITALY

Biography

See p. 297

Zdenko ŠIMIĆ
Scientific Officer
Knowledge for Nuclear Safety, Security & Safeguards Unit
Joint Research Centre
European Commission
Petten,
The NETHERLANDS

Biography

See p. 298

SESSION CHAIRS

SESSION 2

Frank VERSCHUEREN
Process Safety Inspector
Ministry of Labor,
BELGIUM

Biography

Frank Verschueren has a Master in Chemical Engineering. He worked in several sectors (Non Ferro Metallurgy, Printing and Automotive) with several managerial functions (Production, Projects, R&D, Quality).

From 2003 he works for the Ministery of Labour as Process Safety Inspector (Major Hazards Industry in Belgium).

His knowledge domains are Human and Organisational Factors, Learning from Incidents, Reactor Safety Technology, Psycho-social aspects.

[71] At the time of this publication, Ana Lisa VETERE ARELLANO has moved to the Knowledge for Security & Migration Unit.

He lectures at the Universities of Antwerp, Brussels and Gent and has given presentations in several countries.

The last years he is involved in Safety Research as vice-chairman project group "Foresight in Safety" (ESReDA) and Chairman expertgroup Safety and Security (Flemish Engineers association).
Frank.VERSCHUEREN@werk.belgie.be

Eric MARSDEN
Programme manager
Foundation for an industrial safety culture (FonCSI)
Toulouse,
FRANCE

Biography
see p. 330

SESSION CHAIRS

SESSION 3

John STOOP
Managing Director
Kindunos Safety Consultancy Ltd
Gorinchen,
The NETHERLANDS

Biography
see p. 302

Bastien BROCARD
Researcher
Research and Development
Département Management des Risques Industriels
Eléctricité de France
Palaiseau,
FRANCE

Biography

After ten years of operational experience in a nuclear power plant and in EDF Nuclear Division headquarters, Bastien Brocard joined EDF R&D in 2008 to work on the fields of industrial risk management, operating experience feedback, nuclear safety and human reliability assessments.

bastien.brocard@edf.fr

SESSION CHAIRS

SESSION 4

Tuuli TULONEN
Senior Officer
Finnish Safety and Chemicals Agency (Tukes)
Tampere,
FINLAND

Biography

Dr. Tuuli Tulonen is currently working as a Senior Officer at the Finnish Safety and Chemicals Agency (Tukes), the national authority to endorse the safety and reliability of products, services and industrial activities in Finland. She is responsible for the Agency's multi-sectorial accident database; her work concentrates on analyses of accidents occurred in sectors supervised by Tukes, e.g. chemicals, mining and electricity. Her background is in occupational safety research (Tampere University of Technology). She completed her dissertation on electricians' electrical accident risks in 2011.

tuuli.tulonen@tukes.fi

Fabiana SCAPOLO
Deputy Head of Unit
Foresight, Behavioural Insight & Design for Policy
European Commission
Joint Research Centre
Brussels,
BELGIUM

Biography
see p. 300

SESSION CHAIRS

SESSION 5

Milos FERJENCIK
Associate Professor
University of Pardubice
Pardubice,
CZECH REPUBLIC

Biography
see p. 319

Dan SERBANESCU
Nuclear Safety Expert
Societatea Nationala Nuclearelectrica S.A.
Bucharest,
ROMANIA
***For participation in ESReDA actions he represents the* Division of Logic and Models – DLMFS / CRIFST of the Romanian Academy**

Biography
see p. 305

SESSION CHAIRS

SESSION 6

Sverre RØED-LARSEN
Project Manager
SRL HSE Consulting
Oslo,
NORWAY

Biography
see p. 302

Frank VERSCHUEREN
Process Safety Inspector
Ministry of Labor,
BELGIUM

Biography
see p. 340

SESSION CHAIRS

SESSION 7

Yves DIEN
Researcher
Club Heuristique pour l'Analyse Organisationnelle de Sécurité (CHAOS)
Meudon,
FRANCE

Biography
see p. 306

Bastien BROCARD
Researcher
Research and Development
Département Management des Risques Industriels
Eléctricité de France
Palaiseau,
FRANCE

Biography
see p. 352

SESSION CHAIRS

SESSION 8

Nicolas DECHY
Specialist in human and organizational factors
IRSN (French National Institute for nuclear safety and radiation protection)
Fontenay-aux-Roses,
FRANCE

Biography
see p. 308

Miodrag STRUCIC
Scientific Officer
Nuclear Safety & Security Unit
Joint Research Centre
European Commission
Petten,
The NETHERLANDS

Biography
see p. 343

SESSION CHAIRS

SESSION 9

Tuuli TULONEN
Senior Officer
Finnish Safety and Chemicals Agency (Tukes)
Tampere,
FINLAND

Biography
See p. 352

Sever PAUL
Investigator
Romanian Railway Investigation Agency – AGIFER
Bucharest,
ROMANIA

Biography

Born on the 6th April 1966 in Medias, Romania. He graduated in 1990 Polytechnics Institute from Bucharest – railways specialty, which is rolling stock.

After graduation and until 2003, he worked in the Engine Shed Brasov, in all its sectors of activity:

- 1990-1994 engineer in locomotive repair work;
- 1994 - 1996 position of workshop head in charge with the coordination of locomotive repair;
- 1996-1998, I coordinated theoretical and practical training of locomotive drivers from the position of regional instructor;
- 1998 - 2001 deputy of the Engine Shed Head, in charge with the locomotive movements and the coordination of the driver activity, with reference to the traffic safety;
- 2001-2003 I coordinated the whole activity of the Engine Shed Brasov from the position of Head of Engine Shed (the repair of

locomotives, the locomotive movements and the activity of locomotive drivers, rail machine maintenance) as Chief of Depot;

- 2003-2010 I worked within Romanian Railway Authority – Romanian Railway Safety Authority, like inspector in charge with the traffic safety, performing state inspections and controls;

From 2010 until now I have been working in railway investigation domain within Romanian Railway Investigation Agency - AGIFER, being investigator.
sever.paul@agifer.ro

ANNEXES

Annex A - 53rd ESReDA seminar programme

1st day, Tuesday November the 14th, 2017

7.40	Departure from Hotel, (*Final time will be notified a few days before the Seminar*)
8.00	Arrival of the buses at JRC, clearance of entrance permissions, security matters,
8.15	Arrival at the seminar room, JRC Auditorium, Registration, Welcome coffee
8.30-9.00	**Welcome to the participants, opening, logistics** *Luis Ferreira, ESReDA President* *Georg Peter, Unit Head, Technology Innovation in Security* *Ana Lisa Vetere Arellano & Zdenko Šimić*
9.00-10.00	**SESSION 1.** **Transferring foresight approaches to the safety domain** Chairs: Ana Lisa Vetere Arellano and *Zdenko Šimić*
9.00-9.35	**Invited Lecture I: Foresight as tool to support policymaking and some reflection on how it can be applied to safety management** *Fabiana Scapolo, Deputy Unit Head, Foresight, Behavioural Insight & Design for Policy*
9:35-10:00	**Uncertain future. Unsafe future?** *Sverre Røed-Larsen and John Stoop*
10.00-10.30	**Coffee Break**
10.30-12:10	**SESSION 2.** **Foresight challenges in safety management** Chairs: Frank Verschueren and Eric Marsden
10:30-10:55	**How did aviation become so safe, and beyond?** *John Stoop*
10:55-11:20	**On some issues related to the safety margin and the process of safety foresight for the nuclear power plants** *Dan Serbanescu*
11:20-11:45	**The McNamara fallacy blocks foresight for safety** *John Kingston and Yves Dien*

11:45-12:10	**Foresight for risk prevention and resilience: to what extent do they overlap?** *Nicolas Dechy, Myriam Merad, Laura Petersen, Maria Luisa Pestana, Igor Linkov and Yves Dien*
12.10-13.10	**Lunch and Coffee**
13.10-14:00	**SESSION 3.** **Foresight and technology** Chairs: John Stoop and Bastien Brocard
13:10-13:35	**Potentials, limitations and problems of technologies for enhancing safety and foresight** *Zdenko Šimić*
13:35-14:00	**Cogeneration: technologies, possibilities, challenges** *Tomasz Jackowski, Karol Kowal and Sławomir Potempski*
14.00-14.20	**Coffee Break**
14:20-16.00	**SESSION 4.** **From risk analysis as input to foresight** Chairs: Tuuli Tulonen and Fabiana Scapolo
14:20-14:45	**Invited Lecture II: Emerging risks in food and feed, the importance of foresight** *Ana Afonso, EFSA, Italy*
14:45-15:10	**Roles of incident scenarios in foresight** *Milos Ferjencik*
15:10-15:35	**Foresight in process industry through dynamic risk assessment: implications and open questions** *Nicola Paltrinieri*
15:35-16:00	**Horizon scanning approaches for early sensing of cyber-physical threats to water utilities** *Eivind H. Okstad and Øyvind Dahl*
16.00-16.30	**Coffee Break**
16.30-17:45	**SESSION 5.** **Tools and methodologies** Chairs: Milos Ferjencik and Dan Serbanescu
16:30-16:55	**Analysis and management of accident precursors in manufacturing industry** *Micaela Demichela, Gabriele Baldissone and Salvina Murè*
16:55-17:20	**The role of mathematics in the enhancement of safety** *Bernard Beauzamy*

17:20-17:45	**Enhancement of safety imagination in socio-technical systems with gamification and computational creativity** *Antonio De Nicola, Andrea Falegnami, Riccardo Patriarca, Giordano Vicoli and Maria Luisa Villani*
17.45-17:55	**Close of Day 1, Dinner logistics**
18:00	**Bus to Hotels**
19.45	**ESReDA 53rd Seminar Dinner**

2nd day, Wednesday November the 15th, 2017

7.45	**Departure from Hotel**
8.00	Arrival of the buses at JRC, clearance of entrance permissions, security checks of luggage etc.
8.30	Arrival at the meeting room, Welcome coffee
8.45-10.10	**SESSION 6.** **Foresight for safety management** Chairs: Sverre Roed Larsen and Frank Verschueren
8:45-9:20	**Invited Lecture III:** **Strategy and projects for a predictive safety regulation and safety management** *Antonio d'Agostino, ERA, France*
9:20-9:45	**Justifying safety interventions based on uncertain foresight: empirical evidence** *Eric Marsden*
9:45-10:10	**Is whistleblowing a promising "tool" for event occurrence prevention?** *Yves Dien*
10.10-10.40	**Coffee Break**
10.40-12:05	**SESSION 7.** **Early warning signs: Understanding threats through monitoring** Chairs: Yves Dien and Bastien Brocard
10:40-11:15	**Invited Lecture IV:** **From maritime multi-sensorial data acquisition systems to the prevention of marine accidents** *Lorenzo Fiamma*

11:15-11:40	**Evolution of remote performance monitoring in ship's safety decision making reinforced by Analytic Hierarchy Process** *Ioannis Dagkinis, George Leventakis and Nikitas Nikitakos*
11:40-12:05	**Increasing forced unavailability of power plants due to economical conditions** *Henk Wels and Thijs Slot*
12:05-13.05	**Lunch and Coffee**
13.05-13.55	**SESSION 8.** **Learning from experience to improve foresight in safety** Chairs: Nicolas Dechy and Miodrag Strucic
13:05-13:30	**The Learning Review: Adding to the accident investigation toolbox** *Ivan Pupulidy and Crista Vesel*
13:30-13:55	**A model for analyzing near-miss events by adopting system safety principles** *Silvia Maria Ansaldi, Maria Grazia Gnoni and Paolo A. Bragatto.*
13:55-14:15	**Coffee Break**
14.15-15.30	**SESSION 9.** **From database management to foresight** Chairs: Tuuli Tulonen and Sever Paul
14:15-14:40	**Use of event and causal Factor Short Chart reports to assess and simplify accident reports** *Miodrag Strucic*
14:40-15:05	**HIAD - Hydrogen Incident and Accident Database** *Daniele Melideo, Eveline Weidner, Francesco Dolci and Pietro Moretto*
15:05-15:30	**Cognitive inhibitors for threat assessment and automated risk management** *Jochen L. Leidner and Timothy Nugent*
15:30-15:50	**CLOSING SESSION** Chairs: Ana Lisa Vetere Arellano and Zdenko Šimić **Closing speeches** *Ana Lisa Vetere Arellano and Zdenko Šimić, JRC* *Frank Wastin, Unit Head, Knowledge for Nuclear Safety, Security & Safeguards* *Luis Ferreira, ESReDA President*
16.00	**Bus to Airport and Hotels**

Annex B - About the seminar

Seminar scope

Conventional safety management relies on prevention and protection approaches, but it is clear, especially after disasters, that this is not enough. Reactive approaches after events are valuable strategies to provide information and lessons on risk management deficiencies. The analysis of major accidents and crises has shown that there were early warning signs that could have been heeded and used as valuable information to design "relevant tools" and proactive strategies for preventing major events. Such missed opportunities point towards the need to improve foresight methods for enhancing safety management.

Several high-technology sectors, such as aviation and nuclear power have achieved a high performance level. Their call for a next generation of safety enhancement strategies and more proactive approaches have broadened to other sectors during the last decades. The shift from safety management approaches in which improvement is predominantly based on hindsight to include more foresight approaches has many hurdles to overcome, in theory, as well as in practice.

- How can safety imagination be enhanced: can we go beyond scenario approaches and techniques?
- How can foresight theories, methods and techniques contribute to broad risk assessments in order to improve systematic and holistic safety management?
- Addressing short term foresight versus long term planning: which methods/approaches are more appropriate for one and the other?
- How can we anticipate the new multi-faceted risks created by new technology, the digital revolution, industry 4.0, etc.? What can be done to improve our management of emerging risks?
- How to detect and handle early warning signs (EWS), weak signals, accident pre-cursors, etc.? Can the analysis techniques developed for “big events” (accidents, near misses) be applied to “tiny events” (EWS, weak signals), or are new classes of techniques needed?
- Which anomalies/surprises should we pay attention to? How to discriminate the signal from the noise? How to deal with and benefit from whistleblowers?
- How to increase the visibility of EWS? Are there tools and methods available? If yes, which are they?
- What role do leading indicators play and can they help achiev foresight with efficiency? If yes, how?
- Are new methods and technologies related to “big data” part of the solution?

- How does the social climate impact risk awareness and an organization's ability to identify early warning signals (reporting culture, speak-up behavior and psychological safety, debate, attitude towards bad news, etc.)?

- How can safety analysts generate the political capital needed to produce organizational change when they cannot point to a past accident to demonstrate the need for improvement and face the cost challenge?

- Is knowledge of the past obsolete? Is current knowledge management practice and organizational learning in organizations well-structured to tackle foresight in safety?

- How can foresight improve resilience and accident prevention?

- How did some sectors become highly reliable, ultra-safe, non-plus ultra-safe? Why are there such big differences (performance, approach) across sectors?

The 53rd ESReDA seminar will be a forum for exploring these questions. We aim to discuss theories, concepts, and experiences of enhancing foresight in safety. Authors are invited to present their proposals and discuss successes and failures in foresight and to identify future needs in safety research and training. We want to encourage new ideas, scientific papers, conceptual papers, case studies and cross-sectoral research on the theme of foresight in safety. This seminar will bring together researchers, practitioners, specialists and decision-makers to discuss strategies to improve foresight.

Target groups and domains of application (examples)

Papers for the seminar are welcome from various stakeholders (industrialists, regulators, safety boards, universities, R&D organisations, engineering contractors and consultants, training specialists) and could address different sectors:

- Energy sector: nuclear and non-nuclear (e.g. fossil, hydro) power plants and networks;
- Process industry: oil and gas, chemical and petrochemical facilities;
- Transport (rail, road, air and maritime): supply and distribution network, operation;
- Aerospace industry;
- Critical infrastructure: electricity, water, telecommunications, information systems;
- Public sector and government.

This seminar is aimed at addressing issues met by different industries. Other topics may be included if they fit well within the theme of the seminar and are applicable to foresight in safety, such as natural disasters, na-tech disasters, food safety, sanitary crisis, and banking.

Seminar organisation

Location

European Commission Joint Research Centre (JRC)
Via Enrico Fermi 2749
I-21027 Ispra (VA)
ITALY

Organization

The Seminar is jointly organised by ESReDA and JRC.

Seminar Chairman

L. FERREIRA (ESReDA President, Professor at University of Porto, PORTUGAL)

Technical Programme Committee Chairs

Ana Lisa VETERE ARELLANO (JRC Directorate E – Space, Security and Migration, ITALY)

Zdenko ŠIMIĆ (JRC Directorate G – Nuclear Safety and Security, The NETHERLANDS)

Technical Programme Committee Members

Ludwig BENNER Jr. (Investigation Process Research, USA)

Bastien BROCARD (Électricité de France S.A., FRANCE)

Nicolas DECHY (IRSN, FRANCE)

Yves DIEN (CHAOS, FRANCE)

Antonio FELICIO (ESReDA, PORTUGAL)

Milos FERJENCIK (University of Pardubicze, CZECH REPUBLIC)

Paulo MAIA (EDP, PORTUGAL)

Eric MARSDEN (FonCSI, FRANCE)

Sever PAUL (AGIFER, ROMANIA)

Sverre ROED-LARSEN (SRL HSE, NORWAY)

Fabiana SCAPOLO (JRC Dir. I - Foresight, Behavioural Insight & Design for Policy, BELGIUM)

Dan SERBANESCU (Romanian Academy, ROMANIA)

Miodrag STRUCIC (JRC Directorate G – Nuclear Safety and Security, The NETHERLANDS)

John STOOP (Kindunos, The NETHERLANDS)

Tuuli TULONEN (Tukes, FINLAND)

Frank VERSCHUEREN (Ministry of Labor, BELGIUM)

Opening of the Seminar

Georg PETER (EC JRC Directorate E – Space, Security and Migration, Unit Head, ITALY)

Closing of the Seminar

Franck WASTIN (EC JRC Directorate G – Nuclear Safety and Security, Unit Head, The NETHERLANDS)

Logistics

Orsolya SUDAR (EC JRC Directorate E – Space, Security and Migration, ITALY)

Maria IOAKEIMIDOU (EC JRC Directorate G – Nuclear Safety and Security, The NETHERLANDS)

European Commission Joint Research Centre (EC JRC)

As the European Commission's science and knowledge service, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle. Its work has a direct impact on the lives of citizens by contributing with its research outcomes to a healthy and safe environment, secure energy supplies, sustainable mobility and consumer health and safety.
Two directorates are supporting organization of this seminar:
JRC Directorate E – Space, Security and Migration
JRC Directorate G – Nuclear Safety and Security
https://ec.europa.eu/jrc

European Safety, Reliability & Data Association (ESReDA)

European Safety, Reliability & Data Association (ESReDA) is a European Association established in 1992 to promote research, application and training in Reliability, Availability, Maintainability and Safety (RAMS). The Association provides a forum for the exchange of information, data and current research in Safety and Reliability.
ESReDA membership is open to organisations, privates or governmental institutes, industry researchers and consultants, who are active in the field of Safety and Reliability. Membership fees are currently 1000 EURO for organisations and 500 EURO for universities and individual members. Special sponsoring or associate membership is also available.

For more information on ESReDA, contact: Inga.Zutautaite@lei.lt
ESReDA General Secretary, Dr. Inga Žutautaitė
Senior Researcher at Lithuanian Energy Institute

ESReDA address: European Safety, Reliability & Data Association, an International Non-Profit Scientific Association under the Belgium law (June 27, 1921, Title III). Headquarter: ESReDA, rue Gachard 88 Bte 14, B-1050 Bruxelles, Belgium, Siret: E00005802.

Any interested party is welcome to contribute to ESReDA project groups. See https://www.esreda.org/projectcasestudy/

About the ESReDA Foresight in Safety Project Group

Background

To avoid occurrence of events (accidents, incidents or crises), prevention is often seen as the main, not to say the only, goal of (industrial or system) safety.
Since the nineties, 3 ESReDA's working/project groups have obtained results regarding improvement of safety thanks to learning from experience (e.g. accident database, accident investigation; dynamic learning as a follow-up from accident investigation). They especially:

- Gave overview of accident investigation practices, institutions and regulatory framework in Europe;
- Gave overview of accident investigation practices, institutions and regulatory framework in Europe;
- Gave guidance of principles for how to conduct accident investigations and design event and accident databases;
- Gave guidance for dimensions to be taken into account for dynamic learning after an event;
- Provided some requirements for designers of training in the domain of accident investigation and learning;
- Gave overview of the main barriers to learning from events.

This work has been documented through different publications (books, reports, guidelines, publications, ESReDA seminar proceedings), some freely available on the ESReDA website and others that are mainly available at ESReDA editor (DNV library).

Some results of these previous works showed that, before event happened, there were early warning signs (EWS) that could have, to some extent, provided useful information and to some extent been "relevant tools" for preventing events occurrence.

Goals

Goals of the Project Group "Foresight in Safety" are:

- To better define these EWS (e.g. weak signals, precursors, near misses …);
- To focus on the human and organizational mechanisms for their treatment (e.g. role of whistle-blowers, role of learning, enabling features of organizational culture and concepts such as mindfulness, chronic unease).

To fulfil these goals the Project Group aims will try to identify how to:

- Enable organizations to deal with unexpected situations, situations not described by rules and procedures;
- Link them with vulnerabilities reliability and resilience of organizations;
- Characterize contrast between and change from apathetic to foresighted approach;
- Apply a systems perspective regarding life cycle analysis (from design to operations and further) including the synergy between feedback and feed-forward controls;
- Address the need for collaboration between technological and sociological disciplines;
- Articulate them with monitoring of Safety Performance (e.g. KPIs, SPIs ...);
- Make them visible in Databases treatment;
- See interest of use of scenario techniques and simulation underlying dangerous operations;
- ...

Duration

Expected duration of the Project Group is 2 to 3 years. The Project Group was launched in September 2015 after a kick-off meeting in Paris at EDF R&D and IRSN.

The PG have the following meeting schedule:

- Ispra, ITALY
- Petten, The NETHERLANDS
- Prague, CZECH REPUBLIC
- Ispra, ITALY

Deliverables

Work of the Project Group will be made visible through a deliverable, including articles tackling issues listed above and through organisation of the 53rd Seminar on "Enhancing Safety: the Challenge of Foresight".

Participating Organisations

Agenţia de Investigare Feroviară Română (AGIFER), Romania

Club Heuristique pour l'Analyse Organisationnelle de Sécurité (CHAOS), France

Électricité de France Recherche et Développement (EDF-R&D), France

European Commission Joint Research Centre (JRC), Belgium

Federal Public Service Employment, Labour and Social Dialogue, Belgium

Finnish Safety and Chemicals Agency (TUKES), Finland

Fondation pour une Culture de Sécurité Industrielle (Foncsi), France

Gestão da Produção de Energia, S.A. (EDP), Portugal

Institut de Radioprotection et de Sûreté Nucléaire (IRSN), France

Investigation Process Research, USA

Kindunos Ltd., The Netherlands

SRL HSE Consulting, Norway

University of Pardubice (UP), Czech Republic

ESReDA former related Project Groups

ESReDA has supported several project groups that have produced deliverables and books. Available publications are listed on ESReDA website. https://www.esreda.org/esreda-publications/

ESReDA former project groups deliverables on "accident investigation" (2001-2008) and "dynamic learning as a follow-up from accident investigations" (2009-2015) edited books and electronic reports available on ESReDA website.

https://www.esreda.org/projectcasestudy/dynamic-learning-as-the-follow-up-from-accident-investigations/#more-322

JRC Science Hub
https://ec.europa.eu/jrc

JRC111103

EUR 29488 EN

PDF ISBN 978-92-79-98156-2 ISSN 1831-9424 doi:10.2760/713354

Luxembourg: Publications Office of the European Union, 2018

How to cite this report: Vetere Arellano, A. L., Šimić, Z. and Dechy, N., *Enhancing Safety: the Challenge of: Proceedings of the 53rd ESReDA Seminar hosted by the European Commission Joint Research Centre*, EUR 29488 EN, Publications Office of the European Union, Luxembourg, 2018, ISBN 978-92-79-98156-2, doi:10.2760/713354, JRC111103.

KJ-NA-29488-EN-N

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office

doi:10.2760/713354
ISBN 978-92-79-98156-2