JRC CONFERENCE AND WORKSHOP REPORT

Using Knowledge to Manage Risks and Threats: Practices and Challenges - Proceedings of the 58th ESReDA Seminar

Hosted online by the European Commission, Joint Research Centre, 15-16 June, 2021.

Šimić, Z., Simola, K., Tulonen, T, Marsden, E.

2021

ESReDA

European Safety, Reliability & Data Association

Joint Research Centre

EU Science Hub
https://ec.europa.eu/jrc

JRC126686

PDF ISBN 978-92-76-42383-6 doi:10.2760/443612

Luxembourg: Publications Office of the European Union, 2021

How to cite this report: Šimić, Z., Simola, K., Tulonen, T, Marsden, E., *Using Knowledge to Manage Risks and Threats: Practices and Challenges - Proceedings of the 58th ESReDA Seminar*, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-42383-6, doi:10.2760/443612, JRC126686.

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 and available ESReDA proceedings please consult:

http://www.esreda.org/

Table of contents

Preface

Risk management and knowledge management are still developing and maturing both theoretically and practically. The connection between knowledge and risk management is essentially assumed and implicit with not enough explicit combined study and use. This seminar was organized in order to explore relations and complementarity between knowledge, risk and management in a cross-cutting way.

This seminar was initiated and organized by two ESReDA project groups: Foresight in Safety (at the end of its term) and Risk, Knowledge and Management (newly started). The original plans for the physical seminar had to be changed due to the Covid-19 pandemic and finally the seminar was organized as an online event one year after the original date.

The seminar program included 25 presentations, of which five were keynote lectures, and one forum to discuss the main theme. Keynotes and other presentations included the views and experience of different stakeholders from universities, research centres, industry and safety authorities. The topics addressed were related to knowledge and risk management from various perspectives: safety, risk assessment, use of scenarios, resilience, horizon scanning, early warning signals, database management, big data, data visualization, etc., and from various industries: including e.g. nuclear, chemical, electricity, telecommunications, railroad and aviation.

The seminar was well attended, with 58 participants from 24 countries (Australia, Austria, Belgium, Bulgaria, Croatia, Czech Republic, Finland, France, Greece, Italy, Lithuania, Luxembourg, Moldova, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, South Africa, Spain, Switzerland, United Kingdom and United States).

The discussions during the forum session, like all discussions during the seminar, demonstrated the relevance of the topic, the level of interest from participants and the number of open questions. Feedback obtained concerning the seminar, both informal and collected using an online poll, was very positive in respect to organization, presentations, discussions and takeaways. Seminar presentations, discussions and feedback illustrate the importance of the subject of risk and knowledge management. The seminar has already inspired a proposal of a new project group concerning the monitoring and verification of autonomous vehicles, and it will most certainly help continuation of the work for the related project group "Risk, Knowledge and Management".

The editorial work for this report was supported by the Joint Research Centre of the European Commission in the frame of JRC support to ESReDA activities. A special thanks is due to A. Liessens (JRC) for the editorial work.

Zdenko Šimić
EC Joint Research Centre

Kaisa Simola
EC Joint Research Centre

Tuuli Tulonen
Finnish Safety and Chemicals Agency (Tukes), Finland

Eric Marsden
Foundation for an Industrial Safety Culture, France

IAEA Knowledge Management Programmes to Support Organizational Capacity Building

Tea Bilic Zabric, International Atomic Energy Agency, t.bilic-zabric@iaea.org

Abstract

Nuclear technology requires a high level of technical and managerial expertise and competencies that must be developed and transferred to current and future generations. The IAEA assists its Member States in retaining and transferring this knowledge by developing methodologies, guidance documents, and tools for establishing or improving nuclear knowledge management (NKM) programmes. The paper will introduce projects as mechanisms to deliver IAEA services that focus on (1) strengthening national level through support in developing educational requirements (2) strengthening organizational level by performing assists visits for assessing specific topics of knowledge management programme.

1 Introduction

The impact of losing critical knowledge was recognized by many of the nuclear energy organizations in the late 1990s and early 2000s when a significant number of first generation nuclear professionals left the industry or retired, consequently the industry lost significant years of knowledge and experience gained from these individuals. This issue became more significant due to stagnation in growth of nuclear energy industry coupled with declining interest to pursue nuclear education. This issue prompted nuclear organizations to increase their focus on activities to mitigate the risk of critical knowledge loss. A second important issue was the opening of energy markets, which increased the migration of experienced staff. This challenge has encouraged managers in nuclear organization to act, but also it has allowed newcomers to develop their education and training programmes using experience of countries with advanced knowledge management programme. After the Fukushima accident nuclear organizations recognized the importance of the relationship between nuclear knowledge management and decision making. To ensure high levels of safety and economic operation of nuclear power plants, appropriate technical expertise and experience must be developed and be available throughout the nuclear organization life-cycle.

The IAEA Action Plan on Nuclear Safety (the Action Plan), which includes 12 main actions, defined a programme of work to strengthen the global nuclear safety framework. One of the actions focused on strengthening and maintaining capacity building: "*Member States with nuclear power programmes and those planning to embark on such a programme to strengthen, develop, maintain and implement their capacity building programs, including education, training and exercises at the national, regional and international levels; to continuously ensure sufficient and competent human resources necessary to assume their responsibility for safe, responsible and sustainable use of nuclear technologies*...".

2 IAEA Programmes to Support Organizational Capacity Building

Capacity building is a major step in the process of ensuring a sustainable supply of competent human resources capable of applying nuclear technologies in a safe, effective and sustainable manner. The building of competence for all parties with responsibilities for deployment, operation and oversight of nuclear organization is a requirement of the IAEA

safety standards but also a prerequisite to ensure continuous performance improvement ,business excellence and stakeholder support. The IAEA assists Member States operating and expanding nuclear power programmes, as well as those using nuclear technology in medicine, industry and agriculture, through a wide range of support services such as expert and peer review missions, training courses, conferences, technical meetings, workshops, publications, databases and guidance documents.

Nuclear facilities, R&D programmes and projects are often subject to long timelines and often require high investment. In the long-term, nuclear organizations and their staff change, so useful knowledge or expertise is at risk of being lost. Preservation of and access to existing nuclear knowledge as well as sharing of knowledge can contribute to development and effective decision making throughout all phases of a nuclear plant lifecycle. Various knowledge management practices have been developed to address challenges related to capacity building.

The IAEA programme on nuclear knowledge management focuses on:

- Developing methodologies and guidance documents for planning, developing and implementing nuclear knowledge management programmes;
- Facilitating nuclear education and networking;
- Assisting Member States by providing products and services for maintaining and preserving nuclear knowledge; and
- Promoting the use of knowledge management tools and supporting interested Member States in their use.

2.1 Nuclear Education and networking

Several initiatives have been undertaken by the IAEA in the areas of nuclear education and networking. This section highlights some of them. Initiatives to foster regional networking between nuclear knowledge providers are one of cornerstones of the IAEA's NKM (Nuclear Knowledge Management) programme. The main objectives of the nuclear education networks are to facilitate improvements in quality and availability of nuclear engineering and science programmes at the bachelor's and master's levels. This is accomplished through the following:

- Delivering Nuclear Energy Management (NEM) and Nuclear Knowledge Management (NKM) schools
- Sharing of information and materials of nuclear education and training;
- Developing harmonized approaches for education in nuclear science and technology by establishing reference curricula and facilitating mutual recognition of degrees;
- Promoting effective cooperation and sharing of resources and capabilities at national and regional level;
- Facilitating the exchange of students, teachers and researchers; and
- Serving as facilitator for communication between the network member organizations and other regional networks.

The NEM Schools provide international educational experiences aimed at building future leadership to manage nuclear energy programmes. They promote and foster knowledge of a wide range of issues related to the peaceful use of nuclear technology and provide a worldwide networking opportunity for future managers in nuclear energy.

During the in-person schools, selected participants are provided with wide range of different teaching and training activities including lectures, site visits, discussions, group work and presentations. Virtual schools have some limitation like lack of site visit and face to face networking and discussion. However they provide possibility of reaching much

larger numbers of participants, in more countries and they are particularly accessible to students who have other responsibilities, such as caring for family members. These virtual schools also use the latest technology to implement chat rooms and broad panel discussion. Each school typically consists of a series of core and elective modules, designed to provide a broad foundation education across the range of key and significant topics related to the IAEA and nuclear technology. The core topics are mandatory and are required to be taught in every NEM School. The elective topics are optional and can be tailor-made to suit the host organization's requirements. NEM schools includes lectures on management and leadership in nuclear organizations, energy planning and economics of nuclear power, management of knowledge and human resource development, stakeholder involvement and public communication, the fundamentals of nuclear energy in technology, nuclear safety and security, nuclear safeguards, radioactive waste management.

The Nuclear Knowledge Management (NKM) Schools are unique courses aiming to provide specialized education and training focused on the development and implementation of knowledge management programmes in nuclear organizations. The Schools focus on knowledge management methodologies and practices and explores various dimensions of NKM tools and techniques, challenges and benefits, culture influences and relationship with human resource preservation and sharing. The curriculum is organized into four modules, each composed of several specific topics and making up a total of approximately 18 hours of lectures. Learning is supplemented with examples, good practices and lessons learned from NKM programmes in different types of nuclear organizations. The main topics of the Schools are integrated approach to NKM, planning and modelling for NKM, succession management, coaching and mentoring for NKM, risk assessment in NKM, knowledge capture and transfer, competency mapping, principles of knowledge sharing culture, milestones of NKM implementation, indicators for a comprehensive NKM system, use and importance of lessons learnt and corrective action programmes, nuclear information management.

Among other instances, both the NEM and NKM Schools are jointly organized annually by the IAEA with The Abdus Salam International Centre for Theoretical Physics (ICTP) in Trieste, Italy. Additional, regional Schools are organized on a yearly basis in Japan, Russia and USA. Requests for organizing regional and national schools are increasing, so new candidates for frequent implementation of the Schools are Canada, Australia, China and African countries.

Another developing and important NKM initiative is the International Nuclear Management Academy (INMA) programme. It provides guidance for master's degree programmes with a specialized focus on advanced aspects of management and leadership in the nuclear and radiological sector.

INMA master's degree programmes in nuclear technology management (INMA-NTM programmes) are designed to meet the requirements of the nuclear and radiological sectors, and, preferably, be available part time and by distance learning or short format courses to be accessible to currently employed nuclear professionals by providing managers with a broad understanding of nuclear technology and management best practices in a nuclear or radiological context. INMA-NTM programmes facilitate an ongoing supply of highly qualified managers needed by nuclear energy sector employers, including nuclear power plants, waste management facilities, research and development laboratories, radiological facilities, regulatory bodies, technical support organizations, new build projects and nuclear energy related government ministries.

In detailing the common required elements of INMA-NTM degree programmes, IAEA provides the assistance to universities wishing to establish a master's degree programme in NTM, including the formal process of INMA-NTM programme endorsement. It also fosters university collaboration and sharing, and provides supporting tools. Developed by the IAEA in collaboration with the nuclear engineering and business faculties of several universities, and with nuclear employers around the world, INMA offers a sustainable educational framework that enables participating universities to implement high quality master's level management programmes for the nuclear and radiological sector.

To ensure that the curriculum for the programmes matches the requirements of industry, a consultation with industry was conducted to ask which key competencies are required for a nuclear and radiological sector. Fifty curriculum topics are specified that are expected to form the basis of any INMA-NTM programme. They are grouped into the four categories:

a) External environment: The curriculum topics relating to understanding or managing aspects of the nuclear organization's external environment such as political, legal, regulatory, business and societal environments in which nuclear managers operate.

b) Technology: The curriculum topics relating to the basics of nuclear technology, engineering, and their applications that are involved directly or indirectly in the management of nuclear facilities for power and non-power applications.

c) Management: The curriculum topics relating to the challenges and practices of management in the nuclear and radiological sectors with due consideration of safety, security and economics.

d) Leadership: Requires an understanding of the technology and management of a nuclear facility with due consideration of the external environment in which it operates. Leadership requires vision, strong ethical behaviours, clear foresight and goal setting, commitment to safety and security, good communication skills with all stakeholders, and a professional disposition in all situations.

INMA framework development and university programme implementation is supported with facilitation of IAEA through meetings, guide documents, and peer review missions.

The IAEA promotes partnerships among nuclear education and training institutions across the globe. It has directly fostered regional educational networks in Asia, Africa, Latin America and the Caribbean, and in Eastern Europe and Central Asia.

Ensuring an adequate and sustainable pipeline of qualified nuclear professionals to meet the specific national demands of the nuclear and radiological sector is a continual challenge for many Member States. Educational networks have been utilized to overcome limited funding and resources for the establishment and delivery of national nuclear educational programmes. Co-operation and collaboration with industry has supported national and international networks leading to the expansion and enhancement of many nuclear educational programmes. Globally there are different types of networks in global nuclear arena, from small bilateral university and industrial partnerships to regional networks that bring together educational organizations and employers across a continent. IAEA is sharing lessons learned from the different phases of conception, establishment and operation of successful networks which are beneficial for others aspiring to develop or improve nuclear education programmes. A capturing of international experience provides a better understanding of the contribution educational networks play in capacity building, underlining the IAEA's role in promoting and facilitating collaboration among educational institutions through support to the networks.

2.2 NKM Methods and Services

The IAEA is providing support to Member States in establishing methodologies and services for developing a strategic knowledge management programme for nuclear organizations.

Knowledge Management Assist Visits (KMAVs) are designed to assist Member State's nuclear organizations establish knowledge management programmes that can contribute to both safety and business objectives.

For nuclear organizations the support to implement strategic knowledge management programme is provided at 3 different levels.

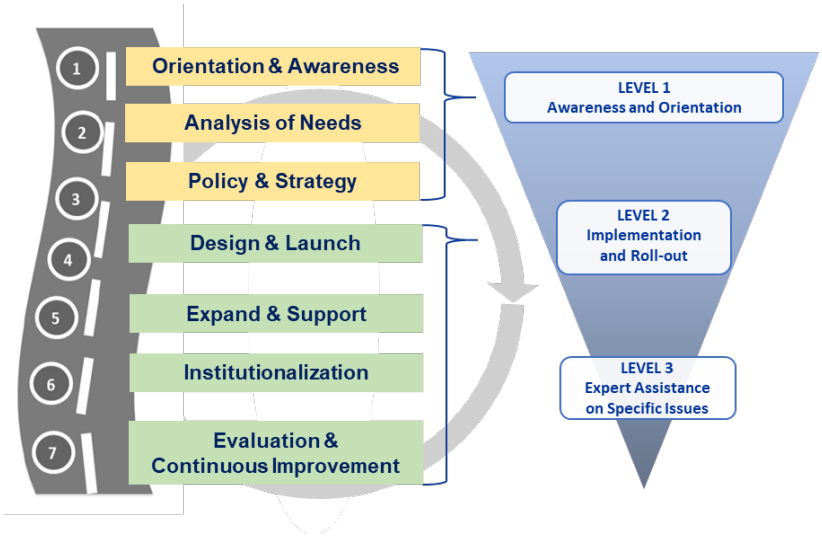
KMAVs are usually conducted at an level but occasionally knowledge management strategies and their implementation can be targeted at corporate level. Therefore, the IAEA has developed a methodology to assist Member States in implementing knowledge management primarily at the level of nuclear organizations. Accordingly, KMAV services

(missions) are organized at three levels depending upon the level of maturity it possesses and its needs in the area of knowledge management:

- LEVEL 1 Missions: Provide orientation and awareness enabling to initiate the development of a strategic knowledge management programme in nuclear organizations;
- LEVEL 2 Missions: Help to improve an existing knowledge management programme through IAEA assessment process and identifications of suitable KM solutions;
- LEVEL 3 Missions: Provide assistance to review specific areas of established knowledge management practices of a respective nuclear organisation and provide expert advice on further improvements.

The three levels of services are aligned to the roadmap consisting of the 7 stages required to implement a matured knowledge management programme (see Fig 1 below).

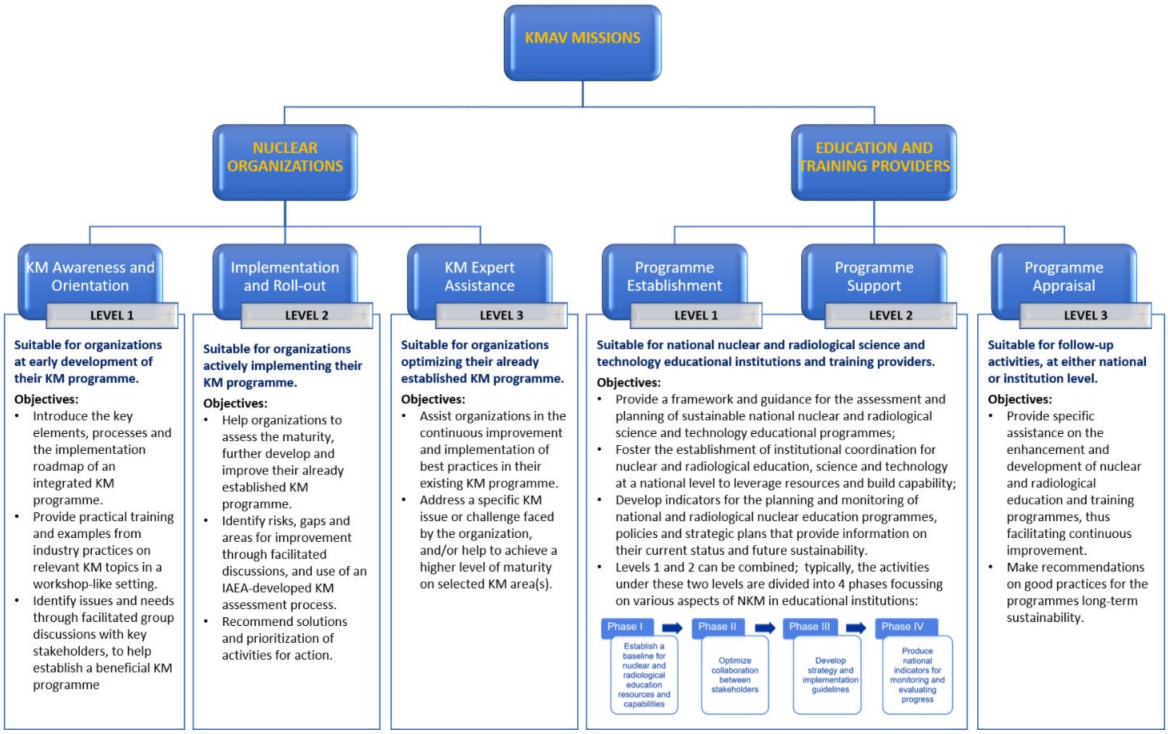
Figure 1. Roadmap for implementation of knowledge management.



The output of each mission is a report which identifies gaps in existing knowledge management programme and provide suggestions and recommendations to improve the knowledge management programme. Up to now IAEA has performed more than 70 KMAVs.

For universities and organizations that provide nuclear and radiological education and training, the IAEA has developed a methodology to support implementation of a sustainable nuclear and radiological education system. It includes a framework for planning and assessing the education sector's contribution to the facilitation and development of applications of nuclear and radiological science and technology to meet development priorities. The outcomes of this process, including an analysis of the required human and financial resources to support the national development objectives, is aligned with the IAEA Country Programme Framework which defines the agreed priority development needs and interests to be supported through technical cooperation activities with the IAEA and reflects national development plans and priorities, country specific analyses and lessons learned from past cooperation.

Figure 2. KMAV framework for nuclear organizations and education and training providers.



The IAEA initiative is to help Member States better understand the issues and challenges related to the effective management of knowledge for both new and existing nuclear facilities over the life cycle and to improve understanding of the strategic importance, shared responsibility and specific challenges involved in sustaining the nuclear knowledge base needed to ensure high levels of safety over the entire nuclear life cycle. It considers the complexity of each national nuclear energy programme and its related technological infrastructures and organizational systems.

The IAEA is developing and providing practical guidance for knowledge management implementation. The objectives of this initiative is to: clarify stakeholder involvement and responsibilities; create more awareness of the challenges and threats to maintaining knowledge; identify issues related to new builds (timely establishment of educational system); identify the types and importance of information systems to support knowledge management. Another (and related) purpose of the initiative is to facilitate international collaboration and sharing of knowledge, experience and best practices to address key challenges and issues that need to be resolved in this area.

3 Conclusions

All the time, in everything Member States are responsible for implementation of nuclear knowledge management and capacity building in their countries. The IAEA, is committed to its role of continuing to provide practical assistance to help ensure the entire nuclear sector finds ways to continuously strengthen NKM and enhance safety and improve performance and business processes. In particular, by strengthening nuclear education and knowledge management in the Member States the IAEA can help nuclear organizations be more proactive in ensuring an adequate knowledge base is established and maintained: in areas of human competency; in areas of management systems and business/work processes; and in areas of nuclear science, engineering and technology. In the post-

Fukushima era, awareness of the importance of and need for effective KM continues to grow.

References

A number of IAEA publications on NKM are currently in the process of development. Currently available publications include:

1. Guide to Knowledge Management Strategies and Approaches in Nuclear Energy Organizations/Facilities, Nuclear Energy Series, No. NG-G-6.1, 2019
2. Planning and Execution of Knowledge Management Assist Missions for Nuclear Organizations, IAEA-TECDOC-1880 Rev 1, 2019 International Nuclear
3. International Management Academy Master's Programmes in Nuclear Technology Management, Nuclear Energy Series, No. NG-T-6.12, 2020
4. Knowledge Loss Risk Management in Nuclear Organizations, Nuclear Energy Series, No. NG-T-6.11, 2017
5. Nuclear Engineering Education: A Competence-based Approach in Curricula Development. Nuclear Energy Series No. NG-T-6.4, 2014.
6. The Impact of Knowledge Management Practices on NPP Organizational Performance - Results of a Global Survey. IAEA TECDOC 1711, 2013.
7. Knowledge Management for Nuclear Research and Development Organizations. IAEA TECDOC 1675, 2012.
8. Comparative Analysis of Methods and Tools for Nuclear Knowledge Preservation. Nuclear Energy Series No. NG-T-6.7 STI/PUB/1494, 2011.
9. Status and Trends in Nuclear Education. Nuclear Energy Series No. NG-T-6.1 STI/PUB/1475, 2011.
10. IAEA Action Plan on Nuclear Safety, 2011

Agri-food Implications of Fukushima Nuclear Accident - Lesson Learned for Risk Management

Hrabrin Bachev, Institute of Agricultural Economics, Sofia, hbachev@yahoo.com

Abstract

On March 11, 2011, the strongest ever recorded in Japan earthquake occurred which triggered a powerful tsunami and caused a nuclear accident in Fukushima nuclear plant. The latter was a "manmade" disaster having immense impacts on people's life, health, and property, infrastructure, supply chains, economy, policies, natural and institutional environment, etc. This paper presents work in progress and assesses preparedness for and agri-food impacts of the Fukushima nuclear disaster, identifies challenges in post-disaster recovery, and withdraws lessons for improving disaster risk management. Japan was not well prepared for such a huge disaster while the agri-food sector and consumption have been among the worst-hit areas. The triple disaster was a rare but high-impact event, therefore, it is necessary to "prepare for the unexpected". Risk assessment is to include diverse hazards and multiple effects of a likely disaster, it is to be discussed with all stakeholders, and measures taken to educate and train all for complex disasters. It is necessary to modernize property rights, regulations, safety standards, and norms, enhance the capability of responsible public authorities and improve coordination between diverse actors. It is important to set up mechanisms for effective public resource allocation and reduction of agents' costs. Different elements of the agri-food chain have dissimilar capabilities requiring differential public support. There is a strong "regional" interdependency of agrarian, food, and rural assets (and damages), and it is important to properly locate risk and take prevention and recovery measures. Disaster response demonstrated the important role of small-scale farms and food organizations, and the high efficiency of private, market, and collective governance. Before, during, and after a disaster, all available information from all sources is to be immediately publicized in understandable form through all possible means. Disaster provides an opportunity to discuss, introduce and implement fundamental changes in agricultural, economic, regional, energy, disaster management, etc. policies. It is important to learn from past experiences, prepare for multiple disasters, and make sure that "lessons learned" are not forgotten.

1 Introduction

On March 11, 2011, the most powerful earthquake ever recorded in Japan (magnitude of 9 Mw) occurred known as the Great East Japan Earthquake (GEJE). It triggered powerful tsunamis which caused a nuclear accident in one of the world's biggest nuclear power stations - the Fukushima Daiichi Nuclear Power Plant (FDNPP). Radioactive contamination spread through air, rains, dust, water circulations, wildlife, garbage disposals, transportation, and affected soils, waters, plants, animals, infrastructure, and population. Japanese agriculture, food industry, and agri-food consumption have been among the worst affected areas from the Fukushima Nuclear Accident (FNA) (Bachev and Ito, 2014, 2018; Bachev, 2019; FAO/IAEA, 2018; Hamada and Ogino, 2012; JFC, 2011-2014; Johnson, 2011; Koyama, 2013; Kunii et al., 2018; Monma et al., 2015; Nakanishi and Tanoi, 2013; Nakanishi, 2018; Oka, 2012; Sekizawa, 2013; Todo et al., 2015; Takebayashi et al., 2020; Ujiie, 2012; Watanabe, 2013). This paper presents the current results of a long-term on-going study and assesses preparedness for and long-term agri-food impacts of FNA, identifies challenges in post-disaster recovery, and withdraws lessons for improving disaster risk management. A multidisciplinary approach is applied and diverse types of

monitoring, statistical, experts, stakeholder interviews, research, etc. data are used in the analysis.

2 Assessment of Preparedness and Agri-food Impacts

The Agri-food sector of Japan was not well prepared for such a big disaster and badly affected by FNA (Bachev, 2014, 2019; Bachev and Ito, 2018). Adverse long-term effects on agriculture, food industries, and food consumption are in the following areas:

First, enormous production and income reduction due to radiation contamination, mandatory and voluntary shipment restrictions, increased inputs, production and marketing costs, costs of adaptation and implementation of new safety standards, diminished market demands and prices of agri-food products, etc. (Table 1). Initially, almost 55% of all farms were affected negatively by GEJE as in the worst-hit (Fukushima, Iwate, and Miyagi) prefectures 90% of holdings suffered mostly due to "prices decline" and "harmful rumours" (JFC, 2013). Damages to agriculture have been particularly big in areas around the nuclear plant, where farming and related activity is suspended or reduced affecting 8% of farmers and 9% of farmlands of Fukushima prefecture. Effective recovery in mostly impacted prefectures has been deterred by FNA impact, unavailable land and equipment, undecided settlement place, funding problems, etc. as the importance of FNA as a factor for "not resuming farming" increased (MAFF, 2019). Almost 60% of food companies (82% in most affected regions, 94% in Fukushima prefecture) were also severely affected by FNA due to cancelled orders, reduced sales and prices, increased input supply costs, etc. (JFC, 2014).

Second, there was radioactive contamination of farmlands, agrarian physical and biological assets, and infrastructure from FNA's fallout. Radioactive caesium contaminated 8% of the lands of Japan, 40% with radiation exceeding allowable level (MECSST, 2011). Heavily contaminated farmlands are located in 8 prefectures where radiation contamination ranges from 16-56600 Bq/kg (MAFF, 2013). There have been huge public and private costs for cleaning farmlands and agrarian assets. Up-to-date 94% of farmland has recovered as well as 97% of fishery processing facilities have reopened (MAFF, 2021). Nevertheless, in 12 most accident-affected municipalities restoration of farming has been progressing slowly while some heavily contaminated areas require long-time before farming could resume. The agri-food sector is a major employer in affected regions, and after FNA thousands of farms' livelihood and businesses are destructed as a result of loss of lives, injuries, displacement, damages on property, infrastructure, community, and business relations. Much of the long-term damages from FNA on farmers' livelihood and possessions, physical and mental health, environment, lost community relations, etc. can hardly be evaluated in quantitative terms (Bachev and Ito, 2014, 2018).

Third, up to FNA there was no adequate system for agri-food radiation regulation and food safety inspection in Japan. Provisional regulatory limits for radionuclides in agri-food products were introduced after FNA which were upgraded to the world's strictest in 2012. Widespread inspections on radiation contamination have been introduced, and numerous production, shipment, and consumption restrictions on agri-food products imposed. Regular radiation tests have been carried on numerous agri-food products in 17 prefectures, including all rice bags and beef meat in Fukushima prefecture. There have emerged many private and collective inspection systems introduced by farmers, rural associations, food processors, retailers, local authorities, consumer organizations, independent agents, etc. some of which employing stricter than official safety norms. There are several products from contaminated areas of 17 prefectures, still subject to shipment restrains (outside Fukushima mostly covering mushrooms, wild plants, fish). Consequently, the number of agri-food items with the level exceeding safety standards diminished to zero in recent years all groups but mushrooms, wild plants, fishery products, wild bird, and animal meat (MAFF, 2020). Modernization of the food safety system has taken time and is associated with enormous public and private concerns, debates, and costs.

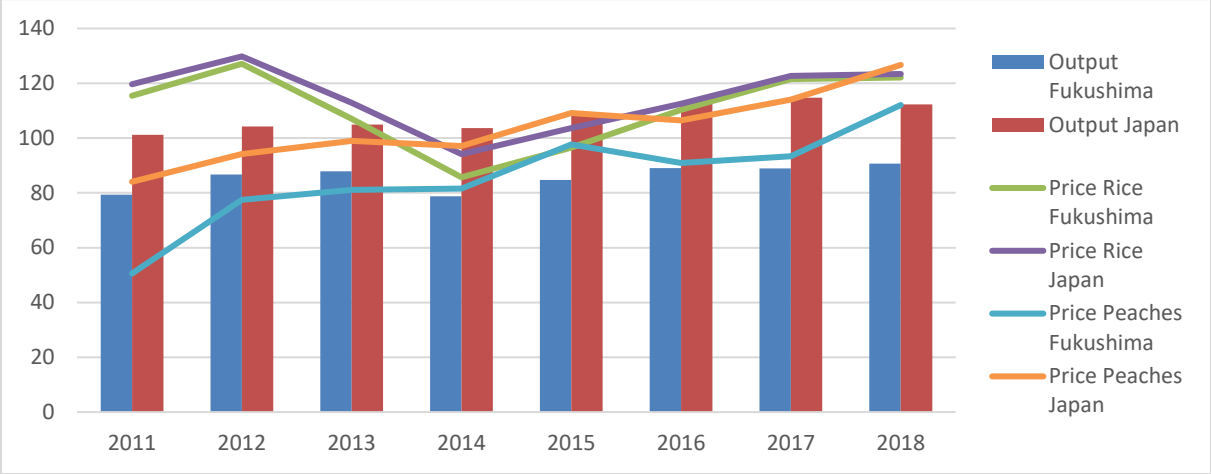
Table 1. Agricultural Long-term Impacts and Major Challenges of Fukushima Nuclear Disaster

Related to	Impacts	Challenges
Farmers Agribusiness managers Hired Labour	Physical and physiological destruction Evacuation	Support system and consultation for evacuees Creation of infrastructure and environment for people to return and stop leaving Shortage of farm managers and labour
Lands and assets	Contamination Destruction	Cleaning remaining farmlands Inspecting and reinforcing agricultural facilities
Production	Reduction or suspension of activities	Full scale recovery and revitalisation Multiple risks management preparation Enrolling in the agricultural insurance Complying with hygiene and safety standards
Distribution and marketing	Destruction Shipment bans and restrictions New marketing channels	Dispelling current and emerging rumours to revive agriculture, food processing, fisheries and rural tourism Promotion of Fukushima products
Economy	Increased costs Lost income Lost employment Lost capital value	Sustainable public support Modernisation New income opportunities in affected regions
Food regulation	Modernisation of standards, rules and institutions	Trust Effective enforcement
Food inspection	Modernisation of organisation and methods Huge costs Private and third party modes	Keep and improve monitoring system Build trust Recover private and collective costs
Organisation and risk management	Innovations Private, collective, and hybrid modes Food chain management Land consolidation	Educating, training, informing, preserving Future of traditional farming Decentralisation of risk management
Information	Increasing Diversification Reliability	Trust Enormous costs
Natural environment	Long-term contamination Destruction of biodiversity and ecosystems	Recover damages to wildlife, soils and natural ecosystems Safe transportation of contaminated soil to Interim Storage Facility Final disposal site for contaminated waste Decontamination of Difficult to-return Zone
Research, technological and product innovations	Huge dynamics of activity and forms New perspective areas	Costs, efficiency, priorities Destructed international cooperation due to Corona crises
Agri-food consumption	Increased health concern, checks, and oversupply Secure procurement modes	An effective system for informing consumers Consumption of domestic and local agri-food products
Policies	Increased public support Shifting priorities Modernisation of Food Security, Energy, Health care, Environmental etc. policies Ongoing debates	Involving all stakeholders Building disaster-resilient communities and supply chains Increasing domestically and local agri-food consumption Agri-food export promotion

Source: Author.

Fourth, immediately after FNA there was the destruction of supply of potable water, foods, and necessities in most affected regions. Unprecedented for modern Japan food shortages occurred in disaster areas and big cities but food supply was quickly restored and important infrastructure rebuilt. There have been numerous restrictions on production, sales, shipments, and consumption of agri-food products in affected regions which stopped, delayed, or reduced effective supply of a range of products. Due to genuine or perceived health risk many wholesale traders, processors, and consumers stop buying agri-food products originated from "Northern Honshu", even in cases when it had been proven that food is safe (MAFF, 2020). "Reputation damage" is particularly important for many traditional products like rice, fruits, vegetables, mushrooms, milk, butter, beef, etc. which demand and prices significantly declined (Figure 1). Demands and prices for Fukushima agri-food products have been recovering but many consumers continue to select the region buying "rarely" or "not at all" from affected regions because they "worry about safety" (JFC, 2014; Takebayashi et al., 2020). Numerous consumers continue to disbelieve inspection systems and employ other ways to procure safe food through direct sales, contracts, origins, own or co-production, imports, etc.

Figure 1. Evolution of Total Agricultural Output, and Prices of Rice and Peaches in Fukushima Prefecture and Japan (2010=100)



Source: Fukushima Prefectural Government, MAFF, 2021.

Fifth, FNA adversely affected international trade as 54 countries and regions imposed restrictions on agri-food imports from Japan, including major importers such as China, USA, Indonesia, Malaysia, South Korea, etc. As a result of strict inspection measures, promotion of a third-party GAP certification, information sharing, etc. many countries have eased or eliminated import restrictions but still, Fukushima products are not fully included (MAFF, 2021).

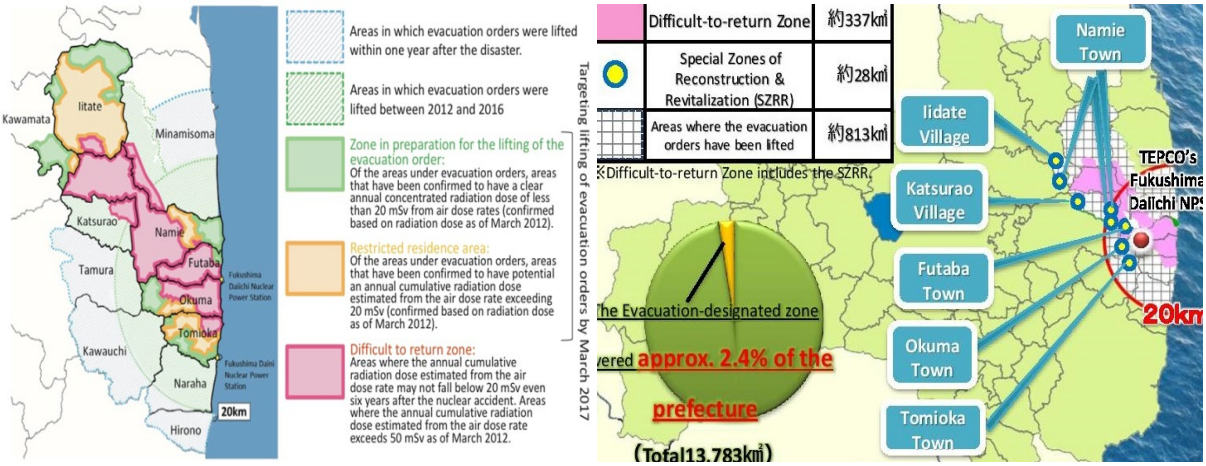
Sixth, FNA has positive effects on the agri-food sector in non-contaminated regions in which prices, demands, production, and sales opportunities have increased. Recovery from GEJE has been also associated with the consolidation of farmlands in reconstructed areas as well as the emergence of new (community, private, market, collective, hybrid, food chain, etc.) organizational and risk management modes. Besides, there has been a boom in technological, product, and organizational innovations in agrarian and other sectors, and enormous growth of new sectors (radiation testing, decontamination, energy saving, renewable energy, nuclear safety, debris cleaning, processing and disposal, research and development, robotics, ITC, no-soil and solar sharing farming, smart agriculture, branding, etc.) with huge investments of leading players, central and local governments, and numerous newcomers, joint ventures, etc. All they created new employment and income opportunities in affected regions and Japan.

Our survey has found out that major factors for long-term persistence of FNA negative impacts on agriculture are: consumers' unwillingness to buy, long-time required for deactivating radiation, insufficient support from central government, produce low prices, low confidence in official information, lack of information, bad reputation, and little preparedness of public authorities (Bachev and Ito, 2018). The most important factors for food industries are lack of information, consumers' unwillingness to buy, long-time required for deactivating radiation, little preparedness of public authorities, bad reputation, insufficient support from central government, and low confidence in official information. The most important factors for food consumption are lack of information, low confidence in official information, insufficient support from the central government, and a bad reputation.

3 Persisting Disaster Recovery Challenges

After FNA a large-scale evacuation affecting 470000 people or 9% of the Fukushima prefecture population and 12% of prefecture territory was carried. Evacuation areas and the number of evacuees gradually have decreased (Figure 1). Nevertheless "evacuation designated zones" still cover 365 km2 (2,4% of Fukushima prefecture territory) while 41000 Fukushima residents continue to live as evacuees (75% in other prefectures), including 2000 in temporary housing (RA, 2021).

Figure 2. Evaluation zones in Japan (past and 2021)



Source: Fukushima Prefectural Government

Evacuation and reconstruction is associated with number of challenges: failure for timely evacuation from certain highly contaminated areas, slow response of authorities, lack of sufficient public information in first stages of disaster, mistrust to public and private institutions, multiple displacements of many evacuees, divided communities and families, bad communication between different organizations, lack of financial resources, insufficient manpower and building materials, ineffective use of public funds, discrimination toward some evacuees, emotional conflicts between evacuees (about "self-evacuation", compensations, rebuilding modes), insufficient and unequal compensation, unequal decontamination and recovery of individual sectors (fast of construction industry, slow for farming, services, food processing, fishery) and regions (much slower for Fukushima), workers moving away from agri-food sector, unequal payment for work in traditional industries and government's emergency programs, substandard labour conditions for decontamination workers, increased individual and organized crimes, population decline (out-migration), long-time to obtain consent for reconstruction plans, difficulties of land acquisition for building cities, spikes in construction material prices, manpower shortages, lack of contractors, numerous lawsuits against TEPCO and authorities, delay in establishing Reconstruction Agency for coordinating multiple recovery efforts, unclear government

guidelines for nuclear disaster recovery, revisions in national energy, disaster prevention etc. policies, lack of detailed contamination map for all agricultural lands, improper use of extension officers (obtaining samples while suppressing consulting, introducing technology, education), etc. (Bachev and Ito, 2018).

Many evacuees, especially younger ones, refuse to return even after decontamination is completed because of persisting high radiation in forests around houses and hot spots, health risk, destructed business and community infrastructure, established life in other regions, etc. Major reasons for slow progress are: delayed reconstruction, lengthy lands decontamination, existing hotspots, restricted mobility in evacuated areas, calls for more decontamination, difficulties in the safe disposal of contaminated soil and debris, population fears regarding radiation hazards, concern about the safety of intermediate nuclear waste storage facility, lack of job opportunities, destructed business, unrestored critical services and infrastructure, absence of communities consensus for certain projects, uncertainty for future developments, etc.

Insufficient decontamination of farmland and irrigation canals, decreased motivation among farmers, and local anxiety over rumours about produce are major reasons for the low resumption of farming in the evacuation zone. It has been difficult to farm efficiently (e.g. water control in paddies) since farmers were forbidden to stay permanently, there is uncertainty associated with marketing, and radioactive water runoff from mountains to reservoirs and paddy fields.

Food safety measures let Fukushima agri-food products become "safest in the world" but enormous public and private actions to increase safety and transparency have not to recover consumer trust. Demand for agri-food products from affected regions in Japan and internationally stay low due to lack of sufficient capabilities in the inspection system, inappropriate restrictions (initially covering all shipments in prefecture rather than contaminated localities), revealed rare incidences of contamination in commonly safe origins, low confidence in official "safety" limits and inspections, lack of good communication, harmful rumours ("Fu-hyo"), or unauthentic products (Bachev and Ito, 2018; MAFF, 2021). Recent data indicate that despite enormous public support the sales in the fishery and food processing industries have only recovered to 31.2% (70,7% in the construction industry) (FPG, December 2020). Demand for agri-food products has been "recovering" but wholesale prices are lower than national (Figure 1). That is a consequence of an increased number of inspections, reduction of radioactive contaminations, improving consumer confidence in inspection and safety, "forgetting" contamination issue by some part of the population, preferences to lower prices regardless of quality by some consumers, changing marketing strategies (not promoting/labelling products as "Fukushima origin"), increasing procurement by restaurants and processors, etc. All these have led to outmigration of the younger generation from Fukushima prefecture and low interests in most affected subsectors like agriculture, food processing, fisheries, etc.

There are challenges with the safety inspection system. Due to lack of personnel, expertise, high-precision equipment, the water, food, and soil tests are not always accurate (detecting single-digit according to new regulation), consistent and comprehensive. Food safety inspections are carried out at the distribution stage (output for shipment, export), and do not (completely) cover produces for farmers' markets, direct sales, food exchanges, and self-consumption. Capability for radiation safety control in Fukushima prefecture is high while in other prefectures strict tests are not carried out while contamination has "no administrative borders". Many private/collective testing equipment is not with high precision and samples are properly prepared (by inexperienced farmers). There are considerable discrepancies in measurements of radiation levels (air, food) done by different entities in the same location. Certain sold products are labelled as safe despite contamination and some tested agricultural products are further cooked or dried reaching higher radiation during consumption. Uptake of radioactive materials with food increases during the summer season (fresh vegetables/fruits consumed) and there are untested wild plants and home-produced food widely consumed by locals.

Agri-food inspections, regulations, and countermeasures are conducted in different agencies with "own" policies and not (well)coordinated procedures – Ministry of Agriculture, Forestry and Fisheries (soil contamination surveys and agri-food inspection), Ministry of Health, Labour and Welfare (food safety standards regulations), Ministry of Education, Culture, Sports, Science and Technology (monitoring air radiation), Ministry of Environment (decontamination and waste disposal), Consumer Affairs Agency (food safety training, Reconstruction Agency (restoration and decontamination). There are no common procedures, standards, and coordination between monitoring carried out at different levels and different government, professional, research, etc. organizations. Neither there is a common framework for centralizing and sharing all information and making it available to interested parties and the public.

Official "area-based" system for shipment restrictions harms many farmers producing safe commodities, instead of permit shipment by selected farmers is more appropriate. Extending random sampling tests of circulating produce (shipment level) with management/control at the production "planning" stage is superior. According to many, the biggest hurdle is the lack of a clear radiation risk standard that can be universally accepted since there are ongoing discussions among experts about "safety limits" and that confuses producers and consumers. Another challenge of the inspection system is the costs for local authorities, farmers, the food industry, etc. Fukushima prefectural government maintains several tested items, funding is depleting while the central government decreases screened items number. Much of the inspection costs of cooperatives, farmers, food processors, etc. are not compensated.

There are challenges with emerging new technologies and organizational modes – for high building and running costs, difficulties in cultivation technique, human development, food certification system, needs for stable marketing through integration, the requirement for entrepreneurship, collective actions, big investment, taking over by non-agrarian capital/entities, which are not available, well-accepted or legitimate. A negative outcome from restoration projects has been that farmland partitions expanded in Iwate, Miyagi, and Fukushima prefectures (MAFF, 2021).

Another challenge is a health risk for the population caused by radiation exposure. Thanks to timely measures (warnings, protection, evacuation, monitoring, decontamination, food inspections, treatment), radiation levels for the population have been well below the norms damaging health (WHO, 2013). Air dose rates around the country and within critical places in Fukushima prefecture have been higher than before the disaster but comparable with major cities in Japan and overseas (FPG, 2021). Surveys in most affected regions indicate that annual radiation intakes from foods are less than 1% of the maximum allowed and decreasing, while in the country as a whole is insignificant (MHLW, 2020).

Official "safe" radiation exposure levels were drastically increased from 1 mSv to 20 mSv per year in 2011. There have been debates and great concerns about health effects from cumulative exposure above and within the official limit. That worries are enforced by controversial opinions of experts, slow process of decontamination in some areas, the unresolved issue with safe disposal of contaminated debris, deficiency in food safety control, continuing radiation leakages in the nuclear plant, etc. Since FNA complaints and hospitalization have been increasing in Fukushima prefecture (Bachev and Ito, 2018). Nevertheless, the health effects of radiation release are "primarily psychological rather than physical" since many consumers and producers "lose peace of mind" having food with (lower than official safety limit but) radiation contamination. Long-life as an evacuee, lost property and employment caused many to develop physical or mental (stress, anxiety) problems, and "disaster-related deaths" reached several thousand. However, it is becoming increasingly difficult to identify relationships between health problems and deaths and FNA due to a long period.

TEPCO (operator of the nuclear power station) has paid trillions of yens in compensation related to FNA but still, there are thousands of claimants seeking or disputing compensations from TEPCO or authorities. Estimated compensation amount grows up constantly due to new governmental guidelines or as a result of court decisions for

compensations. The number of false claims and swindling compensation funds for millions of yens has been also reported. Progress in compensation payments has been slow and uneven due to delays in TEPCO's review process; great paper works; lengthily negotiation; delays in payments; partial payments; disputing origin of damages; denying claims when production/distribution are restrained voluntarily; farmland, property, and discontinuation of business damage uncompensated; disagreements overcompensation "closing date; insufficient amount to restart farming/sustain consumption; inspection, administrative, radiation map preparation, etc. costs of organizations uncompensated; damages support unclearly specified in guidelines; negotiation asymmetry for farmers marketing through cooperatives; high lawyers costs; "safety tests" costs of farmers and consumer associations uncompensated; lack of clarity how certain claims be compensated; cash-flow difficulties and interest payments; uniform compensation "per ares" while differences in products, value-added, method (organic, conventional), etc.

Central and local governments have been spending tens of trillions of yens for reconstruction and revitalization actions (RA, 2021). There has been huge progress in these areas and numerous "good examples" but overall long-term effects of all this spending on the agro-food sector are difficult to access.

There is also uncertainty about full costs related to FNA due to expanding costs for decommissioning and counter adverse impacts. Decommissioning of nuclear reactors is at the beginning stage and there are many challenges related to lack of experiences, available technologies, uncertainties and risks, multiple failures, public concerns, lack of disposal site, impacts on populations and other industries, etc. In addition, there is a huge amount (16-22 mil.m3) of soil, leaves, mud, and other radioactive waste which has been stored in thousands of "temporary" storage sites across 13 prefectures. There is also a big amount of "designated waste" (143,689 tons) containing radioactive substances measuring more than 8000 Bq/kg. A temporary (30 years) storage facility for radioactive waste near the nuclear plant operates since 2017 while a site for final disposal of radioactive waste is not chosen because of the opposition of residents and industries in other prefectures. According to some experts undertaken large-scale decontamination creates new eco-problems: huge amounts of radioactive waste, removal of topsoil, damage to wildlife habitat and soil fertility, increased erosion on hillsides and forests, intrusion by people and machinery into every ecosystem, etc. Due to challenges with handling treated waters (accidental leakages, control release in the ocean, etc.) now to work not to generate "new" harmful rumours towards the Fukushima agriculture, forestry, and fisheries industry and tourism industry is high on the agenda (FPG, 2021).

There have been several new disasters in Japan (Typhoon Hagibis, Classical swine fever, ongoing Coronavirus epidemic, etc.) affecting additionally population, sectors, and food supply in the Fukushima accident regions and beyond. Besides the destruction of production (damages on crops, livestock, facilities, shortage of immigrant labour, etc.), they particularly badly enhanced the effects on demands of Fukushima agri-food products (closure of schools, restaurants, restriction on tourisms and countryside stays, cancelation of revitalization and traditional events, stagnation of acceptance of foreign technical interns, overstocking by households and businesses, decrease in exports, etc.). There have been emerging alternative modes of marketing like home and post-delivery, processing of milk as well as information campaign on preventing and safety measures, promoting domestically and locally grown foods consumption, new support measures, etc. Special attention is being put on developing disaster-resistant communities able to withstand intense and frequently occurring disasters by promoting disaster prevention measures, disaster mitigation, and building national land resilience as well as several initiatives towards securing a stable food supply including formulation of guidelines on business continuity for the entire food supply chain (MAFF, 2021). Ongoing Coronavirus crises have also had some negative impact on international cooperation on FNA with overseas partners due to the impossibility for onsite visits and investigations, and face-to-face meetings.

A "new" challenge for the government agencies, communities, educational, business and professional organisations, etc. is to make sure that lessons learned are not forgotten and

to effectively inform and prepare individuals, farmers, agro-businesses, communities, and government bodies for multiple risk management.

4 Lessons from Japanese experiences

Major lessons from FNA readiness, impacts, and recovery in the agri-food sector are following:

- The triple March 2011 disaster was a rare but high-impact event, which came as a "surprise" even for a country with frequent natural disasters and a well-developed disaster risk management system like Japan. It is necessary to "prepare for unexpected", and design, build and test a multi-hazard disaster risk management for specific conditions of each country, region, sector, etc. Appropriate measures and sufficient resources (funding, personnel, stockpiles, shelter cites, transportation means, etc.) have to be planned for effective prevention, early warning, mitigation, response, and post-disaster relief and recovery from big disasters and accidents. Besides state resources, it is important to mobilize huge private, community, NGOs, and international capabilities, expertise, and means since the large-scale public-private partnership are necessary to identify and designate public and private resources in case of big destruction, evacuation, etc.

- Risk assessment is to include diverse (health, dislocation, economic, behavioral, ecological, etc.) hazards and complementary (food, supply, natural, biological, etc.) chains, spin-offs, and multilateral effects of a likely (natural, manmade, multiple) disaster(s). Modern methods and technologies are to be widely employed (mass and social networks, computer simulation, satellite imaging, etc.) for effective communication, preparation of disaster maps, assessment of likely impacts, planning evacuation routes, relief needs, and recovery measures, secure debris, and waste management, etc. It is crucial to involve multidisciplinary and multi-stakeholders teams as well as wide participation of all stakeholders in all stages of risk management to guarantee a holistic approach, "full" information and transparency, adequate risk assessment, preferences and capabilities, and maximum efficiency and full implementation.

- Risk management system is to be discussed with all relevant organisations and stakeholders, and measures taken to educate and train individuals, organizations, and communities for complex disasters and all contingencies. Individual responsibilities are to be well-specified and effective mechanisms for coordination of actions of authorities, organizations, and groups at different levels put in place and tested to ensure efficiency (speed, lack of duplication, gaps) during an emergency. Individual and small-scale operators dominate in the agri-food sector of most countries, and their proper information, training, and involvement is critical. The latter is to embrace diverse agri-food and rural organizations, consumers, and population of each age group and gender, which all have no disaster management "culture", knowledge, training, and plans (particularly for large and multiple disasters). It is very important to develop risk information and management systems for entering supply chains and appropriately train and fund all related agents.

- It is necessary to modernize (specific, overall) formal institutional environment (property rights, regulations, safety standards, norms, etc.) according to the needs of contemporary disaster risk management. Particular attention is to be put on updating agri-food safety, labour, health, biodiversity, and animal welfare standards, and ensure adequate mechanisms, qualified agents, and technical instruments for effective implementation. The agri-food inspection system is to be improved by creating uniform inspection manuals and standards, enhancing coordination and avoiding duplication, establishing inspection across prefectural borders, and a management system extending random sampling tests of marketed produce with management at the production "planning" stage.

- It is important to set up mechanisms to improve the efficiency of public resource allocation, avoid mismanagement and misuse of resources, reduce individual agents' costs for complying with regulations, and using public relief, support, and dispute resolution

(court) system. That would let efficient allocation of limited social resources according to agents' needs and preferences, intensify and speed up transactions, improve enforcement (rights, laws, standards) and conflict resolution, decrease corruption, and accelerate recovery and reconstruction. It is obligatory to involve all stakeholders in decision-making and control, increase transparency at all levels and stages of disaster planning, management, and reconstruction. In case of evacuation, it is essential to secure proper (police, voluntary group) protection of private and public properties from thefts and wild animal invasion in disaster zones. Special attention is to be given to enhance and increase communities and food chain agents' capability for effective risk management since they (rather than authority or independent organisations) have "full" knowledge and strong incentives to deal effectively with risky events.

- Different agents and elements of the agri-food chain are affected unlikely from a disaster and have dissimilar recovery and adaptation capability. Most farming assets (multiannual crops, irrigation facilities, buildings, brands, biodiversity, landscape) are interlinked with land, and if the land is damaged a rapid recovery (rebuilding, relocation, alternative supply, etc.) is very costly or impossible. Smaller-scale and highly specialized enterprises, small-member communities and organizations, visitors, and tourists are more vulnerable and less able to protect, bear consequences, and recover. All that requires differential public support (intervention, compensation, funding, assistance) to various types of agents to provide emergency relief, accelerate recovery and diminish negative consequences.

- There is a strong "regional" specificity (interdependency) of agrarian, food, and rural assets. If a part of assets/products is damaged or affected (destruction of critical transportation, communication, distribution, electricity, and water supply infrastructure; nuclear, chemical, pathogen, etc. contamination) all agents in respective region are affected (including undamaged lands, livestock, produce, services, households' entire livelihood). To minimize damages, it is important to properly identify (locate) risk and take prevention measures, recover rapidly critical infrastructure, strictly enforce quality (safety, authenticity, origin, etc.) of products, and adequately communicate them to producers, processors, distributors, consumers, and the international community.

- Establishing accessible cooperative, quasi-public or public agricultural (crop, livestock, machinery, building, life, health, etc.) insurance system, including assurance against big natural, nuclear, multiple, etc. disasters, is very important for rapid recovery of affected agents, (sub)sectors and regions. Modernization of outdated (often informal) lands, material, biological, and intellectual property registration, and valorisation system is important for effective post-disaster compensation, recovery, and reconstruction. That is particularly true for numerous subsistent and "semi-market" holdings dominating the agro-food sector worldwide usually suffering significantly from disasters (losing all possessions) but get no market valuation, insurance, and/or public support.

- Specific responses to 2011 disasters highlighted comparative advantages of traditional communities and non-governmental organizations, and less "efficient" but more resilient structures (small-operators, partnerships) and subsectors (like one-season crops, poultry, pig, processing, etc.). The important role of small-scale farm and food organizations, informal networks, and leadership has been proven immediately after FNA till now in rapid agri-food supply, securing food safety and transparency, effective (self)recovery, reconstruction, technological and organizational innovations, networking, and decentralized actions. These governing modes have to be included in the disaster management system, relevant actors properly trained and appropriate responsibilities assigned.

- Good management of information and communication is extremely important in emergency, recovery, and post-disaster reconstruction. FNA proves that any delay, partial release, or controversies of official information hamper effective (re)actions of agents, and adversely affected public trust and behavior (e.g. buying from disaster regions). Before, during, and after a disaster(s) all available (risk, monitoring, measured, projected, etc.) information from all reliable sources is to be immediately publicized in understandable by

everyone form through all possible means (official and community channels, mobile phones, social media, etc.). It is essential to publish alternative (independent, private, scientific, international) information, including in foreign languages, which builds public trust and increases confidence. In Japan, it has been difficult to find all available information related to FNA in a timely and systematized way (updates, diverse aspects, unified measurement, time series, alternative sources), and in most spoken foreign languages, making many foreigners and local sceptical about accuracy.

- Big disaster provides extraordinary opportunity to discuss, introduce and implement fundamental changes in (agricultural, economic, regional, energy, disaster management, etc.) policies, improve disaster management and food security, modernize regulation and standards, relocate farms and houses, consolidate lands and operations, upgrade infrastructure, restructure production and farming organizations, introduce technological and business innovation, improve the natural environment, etc. All opportunities are to be effectively used by central and local authorities through policies, programs, measures, and adequate support given for innovative private and collective initiatives. Special precaution is to be used that public programs, projects, and interventions not to lead to backword "development" like in partitioning of farmlands in most affected by GEJA areas.

- Importance of international cooperation in all areas is proven in FNA responses and recovery through sharing information, knowledge, expertise, know-how, specialized equipment, etc. It is particularly crucial to share internationally advance Japanese experience through media, visits, studies, conferences, etc., and turn Fukushima into a disaster risk management hub for other regions and countries. Positive Japanese experiences are to be adapted (instead of copying) to specific institutional, cultural, natural environment and risks structure of each community, subsector, region, and country.

- It is essential to learn from past experiences and make sure that "lessons learned" are not forgotten. Impacts and factors of disaster, disaster management, and post-disaster reconstruction are to be continuously studied, knowledge communicated to the public, and "transferred" to the next generation. It is critical to prepare for multiple disasters and share "good" and "bad" experiences with disaster prevention, management, and recovery with other regions and countries, to prevent that from happening again in the future.

5 Conclusions

Ten years after FNA there are still several social, economic, health, food safety, technological, environmental, etc. challenges during reconstruction and revitalisation in the region and elsewhere. Agriculture, the food industry, and food consumption are among the worst hit by disaster areas. The Agri-food sector of Fukushima prefecture has been severely affected and there are significant adverse consequences to other regions and food chains nationwide. Many of these negative effects can hardly be expressed in quantitative terms.

Post-disaster recovery and reconstruction give opportunities to learn from and induced considerable policies and institutional modernization in agri-food and other (energy, security, etc.) sectors, improve disaster prevention and management, food safety information and inspection, technological and product innovation, jobs creation, and investment, farmlands consolidation and enhancement, infrastructural amelioration, organizational restructuring, etc.

This study is just a part of an ongoing attempt to assess disaster management readiness, FNA impacts, and summarize lessons for agri-food chains and beyond. Research is incomplete due to a "short" period after disaster, insufficient and controversial data, difficulties to adequately assess long-term implications, cross over with other recent and current disasters and crises. More in-depth multi and interdisciplinary studies are necessary to fully evaluate agri-food impacts and improve disaster risk management.

References

1. Bachev, H. (2014) Socio-economic and environmental impacts of March 2011 earthquake, tsunami and Fukushima nuclear accident in Japan, *Journal of Environmental Management and Tourism*, 5, 127-222.
2. Bachev H. (2019) *Assessment of Preparedness and Agri-Food Impacts of Fukushima Nuclear Accident: Implications for Improvement of Disaster Risk Management*, in Leif Inge Magnussen (Editor) Disaster, Diversity and Emergency Preparation, IOS Press.
3. Bachev, H. and F.Ito (2014) Implications of Fukushima Nuclear Disaster for Japanese Agri-food Chains, *International Journal of Food and Agricultural Economics,* 2, 95-120.
4. Bachev, H. and F. Ito (2018): *Agricultural Impact of Great East Japan Earthquake*, KSP.
5. Brasor P. and M.Tsubuku (2018) Tepco's compensation for 3/11 victims made matters worse, *National*, April 13, 2018.
6. FAO/IAEA (2018) *Nuclear Emergency Response for Food and Agriculture*, FAO/IAEA.
7. FPG (2021) *Station*, Fukushima Prefectural Government.
8. Hamada, N. and H.Ogino (2013) Earthquake Food safety regulations: what we learned from Fukushima nuclear accident, *Journal of Environmental Radioactivity*, 111, 83–99.
9. JFC (2014) *Findings on impact of earthquake on food industry, farm management and purchasing behavior of consumers,* Japan Finance Corporation, Tokyo.
10. Johnson, R. (2011) *Japan's 2011 Earthquake and Tsunami: Food and Agriculture Implications,* Congressional Research Service, Washington DC.
11. Kunii, N., M. Fujimura, Y. Komasa, A. Kitamura, H.Sato, T. Takatsuji, M. Jimba and S. Kimura (2018) Knowledge and Awareness for Radiocesium Food Monitoring after Fukushima Nuclear Accident, *Int. J. Environ. Res. Public Health*, 15, 2289.
12. Koyama, R. (2013) Influence and Damage by Nuclear Disaster on Fukushima's Agriculture, Commercial Studies, 4, 15-25.
13. MAFF (2021) *Annual report,* Ministry of Agriculture, Forestry, Fisheries, Tokyo.
14. MECSST (2011) *Land contamination,* Ministry of Education, Culture, Sports, Science, Technology.
15. ME (2021) *Environmental Remediation in Japan,* Ministry of Environment, Tokyo.
16. MHLW (2020): *Survey of Dietary Intake of Radionuclides*, Ministry of Health, Labor, Welfare, Tokyo.
17. Monma, T. I.Goto, T.Hayashi, H.Tachiya, K.Ohsawa (2015) *Agricultural and Forestry Reconstruction After Great East Japan Earthquake,* Springer.
18. Nakanishi T. and K.Tanoi (2013) *Agricultural Implications of Fukushima Nuclear Accident,* Springer.
19. Nakanishi, T. (2018) Agricultural aspects of radiocontamination induced by Fukushima accident, *Proc. Jpn. Acad.,* 94, 20-34.
20. NRA (2021) *Monitoring info of environmental radioactivity*, Nuclear Regulation Authority, Tokyo.
21. Oka, T. (2012) Application of cost-benefit analysis to regulation of foodstuffs contaminated with radioactive substances, *Japan J. Health Physics,* 47, 181-188.
22. Osawa, M. and K. Ujiie (2016) Changes in consumer leafy vegetable consumption behavior after the nuclear accident, *Food system research,* Vol.23, 3, 213-218.
23. Sekizawa, J. (2013) Appropriate Risk Governance on Radionuclide Contamination in Food in Japan, Issues Learned from 3.11 Disaster, Society for Risk Analysis, 31-35.
24. RA (2021) *Progress to date*, Reconstruction Agency, Tokyo.
25. Takebayashi Y., M. Murakami, S. Nomura, (2020) The trajectories of local food avoidance after FDNPD, *International Journal of Disaster Risk Reduction*, 46, 101513.
26. Todo, Y., K. Nakajima, and P. Matous (2015) How Do Supply Chain Networks Affect Resilience of Firms to Natural Disasters? *Journal of Regional Science,* 55, 209–229.
27. Ujiie, K. (2012) Consumer's evaluation on radioactive contamination of agricultural products in Japan, *Food Syst Res*, 19, 142-155.
28. Watanabe N. (2013) Current State of Losses from Nuclear Accident and Support Measures by JA, Norinchikin Research Institute, Tokyo.
29. WHO (2013) *Health risk assessment from nuclear accident after Great East Japan Earthquake*, World Health Organization, Genève.

Knowledge management for nuclear energy research and policy – JRC activities in foresight

Zdenko Šimić, Kaisa Simola, Jorge Tanarro Colodrón and Ariane Liessens

European Commission Joint Research Centre, The Netherlands

zdenko.simic@ec.europa.eu, kaisa.simola@ec.europa.eu,
jorge.tanarro-colodron@ec.europa.eu, ariane.liessens@ec.europa.eu

Abstract

During the last five years, the European Commission Joint Research Centre (EC JRC) has made a significant effort to develop its knowledge management, with focus on improving policy support. Initiatives such as the development of knowledge and competence centres in different areas of expertise, the deployment of collaborative tools and platforms and the implementation of a comprehensive restructuration that explicitly addressed knowledge management and its related responsibilities are a few of the efforts carried out in that sense. As a new challenge, foresight was considered one of the most relevant competences to be acquired by the new knowledge management practitioners. One initiative to answer this need was the adaptation of the Horizon Scanning process, which was first piloted in various scientific domains, and later established as a continuous activity. This paper presents the insights of the Horizon Scanning exercises carried out in the field of nuclear safety, security and safeguards at the EC JRC.

1 Introduction

The Joint Research Centre (JRC) is the scientific branch of the European Commission (EC) with the role of providing science for policy support. This support is related to benchmarking existing policies and supporting new policy development including anticipatory assessments. The JRC Strategy 2030[1] specifically stresses the need for the JRC to develop anticipation by stating the following in its chapter 8 ("*A stronger anticipation culture*"):

"There are many reasons why the Commission's anticipatory capacity needs to be strengthened. First, it would enable it to identify its knowledge needs very early on. This would give it time to amass the evidence it needs to launch well prepared policies and proposals in a timely fashion. It would be able to future-proof its impact assessments and its REFIT evaluations. Anticipating social changes and public opinion movements would contribute to shaping public debates and proposing new narratives, instead of being on the defensive."

In this context, the *Horizon Scanning* has been identified as one of the necessary tools *"which strives to identify and make sense of weak and diffuse indications of still hazy emerging trends or paradigm shifts"*.

It the last five years the JRC has been addressing this anticipatory challenge and knowledge management in ways that are more explicit. It is now possible to look at this work to capture some lessons learned about KM for foresight and consider its potential and limitations. This paper presents the experience gained from the Horizon Scanning activities carried out in the nuclear field at the JRC, including some complementary

[1] https://ec.europa.eu/jrc/sites/jrcsh/files/jrc-strategy-2030_en.pdf

activities, and suggests new initiatives to improve the knowledge management for policy support.

The following chapter presents in more detail the Horizon Scanning approach and briefly some supporting activities. Examples of the results are presented in the third chapter. The last chapter presents the conclusions.

2 Knowledge management activities

Horizon Scanning (HS) is one of the largest knowledge management (KM) activities consisting in the systematic outlook to detect early signs of potentially important developments. These signs can be weak (or early) signals, trends, wild cards or other developments, persistent problems, risks and threats, including matters at the margins of current thinking that challenge past assumptions. It seeks to determine what is constant, what may change, and what is constantly changing in the time horizon under analysis. [1]

In addition to Horizon Scanning there are other supporting, complementary and separate KM activities. They include tools for innovation monitoring, deep dives, policy briefs, status reports and a foresight network. This paper focuses on the Horizon Scanning and just briefly describes the other activities for completeness. The following subchapter presents the Horizon Scanning process followed at the JRC in the nuclear directorate. A subchapter follows with a brief description of the other activities.

2.1 Horizon scanning approach

The Horizon Scanning for Nuclear Safety, Security & Safeguards exercise is an initiative that attempts to provide anticipatory support by:

- Embedding a culture of anticipation throughout the JRC nuclear directorate.
- Developing expertise in the detection and analysis of early signs to identify important emerging issues.

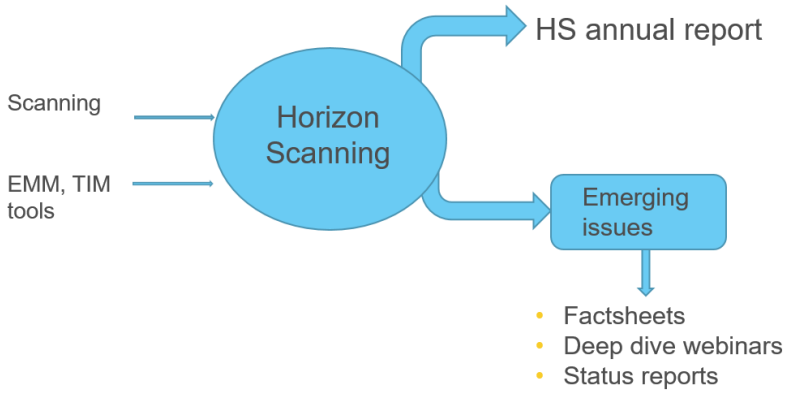
Distinct groups of experts lead the different actions carried out through the process:

- *Scanners* from across the JRC nuclear directorate carry out the continuous scanning of nuclear technology sources, picking up single ideas that are recorded in a content management platform. They also participate in the pre-filtering sessions and the sense-making workshops where they review the scanned ideas, select sets of relevant items and develop foresight stories.
- *Aggregators* lead the pre-filtering sessions and yearly sense-making workshops, collecting the relevant scanned ideas and organising the discussions for the scanners, taking the time to discuss and share views and intuitions.
- *Data analysts* carry out the yearly bibliographic data analysis performing a quantitative study of the scientific literature addressing the research topics underlying the clusters of ideas identified during the workshops.

The foresight stories aim to capture the possible impact in ten years and more of the weak signals considered most interesting today. They are the main outcome of the yearly sense-making workshop, a creative process in which the group reflects jointly about the further-reaching consequences of on-going and emerging trends.

In 2020, all Horizon Scanning activities were held online due to the restrictions on physical meetings related to the COVID-19 pandemic. The pre-filtering sessions were held in a virtual meeting room. For the sense-making workshops, the virtual meeting room was complemented with the use of breakout rooms for parallel discussions in smaller groups. In addition, special software allowing to work with all participants together on a virtual whiteboard was used.

Figure 1. High-level Horizon Scanning workflow with connection to complementary activities.



Below we describe in more detail the four stages of the *Horizon Scanning for Nuclear Safety, Security & Safeguards* as implemented at the JRC, namely: Scanning; Pre-filtering; Sense-making workshop; Reporting.

Scanning

Within the scanning phase, the scanners capture information coming from a large variety of sources. These *ideas* are often "raw" information (not necessarily analysed by someone else), reports on single developments, fact-based and objective, concise, new developments from many unrelated domains. Just "opinions" or "advice" are not considered relevant for the exercise. Looking for what "*can happen"* or "*will happen"* instead of what "*should happen"* or "*must happen"*.

The sources are materials or media providing well identified "raw" latest information. They may include journals providing concise news reports (e.g., Nature), scientific publications, reports, professional journals, conference proceedings, trade and business publications, magazines and newspaper, social media, blogs etc. The sources may also include already existing specialised scanning systems. For example, the Europe Media Monitor or shortly "EMM" is being used for systematic and automatic retrieval of relevant news about innovative or disruptive developments on nuclear technology.

The items found during the scanning process are stored in a content management system. Once stored, the items become "ideas". The ideas are encoded according to the following principles:

- The new idea describing the item must have an informative title, a summary (up to ½ page), a brief explanation about its importance, the date of publication and the link to the source or attachment.
- The idea can be classified under one or more categories available in the edition screen, ticking at least the "nuclear" category. Other categories are economic, environmental, health, political, social, technological, food, security. In addition, it is possible to add new categories as tags.

The content management system allows also voting (up or down) and commenting each idea. Before every session or workshop, which takes place 3-4 times a year, the aggregators select, prepare and format the captured ideas providing the list to all participants in advance.

Pre-filtering session

The purpose of pre-filtering is to preselect and prepare ideas for the sense-making session. These sessions allow to involve the scanners in the selection of ideas and to take the time to discuss and share views and intuitions.

When enough ideas related to nuclear are collected (usually 80-100) a pre-filtering session is planned, to which all scanners are invited. The aggregator responsible for

managing the session extracts the ideas collected and formats them for the review of the scanners. The ideas are sent to the participating scanners about a week in advance of the pre-filtering session. Before the session, the participants must go through the list of ideas and select the ideas they consider of most relevance (usually 5-10). The participants also elaborate why they think the chosen ideas are important.

During the session, the participants put forward their selected ideas explaining why they are important. This key aspect of the selection is the basis for discussions. The aggregators write down the selected ideas and harvest the essence of the discussions.

The outcomes of each pre-filtering session are recorded in a document, which is complemented and completed with the following pre-filtering sessions.

Sense-making workshop

The preparation for the workshop requires from the participants to go through the list of shortlisted ideas prepared in the previous pre-filtering sessions and to think about how they would fit together to suggest an emerging trend or phenomena and to gather those fitting together into clusters. They should write down the names and numbers of the ideas clustered and give the cluster a title to be presented during the workshop session. The sense-making workshop is not a classification exercise, so there is no need to assign all ideas in clusters. The aim of the workshop session is neither to criticise the abstracts nor to cover everything but rather to collect concepts which indicate new trends and emerging issues. Each participant is expected to present about three clusters.

Table 1. The structure of the sense-making workshop.

Stage	**Description**
1. *Clustering of ideas*	Participants write down individually their own clusters (title, premise, and the numbers of the related ideas) on yellow post-its.
2. *Presentation of clusters*	Participants take turns to present their clusters and put them on a wall or board (real or virtual).
3. Grouping the clusters	The participants discuss the clusters to validate their different titles and group the ones strongly related into wider or more appropriate narratives recorded (title and numbers) on pink post-its.
4. Grouping the participants	The participants separate the groups of clusters on the wall into 3 to 4 sections. The participants choose the section to further work on, and the organisers cover less popular topics. Each group shall develop 1 or 2 foresight stories related to the clusters available in their section.
5. Development of foresight stories	A representative of each small group presents and explains the group's foresight stories in the plenary meeting. Participants can ask questions and make comments to ensure the story is well understood. After reformulating if needed, each final story is put to the wall in a pink post-it, aiming to capture a total of 3 to 5 stories.
6. Characterisation on horizon line	The stories are characterised using a 3 horizons model* that is often adopted in the Horizon Scanning to define time frames for thinking about emerging issues (e.g., Garnett at al. 2016[2]).
7. Link with the JRC programme	For each of the stories, participants examine where the emerging issue fits in the JRC programme. For this part, one of the scanners was asked in advance to prepare an overview of the JRC programme.
8. Final capture	The results of the session are recorded and documented.

* In this model 'Horizon 1' is the present and the near future (1-5 years), 'Horizon 2' is the less immediate future (5-10 years) and 'Horizon 3' is the mid to long term future (10+ years).

[2] Garnett, K., Lickorish, F.A., Rocks, S.A., Prpich, G., Rathe, A.A. and 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: 82-91.

A cluster is a group of two or more ideas that can be linked in some way as a potential evidence for an emerging issue. Emerging issues may be latest trends, weak signals, drivers/enablers of change, or discontinuities. They may also include outlier behaviour, unconventional wisdom or innovative technologies that could indicate future changes with potential significant impact on society and policy. Usually, the emerging issues are developments at an early stage that had not been seriously considered yet. The participants usually tend to find clusters that confirm their previous ideas or feel that cluster is "unthinkable". This is acceptable because the participants should not hold back: the workshop is meant to be a safe space to allow for and open and creative exercise to unfold.

Table 1 lists eight stages of the sense-making workshop. Teamwork and collaboration among the participants are especially relevant for refining and merging the clusters into stories (Stage 3), for the development of foresight stories (Stage 4) and for mapping the stories (Stage 6).

Reporting

The nature of the exercise entails that identified clusters and related stories are neither predictions nor research conclusions; they are only indications or intuitive guesses made using a creative process of connecting the potential consequences of different recent developments. The final yearly report focuses on the main foresight stories developed out of the distinct clusters of ideas mapped during the workshop, identifying the related possible risks and opportunities. It also includes the bibliographic data analysis, carried out with TIM, of the scientific literature addressing the research topics underlying those clusters of ideas. This parallel exercise aims to complement the intuitive and qualitative outcomes of the workshop with a systematic and quantitative analysis.

2.2 Complementary KM activities and tools

This Horizon Scanning activity is supported, complemented, expanded and connected with other knowledge management activities and tools. Here we briefly present some of them: Tools for innovative monitoring (TIM); status reports and policy briefs; deep dives; and the foresight network. There are other complementary activities related to KM, like participation in cross-cutting multidisciplinary activities (e.g., various project groups and seminars), which are not described here for brevity. Only the activity most significantly related to Horizon Scanning (i.e., TIM) is described in a separate subsection.

Status reports and policy briefs are prepared for selected topics (from HS or elsewhere) to address them from the perspective of European Commission and European Union. One recent example is the report on the development, advantages and challenges related to micro nuclear reactors.

Deep dives are organized for selected topics identified in the HS or elsewhere. They involve one or two invited experts (usually from outside the JRC), dedicated panellists and a broad audience, mainly from the JRC. This activity includes an introductory presentation from experts and a Q&A including panellists and audience. Recording of both the complete webinar and a summary are made available on the intranet.

The JRC foresight network and the megatrends are part of the wider JRC effort, not limited to nuclear, to enhance scientific policy support.

2.2.1 Tools for Innovation Monitoring (TIM)

In parallel to the Horizon Scanning exercise, a bibliographic data analysis is performed with the aim to complement the Horizon Scanning conclusions with additional valuable insights about technologic developments such as:

- The relations amongst technologies, visualising how often they appear together in the literature.

- The maturity of the related research by observing the amount of scientific literature available on the technology as well as its evolution through time.
- Their *"activeness"* considering the number of publications on the technology released over the last three years in relation to the total number of scientific publications for the technology.
- The countries with more scientific activity on the selected topic.

The JRC Tools for Innovation Monitoring (TIM) is a text mining and visualisation tool, which searches in scientific publications, patent data and data from R&D projects funded by the EU. TIM explores the characteristics and relations between the 'final clusters' identified after analysing the results of the query from related scientific literature, patents and R&D projects funded by the EU.

TIM produces visualisations of the data with edges and nodes (graphs). In this case, a graph is created with all the datasets defined. These datasets are created using a search query that should contain the intended keywords connected by Boolean operators for each of the technologies corresponding to the identified cluster.

Datasets referring to the different technologies can be compared, and their relations identified by analysing the resulting graph. This means that to study one specific technology in TIM, it is necessary to create first its related dataset, one for every technology. This series of datasets can be then visualised as a graph defining what in TIM receives the name of a '*datasetgram*'.

In this type of visualisation, each node represents a dataset related to a particular technology. The colours identify the groups of nodes that tend to have more documents in common among each other. These groups are detected using the so-called Louvain Modularity algorithm described by Blondel et al in https://arxiv.org/abs/0803.0476

Each dataset is studied separately using the insights acquired from TIM to identify promising technologies that are non-obvious or just recently identified but with the potential to gain significant weight in the future. Promising innovative technologies can be found in small nodes linked at least with several other nodes. They must have an 'activeness' TIM indicator of above the average.

TIM experts and developers are available to help with the review of the proposed query strings for the datasets, to advise on the use of the tool as well as to help with the interpretation of the results used in preparation of the conclusions for the report.

3 Examples of results

This section presents examples of results from the Horizon Scanning and the supporting TIM activities. These examples are given here only as illustration without the intention to discuss their context, use and further evolution.

3.1 Example of Horizon scanning results

The scanning of relevant news items, then the filtering of these items followed by a sense-making workshop resulted in the following three foresight stories:

The European leadership on radioisotope production

Radioisotopes are materials with specific radioactive properties that can be manufactured to meet specific needs.

The most important use of radioisotopes is in medical applications like for example treating cancerous diseases. Other uses are in sensors to detect explosives in airports and leakages in pipes, or to measure the thickness of various materials.

Radioisotopes are produced in research reactors and in particle accelerators. Thanks to the considerable proportion of research reactors operating within Europe, the EU can be

considered a leader of radioisotope production at a global level. On the other hand, many of the present research reactors will soon reach the end of their operating life, what might bring that leadership into question.

Future of nuclear energy in the EU

With the challenging targets of decarbonisation within the European Green Deal, the transition from fossil fuels to cleaner energy production has become even more topical. The possibilities of nuclear to contribute to the decarbonisation are various: continued operation of existing nuclear power plants can respond to an increasing electricity demand and can supply energy for hydrogen production. Small modular nuclear reactors are identified as potential systems in support to the variability of the electrical power generated by intermittent Renewable Energy Sources (RES) like solar panels and/or wind turbines.

Although nuclear could play a significant role in reaching the European Commission's ambitious decarbonisation targets, the opinions on the use of nuclear energy are highly polarised. This has caused a detrimental political context for the nuclear industry at the EU level. Meanwhile the European nuclear industry is losing market to Russia and China, who have become dominant players in the nuclear power market.

Participatory engagement for nuclear

The European nuclear power industry, although not anymore a world leader, is a well-equipped competitor at the global stage. At the same time, European public institutions at various levels of administration are often considered amongst the most transparent, participatory, trusted, and effective in the world. Although one would expect this to give stability to the sector this link has become sensitive to disruptions brought by digital connectivity. The combination of the political struggle for higher public engagement in policymaking on one side, and the intensified dynamics of public perception driving business success on the other side, is to shape the future of European nuclear power. Starting by bringing the power supply closer to the consumer, it may end up evolving into a more open, future-looking and engaging sector to remain afloat.

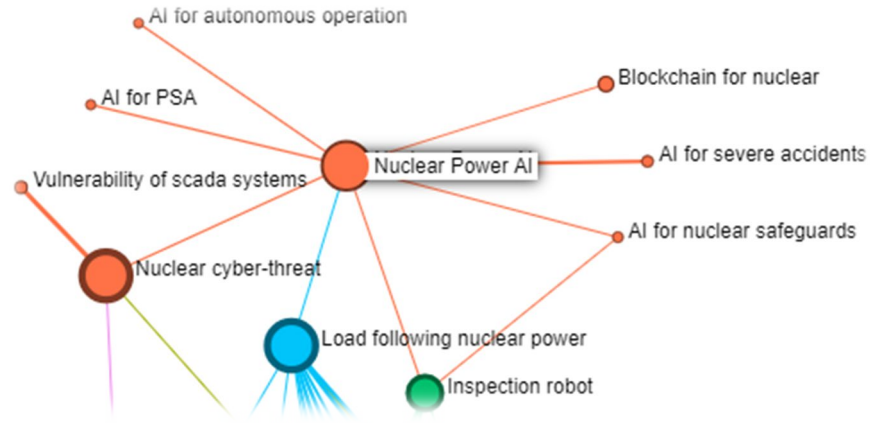
3.2 TIM example

TIM results are illustrated in relation to the artificial intelligence (AI) for nuclear applications. In the nuclear sector, AI can be used in different areas (e.g., safeguards and surveillance). Figure 2 shows all identified AI applications in the nuclear sector. AI applications for severe accidents and safeguards are identified as emerging trends.

Figure 3 shows the trend for the AI dataset document type including journal articles, conference proceedings and patents. It should be noted that the apparent decline for the last year is probably due to partial input (i.e., the analysis was performed before the end of last year).

Figure 4 shows TIM network graph on the worldwide distribution of "nuclear power AI", with a separate graph for the EU.

Figure 2. TIM datasetgram centred on "nuclear power AI".



Node label: indicative title of the subject of the related search query.

Node size: number of documents retrieved by the search query.

Node colour: Similarity according to the Louvain Modularity algorithm.

Edge thickness: number of documents retrieved simultaneously by two different search queries.

Figure 3. 'Nuclear Power AI' dataset document type distribution.

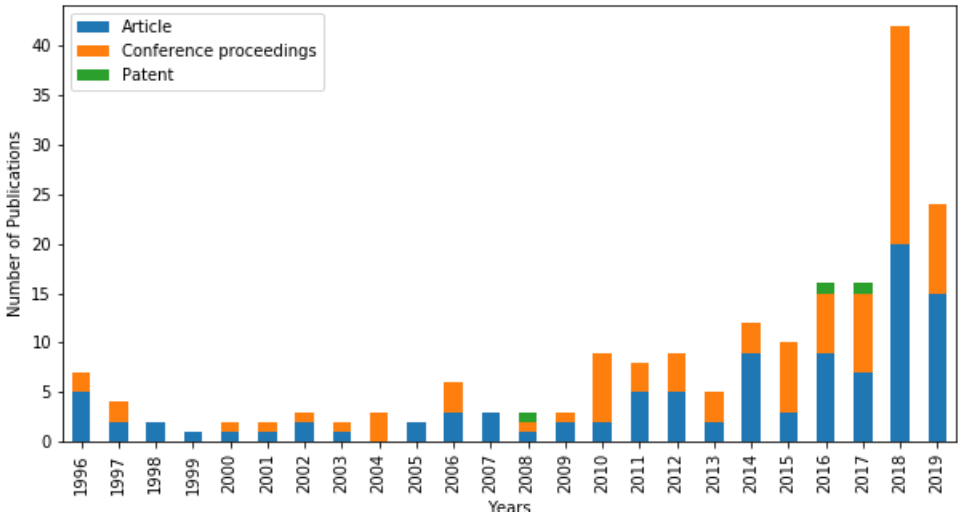
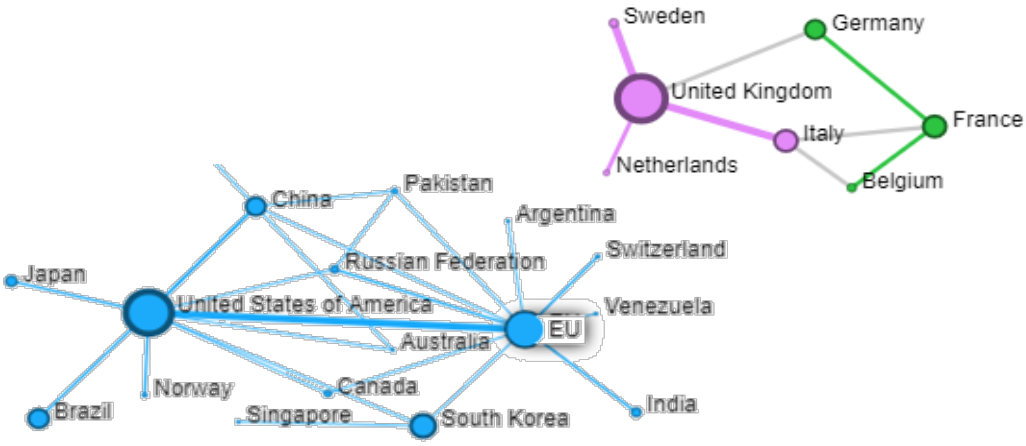


Figure 4. TIM network graph on 'Nuclear Power AI' world (blue) and EU (green and pink) publications distribution (see Figure 2 for legend).



4 Conclusions

Horizon scanning (HS) exercises focusing on nuclear technology have been carried out at the JRC involving experts with diverse backgrounds. To capture cross-cutting issues, experts from energy, health and risk management fields have also been involved in the exercises. Specific topics related to nuclear energy like micro reactors and climate change were identified during the exercise and dedicated reports were prepared considering and presenting the related risks and opportunities. Several competences were acquired during the first five years of the implementation of the Horizon Scanning process. The in-house knowledge about the identified emerging topics was enhanced. Soft skills related to the guidance of the processes followed during the exercise were developed, including participatory leadership, harvesting methodologies, working with stories and team building. Proficiency was achieved in the use of the data mining tools developed by the EC JRC to collect ideas from the Internet, with the Europe Media Monitor (EMM), and to visualise research trends, with the Tools for Innovation Monitoring (TIM).

The entire process keeps evolving based on the experience acquired and the people involved. It seems important to recognise that KM activities like Horizon Scanning have both explicit (already mentioned before) and implicit benefits. Implicit benefits are related to improving organisational communication and recognising, in different setting, existing expertise and potential important gaps.

Finally, it was important to optimise the resources required for new KM activities like Horizon Scanning to avoid impacting other activities. Very few people are engaged in the coordination and management of the activities and always in combination with other duties. This could be achieved by a continuous improvement of the process and by maximising the use of collaboration and automation tools.

Acknowledgements

We are grateful to all those colleagues from the JRC who contributed to the nuclear Horizon Scanning activities with their ideas, suggestions, comments and other contributions and for their engagement in discussions during the various meetings and workshops.

References

1. Models of Horizon Scanning – How to integrate Horizon Scanning into European Research and Innovation Policies. European Commission 2015.
2. EU, Joint Research Centre, TIM Analytics, www.timanalytics.eu/
3. J.T. Colodron, Z. Simic, K. Simola, Micro Nuclear Reactors Status Report, JRC Science for Policy Report, JRC 118970, 2019
4. Strategic foresight, ec.europa.eu/info/strategy/strategic-planning/strategic-foresight_en
5. Foresight On Newsletter, 2020 collection and February 2021 issue, ec.europa.eu/info/publications/foresight-newsletter_en
6. The Megatrends Hub, knowledge4policy.ec.europa.eu/foresight/tool/megatrends-hub_en

A method to manage critical knowledge and associated risks

Eelco Kruizinga, DNV, eelco.kruizinga@dnv.com

Jeroen Alberts and Rob van der Spek, DNV, Jeroen.alberts@dnv.com , rob.van.der.spek@dnv.com

Abstract

Combining risk management and knowledge management practices, DNV has, over the past 3 decades, developed a toolbox for managing knowledge risk, and has recently been integrated into the DNV's safety and sustainability rating framework ISRS. This paper offers an insight in the toolbox and presents a method to a) identify knowledge that is critical to operation – i.e., knowledge that is essential to delivery, yet hard to replace once lost, b) create a risk picture of that knowledge and c) create an action plan to mitigate the risk. The method has been applied in a variety of (high risk) sectors, including the nuclear and gas industry.

After introducing the direct consequences and second-order impacts of critical knowledge loss (e.g., non-availability of knowledge at the point of action, leading to productivity losses), the paper provides an overview of several types of tools to manage knowledge risk and then continues to detail the steps of the method and provides a worked example for each of the steps.

The method maps the knowledge required to perform key activities in (a part of) an organisation by seeking inter-stakeholder consensus using interactive discussion methods, supported by electronic tools. After agreeing the critical knowledge areas, the risk profile of each knowledge area is developed, by scoring on the dimensions of level of proficiency (i.e., the quality of the knowledge), codification and diffusion. Tailoring options to additional or alternative dimensions are discussed. Scores are obtained for both the current state as well as the required state of each of the three dimensions.

Using a risk calculation model, a risk heat map for the knowledge areas is generated, revealing priority gaps for knowledge risk management in the organisation. As a novelty, an interactive dashboard can now be used to interrogate the risk data and to track progress: the paper presents an example of such dashboard.

An action plan is then agreed, with actions chosen such that they ensure closure of the prioritised gaps. Actions are drawn from a knowledge management toolbox that categorises interventions based on their effect on proficiency enhancement, codification improvements and diffusion effectiveness.

Monitoring of the action plan and associated risk register is then discussed. The paper concludes with recommendations for those who seek to introduce rigorous management of knowledge risk.

1 Introduction

The knowledge held by organisations is a key asset in ensuring safe and sustainable operation. Knowledge may be critical, i.e., once lost, it is hard to replace and impact on performance is observed as a result, either directly or after passing of time. Such critical knowledge may be at risk of degradation or loss, through factors such as staff changes, insufficient learning or poor documentation processes.

For this article, we define knowledge as:

> Justified true belief that allows us to interpret the world around us, to predict the future, assess the potential consequences thereof and determine what action to take.

Also, in this article, we focus on knowledge in organisations particularly related to safety, rather than the broader knowledge to deliver the business.

Safety knowledge is important because it:

- Enables resilience by allowing the business to respond effectively to short term events (ability to deal with the unexpected) and long-term changes;
- Provides the basis for understanding of threats: "What could possibly go wrong?";
- Guides the design of assets and processes aiming at eliminating or reducing the risk;
- Steers the development and implementation of physical and organisational barriers to protect against residual risks and
- Provides staff and leaders with the competence to act safe and inspires other to do alike.

The effects of not taking sufficient care of safety knowledge may include the following:

- Mistakes are duplicated because earlier ones were not recorded or analysed;
- Risk remain high because people are not aware of activities in the past or their outcomes;
- Incidents occur because knowledge is not available at the point of action;
- Good ideas and best practices are not shared, raising risk exposure;
- Only 1 or 2 key employees hold critical knowledge creating continuity risks;
- The organisation learns too slowly which results in a degrading safety management system or inadequate controls;
- Employees are frustrated because the right knowledge resources are not available, or their insights are not leveraged.

Knowledge management provides the instruments to address the unintended consequences of insufficient care for safety knowledge in an organisation.

The next section provides a framework for understanding knowledge management and proposes techniques to identify knowledge risk.

2 Knowledge management

2.1 Focus on critical knowledge

Knowledge management (KM) is a discipline that promotes an integrated approach to identifying, capturing, validating, storing, retrieving, retaining, transferring, sharing and developing an organisation's critical knowledge assets. These assets may include images, documents, policies, procedures and expertise held by individual employees.

So, knowledge management is not focussing on addressing all of an organisation's knowledge assets, but rather what is deemed critical now and what will become so in the future.

Critical knowledge is subject to several degradation mechanisms that are the target for a system for managing knowledge. These mechanisms include:

- Staff turnover, including retirement;
- Poor IT;
- Lack of learning and innovation;
- Changes in the labour market resulting in scarcity of expertise for example;
- Insufficient analysis and documentation of experience, hindering re-use of knowledge and triggering repetition of earlier mistakes.

To understand and address the risk associated with suboptimal management of critical knowledge, DNV has developed a method that is consistent with current risk management practices yet is focussed on the particular nature of knowledge itself.

2.2 Knowledge risk

Managing knowledge risk is a key objective for the management of safety knowledge.

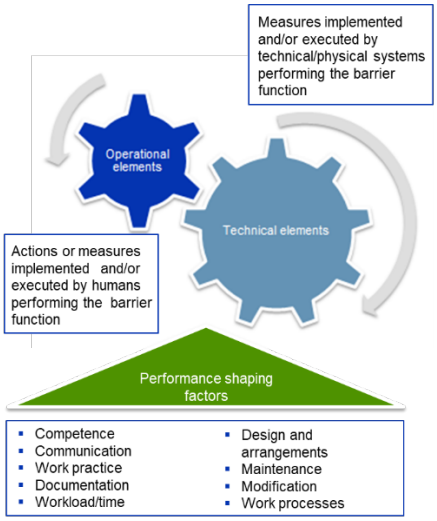
Our method provides a mechanism to:

- Identify what is critical safety knowledge, now and in the future;
- Determine the current and required health of each critical knowledge area;
- Propose interventions to close any gaps.

It should be noted that calculating the actual risk is difficult as knowledge itself indirectly impacts risk. Safety knowledge is typically required to design, implement and maintain barriers (see figure 1).

Safety knowledge that is of insufficient quality or is not documented well enough or is not spread well enough across employees (and contractors) will result in degradation of barriers and by effect increase the risks the barrier aims to reduce by its design.

Figure 1. Performance shaping factors of a barrier include a knowledge component



In our method knowledge risk is a proxy that is defined as gap between desired and actual levels of 'health' of knowledge weighted by the current and future importance of a knowledge area, where 'health' is operationalised via three dimensions of knowledge:

- Proficiency (P): the quality of the knowledge (varying from being a beginner, to being the world class expert in a knowledge area);
- Codification (C): the level to which knowledge has been captured in documentation (varying from just being in people's heads, to fully embedded in work instructions);

- Diffusion (D): the level to which knowledge is shared across a workforce (varying from just one or two people being knowledgeable, to full spread across the organisation).

Although there are other dimensions that can be analysed, such as the degree to which knowledge is 'in-house' or 'outsourced' to the supply chain, DNV has found that P, C and D levels provide a robust way for analysis and subsequent tracking of progress with respect to the closing of gaps between current and required P, C and D levels

In the sample score sheet in figure 2, each critical knowledge is scored for its current and expected future importance to the business. Thereafter, current and desired scores for P, C and D are determined. The future no intervention scores for P, C and D (the 'will be' columns) are derived from an underlying formula.

Figure 2. Sample score sheet to assess critical knowledge areas.

	I IMPORTANCE		P PROFICIENCY			C CODIFICATION			D DIFFUSION		
Knowledge Area	Current	Will be	Current	Will be	Should be	Current	Will be	Should be	Current	Will be	Should be
Transformational in the GCF context	8,9	8,11	3,7	3,6	6,67	4,5	3,2	7,78	4,2	2,3	7,56
Climate Science, Rationale, Methodologies	7,4	7,8	3,2	4,5	6,6	2,8	3,8	7,1	2,9	3,4	7,1
Institutional C[illegible] GCF	7,6	8,2	4,7	4	7,5	4,3	3,7	7,4	4,3	3,4	7,4
Thematic Area	7,4	8,1	4,2	4,8	7,5	3,1	3,6	7,6	2,8	3,3	7,7
Policy & Regul	7	8	3,9	4,1	6,9	3,3	3,1	7,1	2,8	2,7	7,1
Science Policy	6,6	7,13	2,6	3,8	6,13	1,8	2,8	5,63	1,7	2,7	5,88
Innovative Climate Finance Solutions	7,5	8,2	4,2	4,6	8,2	2,6	3,6	7,8	2,7	3,4	7,8
Brokering Knowledge	7,2	8,4	3,1	3,9	7,6	2,2	2,9	7,9	2,4	2,9	7,3

Knowledge area listing

In the case of safety knowledge, we typically encounter knowledge areas such as:

- Domain knowledge, such as drilling, chemical engineering, structural engineering;
- Contextual knowledge, such as geological knowledge, civil activities;
- Human factors, such as understanding of human behaviour;
- Safety management knowledge, related to for example Safety Management Systems, barrier management and safety culture.

From the assessment scores, a risk profile is calculated, identifying current and future risk associated with P, C and D characteristics of each critical knowledge area (see figure 3), providing input to creating a knowledge management action plan.

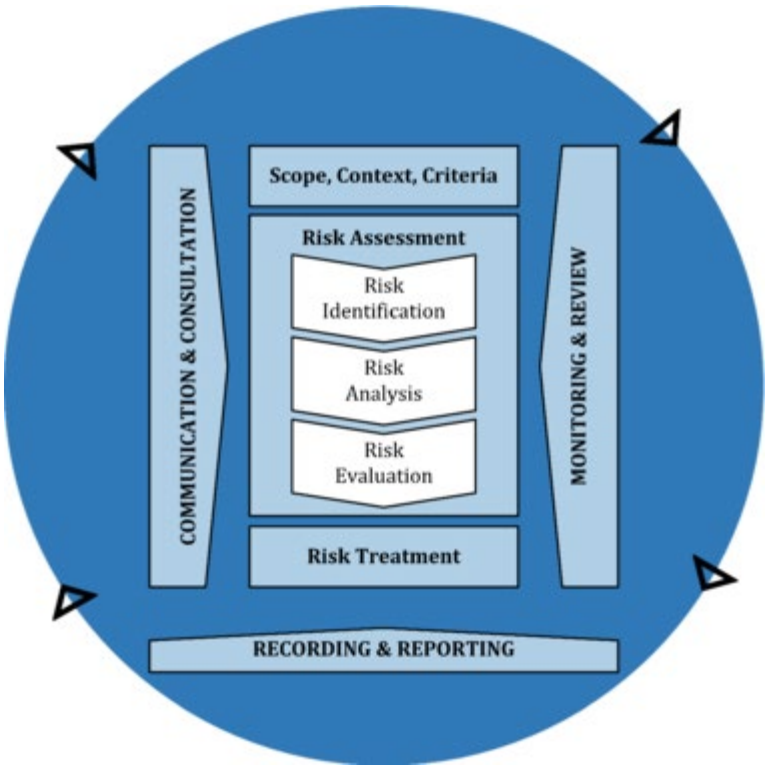
Figure 3. Knowledge risk for critical knowledge areas.

	KNOWLEDGE RISK							
Knowledge Area	Curr P-Risk	Curr C-Risk	Curr D-Risk	Current Total Risk	Fut P-Risk	Fut C-Risk	Fut D-Risk	Future Risk with current plan
Transformational in the GCF context	5	6	6	6	6	6	7	6
Climate Science, Rationale, Methodologies	5	6	6	6	5	5	5	5
Institutional Ca[illegible] GCF	5	5	5	5	6	6	6	6
Thematic Areas	5	6	6	6	5	6	6	6
Policy & Regula	5	5	6	6	5	6	6	6
Science Policy I	5	5	5	5	5	5	5	5
Innovative Climate Finance Solutions	5	6	6	6	6	6	6	6
Brokering Knowledge	6	6	6	6	6	7	6	6

Knowledge area listing

The way DNV addresses knowledge risk aligns with the risk management process as specified in ISO 31000 (see figure 4). Risk assessment, risk treatment and monitoring and review, as well as wider communication and consultation are consistent with the DNV method for knowledge risk.

Figure 4. ISO 31000 framework for risk management: Process.



In the next section, we will provide more detail on how knowledge risk analysis, risk evaluation and risk treatment are undertaken in the DNV method.

3 Identification of critical knowledge

The first step in the risk assessment is the identification of what constitutes critical knowledge. The way DNV normally facilitates this process is to bring together a cross-section of the organisation with relevant backgrounds in a workshop format. Prior to this session, the scope of the assessment is agreed. The scope may concern the entire organisation, or a specific element of it (a particular project, an asset under management, a product, or a service, for example).

In the workshop, the following questions are addressed in a brainstorming and critical reflection format:

1. What knowledge areas critical **now** for delivering success, giving the scope of the assessment?
2. What knowledge areas are critical in the **future** for delivering success, giving the scope of the assessment?

The future may be in a year from now, or further away in time, depending on the agreed scope.

We encourage participants to think of the know what, know-how and know who for each knowledge area.

Each knowledge area is then scored on its relative importance:

- 1-3 This knowledge area has little impact;
- 4-5 This knowledge area has minor impact;
- 6-7 This knowledge area has medium impact;
- 8-10 This knowledge area has high impact.

In most cases, the workshops pay further attention to the key characteristics of each knowledge area, for example the rate of change, whether the knowledge is acquired through experience or study, how many people are competent, etc.

The scoring is done either using prepared worksheets or interactively using an online voting tool such as provided through e.g. Mentimeter, an on-line platform for taking audience inputs.

4 Creating a risk profile per critical knowledge area

After establishing what constitutes critical knowledge for the scope of the assessment, each knowledge area is analysed in further detail.

Through a facilitated process, either by using, participants agree scores on P, C and D, using the following legend:

For proficiency (P):

(Score 1-3): Beginner: we are only just beginning to build up knowledge in this area. Our knowledge is useful, but certainly not comprehensive;

(Score 4-5): Apprentice: has basic knowledge and can apply it under supervision. We need coaching and mentoring to apply what we know and guidance if we want to apply new knowledge;

(Score 6-7): Professional: can perform independently. We are efficient at applying what we know and we have confidence in the quality of the knowledge;

(Score 8-10): The authority: is leading in this knowledge area. Our corporate memory is the leading repository of knowledge.

For codification (C):

(Score 1-3): Knowledge is held only in the heads of our staff. It is rarely documented in our corporate memory;

(Score 4-5): Knowledge is codified in project descriptions, stories or other forms of documentation, but limited structuring has been done. Individuals file documents without applying their own structures; it is not easily accessible in our corporate memory;

(Score 6-7): Knowledge has been codified into structured electronic documents. There is a systematic and coherent storage procedure, that allows anyone to access documents in our corporate memory;

(Score 8-10): Knowledge has been embedded in best or good practices, which give direction to actions of our employees. Our documents enable us to best exploit our available knowledge.

For diffusion (D):

(Score 1-3): Knowledge is held by some of us, but not necessarily visible to others. We don’t really know what we know; our corporate memory lacks transparency;

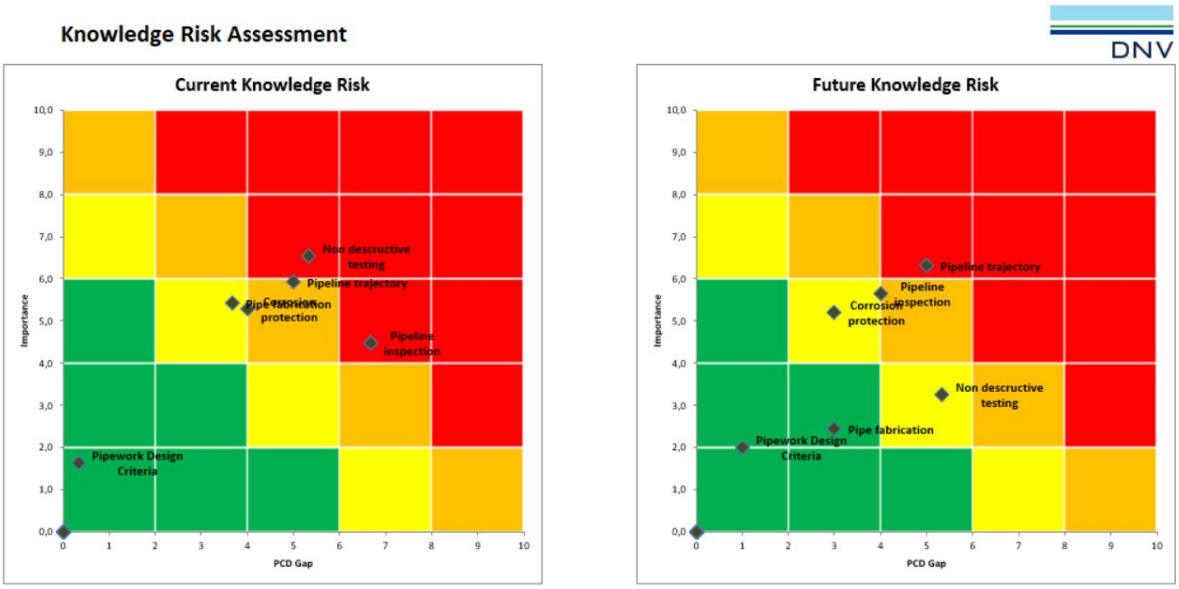
(Score 4-5): Knowledge is held by some of us, and we know where to find it. We know who to ask; our corporate memory is transparent;

(Score 6-7): Knowledge is held by some of us, and the rest of us are informed on a need-to-know basis. We know who to ask, and are aware of any new relevant developments;

(Score 8-10): We actively manage our knowledge in knowledge networks. In our key knowledge areas, we actively share in knowledge networks, so that our corporate memory is more robust against individual knowledge loss and more staff are proficient.

The scores are entered into a score sheet, that then calculates the risk profile, resulting in a matrix such as the one presented in figure 5.

Figure 5. Example knowledge risk profile. Source: DNV, 2021.



Then the priority gaps in P, C and D are discussed with the participants in the workshop to build a common understanding of which gaps result in the best improvement in the risk profile.

In most cases, a further understanding needs to be built around which measures are already in place that by themselves will close the gaps over time and what extra measures require taking.

5 Addressing knowledge risk

DNV maintains a comprehensive repository of measures that can be taken to address any P, C or D gap. Proficiency enhancing measures vary from training individuals to systematic R&D, whereas codification measures include expert knowledge elicitation and capture techniques as well as provision of lessons learned systems. Diffusion gaps can be addressed by measures such as communities of practice, peer learning groups or lunchbox talks.

In many organisations, there is no single responsible for addressing knowledge risk and as such the measures to be taken may fall under the auspices of various departments, including human resources, HSEQ, ICT or business improvement.

Addressing knowledge risk requires a holistic and programmatic approach for it to take systemic effect. The DNV method ensures that there is a register for knowledge risk and a monitoring tool for closing gaps in proficiency, codification and diffusion of critical safety knowledge.

6 Example applications of the method

DNV has found that application of the method is varying with the type of organisation we have worked for. Some organisations are more focussed on ensuring that there is rapid learning in a portfolio of critical knowledge, others are keen to build up new knowledge to manage risks to emerging technologies, whereas yet others tend to be more focussed on protection against knowledge loss.

The structure and main orientation of an organisation is also a parameter in how the knowledge risk assessment pans out. Organisations that are focussed on their capital assets tend to put those in focus, whereas organisations that are project-oriented focus on their project portfolio when trying to understand their knowledge risk. We have also found that there may be a geographical orientation or an orientation on a particular professional function ('what does function x need to know?') or an issue (e.g., climate change).

From its wide range of applications, we have learned that the method is easy to contextualise to various circumstances.

7 Conclusions

In this paper, we have introduced a method for identification, assessment and treatment of knowledge risk. Through the application of this method, DNV has learned that:

- Poor knowledge management may pose a risk to both the primary processes as well as to the integrity of the safety management system;
- Knowledge risk can and must be managed just like any other risk;
- A knowledge portfolio management is essential to maintain adequate levels of safety and resilience;
- Knowledge health monitoring and development can be operationalised using a structured method;
- Parameters of a knowledge health check can be contextualised given nature of issues;
- Regular knowledge health checks should be part of a periodical review.

Over several decades of use of the method, we have been able to incorporate modernisations in the way we work with our clients, including the use of collaborative voting tools and on-line dashboards representing the results of the risk analysis and a monitoring system to track progress in treating knowledge risk.

References

1. Day, J, Kelleher, M, Kruizinga, E. (2007): A Knowledge Management Journey at BNG Sellafield: Challenges and Opportunities, IAEA conference on knowledge management, Vienna.
2. Day, J, Kruizinga, E., Kelleher, M. (2008): Preservation of plant operatives' technical experience using knowledge management instruments at Sellafield, American Nuclear Society Spring Meeting, Anaheim CA.
3. International Organization for Standardization. (2018). Risk management — Guidelines (ISO Standard 31000:2018) Retrieved from https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en
4. van der Spek R., Hofer-Alfeis J., Kingma J. (2003) The Knowledge Strategy Process. In: Holsapple C.W. (eds) Handbook on Knowledge Management.

International Handbooks on Information Systems, vol 2. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-24748-7_20.

New Demands on Knowledge Loss Risk Assessment

Sanda Pleslic, University of Zagreb Faculty of Electrical Engineering and Computing, Zagreb, Croatia, sanda.pleslic@fer.hr

Abstract

In today's economy, knowledge is considered as the most valuable asset some organization possesses. Organizational knowledge becomes knowledge stored in the heads of individuals and it must be carefully managed. During their work, individuals should create new knowledge, share knowledge within the organization, and primarily use it to achieve better results that enable a comparative advantage of the organization in the market. Although organizational knowledge consists of explicit and tacit knowledge, tacit knowledge has a much greater weight, as is evident from "The Iceberg metaphor". Almost 95% of the total knowledge comes from tacit knowledge, which is difficult to articulate, to code, to transfer and to share. Knowledge management consists of three components: people, processes, and technologies. Although all three components are important for successful knowledge management in an organization, people again are the most significant component. Before start of any knowledge management activity, it is necessary to analyze the existing knowledge in the organization, to see what critical or specific knowledge is necessary for top performance. In the knowledge loss risk management, the first step is risk assessment, followed by a plan and activities to retain knowledge, and finally monitoring and evaluation of what has been achieved. Two factors are important in knowledge loss risk assessment: the position risk factor and the attrition risk factor. In the past, the attrition risk factor was primarily related to the time gap until retirement. Nowadays, it is no longer possible to treat a retirement as the only knowledge loss from some expert at specific position in the organization. Younger experts have different reasons for leaving and shorter deadlines for implementation of retaining plans automatically require different activities. Also, knowledge retention activities must be concentrated and with maximum efficiency. This paper will discuss new demands on knowledge loss risk assessment and the opportunities in implementation plan which are available through new technologies.

1 Introduction

At the beginning of the 20th century, numerous discoveries such as telephones, railways, cars, electricity etc changed and reorganized the way of life and work. One of the most important requirements was how to produce large quantities of certain goods. The number of employees in the factories was extremely important because it ensured an increase in production efficiency. Location distance and rationalization of energy consumption were important parameters. The economy at the time depended on the possession of money, factories, equipment, land, and primarily the necessary tangible resources.

The economy in the 21st century is based on intangible resources such as information, knowledge, and experience. In today's global economy, knowledge becomes more valuable than it was in the past because knowledge produces added value and at the same time knowledge enables the creation of new knowledge. Information technology helps in the current dissemination of knowledge around the world. The more people involved in knowledge sharing and knowledge dissemination, the more valuable that knowledge becomes. Behavior in the new economy is changing. Intellectual property has no more physical characteristics unlike the traditional economy. The human brain becomes the most important element for the growth and progress of an organization

because only employees can develop new ideas, create added value, and introduce innovations. Business strategy in today's economy, in addition to long-term planning of the behavior of the economic entity to achieve the goals must include knowledge, experience and creativity in action. Today organizational systems are based on intellectual capital. [1]

2 Organizational knowledge

Knowledge management as a hybrid discipline is a series of activities carried out in the organization with the aim of increasing existing knowledge and experience that will be used to achieve better results and to achieve a competitive advantage in the market. Knowledge management is based on organizational knowledge as the most valuable resource that an organization has, so it is closely related to the development of human resources in the organization itself. Despite the large number of tools, techniques, methods and processes in knowledge management, the emphasis is on people and the knowledge they have.

From the very beginnings of knowledge management, everyone wanted to have a definition of knowledge as a starting point for defining activities that could be implemented in knowledge management. The variety of definitions that can be found in the literature makes it difficult to choose only one as correct and true: "Knowledge is justified true belief" (Nonaka&Takeuchi, 1995), "Knowledge is experience or information that can be communicated or shared" (Allee, 1997), "Knowledge is the capacity for effective action" (Argyris, 1993), "Knowledge is fluid mix of framed experience, value, contextual information, and expert insight that provides a framework for evaluating and incorporating new experiences and information" (Davenport&Prusak, 1997), "Knowledge is the sum of what is known: the body of truth, information, and principles acquired by humankind" (Merriam-Webster Dictionary, 2021), "Knowledge is understanding of or information about a subject that you get by experience or study, either known by one person or by people generally" (Cambridge Dictionary, 2021) etc. [2, 3, 4]

Organizational knowledge includes individual and collective knowledge, explicit and tacit knowledge, skills, and expertise of all employees in the organization. Also, organizations are increasingly focusing on old and new knowledge. In assessing the risk of knowledge loss, we usually consider only two types of knowledge from the classical division: explicit and tacit knowledge, and their relationship.

2.1 Explicit knowledge

Due to the possibility of coding, documenting, and transferring explicit knowledge can be precisely and formally articulated. It is also easy to retrieve using many management tools in a variety of ways. Mostly explicit knowledge consists of academic and technical information certain context described in formal and standard language. This systematic knowledge most often represents "knowing what". Due to its characteristics, it is ready for sharing and communication in a conventional form such as printed and electronic materials. For using explicit knowledge, a certain level of academic knowledge and understanding is required that can only be acquired through formal education or structured study. Once coded this knowledge becomes available to everyone else to solve similar problems or create new knowledge. Nevertheless, knowledge sharing processes require significant financial investment in organizational infrastructure and information technology, and the environment and atmosphere in the organization must be relatively stable and predictable.

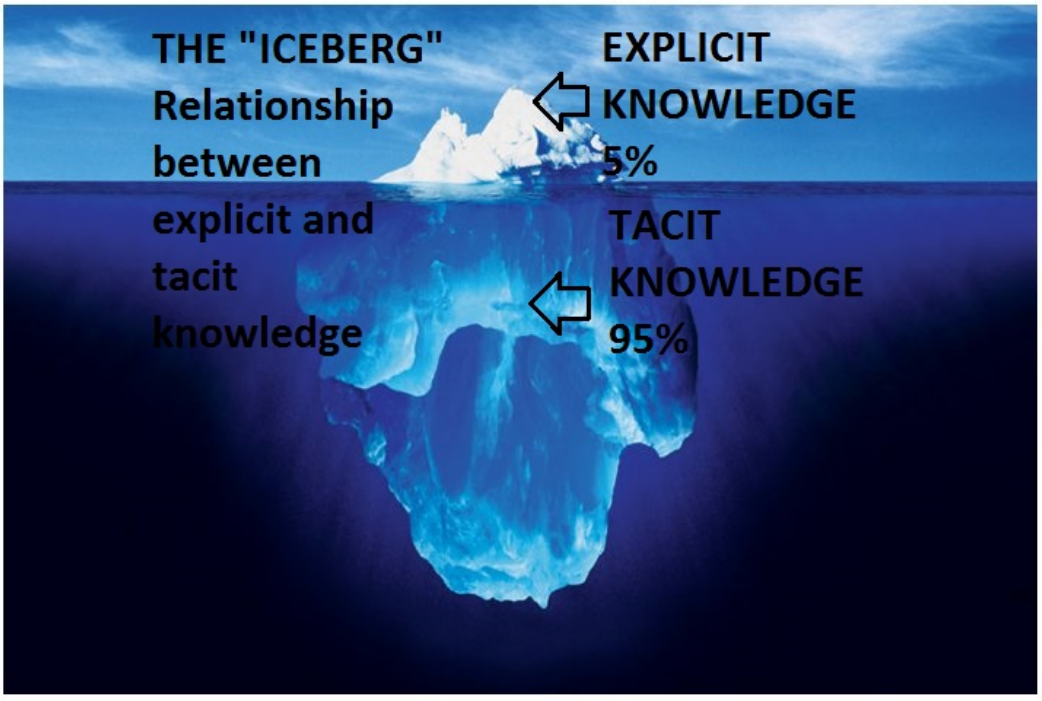
2.2 Tacit knowledge

Something that is subconsciously understood and applied, difficult to articulate because it is personal and specific and depending on the context, is tacit knowledge. It usually comes from experience and direct action, so we use conversation in sharing tacit knowledge. Tacit knowledge cannot be found in coded form because it contains many intangible factors embedded in personal beliefs, experience, and particular value system. The use of tacit knowledge is automatic and requires little or no time to think before applying that knowledge. Whether tacit knowledge has a technical or cognitive basis, it always consists of mental models, perceptions, insights, and assumptions depending on the context. Analogies, demonstrations, and storytelling are most often used to transfer tacit knowledge. It is often underestimated which is why it is not used to the required extent. One way to use tacit knowledge is networking, which is increasingly present in the business world.

2.3 The Iceberg metaphor

The relationship between explicit and tacit knowledge is excellently described by "The Iceberg" metaphor (Figure 1). A floating iceberg rises slightly above the surface of the water, some 5%, and that part represents explicit knowledge. The remaining 95% of the iceberg underwater is tacit knowledge. It is tacit knowledge that constantly supports explicit knowledge, but a two-way interaction between these two types of knowledge is necessary for the successful functioning and operation of an organization.

Figure 1. "The Iceberg" metaphor.



3 Risk management

Risk management is associated with a certain concepts and terms such as opportunities, uncertainty, priorities, impact, analysis, planning, strategy, knowledge, identification, costs, assessment, solutions, decision making, etc. It is a systematic process of

assessing and dealing with risk situations with cost rationalization and with human resources capable of identifying and assessing risks. It is a whole set of procedures that, in addition to identification and assessment, include taking measures or activities to avoid or reduce risk, and then monitoring progress. Since risk management is not related exclusively to business entities or public institutions, but to each business activity, it is necessary to have different approaches, and to act in the short or long-term depending on the given risk. Likewise, risk management must be linked to the achievement of certain objectives. They do not always have to be financial in nature although often it all comes down to just that. In any case, work and life experience and the saved history of the organization will enable us to define goals, and well-defined goals will enable more efficient risk management. Effective risk management is not possible without a developed organizational culture that implies the involvement of all employees in all necessary activities. Common goals, the same system of ethical values and prescribed standards and norms are implied. The mission of the organization and the vision of development are linked to strategic goals, so it is important to include each component in risk management, because only in that case we get a satisfactory result.

4 Knowledge loss risk assessment

The components of knowledge management are people, processes, and technology. They are often compared to the legs of a stool - if one is missing, there is no balance. One component is more important than the other - people. The loss of this component is associated with the loss of knowledge. When we look at the theory of intellectual capital, people are human capital, but they are also strongly connected with social, structural, and relational capital.

Figure 2. The legs of a stool metaphor

How is the risk of knowledge loss in an organization different from other types of risk? In fact, it is the same because in managing the risk of knowledge loss we must follow the same steps as we would follow for any other risk. We can simplify this and view it as a 3-step process: Assess the risk with specific, predefined criteria; Determining the approach to retaining knowledge; Monitoring and evaluation. The goal is to retain knowledge, but not any knowledge but critical or specific knowledge. There is a large amount of knowledge within each organization and therefore there should be predefined criteria that will make a distinction between different levels of knowledge. Critical or specific

knowledge could walk through the exit door of an organization easily. So, it is crucial to recognize them and take whatever action is needed to keep them.

In old approach, first step, the assessment of the risk of knowledge loss with specific, predefined criteria, was designed to identify workers with the greatest potential loss of knowledge and will occur most soon. The assessment was based on 2 factors: Attrition Risk Factor (time to retire or otherwise lose knowledge) and Position Risk Factor (critical position of employees in the organization assigned by the management). For attrition factor we had risk factors starting from 5 (leaving inside 2 years), 4 (inside 3 years), 3 (4 years), 2 (5 years), and 1 (6 and more years). Position risk factor was estimation of level of efforts to replace somebody at certain position in organization based on following criteria: 5 (mission critical knowledge or skills, unique knowledge, undocumented knowledge), 4 (critical knowledge and skills, some documentation exists), 3 (important, systematic knowledge and skills, replacement available in organization, documentation exists), 2 (knowledge and skills based on procedures, non-mission critical knowledge and skills, training programs are ongoing, and can be completed in less than 1 year.), and 1 (common knowledge and skills). Total risk factor was multiplication of above-mentioned factors: 20-25 (high priority), 16-19 (priority), 10-15 (high importance), 1-9 (importance).

Second step in knowledge loss risk management was determination of approach for critical knowledge capturing starting with interviews with employees to identify potential field of knowledge loss and to estimate knowledge loss consequences. Interviews consisted of general questions, problem questions, data and information questions and pattern recognition. After that options for knowledge capturing should be identified with list of priorities and action plan should be developed and implemented.

Third step was monitoring and evaluation of knowledge capture. It means that projected dates of loss of knowledge must be regularly reviewed and updated. Also, knowledge retention plans needed to be constantly monitored. If necessary, identification of areas to be reassessed. And finally, coordination of everyone involved in the process and, if necessary, repetition of all steps if and where is necessary.

5 New demands on knowledge loss risk assessment

Today's employees are changing their way of working and approach to work due to changing external circumstances. The main reasons are most often the introduction of new technologies, globalization and internationalization. Retirement is no longer the main factor causing knowledge loss in the organization. The way knowledge risk is managed in an organization must also change in terms of being a more flexible approach and a faster response to a new situation. At the same time, we are witnessing some extreme cases of loss of knowledge in the organization that come from reasons that are not strictly professional in nature. For example, a sudden win in the lottery encourages players to change their lifestyle, work, value system, habits and so on. If at the same time these players are experts in their work and possess certain critical or specific knowledge, without them the organization will feel a great loss. A similar case is with specialists who discover some hidden talents and decide to dedicate themselves completely to it.

Younger generations of experts change the business environment and their positions much more often than their parents and often these are not just financial reasons. It is often a search for new, more interesting professional challenges or a motivating business environment. The knowledge loss cannot be managed in the old, traditional way. For the beginning, the notice period is now much shorter than it was in some past times. If it is a period of 1 to 3 months, then it is impossible to transfer specific knowledge and skills to a new person in that short period even without immediately conducting a risk assessment and making an action plan to retain knowledge.

Attrition risk factor must change in accordance with the new conditions, so it is more appropriate to use factor 5 for a very short period of 1 to 3 months, which will mean that

prompt action is needed. For factor 4 we still measure time in months. As we move towards lower attrition risk factors, we are approaching the scale we had in the old, traditional model primarily related to retirement, so attrition risk factor 1 can be for a period of 5 years or more.

In the global market, there are more and more smaller organizations that employ many experts in relation to the total number of employees, which results in difficult knowledge loss risk management. In large organizations, it is relatively easy to find someone to replace an expert who has left, or relatively quickly someone can be brought to the desired level of expertise. In certain areas of work, the base of organizational knowledge is created to express very slowly and difficult, and expertise is achieved after several years and a lot of effort. Examples of this are organizations in the field of application of nuclear science and technology. [5, 6]

Organizations in various industries, research and development institutions and scientific and educational institutions face similar problems in managing the risks of knowledge loss. Therefore, the introduction of new metrics in risk assessment is inevitable.

Primarily thanks to the increasingly rapid development of information technology, we find in the market many tools that can be used in knowledge management from knowledge loss. During each new employment and then periodically, each employee in the organization should be evaluated using position and attrition risk factors, which will enable the organization to predict the possible risk of knowledge loss. Also, each employee should be required to keep personal work records, such as a work diary, in the standard manner prescribed by the organization. This documentation should contain critical or specific knowledge and skills and should be available to others in the organizational knowledge base. More than one person in the organization should be familiar with the use of various tools, techniques, and methods. Organizing periodic meetings and workshops with the aim of determining the need for certain knowledge and skills and then sharing primarily tacit knowledge should be part of normal business.

6 Conclusions

No matter where the knowledge loss occurs, in industry, education or the R&D sector, we will most often have a problem with the tacit knowledge loss due to its characteristics. Such knowledge is difficult to articulate, comes from experience, and is subconsciously understood and applied. It is difficult to store in some conventional form, which makes it even more difficult to share. The processes of capturing, maintaining, and sharing critical or specific knowledge in an organization must be developed and regularly applied. According to the new requirements of knowledge risk assessment, knowledge retention plans should be developed and applied with maximum use of advanced tools, techniques, and methods. Knowledge retention should be monitored and evaluated.

Even more important in an organization is the continuous development of knowledge management that includes gathering existing knowledge and connecting people to share their knowledge. The management of the organization should understand knowledge as a strategic resource and support all knowledge management processes. Organizations should be focused on developing and using their own resources in the form of knowledge. Knowledge management processes, including tools and techniques must be clearly defined. The creation, sharing and use of knowledge must be part of a normal work process, not separate. People in organizations need to collaborate, not compete. Everyone’s contribution to knowledge sharing should be recognized and rewarded. Individual behaviour needs to change in order to build an organizational culture. Changes in individual behaviour should be guided by the examples of leaders, middle and senior management, who are engaged as trainers or mentors. Building trust and excellent collegial relationships are tasks for all employees. Learning from colleagues is better than learning from managers. It is necessary to remove all possible obstacles for the most successful knowledge management by improving the organizational structure and processes.

References

1. Collison, C. and Parcell, G. (2005*) Learning to Fly: Practical Knowledge Management for Leading and Learning Organizations*, Capstone Publishing.
2. Firestone, J. M. and McElroy, M. W. (2003) *Key Issues in the New Knowledge Management*, Butterworth.
3. Sanchez, R. (2003) *Knowledge Management and Organizational Competence*, Oxford University Press.
4. Stapleton, J. J. *Executive's Guide to Knowledge Management: The Last Competitive Advantage*, John Wiley and Sons.
5. International Atomic Energy Agency (2006) *Knowledge Management for Nuclear Industry Operating Organizations*, IAEA-TECDOC-1510.
6. International Atomic Energy Agency (2020) *Mapping Organizational Competencies in Nuclear Organizations*, IAEA Nuclear Energy Series NG-T-6.14.

Assessing and Managing Reliability and Risk Issues of Automated Vehicles: Emerging Practices and Challenges

Wolfgang Kröger, Swiss Federal Institute of Technology Zurich (ETH) & Swiss Academy of Engineering Sciences (SATW), wkroeger@ethz.ch

1 Introduction, basic understanding

Automated Vehicles (AV) aim to assist and eventually absolve humans from cumbersome performance of tasks and prevent them from being of a hazard source as in many countries up to 90% of crashes are caused by human errors. According to the Society of Automotive Engineers (SAE, 2018) we distinguish five levels of driving automation. Whereas SAE level 1 and 2 are related to driver support features the subsequent levels include automated driving functions to different degrees: Conditional automation (level 3) allows the driver to focus on tasks other than driving during normal operation but must quickly respond to an emergency alert from the vehicle and be ready to take over. Human attention is not needed in any degree at highly (level 4) and fully automated (level 5) vehicles. Level 4 (as level 3) AV can only operate in limited operational design domains (ODD) such as highways and under certain (weather) conditions. In case of departure from these, the vehicle must stop the trip by automatically parking itself (fallback) while level 5 AV can operate in any road network and under all environmental conditions and bring itself in minimal risk condition.

Together SAE level 4 and 5 vehicles are called autonomous; those which connect with other devices to function most effectively and communicate with other vehicles (V2V) and with infrastructure/ vulnerable road users (V2X) are often termed coordinated and automated vehicles (CAV). The development driven by big car industries and IT-giants is rapidly ongoing (with Google's Waymo supposedly in the lead). However, robust automated driving in urban, indeterministic environment together with other very different road users is still pending (Yurtsever et al., 2020).

2 Safety validation and certification processes

AV rely on machine learning at different phases of pattern recognition, interpreting sensor and image data, and thus improving algorithms. Hence, reliability and safety are not static but change, hopefully increase continuously. Initial guesses of the kind of the detected objects may be wrong but will become more accurate after modifications. However, the question remains when systems are sufficiently mature to be released to public use and how to organize the safety validation and certification process.

Two paradigms have been pursued in the past and become apparent today: on the one hand "self-certification" or "self-assessment" in the USA which favours test-driving, encourages industry to validate internally that designs meet best practice standards and a set of State and, notably, Federal regulatory requirements, then leaving the remaining risk to industry/ vehicle manufacturer. The process is supported by a voluntary guidance document with 12 priority safety design elements for consideration, released by the Department of Transport (USDOT/NHTSA, 2018). Currently, about 80 companies are testing AV on public roadways, several millions of miles were driven under ideal use cases, a first successful Waymo driverless ride without safety-assistant took place in November 2019 in Phoenix/Arizona.

On the other hand "type approval" is mandatory for cars since 1998 in the Europe which does not solely rely on test-driving but allows for virtual testing methods at the require of industry and agreed by the authority that will finally decide on the certification. Therefore, based on intensive use of available and specifically generated data a large set of

representative critical scenarios is fleshed out by key actors against which AV have to be tested on stands and tracks. National specifications follow international requirements, heavily relying on UN-ECE technical rules. The process is evolving under the EU exemption procedure, focussed on advanced assistance systems, the automated lane keeping system (ALKS) in particular, as building blocks towards entire autonomous vehicles (UN, 2021). More recently, Germany established a law allowing for level 4 AV on dedicated open roads, mainly for commercial vehicles like shuttle buses or delivery vans but for privately used cars.

The question "How safe is safe (or good) enough?" is well known from other domains, notably from the nuclear sector. Commonly agreed, even mandatory reliability and safety targets do not exist yet. Functional safety and reliability are driven by software, may change over time and are subject to updates and modifications during operation; hardware failure rates are not constant as usually assumed in reliability theory, software failures are hard to diagnose. Distinguishing three levels of abstraction and related targets, at the highest level automated vehicles should be better than human-driven cars equipped with modern assistant systems; accident-free driving per distance (km), time between crashes or compliance with risk curves and associated tolerability lines are proposed as substitutes. At the system level, the manufacturer has to demonstrate by a robust design and validation process freedom of "unreasonable" risks and ensuring compliance with road traffic rules (UN 2021). At components and subsystems level, functional safety must be ensured by compliance with standards: ISO 262 62: 2018 for development of safety-critical functions and devices during the development process and ISO PAS 21448 for demonstrating safety of the intended functionality (SOTIF), geared to identify real world scenarios.

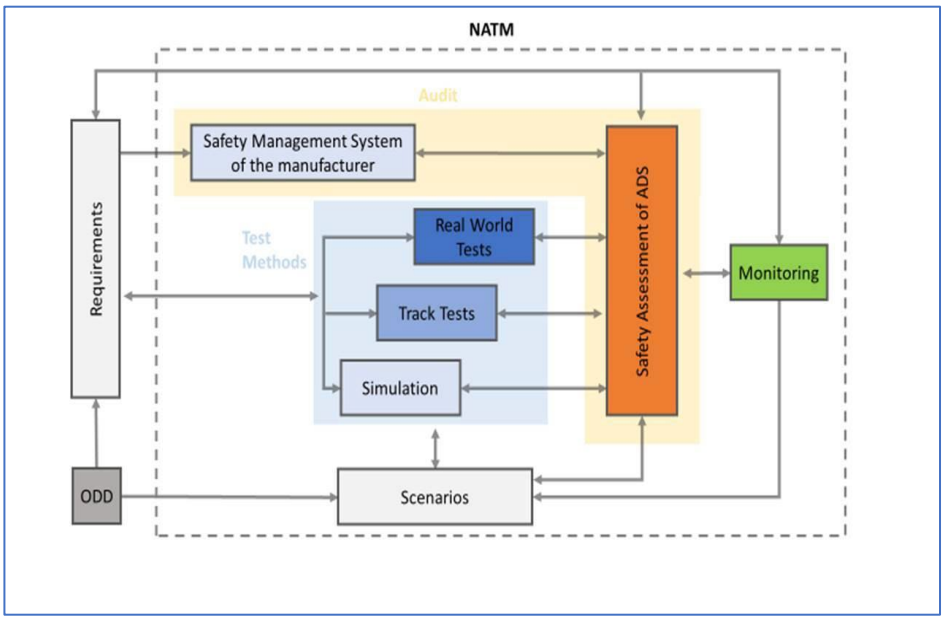
Test-driving in real traffic environments, appears the most logical way to validate the safety of AV and to evaluate and improve systems' performance while taking the complexity of the entire system into account However, this turned out as impossible proposition as the time needed would be by far too long (Kalra and Paddock, 2016). Therefore, various ways out of this dilemma have been identified and pursued. Nevertheless, the whole design-simulation-test-redesign-certification procedure is still not established, neither by industry nor the regulator. Most recently, a working party on automated and connected vehicles (GRVA), established by the UN-ECE in mid 2018, proposed a validation framework called New Assessment/Test Methods for AV (NATM) based on several pillars and five validation methods including a catalogue of critical scenarios and simulation (Fig. 1).

3 Alternative methods for safety validation

As mentioned before the scenario-based approach is favored as part of the type-approval process to validate automated driving functions. Based on the assumption that a large portion of road scenarios in reality are uncritical, it is proposed to identify "critical scenarios" out of a large set of developed scenarios and to expose single vehicles, equipped with automated systems, to exclusively critical scenarios to check their performance under "real world conditions" and on test benches in particular

Within the German PEGASUS project (www.pegasusprojekt.de), a generic simulation-based tool-chain has been developed to identify critical scenarios which are categorized as functional, logical, and concrete with decreasing level of abstraction (Hallerbach et al., 2018). The identification process is realized by a combination of vehicle dynamics simulation that includes the digital prototype of the examined driving function, traffic simulation that provides the surrounding environment and a cooperation simulation that is used to establish a suitable comprehensive simulation environment. The behavior of other traffic participants is part of the traffic simulation environment. The toolchain was applied to use cases for a SAE level 3 "highway chauffeur" that can perform standard driving tasks: entering the highway with exemplary disturbances like sensor error, incorrect precision map and aggressive behavior of other traffic participants.

Figure 1. Relationship between the pillars of the New Assessment/Test Method for Automated Driving (NATM), critical scenarios and safety requirements – the testing might follow a logical sequence from simulation to track and then real-world testing, ODD stands for Operational Design Domain (GRVA, 2021).



Also, within PEGASUS, a holistic framework has been developed to early detect "potentially critical scenarios", caused by performance limitations and functional insufficiencies occurring in the processes of sensing, modelling, and interpreting the environment as well as of maneuver planning (Böde et al., 2019). The originally proposed 5-steps approach aims to assess automated driving functions implemented in a SAE level 3 highway driven vehicle. The method starts with modelling of functions, followed by a hazard analysis, based on traditional methods such as HAZOP including "key words", then adapted and extended fault trees (FT) are used to develop impact chains for identified hazards, called top events. Associated basic events encompass both system-inherent failures and environmental conditions able to trigger failures. Finally, risks are estimated by quantifying the probability of hazard exposure, the severity of potential accidents and the probability of control reactions of persons involved; the risk is then assessed against a tolerability line established by ISO 26262:2018. (Ghadhab et al., 2019) proposed dynamic fault trees (DFT) to model a variety of safety concepts and electrical/electronic (E/E) architectures for the analysis of automated vehicle guidance systems during the design phase. The constructed overall DFT with up to 300 elements consists of (1) the system layer, (2) the functional block layer with different diagrams, and (3) hardware layer. Both, HAZOP studies and fault tree analyses are well-known and broadly applied in the chemical and nuclear domain.

Besides questions regarding completeness, resulting huge number of critical scenarios still seem to exceed the existing capacity in practice so far. Novel approaches have been investigated to reduce the parameter space of critical scenarios and thus the test coverage significantly. Various attempts/proposals deserve attention: (Koné et al., 2020) proposed a hazardous behavior criterion with five severity classes for evaluation of scenarios identified by assuming functional insufficiencies. (Weber et al., 2020) proposed a simulation-based, statistical approach to derive concrete scenarios for highly automated driving functions (SAE level 3 and higher) with a takeover process prompted by the vehicle. The methodology extends the above-mentioned framework of (Hallerbach et al., 2018) for the derivation of logical scenarios and encompasses the statistical evaluation and discretization of influence parameters identified by the traffic simulation package, their application to functional layers of the decomposed automated driving function and finally a deterministic variation of previously discretized parameters which define a concrete

scenario. The application to cut-in and traffic-jam dissolution functional scenarios showed a significant reduction of the parameter space.

Within students' projects, a probabilistic metamodel was proposed, trained by a dataset of input/ output pairs, which surrogates an unknown, generically nonlinear, criticality function, mapping the input scenarios to a risk metric. This so-called criticality function quantifies the severity of the input scenarios by weighting various safety performance indicators, and ultimately can help in reducing the input space dimensionality by identifying the most influential input parameters. Moreover, further attempts to reduce the dimensionality of the exploding parameter space were performed within other students' projects by looking at the most significant parameters using statistical learning techniques. One prominent example is using Linear Discriminant Analysis (LDA) to project the initial huge input parameter space into a lower dimensional one, spanned by the most affecting parameters.

These "traditional" methods of hazard analysis based on reliability theory such as inductive FMEA, HAZOP, Event Tree Analysis (ETA) and deductive FT Analysis have been criticized because they focus on hardware component failures and do not sufficiently consider software failures and human interactions, in addition to not considering the system as a whole entity (Abdulkhaleq et al., 2018; Kölln et al., 2019). STPA (Systems-Theoretic Process Analysis) has been developed (Leveson, 2011) to overcome these limitations in terms of identifying design errors, flawed requirements, human factors implications, software failures and unsafe and unintended component interaction failures. STPA uses a "feedback loop safety control structure diagram" to identify unsafe scenarios and develops a detailed set of safety constraints/requirements. STPA has been applied to develop dependable architecture for fully automated vehicles (Abdulkhaleq et al., 2018), to identify hazardous interactions of automated driving systems (Abdulkhaleq et al., 2018), and regarding the series development of autonomous vehicles (Kölln et al., 2019). Numerous attempts have been made to compare STPA achievements and results with other methods, e.g., (Sulaman et al., 2019) has applied STPA and FMEA on the same forward collision avoidance system; he concluded that both methods, despite different focuses, complemented well and delivered similar results.

4 Anticipated potential risks

In view of the early stage of the development and limited knowledge base it is difficult to specify risks. Some claim that autonomous driving will reduce crash rates by 90% due to elimination of human error, but this overlooks that a new set of crash causations and additional risks can be introduced. Some potentially "high-profile" risks can be anticipated as follows:

- False or interrupted sensor information, distorted signals, software errors; unreliable system functions under adverse conditions.
- Gaps in 5G/GNSS coverage, needed for localization and V2V or V2X communication, loss of services such as weather and traffic information and high-dissolution (HD) maps.
- Extreme environmental conditions not covered by the automated control systems.
- Take-over situations from automated mode after alert may fail, when necessary, at all.
- Operating close together at high speeds on dedicated lanes (platooning), leaving less time to react on unforeseen events and may introduce cascading events with increased crashes severity.
- The catalogue of system requirements and failures may prove incomplete even after diligent validation; failures of inadequate updates may occur.
- Malicious hacking/manipulation of networked components and wireless communication channels, when using the public internet; induced risks depend on defender strategies.

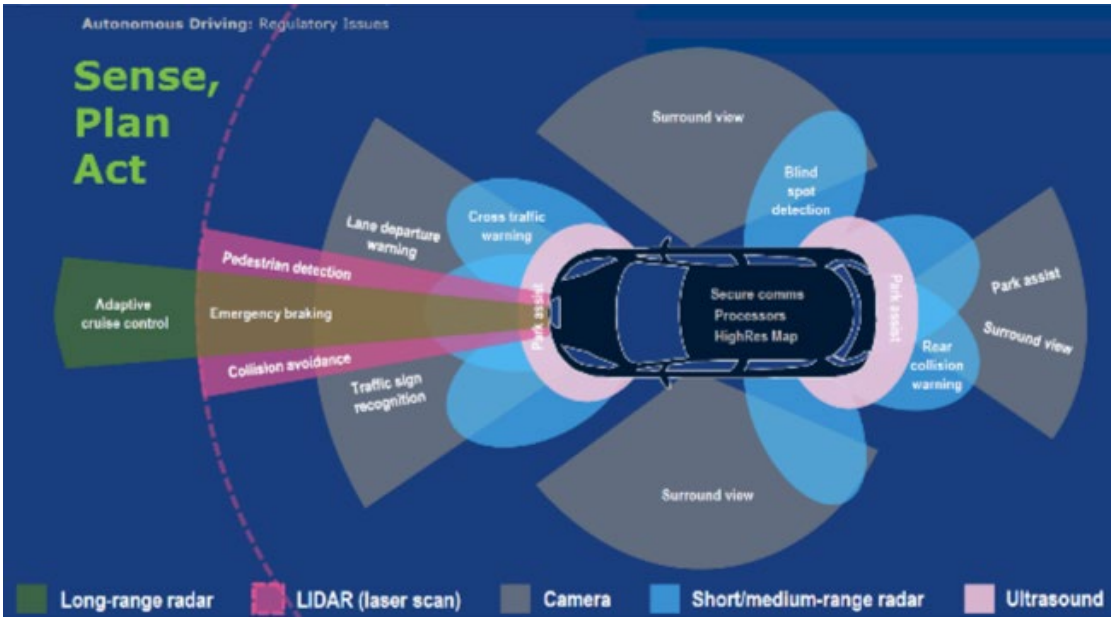
Further risks may relate to the transition phase with mixed traffic, i.e., algorithms might be unable to integrate behavioral patterns and gestures of other vulnerable road users.

5 Some basic characteristics of automated driving systems

Basically, automated driving systems (ADS) take decisions instead of the driver. High-class technologies, algorithms and a knowledge base are required to transfer learned skills and cognitive capabilities of humans to a complex technical system; finally, humans are off the loop and do no longer as redundancy to compensate system failures. Besides necessary external inputs (HD-maps, GNSS), multiple in-vehicle techniques are combined for localizing the vehicle and perceiving the dynamic surroundings. Advanced control systems combine/fuse and interpret information, build a model of surroundings, identify static and dynamic obstacles as well as navigation paths, make decisions and then plan/execute actions by actuating reliable systems for steering, braking and acceleration. The necessary intelligent software with a stack of algorithms and learning processes is based on artificial intelligence (AI). Included hard-coded rules, obstacle avoidance algorithms, predictive modeling, and smart object discrimination, e.g., knowing the difference between a bicycle and a motorcycle, animals and humans, help the software follow traffic rules and navigate obstacles.

State-of-the-art ADS employ a wide array of onboard sensors such as cameras, ultrasonic devices, lidar and radar each with specific ranges (Fig. 2) as well as performance strengths and weaknesses. The layout, of sensor systems differs by manufacturers with regards to applied techniques and redundancy, also to optimize benefits (reliability/safety) and costs.

Figure 2. Varying sensor technologies with application areas and ranges (EC/ERSO 2018)



Some expect connected and autonomous vehicles (CAV) to evolve into a "complex system" or even into a "system-of-systems" rather than just into a "complicated system", a distinction with associated elements and attributes as well as challenges to methods, worth to be carved out.

The term "complexity" is not well defined. However, it is commonly agreed that complexity is something with parts interacting with each other in multiple ways, culminating in a higher order of emergence greater than the sum of its parts or, according to (Aven et al., 2015),

"if it is not possible to establish an accurate prediction model of system behavior based on knowing the specific functions and states of its individual components".

Characteristics of complex systems versus complicated systems are highlighted as follows, see (Kröger and Nan, 2019) for more details:

- Both system types entail a large number of highly connected components, for complicated systems event frequency-consequence curves tend to follow a normal distribution while such curves for complex systems tend to show fat tails and follow power law distribution.
- Rules of interaction between the components of complex systems may change over time and may not be well understood while components of complicated systems have well-defined roles and are governed by prescribed interactions.
- Complex systems are more open, respond to external conditions and evolve, interact with their environment, structures do not remain closed and stable over time and the range of responses to changes in their environment is not limited, all in contrast to complicated systems.
- Complex systems show high dynamic and non-linear behavior as well as sudden regime shifts; behaviors are not fully predictable, opposite to complicated systems.

Despite the early stage of development, we conclude courageously that attributes and behaviors of complex systems fully apply to highly or notably fully coordinated automated vehicles while nuclear power plants can be categorized as complicated systems. Thus, some methods based on decomposition and causal chains, like FT and ET techniques, successfully applied in the nuclear sector within in the framework of Probabilistic Safety Assessment (PSA), alone may prove insufficient for safety validation of coordinated autonomous vehicles.

6 Concluding remarks

Worldwide vehicles of different degree of automation are under massive development and testing or even close to deployment. Certification requirements are in the process of being structured with validation of sufficient reliability of innovative hardware and software components/subsystems/systems, functional and operational vehicle safety as well as freedom from unreasonable risks as key elements. Adequate modelling and testing methods are under development and early case applications, seem to be lagging behind designing efforts, at least for highly to fully automated cars.

High-level coordinated automated driving systems must be understood as learning systems mainly by use of intelligent algorithms based on AI but also by learning from track and real-world testing experience and other domains including the nuclear sector. However, their inherent characteristics must be considered when assigning methods from other areas of application. Traditional reliability analysis needs to be adapted and further developed, respectively, to deal with varying (instead of constant) failure rates, updates, software failures and human factors. Further, traditional deductive methods based on decomposition and inductive methods based on causal chains like logic trees alone deem insufficient for modelling and analyzing the system as a whole entity including complex behavior patterns. Thus, new frameworks and methods need to emerge in parallel to technical development and planning towards full automation (SAE Level 5). Such developments may profit from a combination of available "traditional" methods or from advanced methods from other domains such as complex network theory.

Some (including the author) propose to think about a paradigm shift and claim to strive for "resilience", that means aiming at „soft landing strategies" after undesirable events by strenghtening absorptive, adaptive and restorative capabilities instead of hardening vulnerable elements to reduce risks (Kröger 2019). This could also help to better cope with "the unexpected".

References

Terje Aven, Y. Ben-Haim, H. B. Andersen, T. Cox, E. L. Droguett, M. Greenberg, S. Guikema, W. Kröger, O. Renn, K. M. Thompson, SRA Glossary, Council of the Society of Risk Analysis (SRA), 2015

Asim Abdulkhaleq, M. Baumeister, H. Böhmert, S. Wagner, Missing no interaction – Using STPA for identifying hazardous interactions of automated driving systems, International Journal of Safety Science, Vol. 02, No. 01 (2018).

Eckard Böde, M. Büker, W. Damm, M. Fränzle, B. Kramer, C. Neurohr, S. Vander Maelen, Identifizierung und Quantifizierung von Automations-risiken, OFFIS, July 2019.

European Commission/ERSO, Autonomous vehicles & traffic safety, 2018 (www.erso.eu).

Majdi Ghadhab, S. Junges, J.-P. Katoen, M. Kuntz, M. Volk, Safety analysis for vehicle guidance system with fault trees, Reliability Engineering and System Safety 186 (2019) 37-50.

GRVA, New assessment/test method for automated driving (NATM), WP.29-183-05, March 2021.

Sven Hallerbach, Y. Xia, U. Eberle, F. Köster, Simulation-based identification of critical scenarios for cooperative and automated vehicles, SAE Technical Papers, April 2018.

ISO 26262:2018 International Standard, Road vehicles – Functional safety.

Nidhi Kalra and S. M. Paddock, How many miles of driving would it take to demonstrate autonomous vehicle reliability? RAND Corporation, 2016.

Greta Kölln, M. Klicker, S. Schmidt, Comparison of hazard analysis methods with regard to the series development of autonomous vehicles, IEEE Intelligent Transportation System Conference (ITSC), Auckland, NZ, 2019.

Tchoya Koné, E. Levrat, E. Bonjour, Frédérique Mayer, S. Géronimi, Safety assessment of scenarios for the simulation-based validation process of AV with regards to its functional insufficiencies, Proc. of ESREL2020-PSAM15 conference, Venice, 2020.

Wolfgang Kröger and C. Nan, Power Systems in Transition – Dealing with Complexity, in C. Büscher, J. Schippl, P. Sumpf (editors), Energy as a Sociotechnical Problem, Routledge, 2019.

Wolfgang Kröger, Achieving resilience of large-scale engineered infrastructures, in Farsangi et al. (eds.), Resilient Structures and Infrastructures, Springer, May 2019.

Leveson, Nancy G. "Engineering a safer world: systems thinking applied to safety (engineering systems)." MIT Press Cambridge. 2011.

SAE International, SAE International Releases Updated Visual Chart for Its "Levels of Driving Automation" Standard for Self-Driving Vehicles. 2018.

Sardar Mohammad Sulaman, A. Beer, M. Felderer, M. Höst, Comparison of the FMEA and STPA safety analysis method – a case study, Software Qual J (2019).

UN, Uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems, informal document, Regulation No. 157, March 2021.

USDOT/NHTSA, Automated driving systems 2.0, 2018.

Nico Weber, D. Frerichs, U. Eberle, A simulation-based, statistical approach for the derivation of concrete scenarios for the release of highly automated driving functions, AmE, GMM-Fachbericht, VDE, 2020.

Ekim Yurtsever, J. Lambert, A. Carballo, K. Takeda, A survey of autonomous driving: Common practices and emerging technologies, IEEE Access, Vol. 8. 2020.

Non-financial reporting as an instrument for safety risk management: preliminary findings

Eric Marsden, Foundation for an Industrial Safety Culture, eric.marsden@foncsi.org

Abstract

Risk management is improved when appropriate incentives encourage firms to invest in risk reduction measures. For listed companies, the financial dimension of risk related to major accident hazards is borne by shareholders, who should therefore be informed of these risks. We report on an exploratory study of a small sample of the annual reports and sustainability reports of EU companies operating in high-hazard industry sectors, analyzing the quality of the information presented on the exposure to major accident hazards and the associated preventive measures taken. This analysis of current practice shows that information provided to investors is mostly backward-looking (TRIR) and addresses occupational safety rather than major accident hazards. We argue that a potential channel for knowledge of risks to influence resource allocation concerning prevention is essentially dysfunctional.

1 Introduction

Investigations of major accidents often find that the main contributing factors are poor decision-making and resource allocation by top-level executives and company managers, such as reducing staffing levels and maintenance costs, maintaining production levels despite safety concerns, and ignoring safety concerns raised during system design and certification. One argument put forward by executives to defend their decisions to emphasize profitability, despite the knowledge available concerning the increased risk of major accidents, is their legal obligation to maximize shareholder value.

A basic principle of capitalism is that shareholders make decisions on resource allocation primarily based on the mathematical expectation of their gains. In addition to their extra-financial impacts (harm to individuals and the environment, etc.), major accidents often have significant financial impacts (lost production, damaged facilities, compensation of affected parties, fines, detrimental affects to company reputation), which should be integrated by investors, shareholders, lenders and insurance underwriters in their decision-making. For example, the 2011 Macondo catastrophe generated costs estimated at 145 billion USD for BP [1].

As stated by the US Chemical Safety and Hazard Investigation Board (CSB) report into the Macondo accident [2, volume 3, p. 195],

> As Macondo made clear, major accident events (MAEs) can interfere with drilling operations and production, damage reputation, and cause significant financial distress for a company with predictable, negative outcomes. Consequently, corporate boards of directors must act vigilantly in preventing MAEs from their position as the highest echelon of leadership within the company. It is in shareholders' best interests to understand the relevant information needed to assess the companies in which they invest, and to benchmark the process safety performance of such companies. In doing so,

> shareholders would be positioned to better understand and question companies' business decisions. They can both directly and indirectly help to ensure or improve process safety and major accident prevention efforts of companies engaged in offshore drilling and production. Thus, enhanced reporting not only benefits shareholders, but all stakeholders, including workers, the public, and the environment.

The OECD Guidelines for multinational enterprises [3] indicate (p. 29):

> […] information should be prepared and disclosed in accordance with high quality standards of accounting and financial and non-financial disclosure. This significantly improves the ability of investors to monitor the enterprise by providing increased reliability and comparability of reporting, and improved insight into its performance.

Directive 2014/95/EU of the European Parliament, also known as the non-financial reporting directive, requires large companies whose shares are listed on the stock market to disclose in their management report relevant and useful information on their policies, main risks and outcomes[1]. The US Securities Exchange act requires listed companies to communicate relevant information about risks that are considered to be "material"[2]. Public companies in the USA must disclose information on the material effect of their compliance with federal, state, and local laws in the environmental domain on the company's capital expenditures, earnings and competitive position.

Over the past decade, an increasing number of shareholder lawsuits in the USA are based on the accusation that company managers did not adequately disclose the facts underlying a non-financial risk, and that investors were harmed by the resulting drop in share value, a class of legal action called "event-driven securities litigation" [4].

Furthermore, certain large companies adopt voluntary reporting practices concerning their social impact in the context of their corporate social responsibility programmes, or in response to increasing interest from the financial markets in environmental, social and governance (ESG) issues. The trend towards "socially responsible" investing has had a major impact on share prices in recent years: companies with the highest ESG rates trade at a 30% premium to the poorest performers as measured by their forward price-to-earnings ratios, according to reports in the financial press[3]. Large investors such as the firm BlackRock have decided to divest from their investments in coal due to ESG concerns, and anticipation of the financial risk from future legislation that could affect the value of production assets. However, ESG reporting is not very mature, with a recent white paper from the Yale Initiative on Sustainable Finance describing it as "vast, messy and complicated", with significant inconsistencies in the way in which companies report their ESG data [5].

Despite these legal obligations and societal trends, the current state of extra-financial reporting means that little information is available to shareholders concerning the risks of

[1] More specifically, companies must "provide adequate information in relation to matters that stand out as being most likely to bring about the materialisation of principal risks of severe impacts". Directive 2014/95/EU has been transposed into law in the different member states with certain nuances; in France for example, even non-listed companies that reach certain thresholds are required to report this non-financial information.

[2] In accounting, information is considered to be material if it would affect the judgment of an informed investor.

[3] *'Monstrous' run for responsible stocks stokes fears of a bubble*, Patrick Temple-West, Financial Times, February 21 2020.

major accidents affecting listed companies. In practice, the information reported to shareholders concerning safety is most often limited to occupational safety (injury statistics such as the TRIR), with little or no information on process safety and the risk of major accidents. Whilst occupational safety has some overlap with process safety, performance in these two dimensions is not necessarily correlated[4]. This hinders shareholders' ability to understand the level of risk to which they are exposed by purchasing shares. It also means that a potential channel for knowledge of risks to influence resource allocation concerning prevention is essentially dysfunctional.

The general trends towards increasing sustainability and non-financial reporting is generally thought to have a positive impact on firms' social and environmental actions [6]. However, there is some concern that some company reporting on safety performance amounts to "safewashing" [7], as it attempts to project a positive image of company performance, whilst not always being a valid representation of the level of safety really achieved. Other researchers have used the lens of organized hypocrisy[5] [8] to analyze corporate sustainability discourse as a way for firms to manage conflicting expectations from their shareholders and other stakeholders.

Prior work on similar topics includes [9], which analyzes firms' sustainability reporting concerning occupational safety and health (OSH) issues. [10] undertake a content analysis of firms' CSR reports to determine whether they target mainly shareholders or mainly stakeholders, finding that the reports analyzed are primarily oriented towards shareholders.

2 Existing guidance

The following guidance exists concerning sustainability/ESG reporting and non-financial disclosures:

- The Global Reporting Initiative (GRI) sustainability reporting guidelines are probably the most well-known reporting framework. They include a set of indicators that companies can use as a framework to report on their corporate social responsibility efforts. Over the course of its development since the late 1990s, the GRI has become institutionalized. The indicators are stakeholder-oriented, rather than shareholder-oriented.
- The UN Global Compact requires participating companies to publish an annual *Communication on Progress* report, detailing actions taken towards the UN Sustainable Development Goals.
- The CDP (known before 2012 as the Carbon Disclosure Project) publishes guidance for firms and government entities that wish to report on their environmental impacts, with a particular focus on greenhouse gas emissions. Companies are rated using a *Level of Engagement Score* which assesses actions concerning leadership, management, awareness and disclosure.

[4] For example, the 2007 Baker report into the 2005 BP Texas City accident states that "BP mistakenly interpreted improving personal injury rates as an indication of acceptable process safety performance at its US refineries. BP's reliance on this data, combined with an inadequate process safety understanding, created a false sense of confidence that BP was properly addressing process safety risks". This observation is acknowledged by many firms operating in high-hazard environments, and for example Shell's 2020 annual report includes the statement (p. 88) "several industry safety leadership groups confirm that root causes for serious and high-potential incidents are often different from the majority of lower-consequence events" when discussing the move from a Total Recordable Case Frequency metric to a Serious Incidents and Fatalities Frequency metric.

[5] Management scholar Nils Brunsson has defined organized hypocrisy as a way of handling conflicts by reflecting them in inconsistencies among talk, decisions, and actions.

- The Sustainability Accounting Standards Board (SASB) establishes reporting standards on ESG and sustainability issues, primarily oriented to investors and insurance underwriters. They include 77 sector-specific guidelines. The organization's mission is "to establish industry-specific disclosure standards across ESG topics that facilitate communication between companies and investors about financially material, decision-useful information. Such information should be relevant, reliable and comparable across companies on a global basis".
- The G20 Task Force on Climate-related Financial Disclosures (TCFD) has developed a framework for reporting climate-related risks, with a focus on the transition to a low-carbon economy. The indicators proposed are designed to be integrated in firms' annual reports, rather than in their non-financial disclosures, and to allow investors to compare exposure of different firms at a global level.

These frameworks provide robust guidance concerning ethical issues such as child labour and concerning climate change impacts, but are much less mature concerning safety issues. When safety is addressed, it mostly focuses on occupational safety and health, using indicators such as the recordable injury rate for company workers, rather than on process safety and major accident hazards. As discussed above, in industrial activities exposed to the risk of major accidents, occupational safety metrics are known not to be valid predictors of the level of process safety.

The quantification of measures related to the level of major accident hazard risk is known to be a challenging problem: the standard definition of safety as freedom from unacceptable risk leads to an attempt to measure the absence of unwanted events, rather than the presence of some quality. Major accidents are (luckily!) very rare, so establishing relationships between observable features of a company's activities (for example, the amount of safety training per employee or the number of management walkarounds with a safety focus) and the final level of safety is difficult. Nonetheless, certain industry sectors have developed guidance on non-financial reporting that include robust indicators of the major accident hazards relevant to the sector. For example, IPIECA / iOGP[6] guidance on sustainability reporting for the oil and gas industry [11] has reasonably specific suggestions for presenting safety metrics along different dimensions:

- SHS-1: Safety, health and security engagement
- SHS-2: Workforce and community health
- SHS-3: Occupational injury and illness incidents
- SHS-4: Transport safety
- SHS-5: Product stewardship
- SHS-6: Process safety
- SHS-7: Security risk management
- ENV-5: Emissions to air
- ENV-6: Spills to the environment

Item SHS-6, closest to the aspects that we focus on in this analysis, is based on elements in API Recommended Practice 754 *Process Safety Performance Indicators for the Refining and Petrochemical Industries* [12] and IOGP report 456 *Process safety – Recommended practice on Key Performance Indicators*.

[6] IPIECA and IOGP are international industry associations for the oil and gas sectors. IPIECA (upstream and downstream segments of the industry) focuses on environmental and social performance, and IOGP (upstream segments) on health, safety, the environment and efficiency.

For the chemical industry, guidance on globally harmonized process safety performance reporting is provided by ICCA (International Council of Chemical Associations) and CEFIC (European Chemical Industry Council), in the context of the Responsible Care industry programme. This includes well-defined criteria for defining "tier 1" and "tier 2" process safety events. These criteria concern loss of primary containment ("leaks") or the release of energy and are based on thresholds concerning the effects on human safety and health, the direct cost due to damage from incident, the level of impact on the surrounding community, and the amount of product released (with thresholds dependent on the product). Companies are recommended to report these as an event *rate*, the ratio of events to operating hours, rather than as a count, thus allowing comparison between firms of different size.

3 Analyzing existing practice

To obtain a feeling for current practices, we have undertaken an exploratory analysis of the non-financial reporting practices of a small number of large European firms in different industry sectors that are exposed to major accident hazards. The basic question underlying our analysis is whether the information presented would be useful to a reasonably knowledgeable investor in assessing the effectiveness of the company's management of major accident hazards, and evaluating its level of exposure to the risk of a major accident. Our analysis is based on the integrated financial report, or the sustainability report if published separately and containing more detail[7], for 6 firms from three industry sectors:

- Oil and gas: Shell and Total
- Chemicals manufacturing: BASF and Linde
- Aviation: Lufthansa Group and Air France-KLM

These firms are the largest corporations (based on revenue) from these industry sectors with headquarters in Europe, according to the Forbes Global2000 list. Our analysis is based on information available in May 2021.

As a general rule, metrics used in reporting and the accompanying qualitative information should be useful both to companies in helping them manage operations and decide on resource allocation, and to investors undertaking financial analysis or making ethical judgements. For investment purposes, metrics reported should also allow comparison between companies, including across industry sectors. They should also facilitate the identification of trends in historical performance. Based on these considerations, and taking into account the criteria used for reporting on occupational safety (in particular in the GRI-G4 reporting framework), we have looked for the following information when analyzing the information present in the reports:

- Presence of a quantified indicator concerning the **level of exposure to major accident hazards** during the year. The nature of the hazard will be industry-dependent, but for example for the process industries could concern losses of containment (for example using the iOGP definitions referred to in the previous sections), or events such as collisions and runway excursions for aviation. Information on major accident hazards should be reported as a rate (per number of

[7] Many firms publish this information both in a detailed PDF report, and in summarized form on various web pages in the "investor relations" or "sustainability" sections of their websites. We have typically based our analysis on the PDF reports, as they contain the most detail. These reports are also regulated by the financial regulator of the country where the company's shares are listed.

hours worked, or amount of energy units extracted, for example) rather than as a simple number of events, as the former allows the reader to compare the performance of companies of different sizes, and also allows year-on-year comparisons when the reporting perimeter has changed (for example due to mergers or acquisitions).

- Some qualitative description of **significant incidents** related to major accident hazards experienced by the firm in the past year. This helps the reader to obtain an appreciation for the types of threats that the firm may be exposed to.
- Specific information concerning the identification of possible **cybersecurity threats to safety**, given their increasing importance over the past decade. Neither quantitative information nor detailed descriptions of countermeasures are typically disclosed concerning cybersecurity, where practitioners are accustomed to secrecy. However, we suggest that this risk should be identified among the major risks affecting the firm, and the general management process should be described, possibly with reference to the adoption of external initiatives and standards in this area (similar to the G4-15 GRI item[8]).
- Information regarding the general **safety management process** and the way in which top-level decision-makers (board, executive committee) is informed of major accident hazards and possesses relevant expertise that allows them to understand the information presented. The lack of board-level awareness and competence concerning safety issues has been identified as a significant contributing factor by several investigations into major accidents, such as the 2005 BP Texas City explosion [2].
- Annual amount of safety-related training per employee. This (regarding OHS specifically) is a GRI item, G4-LA9. It is an example of a proactive (leading) indicator concerning safety issues that is easily comparable across industry sectors.

For all quantified indicators, we believe it is helpful for information to be provided concerning previous years, to help the reader identify any trends and assess a company's performance over time.

We have voluntarily avoided a metric such as "number of pages of the report dedicated to safety", because we believe the nature and relevance of the information presented has little relationship with the quantity of material published. We also ignore questions such as whether the note from the CEO (a frequent item in annual reports) mentions safety or not, as various studies show that proclamations concerning safety made by top management are not strongly linked to real safety performance (in fact, there is a slightly negative correlation between the values declared by top-level executives, and the values perceived and stated by company employees in anonymous surveys [13]). It is worth noting that the elements we are discussing constitute only a very small fraction of company annual reports (typically, fewer than 10 pages out of several hundreds).

We make the following observations concerning Shell's sustainability report for 2020:

- Exposure to major accident hazards: tier 1 and tier 2 process safety events are reported, including a comparison with the previous year. They are reported as an absolute number rather than as a rate.
- Significant incidents: the report briefly describes the context of oil spills in Nigeria and the risks created by theft of oil and sabotage on infrastructure, and mentions a roll-over transport accident. Effects of the SolarWinds cybersecurity incident

[8] This element of the GRI standard states that companies should report the "list of externally-developed economic, environmental and social charters, principles, or other initiatives to which the organization subscribes, or which it endorses".

(compromise of a major security software supplier in 2020 which led to the installation of malicious software on the internal networks of a large number of its clients) are mentioned.

- Cybersecurity: the threat to operations is clearly identified among the risk factors. The potential link with major accident hazards is not made.
- The risk management process concerning safety risks is well-defined. Governance mechanisms in place concerning safety include a Sustainability Report Review Panel that assesses the relevance of the information presented in the annual sustainability report, and a Safety, Environment and Sustainability Committee that advises the board.
- Safety-related training: the total number of days in training is reported, but without a breakdown concerning the nature of training.

Unrelated to our criteria, we note that the report includes information on practical changes to safety policy in 2020, including a move to the use of iOGP life-saving rules (instead of in-house rules) and the adoption of a new process safety metric called *Serious Incidents and Fatalities Frequency*, two decisions that in our judgement reflect positively on the management of major accident hazards in the company.

We make the following observations concerning the "universal registration document" for Total for 2020:

- Exposure to major accident hazards: uses standardized process safety performance indicators (tier 1 and 2) and reports on environmental impact (number and volume of hydrocarbon spills). The items are reported with some historical comparison for the past two years, including information on changes to the reporting perimeter. However, they are not reported as rates so don't allow comparison for size of firm. The number of severe road accidents is also reported.
- Significant incidents: includes brief information concerning the most significant accidents, such as a leak on a hydrocarbon pipeline that led to pollution of soil and water and a major fire on an oil refinery that led to material damage.
- Cybersecurity: cybersecurity risks are clearly identified, including the risk of personal injury, property damage and environmental damage.
- The risk management process concerning safety risks is well defined.
- Safety-related training: Total days of training is used as an indicator, and "HSE training" is mentioned as a specific component of training for all employees, but the safety-related training is not broken out specifically.

We make the following observations concerning the 2020 annual report for BASF:

- Exposure to major accident hazards: the rate of process safety incidents (using the ICCA definition) is reported, including historical comparison to 2019.
- Significant incidents: a fatal accident suffered by a contractor working on a high-voltage tower in South Korea is described very briefly, and a transport accident concerning hazardous materials is mentioned.
- Cybersecurity is mentioned but without any specific discussion of the link to process safety. Certification according to ISO 27019:2018 for critical infrastructure, and collaboration with the German cybersecurity organization DCSO are mentioned.
- Safety management process: process safety and product stewardship activities are presented rather briefly.
- Safety-related training: no specific KPI. Training on safety for senior executives with relevant roles is mentioned but not quantified.

We make the following observations concerning the 2019 sustainable development report for Linde (this report, the most recent available at the time of writing, contained more information relevant to our analysis than the company's annual report):

- Exposure to major accident hazards: the tier 1 process safety event rate is reported, including a comparison with the previous 3 years.
- Significant incidents: no description of process safety or industrial safety incidents.
- Cybersecurity: cybersecurity is mentioned in passing, with no specific information on possible links with process safety.
- Risk management process: the safety management targets and activities are described, though with considerably less detail than the other reports discussed in this article. As a member of the Responsible Care programme, the company's conformance to Responsible Care Management System requirements are verified by a third party. The company's KPIs are also audited by an external auditor, though this verification seems to be focused on greenhouse gas emissions according to the ISO 14064-3 standard.
- Safety-related training: a global KPI on number of training hours per employee, as well as the number of hours of safety-related training per employee, are reported, including historical data.

As a general comment, this report (as well as the company's annual report) contains considerably less detail than those of the other companies analyzed in this article.

We make the following observations concerning the annual report of Lufthansa Group for 2020:

- Exposure to major accident hazards: no KPI nor qualitative information provided on operational safety performance.
- Significant incidents: no information provided.
- Cybersecurity is identified as a "top risk" in the annual report, but is not linked to operational safety issues. Little information is provided on risk management.
- Safety management process: little concrete information on safety management is provided.
- Safety-related training: training is mentioned multiple times in the report but not reported quantitatively, and no specific mention of safety training is made.

We make the following observations concerning the universal registration document of Air France-KLM for 2020:

- Exposure to major accident hazards: no KPI nor qualitative information is provided on operational safety (or flight safety) performance.
- Significant incidents: no information provided.
- Cybersecurity: a detailed description of the risks for the company is provided, and an incident that affected the company IT system is disclosed alongside the mitigating measures taken.
- Safety management process: activities undertaken to promote flight safety are well described in the section titled "Operational safety for stakeholders". Overall risks related to airline safety are very well described in the "Risk and risk management" section.
- Safety-related training: the number of training hours per employee is reported as a KPI, but training specifically related to safety is not reported.

4 Discussion

Before entering into a discussion of the observations made, it is important to recognize the very small sample size on which our observations are based (6 company reports). Our analysis is exploratory and does not allow us to reach any systematic conclusions. Furthermore, our analysis is based on information presented in annual reports or sustainability reports, which does not necessarily provide a representative picture of a company's ability to produce safety in its operations. Nonetheless, we are able to make a number of preliminary observations concerning the usefulness of the information available to investors and lenders in these annual reports in evaluating the level of exposure of firms to major accident hazards.

Previous work on the use of sustainability reporting by investors has found that investors have difficulties in interpreting the information presented in the reports for their decision-making. The most significant criticism is that information presented in the annual reports or sustainability reports is not comparable (92% of investors surveyed), due to differences in the reporting framework or data collection methods [14].

The companies we have studied from the oil and gas and chemical sectors use well-defined metrics such as "Tier 1 Process Safety Event". Creation of these industry-wide process safety metrics in the process industries (chemicals, oil and gas) dates back to recommendations issued by the "Baker Panel" and US CSB reports into the 2005 explosion at the BP Texas City refinery. They allow comparison of the performance of companies with respect to major accident hazards, despite the heterogeneity of their activities (particularly present in the chemicals sector).

In contrast, the airlines analyzed in this report do not report any information on major accident hazards or operational safety performance. Airlines do mention major accidents in their annual reports, when they occur, and for example the Germanwings 4U9525 crash in 2015 was reported in Lufthansa Group's annual report (though rather briefly, and from a primarily legal and financial perspective, rather than a safety perspective). However, no information is provided concerning the rate of various precursor events, such as the number of serious aircraft incidents per flight hour, the mean time between failure of safety-critical components, technical or operational anomalies requiring a deviation from the planned flight path, loss of separation distances between aircraft, runway incursions, collisions with birds, and unplanned aircraft changes. These types of indicators are typically followed by airlines and air traffic control service providers (see for example [15]), as well as by national safety authorities, but not reported publicly. This general lack of transparency concerning operational safety performance in the aviation sector (despite the extreme levels of attention paid to safety at all levels of the aviation system, and the high levels of safety performance achieved) is perhaps not unrelated to the importance of public perception of safety in continued willingness to fly.

Other observations concerning the reports analyzed:

- Several companies report process safety events as counts, rather than as rates. This makes comparison between companies and analysis of performance over time very difficult for the reader.
- Only one company in our sample reports specific quantified information on the effort allocated to safety training for employees. It is worth noting that such as metric is difficult to assess, as the initial training and continued professional development for many professionals will include many items that are related both to their

trade/profession and the specific task requirements, and to safety, making it difficult to distinguish general training from safety training.

- Few companies present information concerning safety-related incidents that they experienced and the associated consequences. Though reticence to discuss situations where an anomaly or a failure has produced negative consequences is quite natural, this type of information would be useful to investors and other stakeholders in understanding the types of risks that the company is exposed to, and could allow the company to describe how the safety barriers and risk management procedures in place allowed event consequences to be mitigated.
- The level of information provided concerning cybersecurity threats and the associated risk management process is very variable, despite the very high and increasing importance of these risks today.

5 Conclusions

Information on firms' exposure to major accident hazards and the associated management processes implemented is an important input to the decisions of investors, lenders and insurance companies on allocating financial capital. Indeed, these hazards can lead to very significant financial consequences for firms, as illustrated by the destruction of financial value of BP after the 2005 Macondo catastrophe, and the quality and effectiveness of company safety management processes raise significant ethical concerns that may be significant to some investors.

Our exploratory survey of a small number of the annual reports of large public companies operating in high-hazard industry sectors suggests that there are significant opportunities for improvement of the information on exposure to major accident hazards, to allow investors to appreciate the types of hazards a company is exposed to, the way in which they are managed by the company and integrated in its strategic decision-making, and the resulting safety performance. In particular, some industries such as airlines do not provide material elements on their operational safety, and some companies operating in other sectors present information in a manner that makes it difficult to compare performance of different firms and to assess trends over time. Resolution of these weaknesses would be helped by discussions on an ESG corporate reporting framework that comprises some standardized elements on major accident hazards.

References

1. Lee Y-G, Garza-Gomez X, Lee R. Ultimate costs of the disaster: Seven years after the Deepwater Horizon oil spill. Journal of Corporate Accounting & Finance. 2018;29:69–79.
2. USCSB. Investigation into the refinery explosion and fire at BP Texas City, March 2005 [Internet]. U.S. Chemical Safety; Hazard Investigation Board (CSB); 2007. Available from: https://www.csb.gov/assets/1/19/CSBFinalReportBP.pdf
3. OECD. OECD guidelines for multinational enterprises. OECD Publishing; 2011.
4. Strauss E. Is everything securities fraud? [Internet]. Duke Law School; 2020. Available from: https://ssrn.com/abstract=3664132
5. Esty D, Cort T, Strauss D, Wyatt K, Yeargain T. Toward enhanced sustainability disclosure: Identifying obstacles to broader and more actionable ESG reporting [Internet]. Yale Center for Environmental Law & Policy; 2020. Available from: https://envirocenter.yale.edu/toward-enhanced-sustainability-disclosure-identifying-obstacles-broader-and-more-actionable-esg
6. Bebbington J, Unerman J, O'Dwyer B, editors. Sustainability accounting and accountability. Routledge; 2014.

7. O'Neill S, Flanagan J, Clarke K. Safewash! Risk attenuation and the (mis)reporting of corporate safety performance to investors. Safety Science. 2016;83:114–30.
8. Brunsson N. The organization of hypocrisy: Talk, decisions and actions in organizations. Copenhagen Business School Press; 2003.
9. Evangelinos K, Fotiadis S, Skouloudis A, Khan N, Konstandakopoulou F, Nikolaou I, et al. Occupational health and safety disclosures in sustainability reports: An overview of trends among corporate leaders. Corporate Social Responsibility and Environmental Management. 2018;25(5):961–70.
10. Lindgren C, Huq AM, Carling K. Who are the intended users of CSR reports? Insights from a data-driven approach. Sustainability. 2021;13(3).
11. IPIECA. Sustainability reporting guidance for the oil and gas industry. Module 5 Safety, health and security. IPIECA / iOGP / API; 2020.
12. API. Recommended practice 754: Process safety performance indicators for the refining and petrochemical industries. American Petroleum Institute; 2016.
13. Sull D, Turconi S, Sull C. When it comes to culture, does your company walk the talk? MIT Sloan Management Review. 2020.
14. D'Aquila JM. The current state of sustainability reporting: A work in progress. The CPA Journal. 2018;88(7):44–50.
15. Rose A. Measuring operational safety in aviation. Aircraft Engineering and Aerospace Technology. 2006;78(1):26–31.

New approaches for Autonomous Vehicles certification: learning best practices from Nuclear Reactor Safety

Maria Cristina Galassi, Biagio Ciuffo and Anastasios Tsakalidis, Lorenzo Di Cesare and Calogero Sollima, European Commission, Joint Research Centre (JRC), Ispra, Italy, Maria-Cristina.GALASSI@ec.europa.eu, Biagio.CIUFFO@ec.europa.eu, Anastasios.TSAKALIDIS@ec.europa.eu, Lorenzo.DI-CESARE@ec.europa.eu, Calogero.SOLLIMA@ec.europa.eu

Marco Sangiorgi, European Commission, Joint Research Centre (JRC), Petten, The Netherlands, Marco.SANGIORGI@ec.europa.eu

Antony Lagrange, European Commission, Directorate General for Internal Market, Industry, Entrepreneurship and SMEs, Mobility Unit, Avenue d'Auderghem 45, 1049 Brussels, Belgium, Antony.LAGRANGE@ec.europa.eu

Abstract

The introduction of driving automation in the road transport sector also brings new challenges that require solutions, both in technical but also regulatory terms. As vehicle automation levels rise, the mismatches between innovation/technology and regulation are emerging as gaps that need urgently to be filled. Nevertheless, a series of the new challenges that emerge within the transport sector have already been tackled partially or fully in other sectors, with the most prominent examples considered in this paper coming mainly from aviation, railways and nuclear reactor safety. The present paper summarises relevant solutions and good practices from these sectors that could lead to synergies with a catalytic potential towards the transition of road transport to higher levels of automation and eventually full autonomy.

1 Introduction

The transport sector is undergoing a radical transition towards higher levels of automation and connectivity. Driving automation brings the promise to tackle several negative externalities of road transport, such as congestion, pollutant emissions and road accidents, with the potential to also improve related social issues as urban accessibility and social inclusion [1]. Indeed, increasing levels of automation could significantly improve road safety since human error is recognised as the cause for most car accidents [2].

Automated driving technology is developing at an unprecedented fast pace and a quick response is needed from regulators in order not to slow-down innovation and at the same time ensure the access to the market of safe autonomous vehicle (AVs) [3]. The first regulatory solutions have been put in place in the last two years in order to cover the most urgent needs, but a suitable framework for AVs type approval is needed in the longer term. However, the conventional physical testing alone is not anymore sufficient to evaluate the AVs performance in the uncountable situations encountered in real world, and innovative certification approaches are needed to adequately assess AVs safety.

In the last decades safety-critical automated systems have been already introduced in many other application domains, ranging from transport (aerospace, rail, maritime) to agriculture, healthcare and nuclear plants. Aviation and nuclear energy production represent the sectors with the strongest safety culture, where robust safety analysis and assessment approaches have been developed and validated throughout decades of

operational experience. The automotive sector can build on the existing knowledge in those sectors and elaborate on the applicability of already available methodologies.

The objective of this paper is to highlight the possibility of establishing synergies with safety methodologies and best practices currently applied to safety in these fields, according to the needs identified by ongoing pre-normative research for AVs safety certification at the European Commission's (EC) Joint Research Centre (JRC).

2 Status of EU Regulation on Autonomous and Automated Vehicle technologies

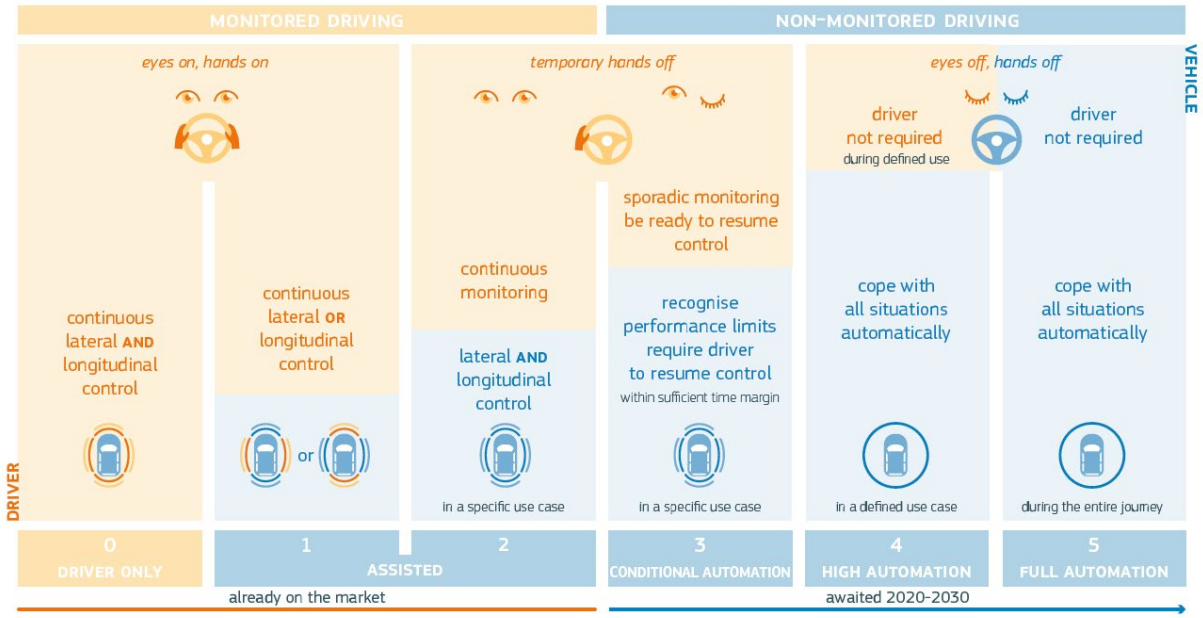
2.1 European Union Approach to Automated Vehicles Approval

The EC adopted a progressive approach to regulate AVs, first of all, supporting on road large scale testing in the European Union (EU) to foster experimentation and at the same time fuel the regulatory discussion.

Then the EC issued Guidelines [4] to harmonise the application of the exemption procedure through Member States (MSs), allowing innovation through the exception scheme allowed under the current legislation [5]. The EC Guidelines introduced minimum requirements on what should be demonstrated by the manufacturer at type approval, and an intermediate step in the approval procedure: once the vehicle is approved in one MS, a Technical Committee will evaluate the certification before its validity is extended at EU level.

Paving the way to driving automation, the EC adopted in 2019 the new EU vehicle General Safety Regulation (GSR) [6], proposed as part of the 3rd Mobility Package, which provides the legal framework for Connected and Automated Driving. The new GSR will be applicable starting mid-2022 and the technical measures for its implementation are expected to be ready by the end of 2021.

Figure 1. SAE driving automation levels.



Source: Own elaboration based on SAE J3016 [7].

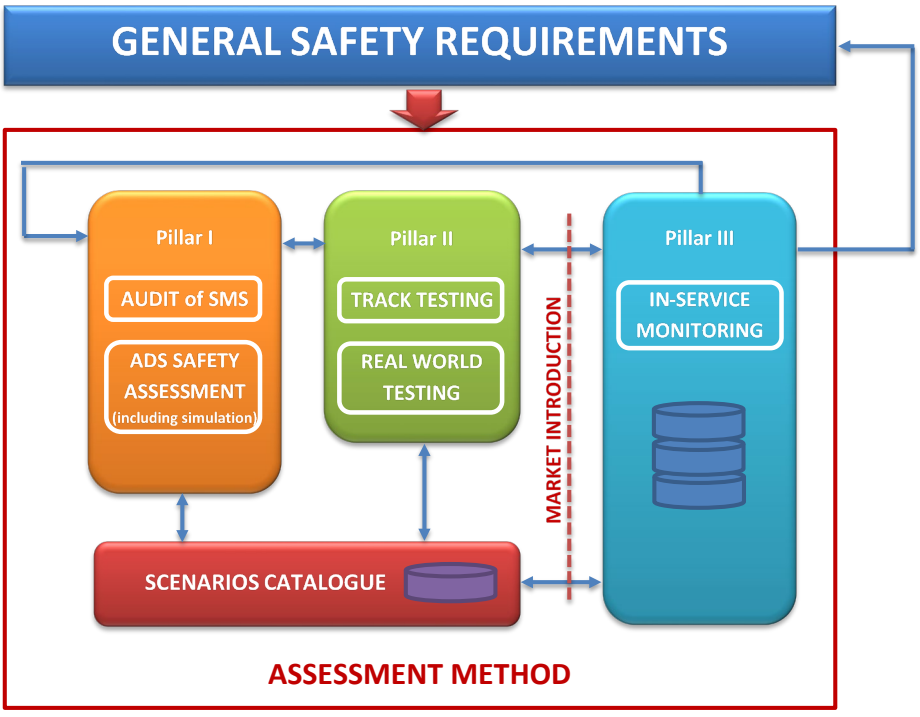
The JRC is supporting the development of technical requirements and new assessment methods necessary for implementing the GSR, with focus on Society of Automotive

Engineers (SAE) levels 3 and 4, what we can refer to as "automated driving" (see Figure 1).

The proposed EU approach consists of three pillars, or phases (Figure 2):

1. The first phase includes an independent audit of the manufacturer Safety Management System (SMS), and the safety assessment of the vehicle. The audit addresses the company maturity in terms of processes put in place to ensure the safety of their products, while the safety assessment concerns the specific Automated Driving System (ADS) under approval and is done through the documentation package provided by the manufacturer to the authority.
2. The second phase consists in the verification through physical testing run by the authority. Also builds on two separate steps: firstly, the AV is tested in a controlled environment (track/proving ground), where critical situations can be addressed safely; then an on-road test will follow in order to evaluate the normal operation of the vehicle in real life conditions.
3. Finally, the third phase consists in the in-service monitoring, so that the assessment of the AV safety performance will continue also after its market introduction. This monitoring exercise has three objectives: to confirm the safety assessment done at type approval; to identify new safety-critical situations (scenarios); to derive lessons learned from the operational experience and share them in the form of safety recommendations.

Figure 2. EU regulatory approach to automated vehicles approval.



Source: own elaboration.

The scenarios catalogue, collecting all relevant safety-critical situations, represents a fundamental element of the new assessment method, as common reference framework for both manufacturers and authorities: the manufacturers will consider it as baseline set of scenarios to be considered during the ADS validation; the authority will refer to the

scenarios catalogue to assess the safety demonstration submitted by the manufacturer and to select the scenarios for the independent verification testing.

2.2 UNECE advancements in regulating AVs

Efforts in the definition of new assessment and test methods have been done also at global United Nations (UN) level [8] taking into account auditing approaches as well as different levels of testing (e.g. simulation & virtual testing, proving ground and field tests), and including operational feedback from real life experience. Indeed, the EU approach for automated vehicles approval described above was developed based on the multi-pillar approach discussed within the Informal Working Group (IWG) on Validation Methods for Automated Driving (VMAD). Vice versa, the EC also fed inputs to the same VMAD discussion with the development of the audit and assessment pillar of the simulation & virtual testing, and the proposal to include the in-service monitoring pillar.

Several questions are still open, starting from how to balance the different approaches in order to ensure an appropriate level of safety [9]. A first concrete step in this direction was done in 2020 with the adoption of the UN Regulation 157 (UNR157) [10], in force since 22 January 2021. The UNR157 addresses the specific use-case of Automated Lane Keeping Systems (ALKS) for highway low speed applications (below 60 km/h), and is currently being amended to also cover lane change and higher speed (up to 130 km/h). At the same time, work is ongoing in parallel to define safety requirements and a generic validation approach for automated vehicles valid for all use-cases.

2.3 Existing Gaps

The previous paragraphs introduced how driving automated is posing new challenges not only to technological advancements but also to regulators: new legislative approaches are needed, that might address the vehicle approval in more flexible but still comprehensive and robust way. This means that not only new assessment methods have to be defined, but also the new tools and expertise needed by the authority.

Table 1 presents a summary of the identified gaps and needs to be systematically addressed for the development and implementation of the new AVs type approval framework, together with a relative priority based on the importance and urgency to address each item.

3 How expertise from other transport sectors can help

Many of the new regulatory challenges that are emerging with driving automation have already been tackled partially or fully in other transport sectors, with the most prominent examples coming mainly from aviation and railways. These sectors provide a series of solutions and good practices that can lead to synergies with a catalytic potential towards the transition of road transport vehicles to higher level of automation and eventually full autonomy.

The aviation sector has a high potential to contribute to synergies that will support the AV safety certification since it is the transport sector that has reached the highest safety levels, while automated technologies and systems have been already contributing to this aim since decades [11]. Taking a closer look into the aviation sector technologies and regulation used to ensure safety could have a supporting role for the update of the regulatory framework covering AVs type approval by extending good practices and aviation processes to road transport. In particular, five areas were identified by Santoso et al. [12] where knowledge transfer would be beneficial:

- Taxonomy, covering the establishment and use of the correct nomenclature to ensure a common understanding and high level of safety avoiding misinterpretations;

Table 1. Needs to implement the EU regulatory approach for automated vehicles approval.

Item	**Description**	**Identified Needs**	**Priority**
Taxonomy	Standard safety-related terminology	Uniquely define standardised safety-related terminology.	++
Schedule	Type approval prior to market introduction	The dialogue between manufacturer and authority should start at an early stage of the AV development	++
Safety Level	Requirements on acceptable safety level	Define minimum requirements for safe AV. Requirements on mitigation strategy.	+++
Audit	Audit of the safety management system	Guidance on how to establish and run an effective safety management system. Criteria for auditing timing, procedure and evaluation (pass-fail criteria). Requirements for auditors' qualification.	++
Safety Assessment	Safety assessment of the automated driving system	Customised methodologies for ADS risk analysis. Standardised reporting of the safety demonstration. New competences to be developed by authorities on AVs safety assessment (including simulation and virtual testing).	+++
Testing	Verification testing by authority	Procedures for track and on-road testing. Best practices for the selection of simulation and virtual testing tools. Methodologies for simulation tools and tool-chains validation.	+++
In-service monitoring	Data monitoring and reporting after market introduction	Reporting criteria and obligations. Responsibility for data collection, storage, analysis. Data access and privacy protection. Preparation of safety recommendations.	++
Scenarios	Common Scenarios Catalogue	Not limited to traffic scenarios. Criteria for the identification, selection and relevance of scenarios. Criteria for catalogue coverage and completeness.	+++
HMI	Human Machine Interface and Interaction	HMI standardisation. Interaction with impaired users.	+++
Connectivity	Communication and Cooperation	Minimum requirements on connectivity.	+
Infrastructure	Role of infrastructure and infrastructure managers	Requirements on infrastructure and infrastructure managers.	+
Traffic rules	National traffic rules	Update and harmonisation of traffic rules across MSs to facilitate AVs deployment	++

Source: Own elaboration.

- Safety, on the establishment of adequate requirements and methodologies to address system safety;
- Design, related to the appropriate requirements covering the new technologies and systems that will be incorporated in vehicles with higher levels of automation;
- Human-machine interface (HMI) and interaction, related to requirements necessary to ensure safe interaction and interface between humans and AVs, including standardisation of safety-critical HMI elements;
- Type-approval process, related to the processes followed to approve the new product and the level of involvement of the authority vs the manufacturer.

In particular, aviation best practices to cover the total lifecycle for safety-relevant systems could also be applied in the automotive sector. The mechanism put in place for operation safety data collection and sharing through the European Co-ordination Center for Accident and Incident Reporting Systems (ECCAIRS) portal and has already been extended to railway and maritime sectors [13].

Many analogies can also be found with challenges addressed in the railway sector [14], from where useful applications and practices can be identified, with a potential applicability to the AVs type approval:

- in the approach to certify and monitor the implementation of the Safety Management System, including legal requirements and competences defined for the authorities;
- in the establishment of well-defined requirements for infrastructure and infrastructure managers, including maintenance;
- in the reporting mechanism for the operational experience.

An interesting commonality between aviation and railway sector is the presence of a dedicated EU agency in charge of providing guidance and requirements for safety, involved in the certification process, and responsible for analysing the safety performance during operation and share lessons learned at European level.

4 Learning Best Practices from Nuclear Reactor Safety

Potential synergies and best practices to support the development of AVs safety certification were also identified in the nuclear energy sector [15]:

- the Probabilistic Safety Assessment (PSA) methodology currently applied to address Nuclear Reactor Safety (NRS) and licencing (i.e., approval) could represent a good starting point also for the automotive sector;
- the expertise in NRS could provide guidance on the comparison of different risk assessment practices also used in other sectors (e.g., chemicals industry, railway transport), suitable for application to complex systems including autonomous vehicles;
- the approach implemented for collection of operational data and storage of the information on ad-hoc database (the European Clearinghouse on Operating Experience Feedback for Nuclear Power Plants [16]) to enhance safety through improvement of the use of lessons learned.

Indeed, PSA is a systematic and comprehensive approach aiming at addressing all relevant events and scenarios covering complete risk. Events are excluded based on predefined cut off low probability/frequency (e.g., 10^{-6}/yr), that means are neither plausible, nor relevant. This methodology could therefore be applied also in the automotive sector to identify the relevant scenarios to be included in the common scenarios catalogue. Discarded scenarios present some minor residual risk, and are not addressed in the design phase or by regulatory requirements.

Linked to the identification of risks, another best practice from NRS is related to the definition of a standardised scale to identify the safety relevance of accident scenarios in terms of potential damages to humans and the environment [17]. At present, different severity scales are used in the automotive sectors for accidents classification, depending on the context in which the analysis is performed (e.g., medical, insurance, or legal investigation).

Additional interesting concepts from NRS that should be further considered for application to the automotive sector are:

- the iterative approach adopted for safety reporting at the licencing, allowing the dialogue between authorities and applicants to start at an early stage before the approval request;
- the defence in depth approach, to create multiple independent and redundant layers of protection to failures and accidents – considering of course limitations due to vehicle dimensions;
- the definition of requirements not only on the prevention but also on the mitigation (strategy and measures) of accident consequences.

To be noted that also the definition of accidents and incidents in the automotive sector should probably be extended to include critical events caused by failures or other anomalies besides traffic conditions (i.e., collisions).

5 Conclusive remarks and way forward

The paper presented an overview of the status of EU Regulation on autonomous and automated vehicles, and of the identified open points to be addressed to enable the implementation of the new type approval approach. Indeed, as vehicle automation level rises, increasingly significant mismatches between innovation/technology and regulation emerge and need to be tackled consistently.

Nevertheless, a series of the new challenges that emerge within the transport sector have already been tackled partially or fully in other sectors. In particular, a series of solutions and good practices from nuclear, aviation and railway sectors have been summarised in this paper that could catalyse the regulatory transition towards automation of road transport.

Relevant lessons learned on taxonomy, safety concepts and safety management, human-machine interface and interaction, in-service monitoring and reporting, and on the approval process itself can be derived from the aviation and railway sectors. In addition, best practice on infrastructure requirements and management can also be drawn from the railway sector.

Relevant guidance can also be derived from nuclear reactor safety, particularly for what concerns the application of probabilistic methodologies for safety assessment, for the selection of risk assessment approaches most to address the complexity of automated driving systems, and for enhancing safety through improvement of the use of lessons learned from operating experience feedback.

In all three sectors considered, the certification process is dealt by (or with the support of) a supernational authority, which is also responsible for defining the reference safety objectives and providing guidance on safety-related matters. This approach guarantees independence and a harmonised safety level at EU level, although more complex and more demanding.

The performed study highlighted that collaboration is essential to tackle the big challenges ahead of AVs regulation, and not only between automotive stakeholders, but also with expertise and lessons learned from other domains.

Acknowledgements

The authors would like to acknowledge the EU institutional funding for the possibility to establish the presented research activities and for the resources made available. Special thanks are due to colleagues from the EU Railway Agency for their guidance and to all colleagues across different JRC Units for their valuable contribution.

References

1. Alonso Raposo, M. et al. (2019) *The Future of Road Transport - Implications of Automated, Connected, Low-Carbon and Shared Mobility*. Publications Office of the European Union, Luxembourg, https://doi.org/10.2760/668964.
2. Milakis, D., Van Arem, B. and Van Wee, B. (2017) Policy and Society Related Implications of Automated Driving: A Review of Literature and Directions for Future Research. *Journal of Intelligent Transportation Systems: Technology, Planning, and Operations*, vol. 21, no. 4, pp. 324–348. https://doi.org/10.1080/15472450.2017.1291351.
3. Fagnant, D. J. and Kockelman, K. (2015) Preparing a Nation for Autonomous Vehicles: Opportunities, Barriers and Policy Recommendations. Transportation Research Part A: Policy and Practice, vol. 77, pp. 167–181. https://doi.org/10.1016/j.tra.2015.04.003.
4. European Commission (2019) Guidelines on the Exemption Procedure for the EU Approval of Automated Vehicles - Version 4.1; available at: https://ec.europa.eu/docsroom/documents/34802 (last accessed 30 May 2021).
5. European Union (2018) *Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles*.
6. European Union (2019) *Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users*.
7. SAE (2021) *SAE J3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, J3016_202104*.
8. GRVA (2021) New Assessment/Test Method for Automated Driving (NATM) - Master Document, *ECE-TRANS-WP29-2021-61e, WP29 184th session, 22-24 June 2021*.
9. GRVA (2019) Framework Document on Automated/autonomous vehicles, Informal document WP.29-177-19, *WP29 177th session, 12-15 March 2019*.
10. United Nations (2020) *UN Regulation No. 157, Uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems, ECE/TRANS/WP.29/2020/81*.
11. European Union (1985) *Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products*.
12. Santoso C. and Rusciano, E. (2019) *Autonomous Vehicles – The new frontier of Automotive Industry. How to address certification challenges in order to boost the autonomous vehicle market from a Vehicle Authority's perspective*, courtesy of RDW.
13. ECCAIRS (2021) *The European Co-ordination Center for Accident and Incident Reporting Systems*; available at: https://aviationreporting.eu/ (last accessed 31 May 2021).
14. Galassi, M.C., Lagrange, A., Guido, P., Mele, R., Ciuffo, B., Piron, O. and Malfait, W. (2021) *ERA – JRC Workshop on Safety certification and approval of automated driving function: Analogies and exchange of best practices between railway and automotive transport sectors*, Publications Office of the European Union, Luxembourg, https://doi.org/10.2760/96772.

15. Sangiorgi, M., Galassi, M.C., Simic, Z., Peinador Veira, M. and Kröger, W. (2020) *Workshop on Best Practices from Nuclear Reactor Safety relevant for AVs safety certification*, European Commission, Ispra, 2020.
16. European Commission (2021) *The European Clearinghouse on Operating Experience Feedback for Nuclear Power Plants*; available at: https://clearinghouse-oef.jrc.ec.europa.eu/ (last accessed 31 May 2021).
17. International Atomic Energy Agency (2021) *The International Nuclear and Radiological Event Scale (INES)*; available at: https://www.iaea.org/resources/databases/international-nuclear-and-radiological-event-scale (last accessed 31 May 2021).

List of abbreviations and definitions

ADS	Automated Driving System
ALKS	Automated Lane Keeping Systems
AV	Autonomous Vehicle
EC	European Commission
ECCAIRS	European Co-ordination Centre for Accident and Incident Reporting Systems
EU	European Union
GSR	General Safety Regulation
IWG	Informal Working Group
JRC	Joint Research Centre
MS	Member States
NRS	Nuclear Reactor Safety
PSA	Probabilistic Safety Assessment
SAE	Society of Automotive Engineers
SMS	Safety Management System
UN	United Nations
UNR157	UN Regulation 157
VMAD	Validation Methods for Automated Driving

GRIP on robot safety with collaborating data-systems

Coen van Gulijk, TNO Healthy living; University of Huddersfield; Delft University of Technology, coen.vangulijk@tno.nl, c.vangulijk@hud.ac.uk, c.vangulijk@tudelft.nl

Wouter Steijn, Jeroen van Oosterhout, Joeri Willemsen, Marit Wilms & Dolf van der Beek, TNO Healthy Living, wouter.steijn@tno.nl, jeroen.vanoosterhout@tno.nl, joeri.willemsen@tno.nl, marit.wilms@tno.nl, dolf.vanderbeek@tno.nl

Abstract

This paper addresses a practical approach in the digital transformation of safety management systems for robot safety. An integrated data-environment is designed to collect and collate knowledge to support day-to-day safety operations for manufacturers the latest generation of AI-enabled robots and cobots on their shop floor. A special problem is the orchestration of different digitally enabled sub-tasks of safety management as well as a customer demand to keep the operation of the system as simple as possible. Along with restrictions on operations and cost, a three step method is developed to canvas the digital environment and this paper focusses on one of these steps: the development of a generic BowTie for data orchestration.

1 Introduction

People in workplaces are confronted with the ingress of cobots or cooperative robots. Whilst there may be benefits in utilizing the strong points of machines (e.g., accuracy and speed) and of human workers (e.g., flexibility and creativity) in cooperative tasks on the work floor there seems to be relatively little attention for Occupational Health and Safety (OSH) concerns. It is not that safety is not considered in the construction of the cobot; in fact all machines need to adhere to the Machine Directive (2006/42/EC)[1] before they may be used in the workplace. That directive stipulates that risk analyses need to be done and safety measures need to be put in place to make the machine safe for use, but it there is no requirement to share the risk analysis with end users. After the cobot is placed the workplace the safety regime is handed over to the Framework Directive (89/391/EEC)[2] which deals with safety for workers at the workplace. This requires an independent risk assessment of the machine in-situ in the workspace but since the risk analysis of the machine is not shared it is entirely independent and often lacks the sophistication of the risk analysis of the machine.

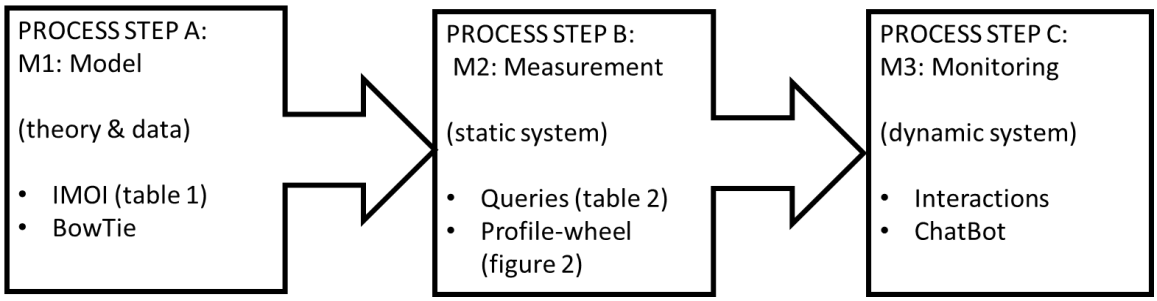
This work develops a risk analysis framework that offers a consistent risk analysis for cobots in the workplace and facilitates linkage to digital safety management systems. We call the framework GRIP - Guarding Robot Interaction Performance - a digital safety management system under development for human-robot interactions (HRI) in an Industry 4.0 setting. GRIP has a strong emphasis on the human factors (HF) and occupational safety and health (OSH) side of the interaction. In GRIP the knowledge framework draws from different sources to utilize practical, scientific and legal information in a single tool. The framework builds on our previous works where we describe the development of the three elements of GRIP: the safety meta-model, the digital measurement instrument, and a monitoring system. This paper focuses on the progress of the work and reports about an element of process step 1: the development of a BowTie.

2 Development of the GRIP Framework

The wider framework of GRIP is based on three foundational elements mainstream approaches. The approach is based on HRI-GRIP: a input-mediation-output (IMOI) model [3]. Originally developed to model teamwork, IMOI identifies the relevant characteristics of each team member that affect the cooperation, the states that emerge from the interaction and the eventual output. We apply the framework of IMOI on the 'teamwork' between operator and robot and have expanded upon the model to provide a structured ontology of relevant characteristics that affect the outcomes of HRI. The third approach implemented in GRIP concerns the legislation in relation to machine safety: the Machine Directive (2006/42/EC) [1]. The machine directive collates all safety requirements for machines and working safely with machines. The novelty of the paper is in the approach to digital orchestration of various interests within the safety management system as well as the attention to end-user requirements in a BowTie.

The framework comprises of a three-step approach to the development of integrated digital safety solutions and to orchestrate the data flows through api's (and prototypes thereof). Figure 1 illustrates the process steps. This approach facilitates the development of a digital ecosystem of interacting software systems.

Figure 1. GRIP framework development in 3 steps.



3 Theoretical Background process step A

This work is based on the Input-Moderation-and provide an in-depth description of the HRI model at the foundation of GRIP [3]. It is beyond the scope of this work to revisit that paper in its entirety but the key elements are summarized here.

Fundamentally, the work is based on a human-robot interaction model with the aim to determine the level of safety for human-robot interactions that takes the relevant aspects of the robot and the environment into account.

In order to model these factors, the approach uses the input-mediation-output (IMOI) approach [4]. The input (I) concerns characteristics of the human worker, the robot, and the environment and interlinked with Reason's [5] taxonomy for safety influencing factors: human, technical and organizational aspects. The mediators (M) are the conditions or states that emerge from the interaction as a result of the input factors, and which will affect the output. The output (O) concerns the desired results of the interaction (I) and which can directly affect the input for the next interaction. It is worth noting that, IMOI is a versatile model that not only allows a linear relationship between the different factors, but also assumes that, for example, mediator factors could affect each other.

Across that initial classification is a horizontal separation that divides the safety factors based on their effect on the human factors (HFI). For this we used a classification into three parts: hardware, software and mindware elements in order to highlight the HFI and OSH aspects. Looking at the input factors, hardware refers to the physical factors and capabilities of the human worker (e.g., PPE or health) or (technical) elements affecting this

of the robot (e.g., lightweight or absence of sharp edges) and the environment (e.g., housekeeping). Software input factors are about the cognitive factors and situational awareness of the human worker (e.g., vigilance or experience) or elements affecting this of the robot (e.g., interface or complexity underlying algorithms) and the environment (e.g., time pressure or noise). Mindware input factors are about the experience and perception of the interaction by the human worker (e.g., trust or attitude) or the elements affecting this of the robot (e.g., appearance or consistency) and the environment (e.g., temperature or resource availability).

Crossing those two classification yields a matrix of areas of interest, as shown in table 1. These mediators ultimately affect the outcome of the interactions of humans with robots and the production outputs and facilitate the identification of risks in human-robot collaborations. For instance, if the human worker loses situational awareness to a certain degree, an incident becomes more probable and the interaction is not safe. This matrix offers a systematic overview of concerns for safety and productivity in human-robot interactions. In that way, the model provides the basis for safety concerns and risk influencing factors for working with robots and cobots and shapes our holistic safety meta-model M1. The next challenge was to make the matrix 'practical' for real work environments. For that we chose the BowTie.

Table 1. IMOI risk influencing factors for human-robot interactions

	Human Input	**Robot Input**	**Environment Input**	**Mediator**	**Output**
Hardware	*Physical factors and capabilities of the human to perform during the interaction*	*Characteristics affecting the physical factors and capabilities of the human*	*Characteristics affecting the physical factors and capabilities of the human*	*Physical workload and workflow during interaction*	*Safe and Efficient HRI*
Software	*Cognitive factors and capabilities of the human to oversee the interaction*	*Characteristics affecting the cognitive factors and capabilities of the human*	*Characteristics affecting the cognitive factors and capabilities of the human*	*Cognitive workload and situational awareness of the human during interaction*	
Mindware	*The human experience and perception of the interaction*	*Characteristics affecting the human experience and perception of the interaction*	*Characteristics affecting the human experience and perception of the interaction*	*Perceived workload, job quality and complacency by human during interaction*	

4 Practical implementation of process step A

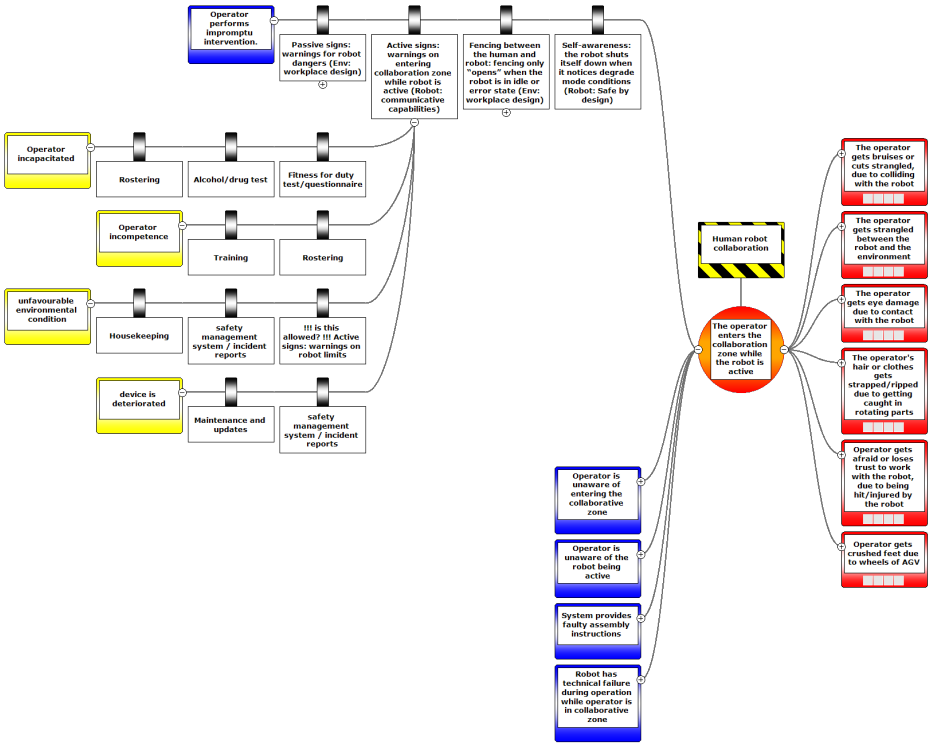
Although the theoretical framework offers the necessary aspects to take into account they are not very practical in a work environment; especially if local safety managers have to work to them a translation into a known safety model was called for. In this case a BowTie was chosen. The use case is an order picker cobot that collects various orders from clients from boxes and puts them into crates for shipping. The system works together with humans when non-standard items have to be added to the crate or when the boxes have to be replaced (by humans) because they are empty. The point-in-case is the event that a worker (unknowingly) enters the collaboration area and a risk of collision arises.

A BowTie connects relevant causes and consequences of a defined risk space which offers handles for safety experts to manage the risk. It creates linkages to responsible persons, documents, tasks and incidents to support safety management in a systematic way. The bowtie approach used in this work is based on the CCPS handbook 'BowTies in Risk Management' which was created as a joint effort of the Centre for Chemical Process Safety and the Energy institute in 2018 [6]. It is beyond the scope of this paper to describe the BowTie that was design for this project in its entirety. Rather, the method for developing the bowtie and the help of the IMOI model for setting it up is described. Figure 2 supports this exercise by showing parts of the practical work-place bowtie. It is explained by treating the individual parts of a BowTie.

A BowTie consists of eight elements. They are: hazard, top event, threat, consequences, barriers, degradation factors and degradation controls (refer to figure 2).

- The hazard is something with the potential to cause harm that stems from the normal business process performed by the organization or industry. In our use case it is the human-cobot collaboration that is the normal business process; it is indicated with a square box with apoplectic colours in a barricade-tape pattern.
- The top event, which could also be known as loss-of-control event or critical event is the central node of the bowtie. It captures the moment that control over the hazard is lost. In this case it is the person entering the collaboration zone when the robot is active. The top event is typically a red circle with a text box.
- Consequences are the adverse outcomes that the top event could lead to and they are placed on the right-hand side of the BowTie. Typically, they include harm and damage but other forms of adverse outcome might be considered as well. In this case, varying types of trauma are described but by using the IMOI framework a different type of consequence was identified as well: fear of working with the robot after an event. Consequences are depicted as red squares.
- Threats are the potential reasons for loss of control. This is where the IMOI is used most effectively in the sense that the matrix in table 1 offers a framework to consider scenario's that wouldn't otherwise be detected. Being caught unawares and poor human-machine communication were identified in this way. Threats are indicated in blue boxes on the left-hand-side of the top event. As there is one central top event and multiple threats to the left and multiple consequences to the right, the diagram starts to resemble a bowtie, hence the name.
- Barriers covers a wide variety of safety controls designed to stop the causal paths within the bowtie. Barriers can be physical or non-physical measures to prevent or mitigate unwanted events. Some of the barriers follow from standard practices on the workplace (such as partial fencing) but they also fit a box in table 1: it is an environmental hardware input. Other barriers were found by making implicit workplace uses explicit; e.g. passive warnings were always on the robot as a robot mindware input but wasn't explicitly managed.
- A degradation factor is a condition, that can reduce the effectiveness of barrier to which it is attached. It does not cause the top event but buy lowering the effectiveness of the barrier it can increase the likelihood of adverse consequences. They are depicted as yellow boxes. The BowTie shown here shows that for a robot mindware barrier (active warning), the human mindware and software need to be in order in the shape of adequate training and fitness.
- To prevent the degradation factor from lowering the effectiveness of a degradation control is put in place. As they may be similar to barriers they are sometimes referred to as escalation barriers. Here too, the IMOI model is an efficient method to identify that standard work practices that are place are taken up as important parts for safety management and identifying interactions that weren't identified before. Rostering is an avid example of that.

Figure 2. Part of the BowTie for an order-picking robot.



5 Next steps in the development of GRIP

The key factors of the HMI-IMOI model presented in a recognizable bowtie format form the basis for the sensible development of measurement (M2) software and monitoring software (M3).

With a basic BowTie it becomes relatively straightforward to design a digital questionnaire that functions as a safety measurement (M2). The questionnaire addresses the performance of various parts of the BowTie by interrelating key elements of the BowTie (such as the presence of certain threats in figure 2) with underlying HMI-IMOI factors (from table 1). This provides insight into what barriers are performing better than others and which underlying influencing factors (from the HMI-IMOI model) are the most troublesome. The outcomes are be shown in a dash-board providing an instant overview of the current safety state of the human-robot interaction in the workplace. The software is still under development at the time that his paper is writ but the basic questionnaire for this bowtie (and two others) is limited to 108 questions because the IMOI framework makes it possible to ask generic questions about underlying factors that influence multiple parts of the Bowtie.

One solution for a more permanent monitoring system (M3) is a ChatBot. In this case a worker can enter their concerns during their working day and the ChatBot helps identify which barriers are involved in the concerns the worker has. This software is currently under development with a commercial partner and the experiences will be reported later.

6 Conclusions

This work reports on the progress of our work on a risk analysis framework that offers a consistent risk analysis for cobots in the workplace and facilitates linkage to digital safety management systems: GRIP - Guarding Robot Interaction Performance. The paper explains

how prior work for a human-machine interaction model is used as the theoretical foundation for the development of accessible digital tools (some existing, some newly developed) to create a coherent system of digital tools to facilitate better, easier and more accessible safety management. The first, and crucial, step is described here: to translate a conceptual safety framework (the HMI-IMOI model) into a practical safety management tool (the BowTie). This process is explained here and it shows that a solid theoretical foundation helps make a better safety bowtie that safety managers can work with.

This works shows that a strong scientific foundation in the shape of a theoretical model makes it easier to design sensible digital safety solutions to work in practice. We believe that it even helps making the actual software solutions relatively straightforward and does not burden the safety manager, or the workers, with elaborate theoretical knowledge.

Acknowledgements

The authors would like to thank Eugene van Someren from TNO's RAPID team in his support in the development of software for the questionnaire. We are also grateful for Smart Robotics and Pilz to provide use cases and expressing their needs for the use-case.

References

1. Directive 2006/42/EC of the European Parliament and the council of 17 May 2006 on machinery, and amending Directive 95/16/EC.
2. Directive 89/391/EEC of the council of the European communities of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers.
3. Ilgen, D. R., Hollenbeck, J. R., Johnson, M., & Jundt, D. (2005). Teams in organizations: from input-process-output models to IMOI models. Annu Rev Psychol, 56, 517-543. doi:10.1146/annurev.psych.56.091103.070250
4. Steijn, W., van Oosterhout, J., Willemsen, J. & Jansen, A. (2020). Modelling Human-Robot Interaction to Optimize Their Safety, Sustainability and Efficiency: Identifying Relevant Characteristics. *In proceedings of ESREL2020-PSAM15, September 2020.*
5. Reason, J. (2000). Human error: models and management. Bmj, 320(7237), 768-770.
6. CCPS (2018) Bowties in risk management, CCPS, New York.

Autonomous fault detection and diagnostics, an enabler to control risks of military operations

Chris Rijsdijk and Tiedo Tinga, Netherlands Defence Academy, c.rijsdijk.01@mindef.nl, t.tinga@mindef.nl

Willem van der Sluis, Naval Maintenance and Sustainment Agency, w.vd.sluis.01@mindef.nl

Abstract

This paper aims to reveal how the Netherlands Armed Forces may mature in autonomous fault detection and diagnostics. Generally, fault detection and diagnostics is important as lacking asset health may amplify the risks of military operations. Autonomous fault detection and diagnostics could make an individual's knowledge explicit and it could be essential to process the expanding amount of data from (health) monitoring systems. The state-of-the-art in autonomous fault detection and diagnostics will be projected on a realistic case study. It will be shown that the autonomous fault detection and diagnostics in this typical case study benefits from model-based limits that were already implicitly used. Model-based limits are known to better cope with the varying and unprecedented nature of military operations than value-based limits. The underlying problem is that the risks assigned to faults tend to evolve more rapidly than the designed-in autonomous fault detection and diagnostics. The challenge to make autonomous fault detection and diagnostics robust against varying risk assessments remains unresolved.

1 Introduction

The Netherlands Armed Forces operate in high risk environments of large diversity. These risks may amplify when asset health is lacking. Therefore, fault detection and diagnostics (FDD) may highly affect risks of military operations. In principle, FDD could be autonomous but in practice, it often involves human effort. Reducing human involvement in FDD may be advantageous, not to cut labour costs but to make an individual's expertise transparent to the organisation. Moreover, individuals just appear to be incapable to process the expanding data sets from (health) monitoring systems. Autonomous FDD may become important as newer generations of weapon systems are expected to generate more data.

This paper will project the state-of-the-art in FDD from review papers on the FDD that has been implemented at the platform systems of the vessels at the Royal Netherlands Navy. This exercise should reveal the maturity of the implemented FDD and some directions to improve or develop.

Section 2 will classify FDD methods from review papers by their limits and by their model selection process. Section 3 will introduce autonomous asset health control and various degrees of non-autonomous asset health control. Section 4 will present a case study to illustrate the FDD of the platform management systems of the Royal Netherlands Navy. Section 5 will reflect on the results and finally Section 6 forwards some conclusions.

2 Fault detection and diagnostics

This Section will introduce FDD as an essential element of asset health control. An asset is an item, thing or entity that has potential or actual value to an organisation [1]. This paper confines to assets being artefacts that are valued for fulfilling requirements. If these requirements have been fulfilled, the asset is said to be healthy. So, any asset health

assessment is encumbered with subjective requirements. Still, *shared* requirements, i.e. a set of commonly accepted requirements for a specific asset, should be assessable by common sense. Common sense about *shared* requirements enables individuals to agree upon the actions to control the asset health. Agreement upon actions is essential in any collaboration [2]. The evolution of asset health will be represented by a process. Figure 1 depicts a process P that interacts with its environment by inputs U and outputs Y. Now, the asset health follows from common sense requirements on the inputs U, on the outputs Y or on the process that relates U and Y.

Figure 1. A process

FDD triggers the actions to control the asset health. Figure 2 classifies FDD methods primarily by the limit that detects the fault. A value-based limit has been built on some instantaneous measurement of an input U or an output Y. A value-based limit holds only when all its influential factors remain constant. A model-based limit has been built on an error of a model that relates the inputs U to the outputs Y. Here, an error expresses some distance between a model property and (*i*) an observation or (*ii*) a known physical quantity. A model-based limit also holds when its influential factors vary. Most research effort has therefore been directed to model based FDD methods [3-9]. Figure 2 further classifies the model based FDD methods by the model selection process. Knowledge-based model selection relies on knowledge of the physics that prescribes the variables, the parameters, and the structure of the model. Knowledge-based model selection is superior in making claims about unprecedented circumstances. History-based model selection is a resort when knowledge of the model properties is lacking. History-based model selection employs data to estimate unknown model properties or to weigh some arbitrary set of candidate models. Because history-based model selection relies on data from the past, claims about unprecedented circumstances become more risky.

Figure 2. Classification of FDD methods

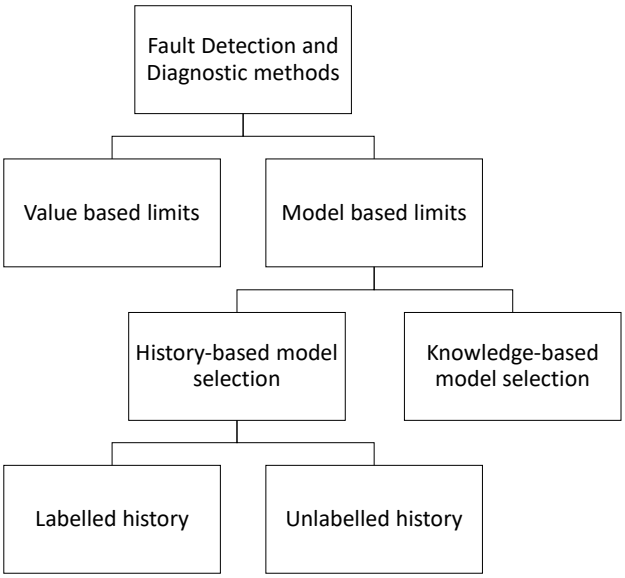


Figure 2 finally shows that history-based model selection may take place from labelled data or from unlabelled data. In the specific case of FDD, the label indicates the presence of the fault. Labelled data allows for supervised machine learning whereas unlabelled data only allows for unsupervised machine learning.

3 Asset health control

This Section will outline asset health control methods. Asset health control expands the objectives of regular FDD:

— Early fault detection. Fault detection is the determination of the faults present in a system and the time of detection.

— Correct fault isolation. Fault isolation is the determination of the kind, location, and time of detection of a fault.

— Correct fault identification. Fault identification is the determination of the size and time-variant behaviour of a fault.

with a recovery objective:

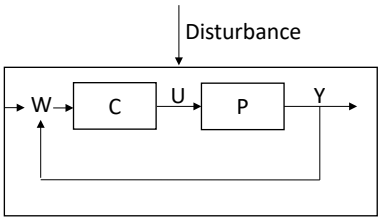
— Timely recovery from the fault.

Section 3.1 will introduce autonomous asset health control and Section 3.2 will introduce non-autonomous asset health control.

3.1 Autonomous control

Many assets respond to disturbances by autonomous control (Figure 3). A disturbance is an unknown (and uncontrolled) input acting on a system [10]. Such a disturbance may lead to a fault. In Figure 3, a fault follows from a deviation from a required input U, from a required output Y, or from a required model property that relates U to Y. Faults could occur abruptly, incipiently, or intermittently. Further, faults induce failures, i.e. a permanent interruption of the asset's ability to perform a required function under specified operating conditions.

Figure 3. Autonomous control.



Autonomous control requires (*i*) precise knowledge of the control model C and (*ii*) a means to automate the control. In practice, the control model C imperfectly represents the process P which means that it could only recover from a subset of the disturbances. The output U of the control model C may be continuous (intermediate value control) or dichotomous (on-off control).

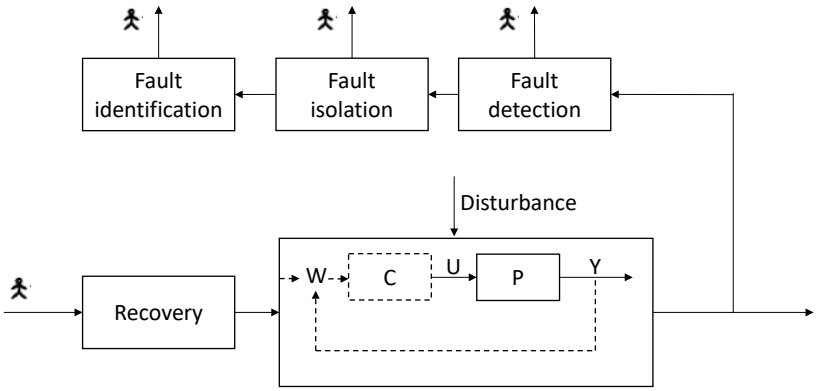
The complementary set of disturbances that is not covered by the control model should be controlled in another way. The autonomous control masks the fault [8],[9], i.e. the feedback loop may propagate a single abnormal process property to all others. Due to the feedback loop, the output Y is subject to influential control factors that vary. Therefore, model-based limits should then be used to control the asset health, as simple value-based limits do not work properly under varying conditions.

3.2 Non-autonomous control

This Subsection will introduce the asset health control of disturbances that involve human effort. Figure 4 shows that non-autonomous asset health control entails fault detection, fault isolation, fault identification and recovery as already mentioned in Section 3. The human involvement may only be limited to just the recovery, but it may also be complete.

The case studies in this paper exemplify a hybrid form of asset health control where fault detection is autonomous, but the follow up is human driven.

Figure 4. Non-autonomous control, where each "person symbol" represents human decision making.



A reduction of the human involvement can be achieved by untangling implicit human expertise and implementing this in the control system. This will make the non-autonomous asset health control more consistent. Ultimately, the non-autonomous control may become fully autonomous. Moreover, autonomous FDD is typically more efficient in analysing large amounts of data [3]. As the amount of data from (health) monitoring systems tends to grow, the importance of autonomous FDD may similarly grow.

4 Case study

This Section will introduce two realistic cases of a sea water cooling system. This sea water cooling system has been installed redundantly on a naval vessel. So, a failure of the duty system can be covered by standby backup systems.

Figure 5. Simplified layout of the sea water cooling system, including sensors measuring the pressure (p) and temperature (T).

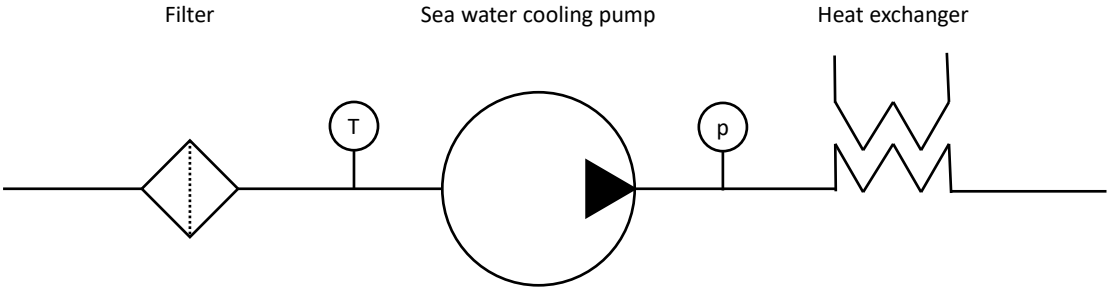


Figure 5 depicts a simplified layout of the sea water cooling system. The designer implemented autonomous fault detection but the fault isolation, the fault identification and the recovery rely on human effort (Figure 4). The limits of the autonomous fault detection are all value-based:

- A low-pressure alarm at the discharge flange to indicate lacking hydraulic power.
- A low-temperature alarm at the inlet flange to indicate (the risk of) ice clogging.
- A high-temperature alarm at the inlet flange to indicate lacking cooling capacity.

As the designer predominantly applied value-based limits to identify faults in all platform systems of this vessel, the autonomous fault detection of the sea water cooling system is not exceptional. Section 2 mentioned that value-based limits may be appropriate as all its

influential factors remain constant. Here, the pressure at the discharge flange and the temperature at the inlet flange are not involved in any feedback control that *defines* their dependency on factors that vary. Moreover, the sea water cooling systems lacks pump speed control or flow control while the suction line and the discharge line are constantly connected to the sea. Therefore, value-based limits may be an appropriate fault detection at first glance.

After several years of deployment, the operator's risk appreciation of the faults in the sea water cooling system evolved [11]. In fact, the operator implicitly implemented model-based limits as he learned to ignore fault detections under specific operating conditions. Moreover, the operator also learned to detect faults that have not explicitly been defined by the designer. The case study is just an attempt to disclose these implicit model-based limits. The model-based limits will appear to be imperfect, but they may be improved by extension (which often requires additional measurements), or by an evaluation of their error.

4.1 Sensor fault

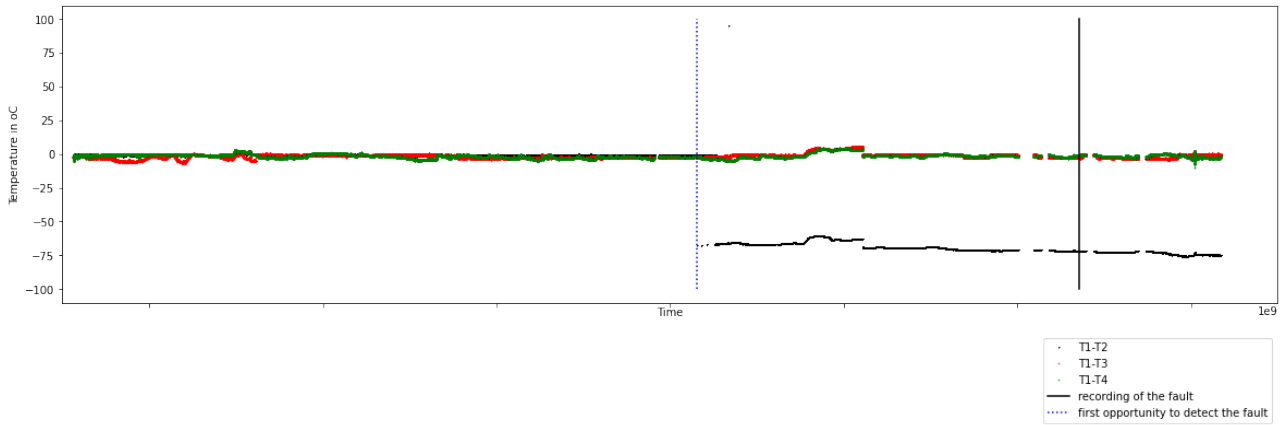
A detected fault may appear to be in the sensor rather than in the asset. So, a fault detection may have several explanations. This case will exemplify a more refined fault isolation (Figure 2). More specifically, this case attempts to better isolate a sensor fault. This fault isolation relies on the knowledge-based model that posits that redundant temperature measurements T_i and T_j should be equal:

$$T_i - T_j = \begin{cases} = 0 & then,\ no\ sensor\ fault \\ otherwise & then,\ sensor\ fault \end{cases} \quad (1)$$

As the sea water cooling system (Figure 5) has been installed redundantly, the sea water temperature is measured by four different sensors. Then, Equation (1) may isolate a sensor fault from a faulty state of the sea water cooling system as defined by the designer's autonomous fault detection system.

Figure 6 shows the evolution in $T_i - T_j$, sensor 1 is compared to sensors 2, 3, and 4. Firstly, all sensors are deemed healthy and halfway the plot sensor T_2 has a fault (as concluded from the large difference with sensor 1). However, even the healthy sensors still show a systematic nonzero difference $T_i - T_j$. A naïve implementation of equation (1) without threshold value would unjustifiably identify many sensor faults.

Figure 6. Evolution in $T_i - T_j$ while the sensors were deemed healthy.



Equation (1) may be improved by (*i*) an extension of the model or by (*ii*) an evaluation of the error. An *extension* would require knowledge of other explanations for the difference $T_i - T_j$ and a means to assess these explanations. An extended knowledge-based model

often requires additional measurements. An *evaluation* of the error would require access to a labelled history. From the labelled history, it follows that Figure 6 is initially free from sensor faults before the sensor T_2 turns to a faulty state. The classification in Figure 2 indicates that from this labelled history, a(n ensemble of) model(s) may be selected that could isolate the sensor fault. This history-based model is a resort as the knowledge (of the measurements) to use a(n extended) knowledge-based model is lacking.

Most likely, even the extended knowledge-based model would again appear to be incomplete and a history-based model on its errors may again become a resort. So, a hybrid approach that uses a history-based model *on the errors* in a knowledge-based model seems appropriate here.

4.2 Pump cavitation

This second case is about a cavitation fault that has not been covered by the autonomous fault detection system of the sea water cooling system, but that excessively occurs in practice. The initial risk assessment has been adjusted by operating experience. Coincidentally, the sensor suite (Figure 5) at some of the pump locations has been extended with a pressure measurement at the inlet flange of the pump which enables to construct an imperfect knowledge-based model that detects the cavitation fault.

A model-based limit of cavitation can be obtained by specifying a minimal pressure at the pump inlet. Such a limit can be defined by the required nett positive suction head ($NPSH_R$), a pump specific pressure A cavitation fault follows from combining this with the available nett positive suction head ($NPSH_A$) as shown in equation (2).

$$\frac{NPSH_A}{NPSH_R} = \begin{cases} \geq 1 & then, no\ cavitation \\ < 1 & then, cavitation \end{cases} \tag{2}$$

Equation 3 defines $NPSH_A$ and Figure 7 specifies $NPSH_R$ for this specific pump.

$$NPSH_A = \frac{p_i}{\rho g} + \frac{c^2}{2g} - \frac{p_v}{\rho g} \tag{3}$$

Here, p_i is the static pressure at the pump inlet, c is the velocity of the sea water at the pump inlet, p_v is the vapour pressure of the sea water, ρ is the density of the sea water and g is the gravitational constant. The parameters g, ρ and p_v follow from deep knowledge and the temperature measurement, but the variables p_i and c remain unknown. Therefore, $NPSH_A$ cannot be compared with $NPSH_R$. However, at some sea water cooling systems (Figure 5) the static pressure at the pump inlet p_i has been measured, which also enables to approximate the velocity by equation (4).

$$c = \frac{q}{1/4\pi d_i^2} = \frac{f(H)}{1/4\pi d_i^2} \approx \frac{f\left((p_d - p_i)/\rho g\right)}{1/4\pi d_i^2} \tag{4}$$

Equation (4) states that the velocity equals the flow q divided by the area $1/4\pi d_i^2$ at the pump inlet. The flow q is a function of the pump head H by the pump characteristic in Figure 7 and the pump head may be approximated by the measured difference in the static pressure at the inlet and discharge flange $(p_d - p_i)/\rho g$. This approximation ignores the kinetic energy in Bernoulli's law due to the difference in the area at the inlet and discharge flange.

Figure 7. Pump characteristic and the specification of $NPSH_R$.

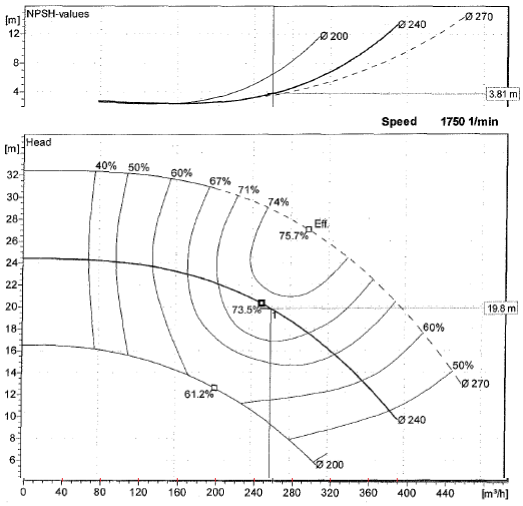
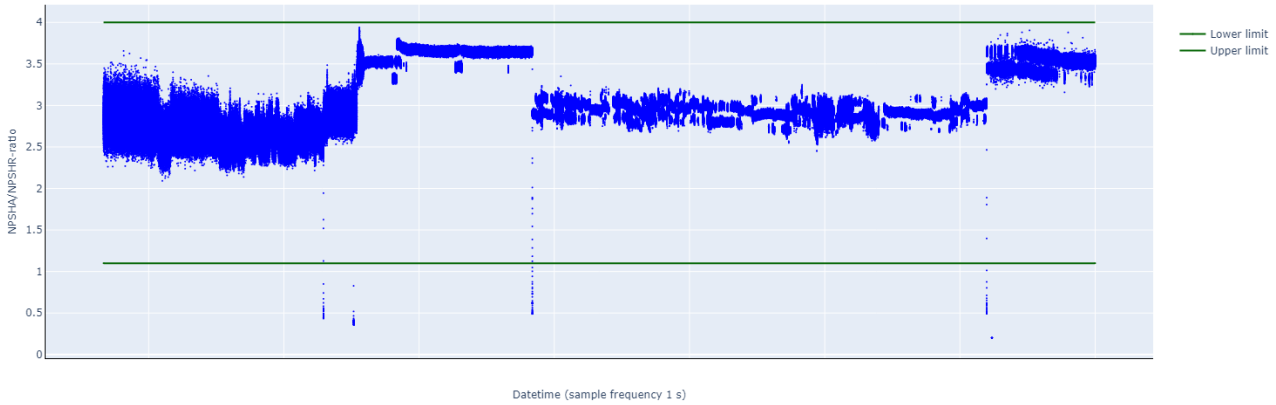


Figure 8 shows that the ratio $NPSH_A/NPSH_R > 1$ all the time which means that cavitation did not occur in this time bracket. Still, the ratio evolves non-stationary while showing "cavitation spikes" at some regime changes.

Figure 8. Evolution of the ratio $NPSH_A/NPSH_R$.



Evidently, the ratio $NPSH_A/NPSH_R$ suggests that the sea water cooling pumps are regularly and unnecessarily operating far away from their best efficiency point. As there is no operational need that drives the pump away from its best efficiency point (Eff) in Figure 7, the nonstationary evolution in the ratio $NPSH_A/NPSH_R$ may been seen as a fault. Possibly, some faults in Figure 8 are just explained by the fact that the knowledge-based model is imperfect. If additional explanations are known or measured, they may be addressed by an extended knowledge-based model.

Here, it is only known that cavitation is an issue across the fleet, but there is *no* labelled history that indicates whether all pump locations were evenly affected or (even better) that indicates *when* cavitation took place at a specific pump. Still, experts defined limits on the ratio $NPSH_A/NPSH_R$ beyond which cavitation *generally* takes place. The lower limit $NPSH_A/NPSH_R = 1{,}1$ in Figure 8 follows from [12] and the upper limit $NPSH_A/NPSH_R = 4$ follows from the maximum pump head in Figure 7. Then, Figure 8 shows that the pump has been operating quite close to the upper limit which makes it vulnerable to discharge cavitation. Discharge cavitation occurs when the pump hardly produces any flow. Then, the sea water will pass at a very high speed through the clearance between the impeller and the pump house. Then, discharge cavitation may occur due to the temporal low pressure behind the impeller blades.

So, unlike the previous case, it was impossible to similarly use a history-based model *on the errors* of a knowledge-based model. In this case, the history-based model *on the errors* of equation (2) has *not* been inferred from data about this specific pump, but from general guidelines that have been inferred from data about other pumps.

5 Discussion

The autonomous FDD of the platform systems at the Royal Netherlands Navy predominantly relies on value-based limits whereas model-based limits are known to better cope with varying and unprecedented operations. Although the operation of the sea water cooling system appeared to be quite stationary and free from autonomous control at first glance, the value-based limits were often implicitly replaced by better model-based limits. By disclosing these implicit model-based limits, the asset health control (Figure 4) could become less reliant on human effort.

Operating experience influences the risks assigned to faults (particularly the frequency component of a risk), whereas the designer's autonomous FDD did not change. If the autonomous FDD were to be updated more regularly, the autonomous FDD would have been better aligned with the concerns of the decision makers.

The case from Section 4.1 showed that the knowledge to extend a knowledge-based model may be lacking. A resort to a history-based model selection *on the errors* of the knowledge-based model appeared to be a pragmatic solution to cover known faults at regular operating conditions. This history-based model selection may follow from a labelled history of a specific asset (Section 4.1) or from guidelines that rely on a history of many assets (Section 4.2).

This specific case study was not hampered by the masking effects of autonomous control, but this does not hold for all platform systems. Then, the ones who intend to make FDD more autonomous should be informed about the applicable control models.

6 Conclusions

This paper observed that the autonomous FDD of the platform systems of the vessels of the Royal Netherlands Navy predominantly relied on value-based limits whereas there were good reasons to belief that model-based limits would in principle be more appropriate under changing and unprecedented operating conditions. This paper demonstrated the benefits of model-based limits in two simple cases that relied on some hybrid form of knowledge-based and history-based model selection.

This paper did not solve the fundamental problem that the risks assigned to faults tend to change more rapidly than the design of the autonomous FDD. This paper just untangled some implicit model-based limits that were already available, but lacking knowledge of (control) models or measurements may obstruct the use of improved model-based limits. If the autonomous FDD could become robust against varying risk assessments, this problem would alleviate.

References

1. International Organization for Standardization (2014) *ISO 55000; Asset management — Overview, principles and terminology.*
2. Rijsdijk, C. (2016) *Maintenance is unjustifiable: an improved inference*, Doctoral thesis, https://doi.org/10.3990/1.9789036541909.
3. Gertler, J.J. (1988) Survey of Model-Based Failure Detection and Isolation in Complex Plants. *IEEE Control Systems Engineering*, vol. 8, issue 6, pp. 3-11.
4. Frank, P.M. (1996) Analytical and Qualitative Model-based Fault Diagnosis – A Survey and Some New Results. *European Journal of Control*, vol. 2, issue 1, pp. 6-28

5. Venkatasubramanian, V., Rengaswamy, R., Yin, K., & Kavuri, S. (2003) A review of process fault isolation and diagnosis Part I: Quantitative model-based methods. *Computers & Chemical Engineering*, vol. 27, issue 3, pp. 293-311.
6. Venkatasubramanian, V., Rengaswamy, R., & Kavuri, S. (2003) A review of process fault detection and diagnosis part II: Qualitative models and search strategies. *Computers & Chemical Engineering*, vol. 27, issue 3, pp. 313-326.
7. Venkatasubramanian, V., Rengaswamy, R., Kavuri, S., & Yin, K. (2003) A review of process fault detection and diagnosis part III: Process history based methods. *Computers & Chemical Engineering*, vol. 27, issue 3, pp. 327-346.
8. Isermann, R. (2005) Model-based fault-detection and diagnosis – status and applications. Annual Reviews in Control, vol 29, issue 1, pp. 71-85.
9. Park, Y.J., et al. (2020) A Review on Fault Detection and Process Diagnostics in Industrial Processes. *Processes,* vol. 8, issue 9: 1123, https://doi.org/10.3390/pr8091123.
10. Isermann, R., Ballé, P, (1997) Trends in the Application of Model-Based Fault Detection and Diagnosis of Technical Processes. *Control Engineering Practice*, Vol. 5, issue 5, pp. 709-719.
11. Rijsdijk, C. et al. (2020) Using ship sensor data to achieve smart maintenance? *Proceedings of the International Naval Engineering Conference 2020, October 5-9 2020,* pp. 1-10.
12. Hydraulic Institute (2012) *ANSI HI 9.6.1-2012 Rotodynamic Pumps Guideline for NPSH Margin*.

Transition towards sustainable aviation. Need for new tools to gain insight?

G.G.M. Boosten Msc Amsterdam University of Applied Sciences, g.boosten@hva.nl

Prf.dr.ir. J.A.A.M. Stoop Amsterdam University of Applied Sciences, stoop@kindunos.nl

Abstract

The development of sustainable aviation turns out to be a 30 year transition process. How to manage this transition process is a crucial for the change and success of the aviation sector in future. The foreseen solutions are mostly driven by technological innovation and improvements of procedures and regulations. The question is if these tools are sufficient to manage the innovation of an entire sector with 100 years legacy or are changes in business models, societal values and human behaviour part of the instrument mix aviation can use? New or adapted innovation models and tools are needed to use the full mix of instruments. The article explores the use of a modified Cyclic Innovation Model which is developed by researchers of TU Delft. The development of Schiphol Airport in Amsterdam and the outlook for its next 100 years is used as a case to understand the complexity of sustainable airport development.

1 Introduction

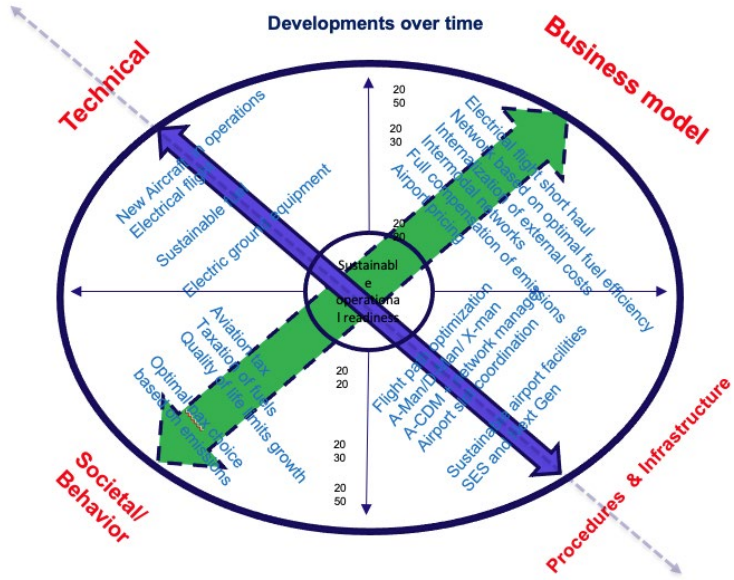
The Covid-19 crisis has had a big impact on aviation; in Europe passenger traffic was down to more than 80% and flights were lagging more than 60% behind the all-time high in 2019. Today the aviation industry is seeking ways to recover from this crisis. The objective is not to return to the level as in 2019 where airports and airspace were operating at maximum capacity and the societal acceptance of aviation was deteriorating because of the hinder and impact on climate change. Although the massive impact of Covid, sustainability and climate change are the most challenging crisis aviation is facing.Due to the success of aviation in reducing noise, fuel burn and emissions which resulted in low fares for passengers the demand for air travel is growing even at a higher rate than technology is reducing the environmental impact of aviation.

Three recent reports illustrate the need for sustainable aviation which ultimately has be in accordance to the Paris Climate Agreements. The first report, Destination 2050- A route to Net Zero European Aviation describes four instruments to achieve this goal. These are aircraft and engine technology, air traffic management and aircraft operations, sustainable aviation fuels and smart economic measures (1). The second report is the EU Sustainable and Smart Mobility Strategy presenting over 100 actions for a seamless intermodal, integrated transport network that will has close to zero emissions in 2050 (2). Aviation is part of this network. The Aviation Round Table Report on the Recovery of European Aviation is the third report. The objective is to link the post covid aviation recovery to the need for sustainable aviation in the near future; how to build back better to ensure that aviation is stimulated to implement policies to meet the EU sustainability standards and thus net zero in 2050 (3). The objective for aviation to become net zero in 2050 -or earlier if possible- and that only option for aviation is to start the transition today is not disputed. The main debate is what the most appropriate steps are to achieve this goal and to what extend these steps will influence the growth potential and business models of aviation businesses. These steps should not be taken at the expense of other societal values such as safety, land use or security. This requires a multi-value integrative approach.

2 Aviation growth paradox and need for cyclic innovation

Aviation has a remarkable track record of technological improvements resulting in constant reduction of noise and emissions per seat mile with every new generation of aircraft. Proposed policies in reports as mentioned therefore strongly build on the continuation of technological innovations and improvements to establish net zero emissions in 2050. However, the paradox of aviation is that the efficiency gain per seat mile and thus cost reductions result in an increase in demand for aviation which is much bigger than the realized fuel savings; the net effect is that aviation's share in global CO_2 emissions will continue to rise despite all realized and foreseeable technological improvements. In many parts of the world like Asia and Latin America large groups of citizens do get means to travel and thus to fly; it will keep the aviation paradox in place for a long time. Therefore, a focus on technological and procedural improvements is necessary but not sufficient. We need to explore the potential of modified business models, changes in passenger behaviour and societal values as shown in figure one. Sustainable aviation requires developments along both axes. An additional insight is that realizing net zero emissions in 2050 will enter the aviation sector into a 30-year transition period with permanent change of technology, infrastructure and procedures, business models, behaviour and societal values. This process will take place in a sector where safety and resilience are key characteristics, and which is by definition not very open to experiments.

Figure 1. Instrument mix of technology, procedures/infrastructure, business models and behaviour/societal values



model developed by author

2.1 The innovation challenges in Aviation

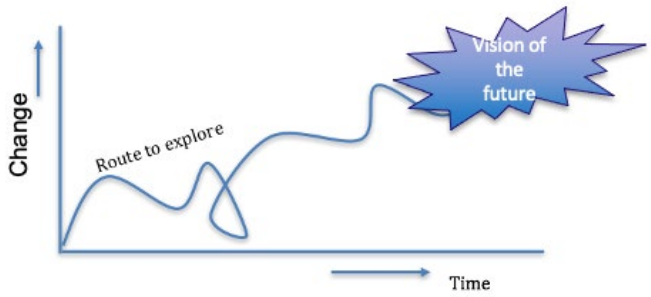
In general innovation can be defined as 'the management of all the activities involved in the process of idea generation, technology development, manufacturing and marketing of a new (or improved) product or manufacturing process or equipment' (4) (P.15). This definition focusses on one product, manufacturing process or equipment while the innovation needed for the transition of aviation to net zero in 2050 will impact the entire global aviation sector; we have to focus on innovation of an entire sector. This challenge

is comparable with the energy transition or how to feed 9 billion people and other SDG-goals.

In literature the aviation sector has been identified as a technology legacy sector (5). Innovation in legacy sectors is constrained by path dependency and technology lock-in; technology, infrastructure, regulation, and business choices made in the past will determine the adaptability of the sector and the options for implementing innovation in future. In other words, the sector must develop a new eco-system for sustainable aviation, but legacy limits the adaptability of the sector and will thus influence the scope of the vision of the future for net zero emission in 2050.

If we combine this with a 30-year transition period to realize the vision of the future in a sector that is resistant to change we have to conclude that the transition path itself will an important element of the innovation process itself. The transition path isn't a well-defined route to the vision for the future; figure 2 indicates that there is no clear roadmap and finding or exploring the route to follow is part of the transition itself.

Figure 2. The exploration of the route to the vision of the future is part of the transition path



Source: Boosten

The development and implementation of certified and approved new technology in aviation will take many years, as will the development of new infrastructure. Changes will be implemented in small steps and for the next decade aviation must rely on best available technology, -slightly- modified existing infrastructure, procedures and regulations. So, the innovation challenge for aviation is not the implementation of new technology or product or service, but a fundamental transition of the entire sector in a 30 year period which should be integrated in a wider scope of overall change of the mobility sector. Such a transition reveals a dualism between derivative solutions and disruptive adaptation. According to Vincenti's disruptive anomaly paradigm (6), such disruptions should be facilitated by new tools and models to overcome the conservative legacy forcefields in the sector.

2.2 Resistance for innovation in legacy sectors

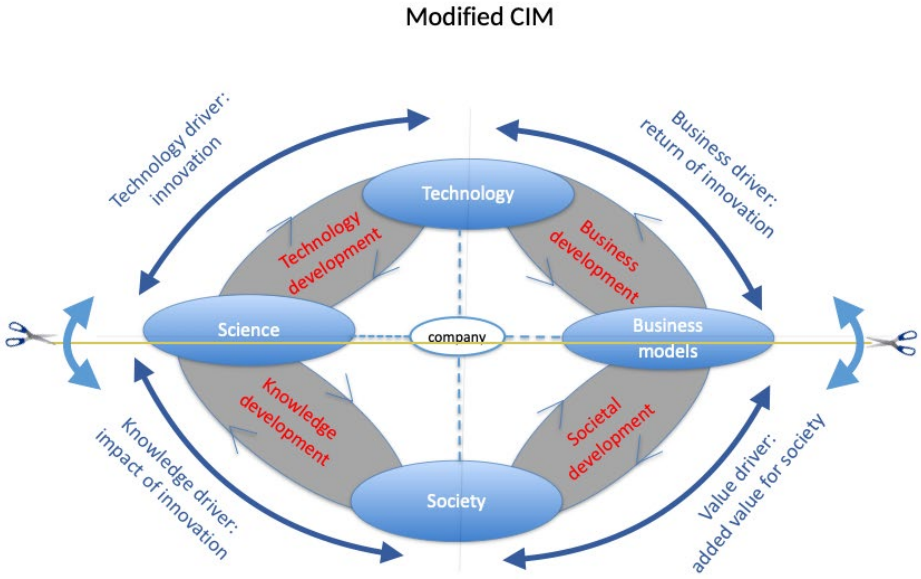
Not all sectors can easily be disrupted. Apart from technology lock-in and path dependency in legacy sectors such as aviation there is a well-defined technological/economical/ political/social paradigm that resists any innovation that might threaten to disrupt the business models of the stakeholders who benefit from it. The resistance for innovation creates barriers for innovation varying from favouring existing technology, discouragement of new entries, reluctance to finance disruptive new entrants, strong lobby by vested interests and incumbents, public habits and expectations and market imperfections (5). Most linear, stage gate innovation models aren't capable to deal with the innovation challenges in aviation. The innovation and transition process won't be step by step but iterative and explorative and doesn't have to start with the invention of new technology. The drivers for innovation can be in business or society as well. There is a need for a new innovation model which is capable to conceptually handle the two axes defined in figure 1,

can address and identify the -possible- barriers in innovation in legacy sectors and allows small iterative steps in interactions between the four instruments for innovation.

2.3 A cyclic innovation model

In an assessment of innovation studies the Cyclic Innovation Model (CIM) developed by the TU Delft has been identified as the best model to describe the cyclic interaction in innovation (7). The CIM model focusses on the cyclic nature of innovation connecting hard sciences with soft values (8) but is mostly applied for one product or manufacturing process. In a sectoral innovation and transition process to sustainable aviation the entire sector must change under pressure of changing societal values and impact of climate change. For this reason, CIM has been modified in such a manner that society and governmental interventions are incorporated (9). The modified CIM (MCIM) as shown in figure 3 can be divided in four quarters which equal the instrument mix for innovation in figure 1. MCIM can address drivers for innovation in each quarter and the model can be used to visualize the interactions and iterations between the instruments for innovation. MCIM can be horizontally and vertically divided. In a horizontal split, the top halve of the model represents the development of the aviation business, where the bottom halve represents the societal acceptance of the added value generated. A vertical split in the model defines the scientific development on the left-hand side and the current operations and business models on the right-hand side. For instance, in the Netherlands aviation has created one of the biggest hub operations at Schiphol Airport; the Dutch society appreciates the large connectivity due to the hub but the impact on the quality of life and climate change is becoming a real big problem which set limits to the aviation business development.

Figure 3. The Modified Cyclic Innovation Model MCIM



Source: Boosten

The cyclic nature of MCIM supports the focus on the various aspects of innovation and the model can be used to identify the force field and thus locate the barriers between stakeholders in innovation. MCIM can be used in the transition process to explore the route towards the vision of the future.

2.4 Summary

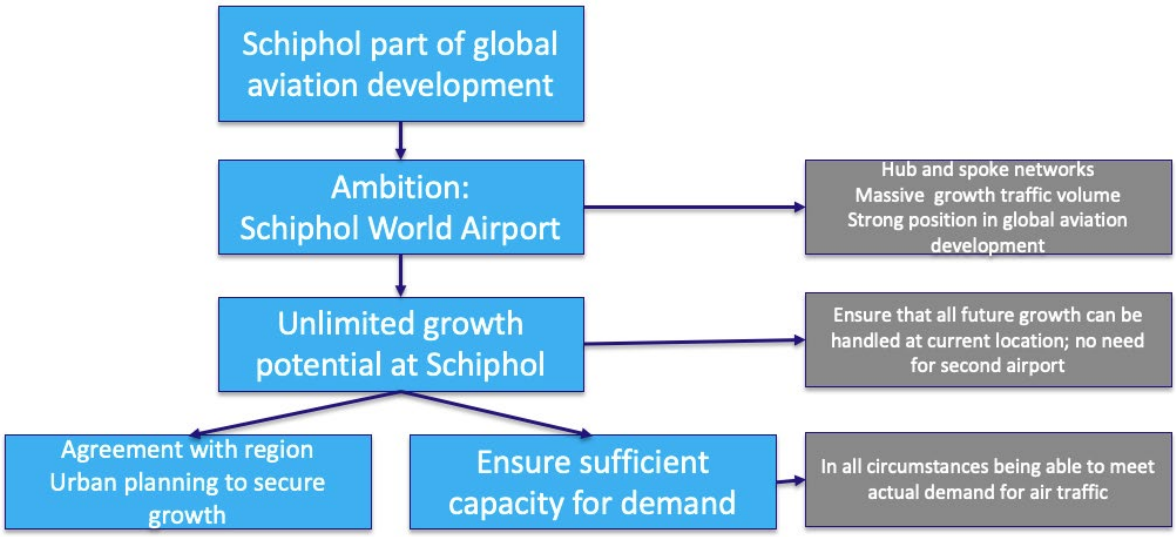
Over the first 100 years of its existence aviation has been very successful in innovation aircraft, airports, and business models; aviation became reliable and affordable for many consumers. This resulted in a paradox that all technological and procedural improvements to reduce hinder and impact on climate change cannot meet the impact of the fast-increasing demand for travel by air. Solving this paradox successfully requires the transition of the entire sector. Sectoral innovation differs from product of production innovation processes; even more if we realize that the transition path towards sustainable innovation will take 30 years and the route to the vision of the future is unclear. A cyclic innovation model provides the insight to understand the forcefield and barriers in sectoral innovation and can be used to explore the route to the vision of the future.

3 The Schiphol Airport case; lessons from 1949

3.1 The Schiphol 1949 masterplan

Amsterdam Airport Schiphol operates already over 100 years at its current location. Being one of the biggest international airports in the world this is a remarkable achievement. The characteristics of the current airport were defined just after the second world war and documented in the Schiphol 1949 master plan (10). Figure 4 shows the key drivers of this master plan.

Figure 4. Key drivers masterplan 1949



Source: Schiphol

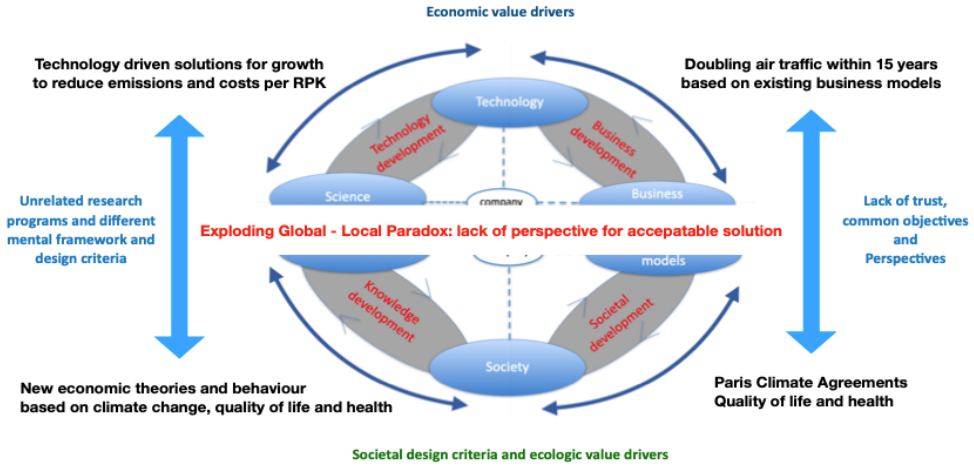
The goal was to develop a world class airport with unlimited capacity which will become an important node in the emerging worldwide aviation network. Using state of the art knowledge those days a challenging vision was presented for an airport with an hourly capacity of 200 aircraft movements, short taxi times and a central terminal area. An airport predestined for hub operations. Pre-covid Schiphol handled over 70 million passengers and almost 500,000 aircraft movements still at the same location and using the Schiphol 1949 planning criteria (11). The technical capacity limits of the airport aren't reached yet. The fact that Schiphol Airport is facing severe growth limitations is due to environmental constraints and hinder caused by aviation. The 1949 masterplan urged local neighboring communities not to develop new housing projects under the departure and arrival routes for the runways. The urban development of these areas in the end had a major impact on the airport operations as from the '60's when the noise contours were introduced and

limitations in runway usage. The hinder caused by the aircraft in the developing urban area surrounding the airport resulted in strong regulations and reduced societal acceptance of the airport; the societal capacity is now the most limiting factor for growth (12)but also generating complex operating procedures to spread the hinder over various regions (13).

3.2 Schiphol situation defined in MCIM

The limitation of the development of Schiphol Airport is the outcome of various developments; MCIM as shown in figure 5 (14) can be used to identify the forcefield resulting from these developments.

Figure 5. Unbalance of economic and societal drivers for airport development



Source: Boosten

Each side of the model has different contradicting drivers for success (15) p.26. The tensions between the top halve of the model, representing the aviation business working hard to meet the expected demand for air travel within the current business models and bottom halve representing the societal needs for quality of life and climate change are resulting in lack of trust and clashes of perspectives on development. Also, the type of research related to both sides of the model are different; the top side is mainly driven by technological and procedural improvements, where the bottom halve has focus on behavioral and business model developments.

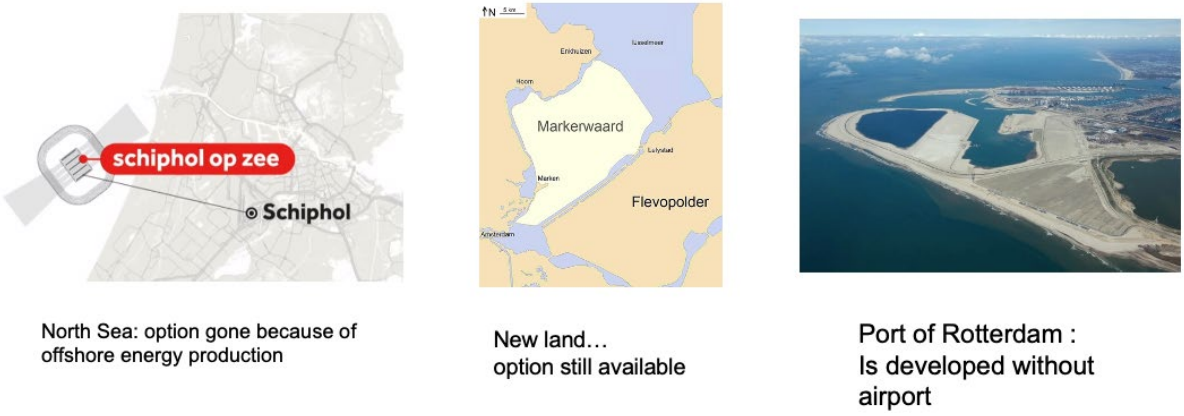
3.3 The next 100 years: possible at same location?

Although Schiphol Airport still had sufficient technical capacity to develop at the current location the societal acceptance of the airport in the 90's diminished due to increasing noise levels and health concerns. For this reason the government started a program (16) to study the growth potential of Schiphol Airport and to investigate possible sites for the development of a second national airport in the Netherlands (17). Referring to these developments Schiphol Airport investigated three possible locations for airport development as shown in figure 6: an artificial island in the North Sea, a new polder in the Markerwaard (a lake) and an extension to the second Maasvlakte (being new development of the Port of Rotterdam). All three were wet locations to preserve the site from being locked in by future urban development. A novelty was that the study also considered partly replacement of the current airport; i.e. positioning the airside at the artificial island, but to

keep the landside access, car parking and terminal at the current location or the outplacement of air cargo to the Port of Rotterdam. Ultimately it was concluded that for the time being the current Schiphol location was the best place for further airport development.

These days references to these locations are made again in the public debate on the future growth of Schiphol Airport (18). We have to conclude that two out of the three locations are no longer available for airport development due to an incompatible combination of functions in the planning. The North Sea is being used as location for massive windmill parks to produce green energy and the extension of the Port of Rotterdam is realized without an airport due to the major hazard footprint of the process industry. The only available location is a new polder in the Markerwaard, which is now a nature reserve.

Figure 6. The three possible water locations for (partly) new airport developments studied by Schiphol Airport in the 90's of last century.



The question if Schiphol Airport is fit for the next 100 years or if a new location needs to be developed can only be answered by exploring the criteria for future airport development. Where capacity and growth were the main drivers for the previous century, we can find the challenges for the next century in de UN Sustainable Development Goals (SDG). Aviation isn't expected to come to a standstill as indicated before the biggest challenge is to accommodate growth within the SDG. Using the MCIM-model we can identify technological developments introducing multiple energy sources to power aircraft, new type of aircraft with fleet differentiation in range and size. New procedures and routes in the sky will allow for the most efficient use of aircraft to fly from A to B. Many changes will be expected in new business models for aviation business which will be driven by sustainability. But most changes and drivers for aviation development will be the result of limitations set by societal acceptance of aviation and defining boundary conditions on balancing regional needs for connectivity and preserving quality of living and climate change. This trend in society will influence human behavior, the need/motives for and value of travel. Next to hard science and technological innovation there will be a growing need for new economic values to be used in aviation business decision making which will support the societal needs based on SDG. Using these insights, the future Schiphol Airport should be ready to accommodate sustainable aviation networks which are based on maximum traffic efficiency per energy (and thus emission) unit. This will result in a broad fleet mix, multiple energy sources, maximum intermodal integration and seamless intermodal transfer for passengers. Hinder free routes for arriving and departing aircraft and hassle-free landside access to the airport. Energy neutral airport facilities should support new airline business models and passenger demands for sustainable travel, circular use of scarce resources and waste and local production, storage, and management of green energy. Implementing these criteria at the current location won't be impossible. But the future development of Schiphol should be considered in broader societal context where there is big shortage on housing and space for urban development in the region. Moving at least the airside of Schiphol to a location a remote wet location would provide optimal

development options for Schiphol Airport and urban development in the Amsterdam region. Such a transfer can only be realized with a realistic transition period that will cover the transition of the entire region for the next 20 years.

4 Conclusions

Sustainable aviation provides unprecedented challenges to the aviation sector. To accommodate a still very large demand for air travel within a framework of zero emissions in 2050 requires a fundamental redesign of the current modus operandi. The dominant conviction that technology, procedures, and regulation will deliver the solution only uses part of the available tools to manage change. As such it relies on extrapolating derivative solutions but does not cover the necessary disruptive nature of the developments. New business models, societal values and changes in human behaviour offer important additional options to change and modify the aviation sector. Innovation models to be used in technology legacy sectors like aviation should be able to deal with the full instrument mix as well as providing insight in a 30 year transition process. The transition process to explore the road to the vision of the future is as important as the innovation in the vision itself. The MCIM models delivers insights in these developments, but further research is needed to explore the characteristics of the model; especially the interactions and iterative processes between the four quadrants and how innovation and transition processes can start in each quarter. Furthermore, we need to explore the options if next to the horizontal and vertical split in the model other, diagonal, spits will deliver insights in the innovation drivers and barriers as identified in the technology legacy sector studies.

References

1. NLR, SEO. Destination 2050. A Route to Net Zero European Aviation. 2020. Report No.: NLR-CR-2020-510.
2. Commission E. Sustainable & Smart Mobility Strategy. In: Transport Ma, editor. 2020.
3. Aviation RT. Aviation Round Table Report on the Recovery of European Avaition 2020.
4. Trott P. Innovation management and new product development 4th edition. Essex: Pearson Education Limited; 2008.
5. Bonvillian WB, Weiss C. Technological Innovation in Legacy Sectors. New York, USA: Oxford Univeristy Press; 2015. 365 p.
6. Vincenti W. What Engineers Know and How They Know It. Analytical studies from Aeronautical History.: The John Hopkins University Press. ; 1990.
7. Noort van den R. Towards the end of global poverty [PhD study]: Technical University Delft 2011.
8. Berkhout G, Duin Pvd, Hartmann D, Ortt R. The Cyclic Nature of Innovation: connecting hard sciences with soft values. G. L, editor. Amsterdam: JAI Press, Elsvier; 2007.
9. Boosten G. Innovation in Legacy Sectors, a hollistic approach [Unplublished Work]. In press.
10. Schiphol. Plan voor Uitbreiding van de Luchthaven Schiphol. Masterplan for Schihpol Airport Amsterdam: Gemeente Amsterdam Amsterdam DdGHeDdPW; 1949.
11. Gordijn H, Harbers A, Nabielek K, Veeken Cvd. De Toekomst van Schiphol: Ruimtelijk Planbureau; 2007.
12. Mota MM, Boosten G, Zuniga C. TIme to Sweat the Assets? The analysis of two airport cases of restricted capacity in different continents. International Transport

Forum Round Table on Optimizing Airport Capacity at Existing Airports; Queretaro Mexico. To be published by ITF2017.

13. OvV. Veiligheid Vliegverkeer Schiphol. Onderzoeksraad voor Veiligheid; 2017 april 2017.
14. Boosten G. Disruptie en Transformatie in Avaition. Toepassing van het Modified Cyclic Innovation Model in de luchtvaartsector en specifike op de Schiphol casus. 2021.
15. Boosten G. The (congested) City in the Sky. The capacity game: finding ways to unlock Aviation Capacity. Amsterdam2017.
16. TNLI. Strategische beleidskeuze toekomst luchtvaart. 1998.
17. Velde RJvd, Schotten CGJ, Waals Jvd, Boersma WT, Munnik JMO, Ransijn M. Ruimteclaim en ruimtelijke ontwikkelingen in de zoekgebieden voor toekomstige nationale luchtvaartinfrastructuur (TNLI). Quick Scan m.b.v. de Ruimtescanner. Bilthoven: RIVM; 1997. Report No.: 711901024.
18. Revier E, Klundert Fvd, Norkunaite G, Escribano EL. Quickscan Luchthaven in Zee. Actualisatie van kennis, kosten en baten. Eindrapport. Waterstaat MvIe; 2019.

Disruptive or derivative, that's the question

John Stoop, stoop@kindunos.nl

Sverre Roed-Larsen, sverre.rl@wemail.no

Abstract

This contribution deals with findings of an analysis into the certification process of commercial aviation aircraft design. The B737MAX case study indicate an overstretching of type design variations, their inherent assumptions and simultaneously downscaling of the certification process from a disruptive to a derivative level. Several lessons learned based on an analysis of the Breguet equation, previous accident investigations into B767, B747 and B737 crashes and human factors modelling assumptions, indicate structural opportunities for safety enhancements. Combining the Kestrel Patent for longitudinal stability with the Good Airmanship 2.0 concept, fundamentally resolves present man-machine interfacing vulnerabilities. In addition, a clear distinction between certification regimes for derivative and disruptive solutions strengthens the foreseeability of future flight performance of the 4th generation commercial aircraft and beyond, in assuring a smooth and safe flight execution.

1 Introduction

Since its conception, the aviation community has seen a synergy between knowledge, experiment and theory to cope with the most serious of all of its challenges: beating gravity. From the start on, aviation embraces operational feedback by investigating accidents. Experimental testing of theories and concepts about aerodynamics, stability and control, materials and propulsion serves as a prospective toolbox in the design and development phase. Type certification serves as a prerequisite for introducing new generations of aircraft at a high-level safety global playing field. Safety investigations, compliant with the ICAO Annex 13 protocol, serve as retrospective problem providers for knowledge development by qualified operational feedback. Famous aircraft designs with unprecedented performance levels emerged from this combined approach since the 1940's, such as the Supermarine Spitfire, P51 Mustang, Messerschmitt 262, Concorde and Sukhoi SU 30. These designs were based on a disruptive engineering design philosophy, combining several scientific schools of thinking, such as physics, mathematics, engineering design and forensics. This approach evolved into Knowledge Based Engineering and Multidisciplinary Design Optimization methodologies (Torenbeek 2013). The discipline of human engineering developed in the 1960's, focusing on human performance analysis and modelling based on cybernetic principles. A distinct engineering design approach of either man or machine was created with an unprecedented safety performance level. Aviation achieved the state of Non-Plus Ultra-Safe systems.

Two major air disasters disrupted this relative stable design and operating environment: the AF 447 and B737 MAX cases. Both cases shocked traditional human performance and design certification regimes. The AF447 case triggered human performance research into a startle and surprise phenomenon and disclosed the inability of present human factor modelling to reliably foresee future human performance under non-normal conditions (Troadec 2013). The B737 MAX cases showed that software applications and pilot training provisions proved to be not fail safe as fallback strategies for aerodynamic pitch control deficiencies in the man-machine interaction during stall conditions. Deregulation and privatisation eroded global standards of aircraft certification and triggered a debate on governmental oversight and corporate responsibilities on safety and risk assessment.

These cases also revealed deficiencies in managing knowledge availability at a sectoral level.

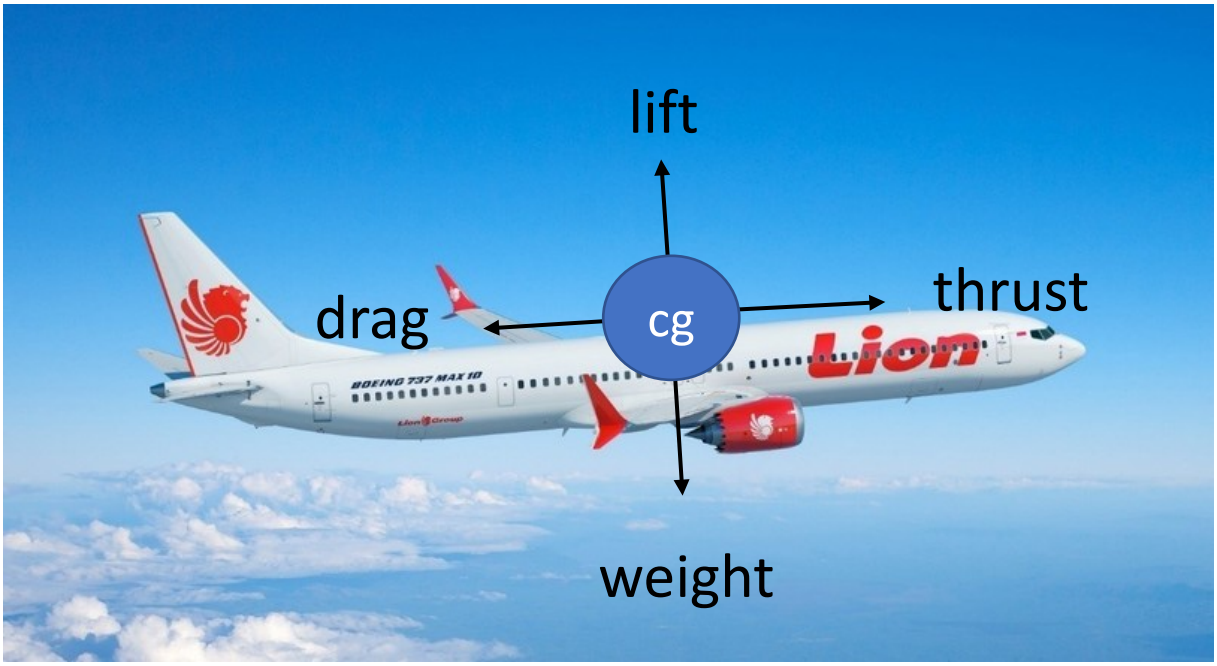
The potential of a gradual drift into disaster has been foreseen by qualified designers, engineers and operators, but was ignored and even dismissed by senior management of leading manufacturers, stigmatizing them as whistle blowers (Dot 2015, 2016, 2020-1, 2020-2, House Committee 2020). In these cases, a decision-making procedure to discriminate between derivative and disruptive design lacked, hampering the provision of substantive proof of assumptions and hesitations to accept a safe performance of new designs without adequate testing, validation and certification (DoT 2015, 2016, 2020-1, 2020-2, House Committee 2020).

This paper elaborates on the need to reconsider the current approach in discriminating between derivative and disruptive design, covering both certification, operational practices, training and management. A proposal is launched to distinguish derivative from disruptive developments by a dedicated decision-making procedure. This procedure takes into account the nature of disruptives, mobilizing knowledge repositories, assessing inherent limitations, uncertainties and assumptions in coping with the unforeseen.

2 Basics in aviation

In aviation, all is about beating gravity. To this purpose, four basic, static forces are defined around a centre of gravity (cg), represented by a concentrated mass point: lift (L), drag (D), weight (W) and thrust (T). In addition, three basic dynamic notions are identified: rotational moments around this centre of gravity on the x, y and z-axis, representing pitch, roll and yaw stability expressed as Cm alpha, Cm beta and Cm gamma. Finally, time as a flight parameter is taken into account to cope with all phases of the flight, the aircraft configurations and dynamic stability in order to control a safe and smooth flight performance.

Figure 1. Basic performance parameters.



Flight performance parameters are designed based on the equilibrium of these forces and moments, and their relative magnitude expressed as L/D, T/W, speed (V) and range. Functional design optimization of the aircraft performance is expressed in the Breguet

range equation (eqn 1), following the basic functions of cruising speed, propulsion, structures aerodynamics and stability and control.

$$\text{Range} = Vt_f = V \times \underbrace{\left(\frac{L}{D}\right)}_{\text{aircraft designer}} \times \underbrace{I_{sp}}_{\text{propulsion system designer}} \times \underbrace{\ln\left(\frac{W_i}{W_f}\right)}_{\text{structural designer}} . \quad (1)$$

Each of the terms in the equation has seen an optimization process of decades, mobilizing a wide variety of scientific and technological knowledge domains, such as aerodynamics, thermodynamics, materials and flight control theories. In addition to the technological aspects of aircraft design, human factors and economics have contributed to other vital design parameters concerning man-machine interfacing, fuel economy, cost, endurance and efficiency considerations, logistics and market developments and last but not least, environmental, sustainability and societal value demands. Such a balanced and encompassing design environment has created a sophisticated multidisciplinary design optimization methodology (Torenbeek 2013). By choosing technology as flywheel of progress in the 1950's by ICAO, commercial aviation has been able to grow into a global network with a high organisational and managerial stability, combined with a high safety level playing field. This strategy also has impacted the development of aircraft. A series of generations of derivative aircraft by building on the success of predecessors entered the market: based on the B727, Boeing successively and successfully developed the B737 Original, Classic, Next Gen and MAX. Each generation was based on the same 1960 classic concept of tube and wing configuration, but was progressively equipped with state of the art technological innovations: upgrading the dimensions for passenger capacity and range, introduction of automation by glass cockpits, fly by wire applications, composite materials, clean wing aerodynamics, propulsion and fuel efficiency, combined with a continuous weight reduction. Each basic function in the Breguet equation was stretched separately to its design limits, in its drive to achieve functional optimization. Over time - and in particular due to the crashes of Lion Air and Ethiopian Air - this restrictive functional optimization revealed two fundamental problems of the overall performance assessment of the 4th generation commercial aircraft, among which the B737MAX: a functional interference between design dimensions and certification process deficiencies.

1. Interferences between the functions in the Brequet equation

Three interferences are identified. First, an interference between aerodynamic lift distortion and engine positioning and dimensions at high angles of attack (AoA) occurred. Due to the gradual growth in diameter size of the new LEAP engine and their nacelles for reasons of increased propulsion power and fuel economy, their relative short distance in front of the wing leading edge and positioning at high angles of attack created flow interference and loss of lift during critical flight phases.

Figure 2. Wing-nacelle aerodynamic interference.

Second, the increased propulsion power of the newly installed generation of high bypass ratio engines encountered a series of incidents with engine overload. A series of engine blowout and uncontained fan blade failures occurred in the new generation of high bypass engines. In order to maintain ground clearances of engines with high bypass ratio's, landing gear adjustments and tail strike prevention measures had to be taken to compensate the increased length of the fuselages. This delicate repositioning of the engines and lengthening of the fuselage restricted the rotation of the aircraft during take-off and landing and impacted the power settings.

Third, a continuous drive for weight reduction aimed at maximizing fuel economy, cost savings, occupancy rates and payload efficiency impacted the stability and control of aircraft that fitted the new LEAP engine. Lufthansa confirms the 16% fuel savings of the new engines, but had to block the last seating row due to center-of-gravity concerns.

In July 2019, Airbus disclosed two outwardly similar, though separate, issues which could result in excessive pitch up behavior, one affecting the A320neo and the other the A321neo. Both issues were detected during analysis and laboratory testing and have not been encountered in actual operation. Airbus has addressed the issues through temporary revisions to the flight manual, including loading recommendations and a change to the center-of-gravity envelope, and would release updated flight control software in 2020. As Lufthansa waited for the 2020 flight software update, it blocked the last row of its aft-heavy layout of 180, offering only 174 seats.

2. Fundamental flaws in the B737 MAX certification process.

Although these trends are not exclusively Boeing specific, combining the three trends, makes the B737MAX an iconic case for corporate loss of design memory. After two years of investigation by American, Indonesian and Ethiopian investigative authorities, and by the US FAA and US Congressional Commissions, hearings and reports on the Lion Air and Ethiopian Air crashes the US House of Congress had to conclude that the design certification process was flawed (Dot 2015, 2016, 2020-1, 2020-2, House Committee 2020).

By the gradually increasing erosion of the B737 aerodynamic stability margins, final versions of the B737 became unstable, requiring a redesign of the Manoeuvering Characteristics Augmentation System (MCAS) device. The selected software solution was not failsafe, due to outsourcing of the software design and delegated self-certification by subcontractors.

Form variation of existing safety measures prevailed over reconsidering functional allocation of safety devices, downscaling residual risks as negligible, because of their assumed very low frequency. Within Boeing management, the ALARP principle was considered sufficiently reliable and dominant over the maximal credible accident approach. Cost and savings eliminated redundancy in sensor applications and corporate oversight over maintenance and repair. This downscaling process enabled application of a reduced certification regime to the level of 'derivative' adaptations on existing versions, rather than going through the full process of recertification. In the design, avoidance of non-normal situations prevailed over recovery from non-normal situations, downscaling necessary pilot training and skills. After designing the B737MAX, Boeing and FAA both outsourced engineering expertise, while reducing corporate and governance oversight over process control instead of substantive assessment of the safety concept. This caused a major loss of corporate memory and corporate culture of shared responsibility for product quality assurance (DoT 2015, 2016, 2020-1, 2020-2, House Committee 2020). Finally, a lack of feedback from pilot observations, maintenance and investigations hampered the process of learning from operational feedback. Consequently, the oversight over interferences between primary functions and the overall performance of the aircraft was lost, both during the design, certification and operational practices (Tkacik 2019, ESReDA 2020).

3 Back to reality: emergent events or serendipity?

In the academic debate on safety paradigms, the assumption of resilience engineering advocates is that socio-technical systems such as aviation are too complex to foresee events such as the B737MAX crashes. Such crashes are 'emergent' properties, inherent to the opaque and dynamic nature of complex systems. Learning from what goes right should be preferred over what went wrong. Such a feedforward learning curve, however, does not take into account the rich legacy of safety investigations that has made aviation non-plus ultra-safe. There is a vast repository of events, conditions and situations that have contributed to the safety performance level of aviation by analysing complex accidents and air disasters. Many of these accidents have become iconic because they represent phenomena with a wider range than an understanding of the isolated event itself. In addition, the aviation community is unique in having a professional community of air safety investigators: the International Society of Air Safety Investigators - ISASI. These are trained and qualified investigators with a background as pilots, academics, manufacturers, inspectors and operational experts in forensic disciplines and technological domains. Their work is organised in a formal mandatory and documented regime under the umbrella of the United Nations ICAO Annex 13. In aviation, national investigation agencies are legally based and institutionalized as independent assessors of air safety with the responsibility to issue recommendations to learn from events in order to prevent recurrence. Beyond the level of single event learning, 18 leading investigation agencies are sharing their experiences and learning in ITSA, the International Transportation Safety Association. To this extent, the aviation safety investigation community differs from investigative practices in other less technologically advanced sectors. By lacking globally institutionalized protocols and formalized methods, such sectors are bounded by analytic simplicity regarding their assumptions, simplifications, metaphors and modelling, such as the Swiss Cheese model, Black Swans, Heinrich Pyramid, Bowtie model and others.

Learning from accidents in aviation, therefore, is an institutionalized part of the legacy of the sector, based on a collective memory and repository of shared experiences. This also means, however, that unanticipated events still may occur. Instead of declaring major events as unanticipated 'emergent properties', new operating conditions and constraints may create catastrophic events due to shifts, drift and changes that have not yet been

observed in practice. The nature of such events can be characterized as serendipity: disclosing *by accident*, occurrences that have not been observed before. According to Vincenti (1990) such events may be based on inherent properties that were triggered by changes in the operational conditions and context of the system.

A question therefore is: could the crashes of the B737 MAX have been foreseen? Were there any properties and conditions that could reasonably predict this outcome?

Three previous major air crashes that occurred with Boeing aircraft contain elements and building blocks that can be recognized in the B737MAX sequence of events:

- **Lauda Air flight 004.** During this flight in May 1991, an uncommanded and unexpected deployment of the thrust reverser occurred in mid-flight. Due to gradual modifications and reconfiguration of the thrust reversers in previous versions of the B767, the airflow over the wing became corrupted during deployment and stalled the aircraft. Manual intervention on the thrust reverser deployment by the crew had been replaced by an electronic safety control mechanism. The aircraft became uncontrollable, killing everybody on board. It took the personal, lasting efforts of Nicky Lauda to clarify and explain the causes of this accident. Earlier tests at low speed and altitude granted in flight deployment as acceptable and survivable. However, high speed and high altitude deployment in mid-air was not included in the tests, but would have informed FAA and Boeing about the danger and unsurvivability of the occurrence.
- **ElAl flight 1862.** In October 1992, a B747 Cargo plane of ElAl crashed into an apartment block in the Bijlmer near Amsterdam, killing all 3 crew and 40 inhabitants. The fuse pins of the engine pylon failed during an overload condition, separating 2 of the engines from the aircraft causing an irrecoverable split flat situation at low altitude. A design analysis of the engine pylon revealed limitations in the static load calculations and fatigue issues. An upgrading of the B707 pylons towards the B747 pylons created overstretching of the static design assumptions. Successively after the crash, the pylons of all B747's were redesigned and replaced.
- **Asiana flight 214.** In July 2013, a B777 of Asiana Airlines crashed short of the runway at San Francisco during landing, killing 3 passengers and caused a hull loss. The National Transportation Safety Board of the USA observed in its report multiple autopilot and autothrottle modes which were not activated and understood by the pilots, who relied on the automated devices for speed control during final descent. The pilot flying unintendedly deactivated the automated airspeed control, loosing awareness of airspeed tolerances and acceptability of the glidepath limits, delaying a go-around execution. The pilot monitoring/instructor performed inadequate supervision over the pilot flying. Contributing to the accident were inadequate descriptions in the Boeing documentation and the companies pilot training.

In reference to the causes of the B737MAX crashes, all basic phenomena had been identified in previous accidents: aerodynamic interference between wing and nacelle, linear extrapolation of the assumptions on dimensions of design parameters, modelling restrictions, test assumptions, mode awareness and automation confusion. These phenomena were already identifiable from the Breguet equation, which was originally derived in 1916.

These accidents raise questions about the track record of Boeing in keeping aware of the lessons learned from accidents. Extrapolation of concepts with respect to aircraft dimensions, automation rate, pilot training and survivability of events depends on the repository of lessons learned from accidents. Issuing recommendations and introducing remedies after specific events may contribute to prevention of similar events, but do not necessarily recognize underlaying phenomena and more generic properties. Systemic trends in man-machine automation towards single pilot aircraft, remote tower control, and unmanned aircraft are based on shared assumptions and modelling of performance prediction. Derivative designs with linear extrapolation of design parameters in aircraft capacity, endurance and propulsion power may cross limits of validity of such extrapolations. Public perception and appreciation of safety, shifting societal values,

efficiency considerations, sustainability and energy transition have their impact on the system performance, which may interfere and yet go unnoticed until they are recognized as a disruptive anomaly. Assessing safety of such extrapolations may be based on misleading risk performance indicators (Wittenberg 1999). At present, risk indicators indicate increased safety because they rely on growth in blockspeed, aircraft size and long haul flights, assuming a linear relation between risk and growth, independent on the size of the population at risk. These risk indicators are related to the individual risk for aircraft airworthiness (flight hours) and passenger safety (passenger km), not to the systemic risk for the aviation sector as such. These indicators suggest an increase in safety performance that is not related to actual safety improvements, but related to systemic growth factors of traffic volumes, and as such, are a mathematical exercise rather than a representation of reality (Wittenberg 1999). To harmonize growth and safety, Wittenberg emphasis the need to balance technical aircraft design engineering and human factor engineering.

This observation poses interesting dilemma's:

- is there a risk asymptote in aviation with laws of diminishing returns, and consequently, an inevitable residual risk due to 'emergent' properties?
- Are we bound to rely on resilience for recovery from unavoidable mishap and unforeseeable non-normal situations?
- Are we bound to see the pilot as the last line of defence against disaster?
- Or can we modify the certification process to foresee unsafe conditions and situations by design and operational feedback through analysis and knowledge development?

At the moment, the certification process as such does not substantively discriminate between derivative and disruptive developments and is seducing to define any change as derivative rather than disruptive for reasons of cost and lead time reduction (DoT 2015, 2016, 2020-1, 2020-2, House Committee 2020). This raises questions about:

- How do you know when you crossed a line in defining anomalies?

How can you discriminate between derivative and disruptive solutions regarding their form, function or concept?

- What can you reliably foresee as prospective performance, lacking data of future exposure?
- Or: are we only reliant on Good Airmanship as the last line of defence and what does that mean?

4 Towards a new man-machine interrelations design?

The original pilot in the early days of fixed wing flight had a functional role of controlling the propulsion power and to manage lateral and vertical flight controls (Mohrmann 2021). They had to understand, maintain and operate the powerplants and electrical systems. With the increase in support systems and automation, their role slowly evolved into operators, involved into conducting prescribed tasks to reduce the physical and mental load during long flights and critical situations. This role removed some tasks (almost completely) from a pilot, but introduced new cognitive demanding tasks and crew resource management skills. This evolution is characterized as 'Aviate, Navigate, Communicate and Manage' and controls the performance during the flight. This evolution is focusing on increasing the performance of the pilot and simultaneously reducing crew costs by reducing the number of crew and training costs of the flight crew in the cockpit. While eliminating certain types of error, it introduced new human-machine interaction issues, such as mode awareness, automation complacency, startle and surprise during system malfunctioning and recovery in non-normal situations. It raises questions about how knowledgeable pilots should be, able to cope with unforeseen situations, anomalies and system failure.

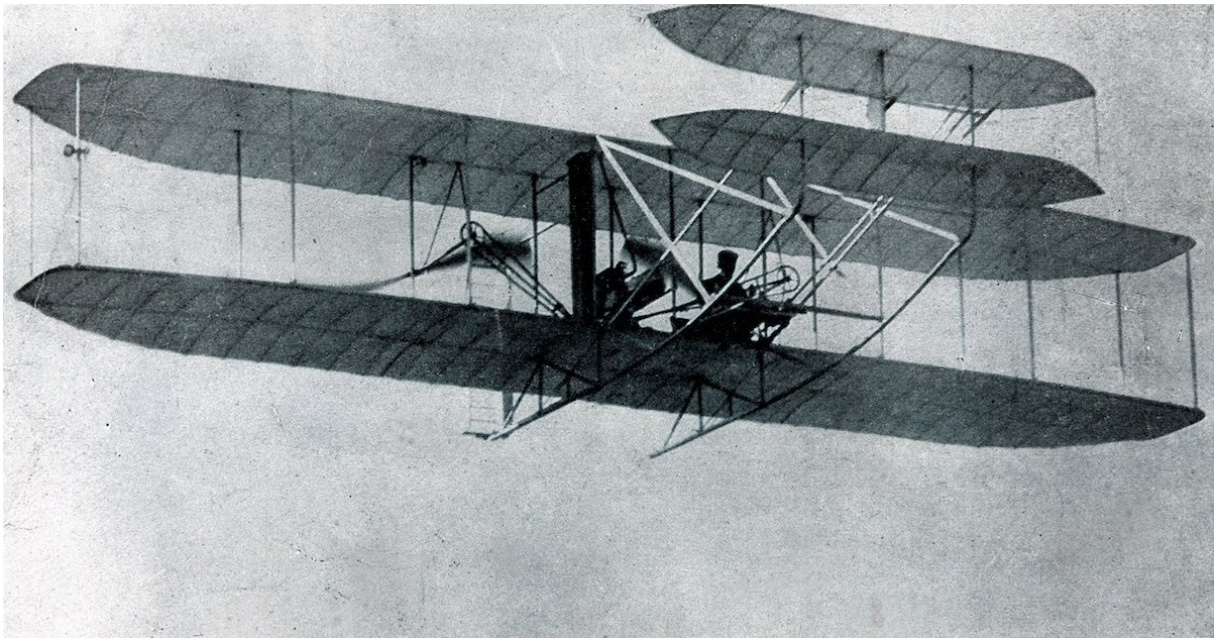
Since the pilot is the last line of defence, the notion of Good Airmanship has been adhered to, similar to Good Seamanship in the maritime sector. Due to advanced automation, single pilot and glass cockpit developments, a more fundamental reconsideration on the pilot role and tasks has become inevitable (Mohrmann 2021). The concept of Good Airmanship 2.0 covers issues related to the pilot as competent problem solver and underlying fundamental design assumptions on the interaction between pilots and their aircraft (Mohrmann 2021). Such a reconsideration has its impact on what should characterize Good Airmanship 2.0: personality, competence-based selection, problem solving and decision-making capabilities, mindfulness and self-regulation ability, gaming ability and neurofeedback experience (Mohrmann and Stoop 2019).

Such a Good Airmanship 2.0 concept, however, cannot be separated from the engineering design of the aircraft. As suggested by Woods (2019) from a psycho-sociological perspective -and in line with the suggestion of Wittenberg in 1999 from a socio-technical engineering perspective - a new unit of analysis is required to cope with the challenges of modern man-machine issues. The focus should be on the man-machine-interface as an analytic unit, instead of the conventional either man or machine analytical approach. A challenging question in this new concept is how to discriminate between derivative, disruptive and innovative approaches. How can we identify and test assumptions, simplifications and modelling issues, and how do we assess the dynamic interaction between man and machine, each with their own engineering design logic?

5 Certification challenges

This man-machine dynamic interrelation is as old as aviation itself. The issue of aerodynamic redundancy in longitudinal stability is as old as the design of the Wright brothers. The control of their first design was based on the canard wing configuration; a stabilizing wing in front of the aircraft. Such a canard wing however, demanded a permanent vigilance of the pilot because the concept was aerodynamically unstable, relying on the timely response capability of the pilot to aircraft behaviour. This issue was initially solved by changing from an aerodynamically inherent instable canard concept to an aerodynamically stable horizontal tail concept with the pilot as the ultimate controller of the aircraft longitudinal stability.

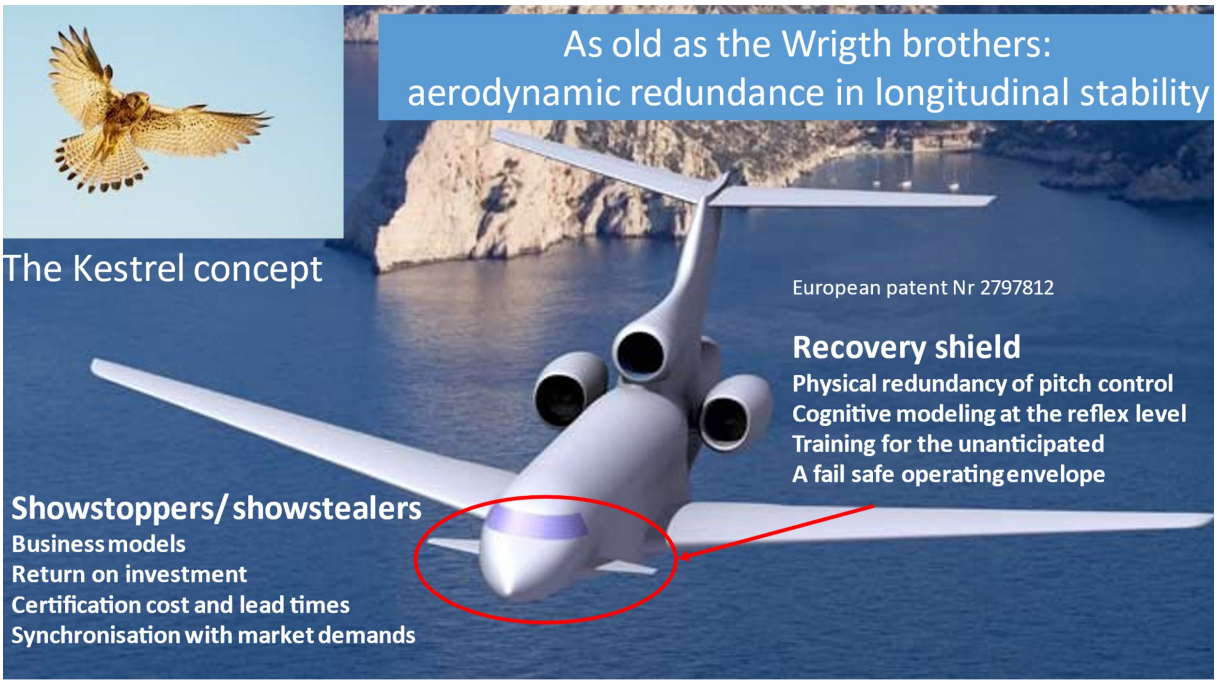
Figure 3. The Wright Flyer canard concept.



After its introduction in the military, the fly by wire concept - by far exceeding a human response capability to dynamic aircraft behaviour - enabled a return to slightly unstable commercial aircraft for reasons of fuel economy and weight reduction. This trend towards slightly unstable commercial aircraft created successive generations of aircraft design, such as the B737 series into the ultimate MAX version. In addition, rather than an ability to manage stall at high angles of attack, avoiding the stall region became preferred because of a reduction of training skills and costs and pilot type conversion flexibility. Drivers for this trend were provided by the business models, return on investment, synchronisation with market demands and competitive challenges with Airbus as the global competitor. During certification, testing and pilot training, for reasons of costs and lead time to market, all these modifications were considered derivative, not disruptive (DoT 2015, 2016, 2020-1, 2020-2, House Committee 2020). These considerations, however, downgraded the safety unnoticed by iterating the optimization process over and over again during the four generations of the B737 development. Consequently, the B737MAX can be considered 'one iteration too far'.

The issue of solving the B737MAX instability has been addressed by a series of derivatives based on form variations of already existing solutions and approaches to avoid huge costs and long lead times of recertification of the aircraft design and exhaustive pilot training efforts (DoT 2015, 2016, 2020-1, 2020-2, House Committee 2020). A more fundamental issue of providing aerodynamic redundancy for the pitch control issue, however, has not been considered feasible and cost-effective. The legacy nature of the sector and competitive edges in a neoliberal market prevent a disruptive approach by an overall redesign of the aerodynamic stability and control system. Since thrust vectoring is not available to the extent as in the military for fighter flight controls, a merging of aerodynamics and fly-by-wire technologies is indispensable and inevitable to design disruptive solutions for introducing redundancy in pitch stability and control functionality. Such a disruptive aerodynamic solution has been developed, based on the Wright brothers Flyer, combined with Fly by Wire principles and is available by the Kestrel concept, patented by the EU Nr 2797812 (Stoop and De Kroes 2012, EU Patent 2020).

Figure 4. The Kestrel concept.



Such a combined introduction of the Kestrel patent and Good Airmanship 2.0 concept in the sector requires a transition strategy beyond the level of a technological invention, its patents and training revisions. Changes will be the result of overcoming limitations in a social acceptance of aviation and commercial boundary conditions regarding other societal values than safety versus economy only. To this purpose, the Modified Cyclic Innovation Model (MCIM) has been proposed as a new initiative and tool to manage innovation in this legacy sector and to overcome the conservative legacy forcefields in aviation (Boosten and Stoop 2021).

By applying the MCIM model, three conditions have been identified to enhance the stability and controllability of the 4th generation of instable commercial aircraft of the tube and wing configuration:

- Identification of show stealers and showstoppers in the innovation process of a non-technical nature, regarding scientific, societal and commercial conditions and constraints
- A complimentary simultaneous analytical approach covering man, machine and their interrelations as the unit of analysis, defined by Woods
- Application of a prospective tool to foresee the behaviour, systemic interrelations and their consequences during the design and certification framework of disruptive solutions that have not yet been operationalized.

6 Conclusions

To prevent learning from accidents with a disruptive innovation, in particular in this paper, attention has been paid to the current certification process. The B737MAX crashes have shown that a specific and explicit regime for certifying disruptive solutions is lacking at the moment. There is no decision support tool with explicit criteria that enables an assessment whether a solution is to be considered and processed as either derivative or disruptive.

In the aviation certification process, a tool is lacking that enables answers during design and certification in discriminating between derivative and disruptive approaches. Such a tool serves the goal of:

- making a distinction between form variation, function allocation and value identification in ranking solutions and allocating specific certification regimes to these solutions
- identification of the pilot and cockpit crew as competent problem solvers in a Good Airmanship 2.0 context
- designing redundancy in the pitch control functionality by combining aerodynamic properties and fly-by-wire control technology as provided by the Kestrel Patent
- dealing with complexity by enhancing the transparency in the system by combining feedback and feedforward across life cycles, system levels, state transitions and actor responsibilities at both the operational, organisational and governance level of the system
- creating a shared knowledge repository from lessons learned on underlying phenomena, repetitive patterns in trends and aspects that enable a thematic and knowledge-based approach on principles, assumptions and modelling.

Such a tool facilitates discrimination between derivative and disruptive adaptations during certification. It is necessary to develop dedicated algorithms and procedures for assessing disruptive anomalies. Use of the tool, however, is conditional: the tool is applicable in the context of the socio-technical system as modelled by the MCIM and should be applied by subject matter experts, knowledgeable in the aviation sector. To achieve, maintain and guarantee oversight, insight and foresight over such a certification process, a role for an aeronautical architect and system integrator should be recognized. Such a role is similar

to the distinct roles as already allocated between maritime engineers and naval architects in designing the role of Good Airmanship as equivalent to Good Seamanship.

References

Official safety investigation agency Accident Reports on:
Lion Air flight 610, 29 Oct 2018
Ethiopian Airlines flight, 10 March 2019
Lauda Air flight 004, 26 May 1991
ElAl flight 1862, 4 Oct 1992
Asiana Airlines flight 142, 6 July 2013

Boosten G. and Stoop J.A., 2021. Transition towards sustainable aviation. Need for new tools to gain insight? 58th ESReDA Seminar, Using Knowledge to Manage Risks and Threats: Practices and Challenges. Alkmaar, the Netherlands, 15-16 June 2021

DoT 2015. FAA lacks an effective staffing model and risk-based oversight process for organization designation authorization. FAA Office of Inspector General Audit report. October 15, 2015

DoT 2016. Safety Issues and Shortcomings with Requirements, Definition, Validation, and Verification Processes Final Report. DoT/FAA/TC -16/39, Dec 2016

DoT Special Committee 2020. Official Report of the Special Committee to review the Federal Aviation Administration's Aircraft Certification Process. Jan 16, 2020, US Department of Transportation

DoT 2020. Timeline of Activities Leading to the Certification of the Boeing 737 MAX8 Aircraft and Actions Taken After the October 2018 Lion Air Accident. US Department of Transportation, Office of Inspector general. Report No. AV2020037, June 29, 2020

ESReDA 2020. Enhancing Safety: The Challenge of Foresight. ESReDA Project Group Foresight in Safety. EUR 30441

EU Patent, 2000. European Union Patent no 2797812, Dec 2020.

FAA 2017. The FAA and Industry Guide to Product Certification. Third Edition, May 2017

House Committee 2020. The Boeing 737 MAX Aircraft: costs, consequences, and Lessons from its Design, Development, and Certification. Preliminary Investigative Findings. House Committee on Transportation and Infrastructure, March 2020

Mohrmann F. and Stoop J.A., 2019. Airmanship 2.0: Innovating human factors forensics to a necessary proactive role. ISASI Conference, Aug 2019, The Hague, The Netherlands

Mohrmann F., 2021. What do we need pilots for? Proposing a more effective natural order in the socio-technical system of flight operations and the larger implications for the aviation industry. In press

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.

Tkacik M., 2019. Crash Course. How Boeing's managerial revolution created the 737 MAX disaster.

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

Troadec J.P., 2013. AF447 presentation by Director of BEA. Second International Accident Investigation Forum, Singapore 23-25 April 2013

Vincenti W., 1990. What Engineers Know and How They Know IT. Analytical Studies from Aeronautical History. The John Hopkins University Press

Wittenberg H., 1999. Safety in aviation; achievements and targets. Memorandum M-353, Faculty of Aerospace Engineering. Delft University of Technology

Woods D., 2019. Essentials of resilience, revisited.
https://www.researchgtae.net/publications /330116587

Existing Knowledge in Risk-Based Electrical Safety Supervision Work

Hennamari Valkeinen and Ville Huurinainen, The Finnish Safety and Chemicals Agency, hennamari.valkeinen@tukes.fi, ville.huurinainen@tukes.fi

Abstract

The Finnish Safety and Chemicals Agency (Tukes) is the electrical safety authority in Finland. It monitors that the Electrical Safety Act (1135/2016), standards and law-based regulations are complied with. This paper focuses on the electrical safety work done by Tukes' Electrical Installations Unit, a relatively small group with seven inspectors. With Finland having more than 20 000 electrical contractors and 4000 installations that require a supervisor of electrical operations, it is crucial that Tukes' supervision work is planned risk-based to target the most problematic areas in electrical safety.

Tukes' work includes both field and document supervision. The Electrical Installations Unit performs approximately 250 supervising visits in a year to meet the contractors and other responsible persons face to face. Tukes is also frequently contacted by both electrical professionals and non-professionals, who provide valuable information about occurred electrical accidents and incidents. This information is looked into, actions taken when needed, and the data is recorded to be used in the planning and execution of risk-based supervision and risk communication. At the end of every year the next year's objectives for supervision are decided based on behaviour or neglected safety issues that are identified potentially most hazardous. The collected information about accidents and incidents is also used to improve legislation and standards and as background information in accident investigations.

Over the past 25 years Tukes' persistent work has provided Finland with a lot of knowledge about potential electrical safety risks and the operators' practices. This is thanks to both recorded accident and incident data, but also to the know-how acquired during long inspector careers, which all have an important role in the planning of risk-based supervision work. The knowledge has prepared Tukes to better manage and regulate potential high-risk behaviour by e.g. targeting inspector resources and press releases to influence the most problematic sectors in the electrical industry before actual incidents occur. The actions have enhanced Finland's high level of electrical safety: Annually there are only approximately two fatalities caused by electric shock and ten fatalities caused by electric fires.

Despite the high level of electrical safety in Finland there are still challenges. For example it is recognized, that not all electric accidents or incidents are reported. This means that relevant information is still lacking. The challenges faced by the authority in its work of supervising and promoting electrical safety in Finland are mainly related to this missing information and people's attitudes in cutting corners with safety issues.

1 Introduction

The Finnish Safety and Chemicals Agency (Tukes) has been the Electrical Safety Authority in Finland since 1995. The electrical safety supervision work is done by two different groups of inspectors and technical advisors. These two groups are the Electrical Installations Unit and the Electrical Products Unit. This article will focus on the Electrical Installations Unit's work. Both groups are relatively small (altogether 12 inspectors) and the supervision work includes the entire Finland except for the autonomous area of the Åland Islands. This is

why it is crucial to target the supervision to e.g. the most problematic sectors in the electrical contracting and electrical installations industry. Learning from previous electrical accidents and incidents plays an important role in Tukes' risk-based supervision work.

2 Electrical Safety Installations Unit

Tukes' Electrical Safety Installations Unit monitors that the Electrical Safety Act (1135/2016), standards and law-based regulations are complied with. The unit has three main areas of monitoring:

- electrical installations (fixed and semi-fixed installations in buildings, infrastructures etc.)
- electrical contracting and electrical work (companies and third-party inspection bodies)
- lift safety (one specialist in the unit - this article will be focused on electrical safety issues and does not include elevators).

There are several methods to monitor electrical safety in these sectors. This includes for example field and document supervision, and guidance given to both electrical professionals and non-professionals by phone or email, or via press releases and newsletters.

The Electrical Safety Act 1135/2016 *"contains provisions on the requirements laid down for electrical equipment and electrical installations, demonstration of the conformity of electrical equipment and electrical installations, supervision of conformity, electrical work and its supervision, and the liability for damage of the possessor of electrical equipment and electrical installation"*[1]. It is the main guideline for electrical safety supervision. There are also several complementing regulations and standards to follow.

Tukes' Electrical Safety Installations Unit has seven inspectors to make sure that regulations and standards are complied with. There are approximately two million electrical installations in Finland. The inspectors perform about 250 field supervising visits in a year, which is about 35 per person. This is not very much considering that there are approximately 4000 electrical installations in Finland that require a supervisor of operations, approximately 20 000 electrical contractors and approximately 110 authorized third party inspectors and three inspection bodies to be supervised.

With this relatively small number of human resources it is important to make sure the unit's resources are focused on the most problematic sectors in the area. There are several ways of collecting information to better target these sectors. One of the most important is the actions of Tukes **electrical incident group** of five inspectors that investigates the received accident and incident information. The long careers of the experienced electrical safety inspectors provide both explicit and implicit knowledge and are a great benefit in risk-based supervision work. The Electrical Installations Unit also has recruited recently and the new, younger inspectors provide the unit with more understanding of new techniques and practices used in the field.

2.1 Supervision of the Responsible Persons, Contracting and Electrical Installations

There are two positions named in the Finnish Electrical Safety Act that are called responsible persons. These are **the electrical work supervisor** and **the operator of electrical installation**. They are the professionals that Tukes' supervision work is mainly focused on and who the inspectors visit and interview on their supervision.

An electrical operator must designate an **electrical work supervisor,** whose responsibility is to ensure that the Electrical Safety Act, regulations and standards are

([1]) Electrical Safety Act 1135/2016, section 1, unofficial translation

complied with and that the employees are qualified and skilled enough for electrical work. This electrical work supervisor must be notified to Tukes' register of operators.

In addition to designating an electrical work supervisor, Finland has a unique national system, when it comes to electrical installations where:

1) the electrical installation includes parts with a rated voltage in excess of 1,000 V, or;
2) the electrical installation has a connection capacity in excess of 1,600 kVA. [2]

These installations require a designated **operator of electrical installation.** It is also required by the Electrical Safety Act to submit a notification of these installations and the name of the operator of electrical installations to Tukes' register of operators for supervision purposes[3]. There are several employees in the Electrical Installations Unit, whose important job is to check and process these notifications to ensure that the data is up to date, as required in the Electrical Safety Act.

2.2 The Electrical Incident Group

According to the Electrical Safety Act 1135/2016, Tukes must investigate accidents and seriously dangerous situations caused by electricity:

"The Electrical Safety Authority shall investigate accidents […] causing serious damage if the Electrical Safety Authority is of the view that this is necessary for establishing the cause of the accident, or for preventing future accidents. The Electrical Safety Authority also has the right to investigate other accidents and seriously dangerous situations that have been caused by electricity, if this is necessary for establishing the cause of the accident, or for preventing future accidents" [4].

Tukes receives notifications every day from both electrical professionals and non-professionals. Based on the authorization given in the Electrical Safety Act (§ 114), these notifications are looked into and actions taken when it is needed. There are approximately 300 electrical incident notifications annually that do not require specific actions from Tukes. Some of the notifications clearly state that the operator has taken all necessary actions already to change their actions in the future and there are no further actions needed. These are e.g. cases, where the operator reports a potentially hazardous incident, but has already fixed their own actions based on what happened, what they learnt and how similar incidents can be prevented in the future.

The importance of the received notifications is important and very often gives Tukes guidelines as to where to focus the newsletters and field supervision. Actions by Tukes are typically needed for example in cases of serious, life-threatening accidents, illegal electrical work or when an electrical contractor has neglected regulations. The electrical incident group's actions (from mildest to most severe) may include e.g.

- information letters telling of the requirements concerning electrical contracting
- requests for clarification of the operator's actions
- administrative decisions based on the operator's clarifications:
    - warning
    - prohibiting the operator, electrical work supervisor or supervisor of operations from performing their duties, for a limited period or until further notice, partially or in full
    - police investigation requests.

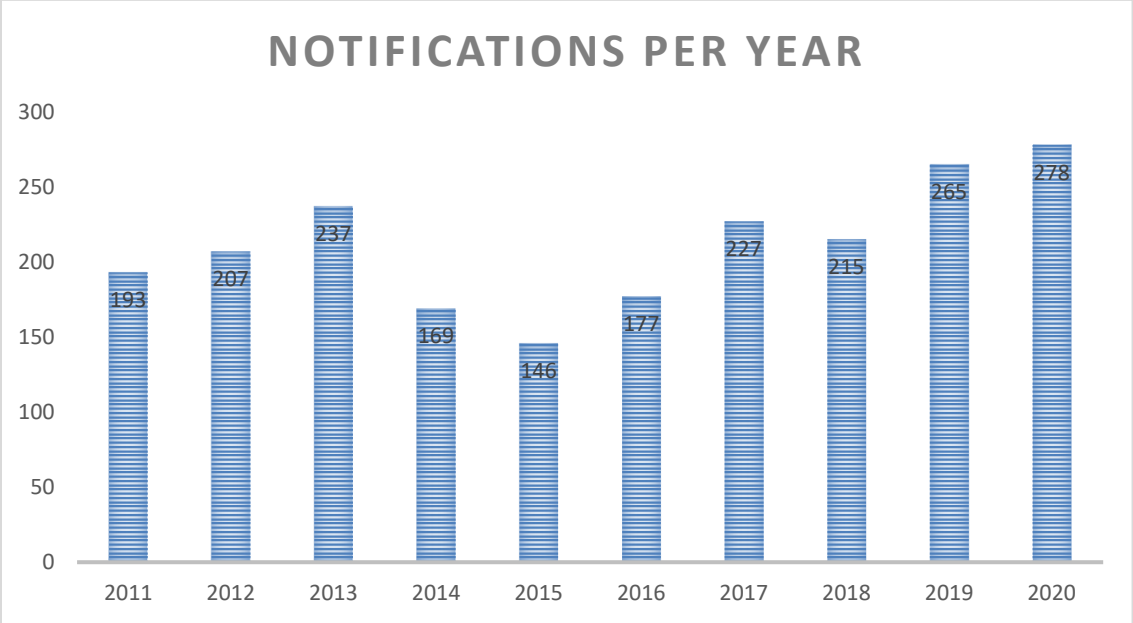
([2]) Electrical Safety Act 1135/2016, section 44
([3]) Electrical Safety Act 1135/2016, section 60
([4]) Electrical Safety Act 1135/2016, section 114

The electrical incident group has a long history. Even more detailed data is available since 2011, when the documentation was transferred to a new database with more features. It has proven to be a useful tool and makes sorting the data easier than before.

The numbers in figures 1 and 2 are actual recorded notification numbers from the database. It is also possible to sort the data based on e.g. notifications made by electricity distribution companies, third party inspectors or non-professionals. It has grown from being a simple knowledge storage to being a crucial part of actual electrical safety supervision practices.

The number of notifications that have required actions from Tukes has been increasing slightly in recent years, being 146 notifications in 2015 and 278 notifications in 2020, as seen in figure 1. Notifications are received from both professionals and non-professionals. Accidents, incidents, etc

Figure 1. Number of accident/incident notifications per year (2011-2020)



Source: Tukes records, 2021.

NOTE: these numbers don't include the 300 annual notifications mentioned above, that do not require actions.

2.2.1 Notifications from Electrical Professionals and Other Authorities

Electrical professionals very typically use SL4 form to inform Tukes about accidents and incidents. These professionals are usually responsible persons who work for industrial facilities, electricity distributors or in electrical contracting companies. The form is available on the Tukes website.

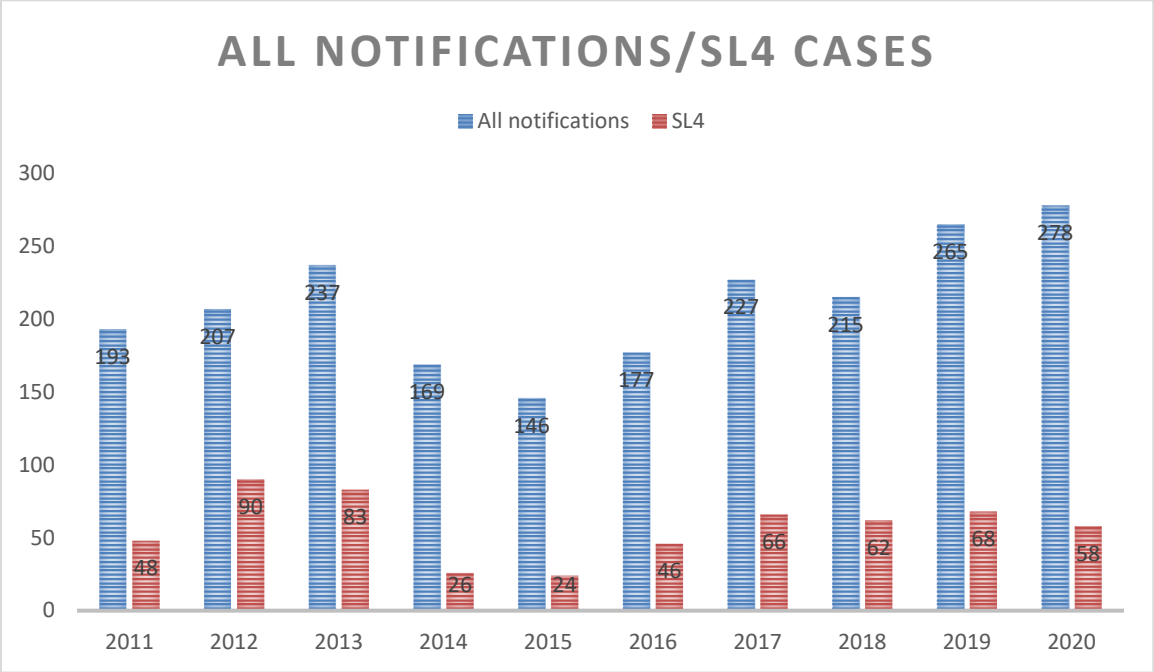
SL4 form includes information about

- what happened,
- where,
- why,
- what events led to the accident or incident,
- how serious the accident or incident was (number of sick leave days) and
- how it could have been avoided.

The SL4 form is intended for the police, rescue authorities, occupational safety and health authorities and the possessor of a distribution network of a distribution area, who by law must report to the Electrical Safety Authority dangerous situations and accidents that have caused severe injuries, property damage or environmental damage involving electrical equipment or electrical installation[5]. The SL4 form is a helpful tool to report accidents and incidents, but it is not compulsory to use it. Other authorities don't always use the SL4 form. They typically contact Tukes when electricity has caused fatalities (either by electric shock or by electrical fires). The number of fatalities caused by electricity in Finland is low: on an average year there are two fatalities caused by an electric shock and ten fatalities caused by electric fires.

The number of SL4 notifications requiring Tukes' actions is annually approximately 20 % of all notifications, as seen in figure 2.

Figure 2. Number of accident/incident notifications vs SL4 cases (2011-2020)



Source: Tukes records, 2021.

2.2.2 Notifications from Non-Professionals

Non-professionals typically contact Tukes through informal channels, such as email, telephone or by filling a question and feedback form on the Tukes website. Non-professionals occasionally use SL4 form too. Their notifications typically include information about illegal electrical contracting or danger-causing errors in the installation work.

2.2.3 The Utilization of Knowledge in Risk-Based Supervision Work

Information gained through Tukes supervision work in the field and notifications received from electrical companies and consumers are both essential parts in detecting early warning signs. This helps focus the supervision activities to the problematic sectors before accidents occur. The information is also conveyed to those responsible for the development work of the electrical safety legislation.

Every year the field supervision objectives are decided based on the accident and incident data collected during previous years. The work of the electrical incident group plays a huge

([5]) Electrical Safety Act 1135/2016, section 114

role in choosing the objectives, as all the objectives are related to the group's work and observations of problems in the field.

Table 1. Field supervision objective examples (year 2019)

1. ELECTRICAL CONTRACTING	Σ
Electrical Incident Group findings	30
Electrical construction sites	25
New electrical contractors (0-2 years in operation)	25
Layman subcontractors of electricity distribution companies	20
Vocational schools with electrical contracting	10
Oil or gas contractors	5
Reactive inspections	42
Σ	157

2. ELECTRICAL INSTALLATION	Σ
Several reported problems, lack of maintenance documentation or Electrical Incident Group findings	10
Electricity distribution companies	8
Operators of electrical installations with multiple installations (>10)	10
Part-time operators of electrical installations (not employed by the possessor)	10
Possessors of massive entities (cities, towns, churches etc.)	8
Skiing centers	8
Reactive inspections	10
Σ	64

3. THIRD PARTY INSPECTORS	35
Σ 1, 2 AND 3	256

Source: Tukes records 2019.

3 Conclusions

Since it is not possible to supervise all operators in the field at the same time, it is crucial to focus actions to recognized problem areas. Notifications from both professionals and non-professionals provide Tukes with valuable information and play an important role in electrical safety supervision work. Electrical safety in Finland is at a high level. The information received is available for future needs and it is possible to return to older cases to see how risks have evolved.

It is recognized, that with today's multiple ways of contacting Tukes the number of notifications has gone up and Tukes receives up-to-date data about problems in the field. Despite this it is also a fact that not every incident gets reported. The operators must by

law report the most serious accidents, but it is certain that practices vary greatly between electrical contractors, electricity distribution companies and even authorities. Incidents with hazardous situations are typically fixed by the operators themselves by e.g. revisiting the guidelines with the employees to make sure no one is cutting corners. Once the situation is fixed, the operators don't always see it necessary to inform Tukes about the incidents. Though, in some cases this information would be extremely helpful to improve electrical safety in Finland. From the viewpoint of the safety authority, this lack of information is one of the major challenges in the promotion of electrical safety.

It is also recognized that with non-professionals even more valuable information is lacking. If a non-professional person does electrical work illegally at their own property and an electric shock or electric fire happens, they are very unlikely to report themselves to authorities. Since the regulations exclude private homes from electrical safety supervision, is very difficult to know what happens at people's homes. On the other hand, non-professionals who buy electrical contractor's services are very likely to report if they detect wrongful actions. Their contacts play an important role in intervening when professionals act against the Electrical Safety Act.

Acknowledgements

I would like to express my thanks to my colleague Tuuli Tulonen, who found time from her busy schedule and was a great help in the writing process.

References

1. Ministry of Employment and the Economy, *The Finnish Electrical Safety Act (1135/2016),* unofficial translation. 1135/2016 English - Translations of Finnish acts and decrees - FINLEX ® .

A creative factory of knowledge to support city resilience management

Antonio De Nicola and Maria Luisa Villani, ENEA – Centro Ricerche Casaccia, Roma

antonio.denicola@enea.it, marialuisa.villani@enea.it

Abstract

In this paper we describe semantics-based models and tools for knowledge elicitation to improve city resilience. The models and tools for knowledge collection are tailored to the specific application, such as emergency management, risk assessment and decision making for recovery, and the expertise and type of users such knowledge is required from. The different types of artefacts, created by means of the tools, are built relying on an ontology that provides the basis for both resilience knowledge representation and control. This will favour building and continuous enrichment of knowledge for resilient cities from different angles, and further enhancement of the automatic functions of the knowledge-based system we have detailed in our previous works.

The overall approach is described by means of examples taken from experimentations with real users of our tools, on different case studies related to resilience management of cities.

1 Introduction

Improving resilience of cities and communities requires a holistic analysis of risks to base mitigation and/or adaptation plans. The increasing frequency and severity of natural events due to climate change, but also unforeseen global crisis such as the COVID-19 pandemia, the strict interdependencies of infrastructures, and the growing spread of high-tech services, are exacerbating the complexity of risk assessment processes and, hence, decision making for a resilient society and organizations.

The increasing pervasiveness of technology is contributing to shaping the concept of cyber-socio-technical system [7] to better represent our society, where humans, cyber artifacts, and technical systems interact together to the purpose of achieving a goal related to the quality of life in urban areas. New IT technology and, especially, modern intelligent systems, like autonomous vehicles, are certainly drivers of smarter cities but also new sources of unknown threats.

Traditional methods for risk assessment are based on risk types and data on past events, which may not be readily updated according to the fast-changing world. Thus, these methods may fail against such a complexity because of the too limited number of identified threats and vulnerabilities and of the incomplete knowledge of unprecedented but potential impacts on systems and people. On the other hand, especially machine learning methods are being proposed to overcome human limits of data analysis and knowledge building, leveraging on open data repositories, sensors data and/or events information from social network platforms as additional data sources.

Machine learning solutions, although very powerful and largely used in the domain of risk assessment, as discussed in the literature, are limited by the context variability but also because they are not able to provide a readily explainable arguments for the predictions they make. Hence, these techniques still do not completely solve the problem of risk imagination foresight and sharing of tacit knowledge that yet mostly pertains to human beings.

Therefore, we argue that human-support is still needed to feed and complement, other than supervise, automatic mechanisms for risk identification and management.

In this line, we have developed a methodological and software framework for model-based risk knowledge co-creation and evolution, with a vision of a tools chain where the experts' activity is required to supervise smart automatic functions of risk scenarios generation and initial assessment of risks related to given geographic or urban areas.

A formal knowledge base is at the core of such a framework, with an extensible ontology devoted to TERritorial Management and INfrastructures for institutional and industrial Usage (TERMINUS), integrating knowledge on environment, critical infrastructures, economic assets, stakeholders, city and community services and related threats of natural, virtual and physical anthropic nature.

We have already developed and validated in experimentations with real users two novel software tools that leverage on such a knowledge base. The first, named M-CREAM [5] allows creative elicitation of emergency scenarios by city planners and services operators. The other one, named ICE-CREAM [3], is devoted to risk modelling and assessment for critical infrastructures and point of interests in urban contexts. The creative-based risk assessment approach of ICE-CREAM has been validated by real risk analysts by means of a GIS-based system [1]. Furthermore, we have developed a semantic model for e-participation to decision-making for post-crisis recovery of cities [6]. This has been experimented at a University summer school with doctoral and research staff on urban planning by using a real case study concerning reconstruction of L'Aquila city, after the earthquake event occurred in 2009.

In this paper, we present such models and tools as an assembly line for knowledge building finalized to resilience management in urban areas. In particular, by means of examples provided by the experts who participated in the experiences above, we show our model-based knowledge creation processes, from a user perspective, to form emergency scenario artefacts, risks and/or decisions for resilient cities.

The rest of the paper is organized as follows. Section 2 presents an overview of the knowledge-based framework, a description of its sub-systems with a summary of our experiences. Section 3 highlight examples of different types of knowledge representations concerning similar aspects of the city.

2 Knowledge-centred approaches for resilience

According to [8] "*urban resilience is the capacity of urban systems, communities, individuals, organisations and businesses to recover and maintain their function and thrive in the aftermath of a shock or a stress, regardless its impact, frequency or magnitude".* Among the ten essentials for making resilient cities[1] by city governments, are: identification and understanding of multi-hazard risks by means of scenarios that refer to current and future risks, and usage of this knowledge to inform decision making. Citizen's groups and other stakeholders should be engaged and involved in discussing the plans for the city's resilience [9].

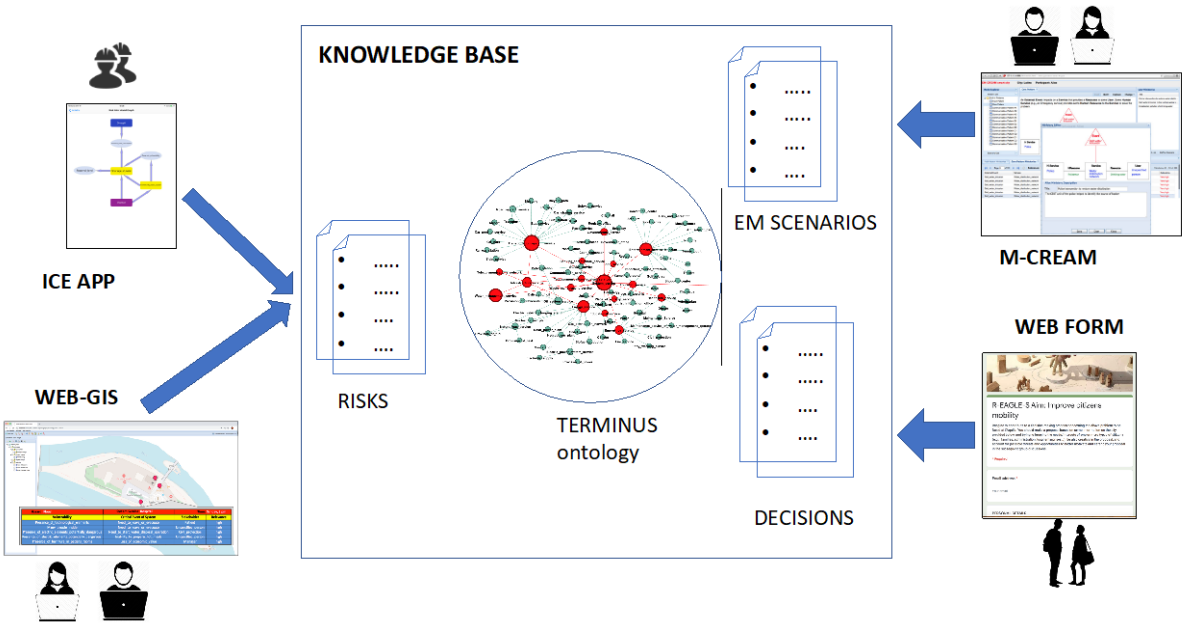
In this line, we propose an architecture for a software system devoted to knowledge creation about emergency management scenarios, multi-hazard and multi-perspective risk assessment, and decision-making for resilience in an urban context. We have addressed these three aspects of the system by means of specific software tools we have developed. These tools rely on a knowledge-based architectural model, consisting of an ontology and of semantics-based techniques to enable knowledge (co)creation on the specific activity, by means of a model-based methodology.

As a step forward, we are designing a system where the various approaches coexist towards a cooperative objective of machine-assisted knowledge creation for urban

[1] https://www.unisdr.org/campaign/resilientcities/toolkit/article/the-ten-essentials-for-making-cities-resilient

resilience assessment and planning, as illustrated in Figure 1. Indeed, every tool is mainly addressed to a specific type of user, so to make him/her able to provide knowledge from his/her own perspective. Indeed, emergency operators and city planners are accustomed to thinking on scenarios, and how events may develop, whereas risk analysts can directly work with risk definitions, and normal citizens are generally comfortable to expressing their needs and impacts for the city in a straightforward way.

Figure 1. Overview of the knowledge factory for city's resilience.



The main component of the Knowledge Base is an ontology, named TERMINUS [1] that is going to be extended with a domain ontology for urban planning for resilience. Other components of the Knowledge Base are artifacts generated by means of semantics-based techniques. These model artifacts are finalized by the users while performing the specific activity using the tools shown in Figure 1.

Following the idea of model-based design in the software engineering field, our objective is to support knowledge representation by means of the tools and facilitate knowledge sharing among the various types of users.

The reminder of this section is devoted to a brief description of the three knowledge-based approaches, from the perspective of the users. These approaches are more deeply described in [5], [1], and [6].

2.1 Emergency Management scenario modelling

We define an `EM Scenario` as a user narrative of a contextualized real or imagined emergency scenario in a city. This scenario is structured as a set of situations grouped in three phases: *start*, to describe the initiating event (trigger) and the (part of) emergency created in a spatial and temporal context of the city; *middle*, to describe what follows, e.g., secondary events and new situations that could arise; and *end*, to describe reactions by the emergency services and decisions. A tool we developed, named M-CREAM[2], aims at supporting users in defining and editing such types of scenarios that will be stored in the system.

[2] http://apic.casaccia.enea.it:8080/Ministories/Ministories.html

For a scenario, each described situation by the user comes as his/her own interpretation of a graphical conceptual model supplied by the tool, named `Ministory`. Therefore, an `EM Scenario` is attached to an `EM Scenario Model` that combines one or more `Ministories`.

These concepts are better clarified by means of the fragment of an imagined EM scenario illustrated in Figure 2, that was created by a Civil Protection operator of Roma premises, who used M-CREAM. Namely, the EM Scenario at right hand side was edited inspired by small graphical models at left hand side, named ministories, selected by the users. Each ministory, essentially illustrates some critical event for a service impacting on its operation towards its users, or towards other services, and/or how the last may react. Thus, for given a contextual configuration related to the city, M-CREAM produces a number of ministories from which the user may be inspired to construct his/her own scenario.

For example, the ministory at the bottom of Figure 2, on the left-hand side, represents a conceptual model of the following situation:

*A **clash** impacts on the **Railway** service, therefore a **Civil Protection operator** is **informed of the critical situation** by means of a **mobile device**, to help in the emergency.*

Such a ministory, which taken out from an imagined context, might seem not so significant, was indeed very useful to a Civil Protection operator, while she was creating her scenario, as a follow up to a chain of events she was constructing.

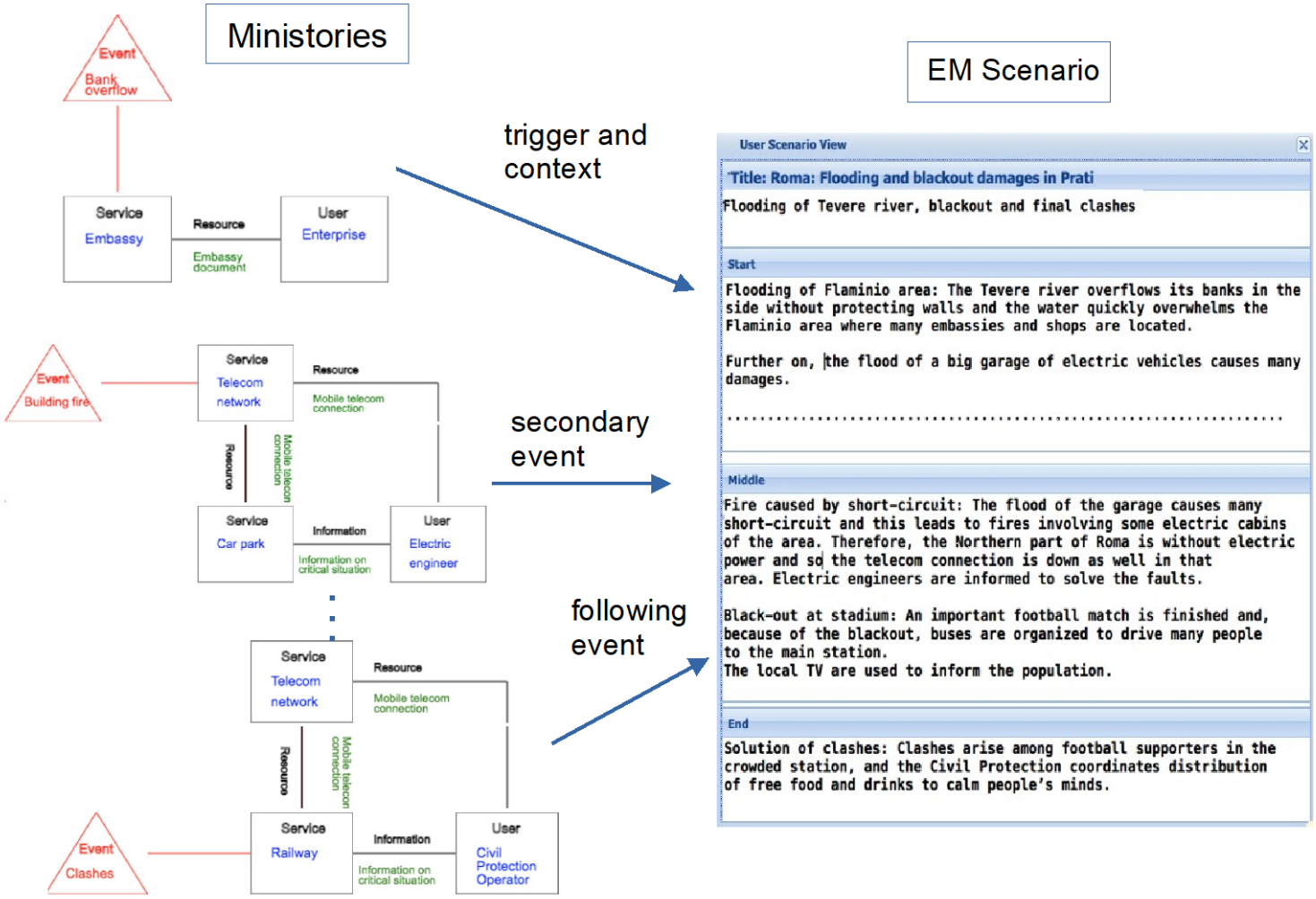
The overall scenario she produced, whose fragments are shown in the right part of Figure 2, originated by a *bank overflow* of the Tevere river, which led to *flood* of a big car park of electric vehicles causing faults in various parts of the electric system and a blackout of the area. Such area involved a *stadium* where an important football match had just finished, so that many people were transferred to the *railway station*. There, *clashes* arose among different groups of football supporters and the *Civil Protection* was involved to calm down the situation by implementing the idea of distributing free food and drinks.

The real operator of the Italian Civil Protection that provided this scenario, was certainly influenced by her work experiences but she also imagined new plausible situations, and their sequences, challenged by the ministories supplied by the tool.

Ministories are automatically generated by M-CREAM by using TERMINUS and patterns that represent abstract bueprints of situations. A pattern is composed of an event, a service impacted by it, users and exchanged resources. Various ministories, which specify the particular events and services/users involved, may be generated by the tool as different combinations of concepts of the ontology. These ministories constitute a search space for EM scenarios construction.

In [5], scenario modeling was presented as a new research problem within the computational creativity area as the implemented system follows techniques for creative design. From a technical perspective, the tool implements automatic reasoning and search methods based on semantic similarity and ranking to help users in the identification of ministories in the search space, leading to plausible scenario contents. This methodology follows the idea that a new design, i.e., a new ministory/situation for a scenario, can result from transformation of aspects of some known design and/or by analogy thinking.

Figure 2. Example of EM scenario and originating ministories.



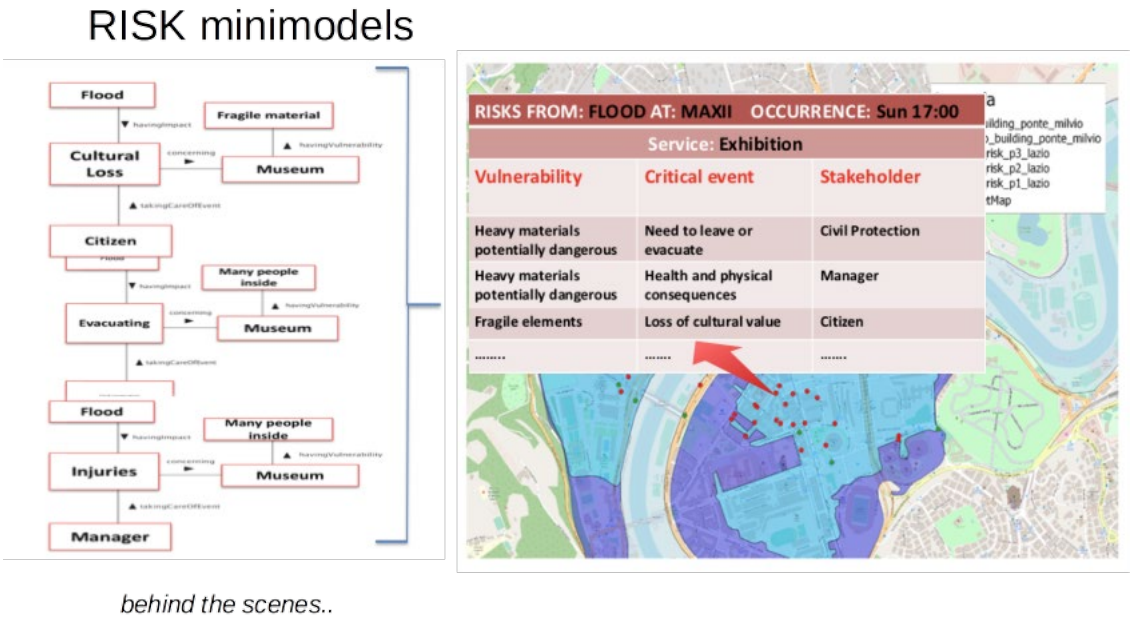
2.2 Risk modelling

Risk elicitation is a crucial activity to realize reliable models for assessment. This activity requires different expertise, creativity as well as some capability of knowledge modelling. An ontological model, i.e., a Risk ODP, of a System Risk has been initially proposed in a previous paper [2], and named Vulnerability Assessment Model (VUM). Such a model was experimented for water system risks derived from climate change hazards.

In subsequent works [1, 4] we defined a simplified model (or Risk ODP) to describe risks so to explicitly represent critical event/impact sets on a service, that may derive from the same hazard. This allowed us to build tool interfaces of our CREAM-based approach that can be contextualized within digital maps of the city, for a better interpretability and usability by both risk analysts and emergency planners.

The user interface with an example of Risk for the MAXXI museum in Rome, and the ontology-based models used to generate its description, are shown in Figure 3.

Figure 3. Example of system risk model as a combination of risk minimodels.



In particular, a `System RISK`, after validation by some risk analyst, is based on a `System RISK Model`, which results from merging a number of risk model fragments, named `RISK minimodels`. These are semantic models automatically generated by the CREAM tool by querying the TERMINUS ontology.

Every risk minimodel describes what vulnerability of the specific system may be exploited by a given hazard and may lead to some critical event for the system. Such event is considered critical from the perspective of some stakeholder.

The risk models generated for a given system/service by our method are based on its semantics, e.g., museum, hospital,.., and so, in principle, these descriptions are common to all other systems/services of that type. However, contextual information from the field provided by the GIS, related to the geographic information and environmental conditions, allow to automatically prioritize these risks for the individual system/service at hand.

2.3 Decision modelling

A real recovery after a disaster can be achieved by involving citizens in the decision-making processes as these decisions will have an impact on their lives.
Social media are used to enable free participation in decision proposals but the work of human facilitators to guarantee focused and effective discussions might be demanding. Moreover, ex-post analysis of content and intent of messages are hindered by the fact that the information is not semantically structured. To the aim of supplying a usable tool to support these processes in an effective way, we defined a semantic model for decision proposals as a composition of different aspects.
In our approach, a `Decision` is elaborated based on a `Decision Model`, of which an example is shown in Figure 4. The decision model is displayed to users by means of a canvas, to be filled with short text that can be mapped to concepts of the ontology. The benefits of a `Decision Model` are to present all the aspects of the decision proposal in a concise way, to easy discussion and to enable co-creation. From a technical perspective, this enables development of a number of automatic functions, such as coherence checks, automatic fills by searching concepts in the ontology, combination and comparisons of multiple decision proposals.

Figure 4. Example of decision model.

DISASTER	DISASTER IMPACT	TARGET	TARGET GROUPS	NEEDS
Earthquake	*The city centre is not very populated. High motorization rate and low use of public transport*	*Improve citizen mobility*	*- Families with children* *- Shop owners*	*- Reduced commuting times* *- Healthier and safer environment* *- Easy access to city centre*
INSTITUTIONAL FRAMEWORK *City council*	**CONSTRAINT** *30% of city centre should be pedestrian area*	**ACTIONS** *Call public consultation for deciding areas and paths* *Identify parking areas out of the city centre*	**INFLUENCERS** *- Chamber of commerce* *- Citizens associations*	**THREAT** *Availability of car parks*
OPPORTUNITIES ***Enhancement of business activities*** *Clean transportation, eBikes market, …*	**DECISION** *Empower public transportation and improve roads for pedestrian and build cycling paths (walkable city)*			

The decision model in Figure 4 was discussed within a University summer school with doctoral and research staff on urban planning, related to the reconstruction of L'Aquila city, after the earthquake event occurred in 2009 [6]. In particular, this relates to the plan of walkable city for urban regeneration already in place for L'Aquila and its impact on mobility. Such plan leads questioning about availability of parking areas, possibly for clean transportation means, to favour mobility of families and tourists and revive the economy of the city, e.g., how to favor mobility to re-populate the city centre addressing the needs of various types of citizens.

3 Multi-perspective resilience knowledge representation

The final objective for our system is to support different types of processes of resilience knowledge (co)creation by means of our tools.

Here, we shortly discuss examples of artifacts that can be produced with our tools related to a common problem, namely: *location of electric car parks in a city*.

EM Management perspective: The EM Scenario in Figure 2 already described the management of an emergency in a city driven by a natural event, i.e., *flood*, which involves a car park of electric cars.

Risk Assessment perspective: The fragment of Risk model shown in Figure 5, for a park of electric cars situated in via Prati Fiscali in Roma is displayed on a digital map and considered by a risk analyst when looking at risks related to services in the Flaminio area impacted by a bank overflow.

Figure 5. Fragment of risk model related to the EM scenario.

RISKS FROM: FLOOD AT: Prati Fiscali OCCURRENCE: Sun 17:00		
Service: Car Park PF		
Vulnerability	Critical event	Stakeholder
Dependence from many electric cabins	Short-circuit	Manager
Reliability of the charge system	Technical damage	User
Reliability of electric power distribution	Blackout	Manager, Citizen
	…….	…….

Decision perspective: Informed decision-making on mobility services and locations by considering vulnerabilities and critical events from different types of natural and anthropic hazards. Indeed, as shown in the example in Figure 4, decisions for mobility should take into consideration the actual availability of suitable places in the city for car parks.

4 Conclusions

The paper describes tools we developed to support knowledge collection about a resilience problem for a city by taking into account various types of users. In particular, we reported on some experimentations performed with real users.

References

1. Coletti, A., De Nicola, A., Di Pietro, A., La Porta, L., Pollino, M., Rosato, V., Vicoli, G., Villani, M.L. (2020) A comprehensive system for semantic spatiotemporal assessment of risk in urban areas. *Journal of Contingencies and Crisis Management*, vol 28, pp. 178–193 DOI: https://doi.org/10.1111/1468-5973.12309
2. Coletti, A., De Nicola, A., Villani, M.L. (2016) Building Climate Change into Risk Assessments. *Natural Hazards*, vol 84, pp. 1307–1325. DOI: https://doi.org/10.1007/s11069-016-2487-6.
3. Coletti, A., De Nicola, A., Vicoli, G., Villani, M.L. (2018) A gamified approach to participatory modelling of water system risks. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in*

Bioinformatics), 10707 LNCS, pp. 168-180 DOI: https://doi.org/10.1007/978-3-319-99843-5_15.

4. Coletti, A., De Nicola, A., Vicoli, G., Villani, M.L. (2019) Semantic modeling of cascading risks in interoperable socio-technical systems. In: Proceedings of the I-ESA Conferences, 9, pp. 119-129 DOI: https://doi.org/10.1007/978-3-030-13693-2_10
5. De Nicola, A., Melchiori, M. and Villani, M.L. (2019) Creative Design of Emergency Management Scenarios Driven by Semantics: An Application to Smart Cities. *Information Systems*, vol 81, pp. 21–48 DOI: https://doi.org/10.1016/j.is.2018.10.005
6. De Nicola, A.; Giovinazzi, S.; Guarascio, M.; Villani, M.L. (2020) Gamified Decision Making for a Participatory Post-Crisis Recovery: a Model Based Process. In: Proceedings of the 30thEuropean Safety and Reliability Conference - ESREL 2020 - Venice, Italy, 1st-6th November 2020.
7. Patriarca, R., Falegnami, A., Costantino, F., Di Gravio, G., De Nicola, A., and Villani, M.L. (2021) WAx: An integrated conceptual framework for the analysis of cyber-socio-technical systems. *Safety Science*, vol. 136, pp. 105-142 DOI: https://doi.org/10.1016/j.ssci.2020.105142
8. Frantzeskaki, N. (2016) *URBAN RESILIENCE. A concept for co-creating cities of the future*. Report. Resilient Europe. European Union: European programme for sustainable development. https://urbact.eu/resilient-europe (last accessed May 2021).
9. UNISDR (United Nations International Strategy for Disaster Reduction) (2015). Sendai framework for disaster risk reduction 2015–2030. https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030. (last accessed May 2021).

List of abbreviations and definitions

CREAM	CREAtivity Machine
EM	Emergency Management
GIS	Geographical Information Systems
ODP	Ontology Design Pattern
TERMINUS	TERritorial Management and INfrastructures ontology for institutional and industrial Usage
VUM	Vulnerability Upper Model

Maximizing-Lessons Learned from Investigations

Ludwig Benner Jr., USA, lbjrus@gmail.com

Abstract

Accidental incidents are experiences from which investigators hope to learn lessons to use in future activities. They are complex dynamic processes, requiring successive interactions among people, objects and energies over time to produce unwanted outcomes. How can incident investigators ensure that they learn all possible lessons from the experience? This analysis addressed that question. The report presents a description of a vital but relatively underappreciated safety investigation data processing function needed to achieve that objective: the input data integration function. The data integration function transforms input data into the building blocks with which a scenario is developed to describe how the incident began and how the outcome was produced. The data integration function connects empirical observations, congruently structured as integratabtle data building blocks into scenarios describing how the outcome was produced.The report describes what the function is, its role in investigations, its implementation procedures, and precautions to avoid flawed integration. The resultant scenarios enable the use of a systematic, logical process to maximize the discovery, definition, documentation and communication of every problem and lesson that can be gleaned from the experience.

1 Introduction

Most people who remember the terrorist's attack on the United States on September 11, 2001 will recognize that one of the major criticisms of the United States government's intelligence community was its failure to "connect the dots" or integrate relevant data to predict that perpetrators' actions were going to produce the disastrous outcome. "Connecting the dots" remained a challenge after the attack, as the incident was dissected by processing inputs from many sources to develop a full description of everything that had to have happened to produce the casualties and damages that occurred.

Accidental incident investigations for safety purposes are similar processes, used essentially to develop scenarios describing how an accidental incident started and produced its outcome. These scenarios are then analysed by many users for various purposes, including identification of lessons learned. Scenarios that describe the incident completely from start to finish maximize the number of lessons that can be learned from an incident. Therefore, a goal for investigators should be to develop a complete description of the incident's origins and outcome .

Successful investigations depend on proper execution of certain essential input data processing functions and tasks, requiring competencies in investigation and reasoning knowledge, tools and skills Today, any of forty different investigation and analysis methods can be used to produce the data in incident investigation reports. Each method differs from all the others in one or more of two dozen documented ways. i .[1]They differ primarily in how they process reported data, and in what they produce.

However, regardless of the method used, every investigator faces the challenge of conducting and managing investigations to develop a comprehensive scenario describing how the incident started, progressed and produced the undesired outcome. That means investigators must

identify, select, acquire, integrate and report surviving input data to create that scenario. Each newly acquired input data item must be processed that way.

Successive interactions among people, objects, or energies are required to start the incident and produce the outcome. The input data processing must identify and document the *flow of those interactions* from start to finish. That means related events constituting interactions during the incident must be connected, or coupled.

Input data processing is iterative, involving interdependent tasks. The iteration requires that each processed data building block be mutually compatible with the others, to enable its integration, and connect-ability to others to define the interactions that occurred. To satisfy these criteria, successful execution of the data integration function tasks is required: preparatory *input data structuring* into congruent building blocks, the building block integration, and the *data linking* or *"connecting the dots"* tasks.

The input data processing needed to produce the descriptive scenarios for the safety knowledge base is the focus of this analysis. ii[2]

2 Analysis Method

The analysis method was a fly-fix-fly or iterative method. Using experiences during actual investigations to define investigation tasks and their execution, and observing the results, each data integration function task was documented and contributed to their analysis over a 35 year period. Concurrently, many related sources such as academic papers, accident reports, investigation manuals, peer dialogues and critiques, and books also contributed to refinement of the function and tasks.

For example, hypothesis identification occurred during the data organization step rather than the beginning of the tracking. It favored input/output graphs rather than causal graphs, because of causal creation and reporting problems.iii [3]

The data sources consisted primarily of descriptions of documented investigation methods, the author's prior studies of incident investigation processes issues, incident data display examples. observations of practices during actual investigations, incident reports created with different methods, and references from the author's extensive personal library of investigation methods and related books and documents.iv[4]

2.1 Terms used in this report

As used in this report, lessons learned are the knowledge of behaviors by people, objects or energies, derived from investigations of experiences, that should be considered in future activities. Incident investigation refers to a process that produces an explanatory description of an accidental phenomenon for safety and analytical purposes, from which lessons can be learned. An accidental phenomenon and incident refer to any kind of unintended undesired dynamic process during which interactions among people, objects and energies produced an unwanted outcome over time, such as accidents, spills, crashes, near misses, fires, explosions, interruptions, etc. Descriptive scenario refers to a scenario which describes how an incident began and how the outcome was produced. Event refers to an action by an entity during an incident, e.g., event = an actor + an action.v [5] Building block (**BB**) refers to an event documented for use to produce an explanatory description of an incident. Input/output interaction refers to the action of a BB that resulted in or influenced one or more subsequent BBs. Linking refers to the connecting of an input BB to a related output BB with a directional action flow symbol, or arrow, to document an interactive relationship. For linked BBs, **iBB** refers to an input BB and **oBB** refers to an output BB. Incident analysis refers to analytical and interpretive actions performed on reported scenarios.

2.2 Assumptions for the analysis

This analysis of the input data processing during investigations to maximize lessons learned is based on certain assumptions that differ from assumptions influencing most present incident investigation practices. This analysis assumes that:

1. each accidental phenomenon, or "incident," is a complicated process during which people, objects or energies interact dynamically over finite time to produce the outcome;
2. people are incorporated into dynamic operating activities to keep the activities operating within dynamically stable boundaries during which changing behaviors and perturbations requiring habituated or adaptive response actions arise;
3. when actions produce or influence one or more subsequent actions or changed states or conditions, they can be coupled to show interactions;
4. both static and dynamic states change only when acted upon by people, objects or energies, but they can influence subsequent events. To overcome the ambiguous use of "event" in safety documents, "event" must be defined; it can be advantageously defined as an actor plus an action for investigation purposes;
5. the development of a scenario describing how an incident began and produced the outcome can be based on the formulation of standardized event "data building blocks" assembled into an array of linked actions to create the scenario;
6. incoming data can be sequenced and managed by integrating it as it is acquired, rather than according to some accident theory, methodology or model, or a "get all the facts, then analyze them" or form and test a hypothesis or other approach;
7. input-output thinking is superior to causal thinking for identifying and documenting actions that produced and influenced subsequent actions during an incident; and
8. this requires understanding of previous actions (inputs) to identify specific problem actions, behaviors or interactions that should be avoided, modified or emulated in the future, or lessons learned.

3 Investigation data processing practices

The selection, acquisition, processing and reporting of input data during investigations is needed during all incident investigations. However, each investigation method documents, processes and presents input data differently. The presentation formats include narratives, tables, logic trees, chains of events, time lines, matrixes, causation models, graphic charts, epidemiological models, functional models, fishbones, etc.

Which format is most likely to maximize the lessons to be learned by the investigation?

3.1 Incident data presentation

To recognize the context of this analysis, it is important to be aware of the many different ways processed input data is now presented. To see hundreds of examples, do a Google search for "acci-map examples" and then click on the Images icon in the tab bar that appears along the top of the page.vi [6]Scroll through the pages of examples to see the diversity of ways used to present such data. As you do that, notice the different ways the content of the building blocks is structured and the diversity of the content of the building blocks connected with linking arrows. Note how some blocks are emphasized, the kinds and directions of the arrows and what they link, and the lack of gaps in some linked arrays. Next, consider how

quality assurance tests could be applied to the linked building block contents and the completed presentation. Next, consider how problems would be discovered and defined with each data display. Finally, ask how users might use the presented data to determine its relevance and need for action in their systems.[vii]

The disparities in ways to present incident data will be readily discernible, as will be the the need for understanding of input data processing practices responsible for such disparities.

3.2 Investigation data structuring function

Investigators look to many kinds of different sources for input data they will process during their safety investigations. These sources can be people, debris, instruments, residues, documents, audio-visual records, injuries, budgets, safety analyses, or anything else that might have captured and retained data about the episode being investigated. The form of the data available from each also differs from source to source, ranging from perishable to permanent and directly observable records, to interviews of people, or scientific inferences from observed states of debris.

The investigation process requires identification of relevant data from each source, and its transformation into a documented input *"data building block"* (BB) with which to create the scenario describing how the outmode happened.[viii] [8] This is the first part of the two-part input data structuring function.

The second part is for investigators to integrate these data building blocks into their temporal and spatial sequence, in a way that enables the valid presentation of sequential and concurrently occurring and overlapping flow of BBs during the incident. This information is complicated to describe comprehensively in narrative format, but can be described clearly with much less effort in a graphical format. Among the display options, an actor/action matrix, adapted from the scheme for displaying each musicians' actions and timing required to perform a musical score, has been found most valuable for this arranging building blocks. It enables the systematic and timely organisation and linking of interacting BBs.

3.3 The investigation data integration function

The data integration function is the identification, definition and documentation, during an investigation, of *relationships* among events from the beginning of a phenomenon to its outcome(s). The function produces links among documented BBs by individual persons, objects and energies, documenting the *interactions* which produced the phenomenon's outcome. It "connects the dots" of incident description BBs to describe and explain the phenomenon. This link creation and documentation function is the *crucial data integration function* for the management of data acquisition efforts, quality assurance tests and production of investigation reports.

Few of the 40 investigation and analysis methods available for investigating incidents [ix] [9] explicitly specify use of or procedures for the data integration function. Links are widely used to connect elements in graphic displays of investigation data, but for most methods, their creation relies on investigators' common sense or intuitive reasoning. Of methods that do specify links, very few have prescribed procedures or criteria for performing the function. This results in links between every kind of BB imaginable because of the disparity among investigation methods.[x][10]

4 Input data structuring and integration function's s roles in investigations.

Each input data processing function has a role in every investigation, which when performed well, makes essential contributions to complete incident investigations and the ability to maximize the lessons that can be learned by the investigation. Performed haphazardly, they can result in misleading information, misdirected responses, conflicts and other problems.

4.1 Data structuring role in investigations

Events are actions by actors xi[11] that introduce changes. Dynamic event interactions produce incident outcomes. Thus events are the primary building blocks (BBs) for creating incident scenarios that make sense. BB acquisition and sequential organisation are essential to every investigation of any phenomenon but each investigation method creates and organizes them differently. A defined input data processing procedure and investigator competence for the sequential BB organisation are also necessary.

BBs must be properly structured and organized to enable satisfactory implementation of the investigation data integration function. The role of data BB structuring is to help investigators

1. **produce reproducible BBs**, transformed from observations, which can be organized and linked to create the scenario describing how the outcome was produced,
2. **enable BBs' integration by sequential ordering**, including concurrent and overlapping BBs, by their temporal and spacial relationships,
3. **enable determination of related BBs** so input/output relationships can be documented,
4. **enable quality assurance testing of BBs** for the validity of their content and completeness
5. **support easily communicated scenarios** describing unambiguously the actions by the individuals, objects and energies that produced the incident outcome, and any uncertainties in the scenario.

4.2 Data integration role in investigations

The data integration function has at least eight important roles to help investigators produce sound explanatory descriptions of what happened.

Links will clearly show how one input building block produced or influenced one or more subsequent output building blocks, or how it takes several input building blocks to produce or influence a single output building block during an incident.

The data integration function enables *progressive development* of incident descriptions, enabling investigation management actions to substantially enhance investigation efficiency. It *provides context* for each event during an incident, to help users expeditiously determine relevance. Properly executed, it *dispenses with the need for causal or other characterizations* by helping investigators assure that *all needed surviving and available* event BB input actions and interactions are documented in the explanatory description. The function supports objective *quality assurance tests* of the building blocks and their relationships, enhancing confidence in the descriptions. It also helps expose any *gaps or uncertainties* among events' interactions in the explanatory description scenarios, or in the successive actions of individual actors in the scenarios. The function provides arrayed data pairs and sets for systematic identification of candidates for *problem definition* and actions or relationships to change.

The roles of the data integration function during investigations include helping investigators to

1. **produce incident descriptions efficiently**. The integration function task can begin with two BBs, and progressively integrate additional BBs as they are acquired, documented and linked. This is a fundamental paradigm shift from the "gather the data, then analyze it" approach. Gaps among BB links quickly point investigators to specific data they still need to pursue. Alternatively, if input data is not yet acquired, gaps guide development of bounded hypotheses to fill the gap, and identify data needed to confirm or refute each hypothesis.
2. **continuously display investigation status.** The continuous progressive input BB ordering and integration process enables individual investigation participants and supervisors to identify, define, direct and manage ongoing data acquisition tasks still needed to complete the explanatory description of how the outcome was achieved.
3. **ensure BBs' accurate timely spatial and temporal ordering and integration of data used in the descriptions.** Creating links from inputs to outputs helps ensure the validity of the time/place sequencing of the BBs in the description. Trying to link a BB containing two or more actors or actions ,or an ambiguous actor like management, occupant, crowd or the firefighters, or multiple actions in a BB to another BB quickly exposes flawed BBs needing repair. Backward arrows are also a definitive indication of flawed sequencing.
4. **purge irrelevant, misleading or bogus data from their investigations.** If a BB cannot be linked to anything on an array, it can be set aside until toward the end of the investigation, when investigators can determine if and how it should be integrated or be ignored.
5. **test the completeness of the history of an individual's, object's or an energy's behavior or actions during the incident.** During an incident everyone and everything involved has to be someplace doing something. Gaps in actors' linked BBs can indicate a time period for which actions are unaccounted for during an incident, especially for people involved or mentioned in witness statements. Various methods from rigorous logic to simulations to performance tests can be used to verify the validity of the links joining I/O pairs, sets and patterns.
6. **reduce latency of investigations.** Investigation latency is the elapsed time between an incident's occurrence and implementation of interim or post-report response actions, or other eventual uses of the incident data. Investigation latency is reduced by the progressive ordering and integration of BBs as acquired.
7. **eliminate the need for event characterizations in descriptive scenarios.** A properly executed integration function helps investigators ensure that all recoverable and relevant event BB input data and relationships are documented in their scenarios. When deemed to be of sufficient value, analysts and other users can still create and separately report event BB characterizations such as failures, errors, inadequacies, causes, findings, conclusions and violations based on the reported descriptions and their own additional input data.
8. **demonstrate and communicate the completeness of the investigator's incident description.** Confirmed links, displayed on an array of a completed explanatory description, document every input/output interaction that was necessary and sufficient to produce the description of how it happened and, if applicable, what remains uncertain or unknown. The displayed array can also facilitate agreement about its validity among entities participating in its development.

4.3 Roles after investigation

Additional roles, after the linked BB array is complete, are the subsequent use of the description for the the discovery and definition of problem behaviours, behavior pairs or behavior sets, or lessons learned. Another role is the of problem behaviors as inputs to scenarios hypothesized during predictive safety analyses. Completed arrays produced by the data integration function enable *the systematic search of completed descriptions to maximize discovery and definition of lessons learned*. Probably the most important role of the integration function, from a user's perspective, is that it produces ordered arrays of linked BBs to *enable systematic examination*, from beginning to end, of I/O pairs, sets or patterns to develop candidate *problem statements* and indictors of a need for response action decisions. Thus it maximizes lessons learned from the incident by the investigation.

When performing predictive safety analyses for restarts, system modifications or new systems, the coupled BB pairs or sets in the BB arrays provide known problem interactions that can be incorporated into hypothesized scenarios used in such safety analyses, with the potential to reduce oversights of possible incident scenarios.

5 Prerequisites for the input data processing functions

Implementation of the input data processing functions includes several prerequisites. They include the selection of

1. a structure for the input building blocks themselves to ensure consistency of BBs to be linked,
2. a structure for sequentially ordered BBs to facilitate the integration of BB interactions,
3. an appropriate reasoning competence for identifying related BBs, and
4. a way to show the progress of the investigation to guide data acquisition choices
5. kinds of links for the integration of related BBs to show their interactions.

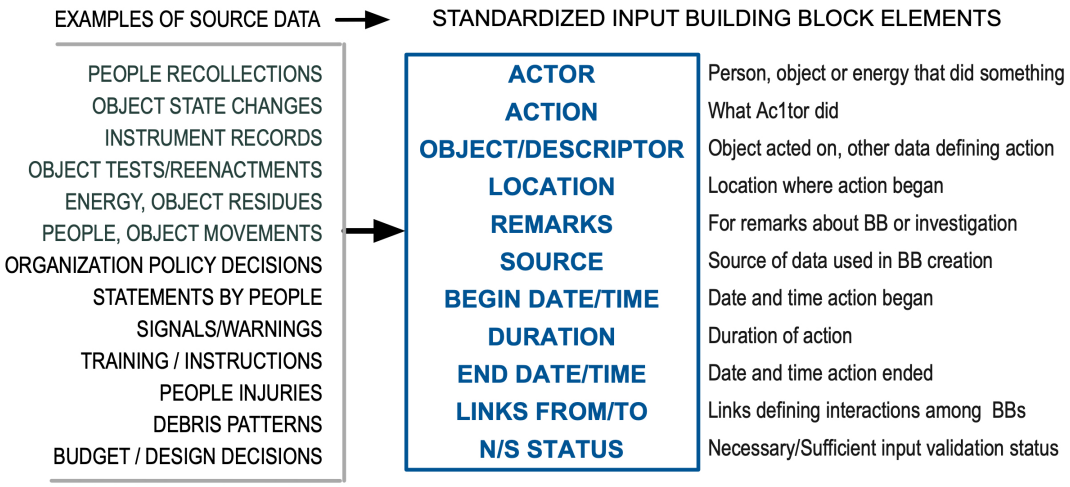
5.1 input data building blocks (BB) structure

To enable success-full integration function execution, the input data building blocks documented for the description must be congruent with each other, having consistent structure, content and grammar, and preferably be standardized. Each event building block (BB) is created from among the many kinds of surviving data identified, acquired and documented by investigators, as illustrated by an example Figure 1.

Investigators integrate those BBs into individual data strings for each actor, in their temporal and spatial sequence as acquired. When a BB results in or influences the occurrence of a subsequent BB during the incident, investigators can link the pair to define an input/output relationship. That relationship must be documented. It is the creation of direct links between connected input and output BBs that documents such relationships. Input/output thinking and links are preferable because they are demonstrably more rigorous, specific and value-fee, and

less vulnerable to error, hindsight or other investigator biases or harmful consequencesxii[12] than causal thinking, causal statement creation and causal attribution.

Figure 1. Event Building Block (BB) documentation



The input BB data structuring function must produce

1. BBs created from empirical data rather than speculations, assumptions or interpretations;
2. BBs whose structure contains adequate information to define each event uniquely so it can be linked logically to one or more subsequent uniquely defined events;
3. BBs whose content *must* include *at least* an actor, an action, times and reference number, to enable the data ordering and data integration,
4. BBs whose grammar must have active voice, singular actors and actions, and be at lowest level of abstraction to be definitive for the ordering, integration and coupled data reporting functions; and
5. for analyses and machine processing, BBs that also contain additional data, such as BB identification code, source, location, array links and test status.the

Conditions don't just happen. Someone or something must act to create a static or dynamic condition, or act on a condition to change it. Conditions may influence how an event occurs. For example the speed of a moving vehicle will influence the degree of damage in a collision. How should conditions be transformed into actor/action building blocks?

The answer is to identify who or what established the condition which influenced a subsequent event, so that becomes the actor in the BB. The action is what the actor did to create or change the condition. In the example, the BB would read "driver accelerated to n mph"rather than something like "speeding *(the condition)* increased the damage." Remember that lessons learned involve finding behaviors to consider in the future, and that includes behaviours which changed conditions.

5.2 The BB sequentially timed ordering structure

To maximize the data integration functions' value and ease of execution, *a graphical structure* for organizing and arraying the event BBs is preferable to narrative descriptions. BBs and links can be and often are described in a narrative format, but in that format relationships are extremely cumbersome to document, control, validate and communicate or envision, because

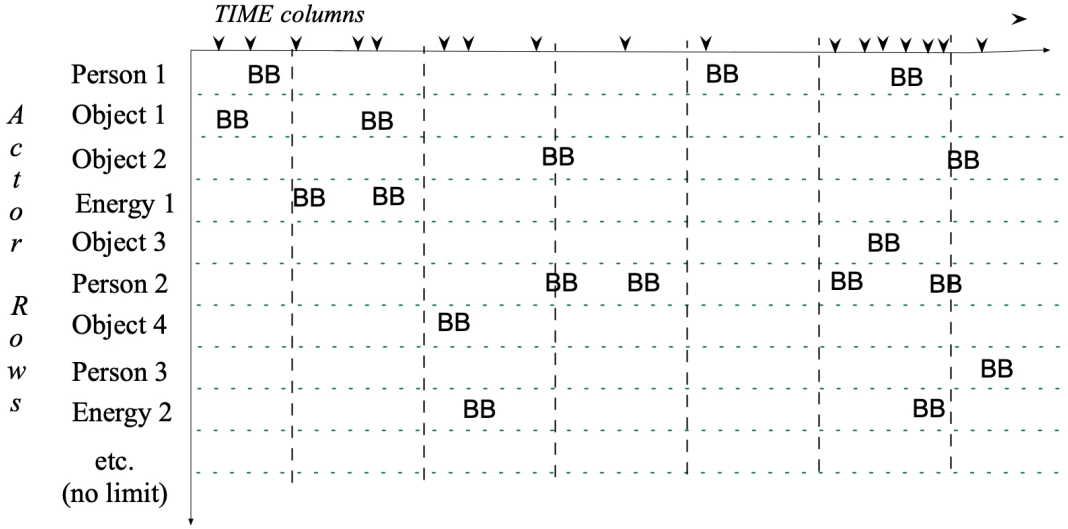
of cognitive memory and data integration limits. Narrative links must be described by words in phrases, sentences and paragraphs, with their linearity, semantic, syntactical and other impediments for describing complicated dynamic phenomena like incidents.

Many graphical structures exist for arraying BBs. Most investigation methods have their own way of displaying BBs to describe what happened, including some with linking arrows. For example, event display choices include Acci-Maps, Events and Causal Factors charts, logic trees, fishbone, SnapCharts®, STEP, BowTie, FRAM and Petri Net displays, among those found on the Images pages mentioned in 3.1. Each has its own way of specifying, documenting and displaying BBs to describe how the outcome happened.

Reproducibility of BBs and links is a major consideration for selecting a graphical BB array structure. For this reason, the data integration function is best undertaken within a multilinear graphical array for integrating and testing the BBs and their links. The array should provide rows, like a stadium track lane or swim lane, for each person's, object's, or energy's string of BBs, where they can be positioned in their relative temporal and spatial sequence. The array should provide time columns to enable the temporal and spatial ordering of BBs on each actor row, and their positioning relative to times of actions in other actors' rows.

A matrix with time/actor coordinates, like the time-actor matrix used to document music making processes or Gantt-type charts, provides a proven structure for arraying the BBs. On the musical score matrix, for example, actions by each instrument and voice describe the individual actions (BBs) and timing required to produce the composer's version of an opera, symphony, song or other composition. That form of music process description enables the *reproduction* of the composition or any part of it by anyone who wishes to do so. Conversely, it also provides a format for documenting a recorded live musical performance as a musical score which can then be reproduced. The music matrix's adaptation to creation of incident descriptions provides a practical proven framework for multilinear recording of sequential and concurrent BBs from surviving incident data, to organize them for the data integration function. Figure 2 illustrates this framework.

Figure 2. Actor/Action matrix configuration



This structure enables investigators to chronologically array BBs by persons, objects or energies that did something during the incident, relative to all previously placed BBs, *as they are acquired - crucial to efficient investigation management*. That array of BBs enables investiga-

tors to "connect the dots" or trace relationships among the displayed BBs in the most reproducible way known thus far. Unidirectional arrows among BBs along an actor row indicate input/output relationships of actions by that person, object or energy. BBs on other actor rows that produced or *influenced* other actors' actions can also be linked with arrows across rows. Arrows to or from BBs in different rows can show relationships among the BBs on those rows during the incident, including concurrent BBs. If two successive actor BBs occurred at different times or locations, with a gap in the events flow about how that happened, investigators will know quickly that they need to pursue more input data to close that gap. Remaining unlinked BBs become candidates for which to acquire additional input BBs or output BBs to create links, or to set aside for later use or disposal.

The time-actor matrix differs from events and causal factors, fishbone, logic trees, bowtie or other graphic data array structures primarily because the events in those display do not have BBs with standardized content or show time-limiting relationships among the event BBs. That prevents links from showing the successive *timed flow* of the event interactions from the beginning of the incident to the outcome, precluding completeness tests and masking time constraints on reactions to what is happening. Thus linking arrows in the other displays can and do link any kind of action, state, omission, categorization, abstraction, or allegation and go in any direction, undermining their descriptive, explanatory and quality assurance value. Specific static or dynamic conditions can become input BBs if they *influenced* how a specific interaction or oBB occurred.

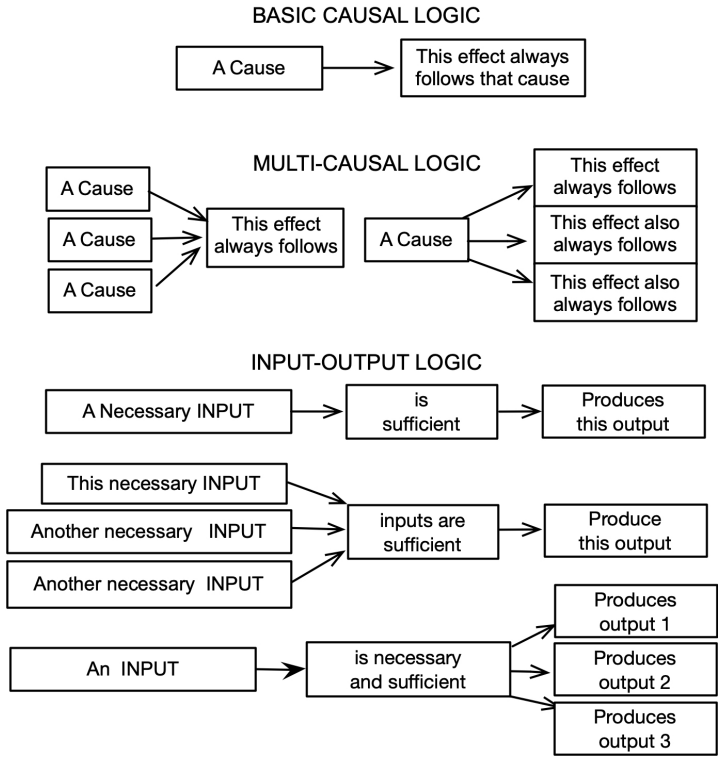
Conventional time lines address events timing sequence, but their tabular structure lists all concurrent events at each listed time, and relationships between times must be formulated by users. This frustrates the creation of orderly documented links to show the flow of interactions among all the events listed at specific times and durations in the table, and events at other times.

The actor/action matrix structure can accommodate as many actors' BBs and links as investigators can find.

5.3 Appropriate reasoning competence prerequisite

A third element of the framework for the function is facilitation of the *reasoning process* for determining the linkages between BBs. The currently dominant binary cause-effect reasoning framework has numerous problems which vex investigators and users. It also has many adverse repercussions because of the nexus between cause and blame, fault and culpability, vulnerabilities to ambiguity, error, narrowness, value-based judgments and interpretations, and many harmful effects of a causal-based reasoning framework.xiii[13] An input/output (I/O) reasoning framework, relying on sound logic for the integration function, as used in operations research and computer coding for example, is more objective and effective in identifying and testing necessary and sufficient inputs. Figure 3 shows the difference in the causal versus the input/output reasoning processes. Ability to use counterfactual reasoning for each linked BB pair or set is also significant.

Figure 3. Causal vs. Input/Output Reasoning



5.4 BB and Link status tracking

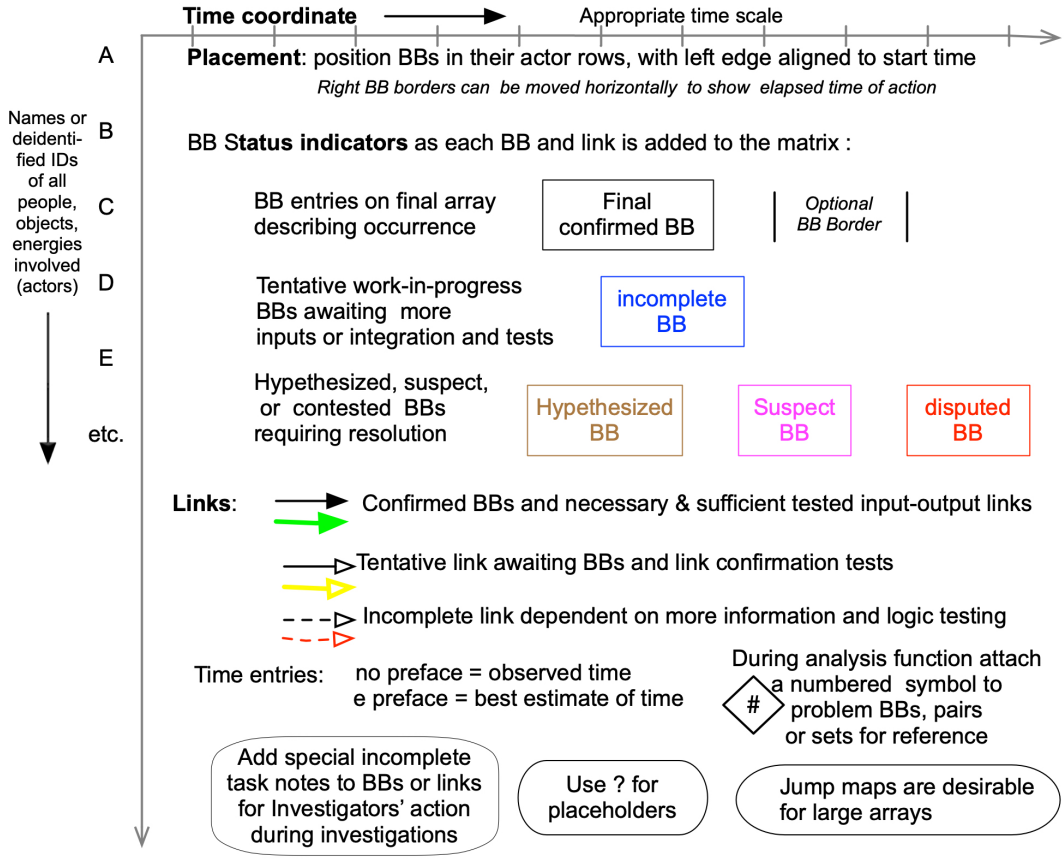
The fourth requirement is the need for some method to *enable differentiation of the status* of the BBs and links as they are placed on the matrix, to show the what investigators still need during an investigation. Because the integration function enables the progressive integration of incoming data, it is important to know what BBs the investigator has and what the investigator still needs to acquire. Knowing the current status of integrated BBs and links provides a basis for timely, *rational and efficient* decisions about additional data acquisition requirements. This is especially important for managing complex incidents involving scattered data sources.

Links between confirmed BBs may be considered *confirmed* if they have passed necessary, sufficient and counterfactual logic, simulation or other tests. Links may be *tentative*, waiting for confirmation tests of one or more BBs or link before the links can be confirmed. BBs linked to an output BB may be logically insufficient to produce or influence the output BB, so their *incomplete* status needs to be shown.

Changing status is too complicated to describe, update and finalize with descriptive narrative sentences. For each status state, the type of status for multiple BBs and links should displayed

graphically until confirmed by validating confirmation tests. For example, see Figure 4 for BB and link status coding suggestions.

Figure 4. BB and link status coding during investigations



BB status indicators can be indicated by border or content colors or borders, as shown. A completed link can be depicted with a solid line and solid directional arrow head. A tentative link can be depicted with solid line and an empty arrow head. A tentative link can be depicted with a dashed line and empty arrow head. If the status changes, the arrow head is easily changed. An incomplete link can be depicted with a dashed line and empty arrow head. Alternatively different link colors can be used to depict BB's or link's status during an investigation.

Preferably, at the conclusion of an investigation all the BBs should be confirmed and all links should be sold arrows with solid arrow heads, or the same color. If unconfirmed BBs or other linking arrow shapes or colors or gaps remain, the reasons should be explained in investigation reports.

5.5 Link testing procedure requirement

To "truth test" the arrayed BBs and their input/output links, an objective procedure needs to be in place for quality assurance purposes. An I/O framework enables such a logic-based link testing procedure, with two phases. The first phase is employed to ensure new links are valid. That includes the necessary, sufficient and counterfactual tests for each linked BB pair or set as the links are created. The second phase consists of performing the same tests at the end

of the investigation, to ensure the final description is complete. That includes performing the same tests for every linked BB pair and set in the completed description, and ensuring an explanation for any gaps in the flow of events.

It is unclear how other graphic frameworks and investigation or analysis methods enable this kind of logical quality assurance testing of their data displays.

6 Implementing the data processing functions

The data structuring and linking functions are facilitated by visual data processing procedures. The data structuring task is a mandatory preparatory task needed to implement the data integration function. To enhance efficient management of the investigation, the data integration function should be instituted as soon as two or a few confirmed building blocks (BBs) are sequentially positioned on a time-actor matrix display.

Data integration function tasks during investigations include determining necessary and sufficient (n/s) input/output (i/o) relationships among displayed BBs, to

- define and create links among iBB/oBB pairs or sets;
- update links' status as the tasks progress;
- close unlinked gaps between BBs if possible especially along rows, or explain them if not possible; and
- test final linked BB array for completeness of the explanatory description.

Upon completion of the function, the linked BB array enables preparation of a report describing interactions that produced the outcome, from beginning of the incident process.

6.1 Data preparation for data integration function

The data integration function is best initiated during the input data acquisition and ordering function as input new BBs are documented and positioned on the time/actor matrix. The function is dependent on confirmed event BBs and their correct placement on the matrix.

This early start begins to help investigators define the additional data they need to acquire next as the investigation progresses and the scenario begins to emerge. Thus, the investigation data acquisition tasks are *steered by the data as it is acquired*, rather than being steered by data expected to be acquire by some accident theory, method, model or prior experience. The difference is like gathering data with tweezers versus a vacuum cleaner.

Acquisition of BBs within an input framework requires documentation of the investigation actions or behaviors that changes during an incident as well as influenced them.

Each BB should have a standardized content and grammar to enable correct BB row and column positioning during entry on the matrix array. That enables expedient implementation of the BB integration function, quality assurance and machine processing for distribution and analyses. An experimental example of a standardized digital BB content is shown in Figure 2. xiv[14]

Feasibility of software to enable local entry of BB data from documented sources, or remote data entry via the Internet has been demonstrated. Software feasibility to position digitized BBs on their proper line and in their proper temporal and spatial sequence has also been demonstrated. Software code to display the latest update of the BB array locally and remotely to enable everyone involved in an investigation to see the current investigation status has also been demonstrated. This enables the integration function to be executed by designated personnel and then viewed as an updated array display anywhere an internet connection exists.

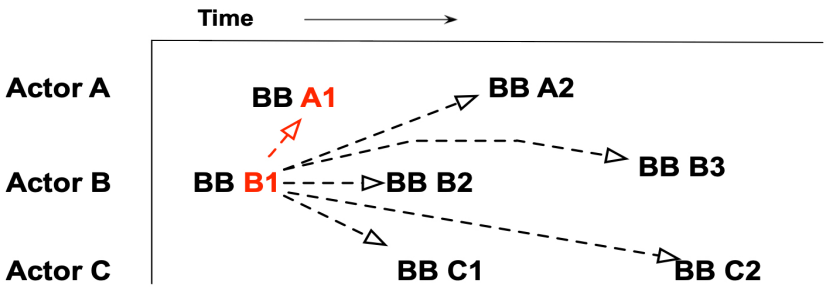
6.2 Identifying iBB/oBB pairs or sets to link

This task requires investigators to examine two BBs at a time, to determine if the earlier input BB (iBB) produced the occurrence the later output BB (oBB) or influenced its nature. This determination of an I/O coupling or relationship is reached by logical reasoning, or from observations of some recorded sequence, experiment, or simulation, as provided by the nature and sources of each BB.

6.3 Creating and updating links

Create links as BBs are added to the array. See Figure 5. Select two BBs on the array. When the earlier BB is found to be *necessary* for the subsequent BB to occur, draw a linking directional arrow indicating the necessary I/O relationship from the early BB to the later BB. The earlier BB becomes the input BB or iBB, and the linked BB becomes the output BB or oBB. Repeat this step with all other later BBs on the array at that time to determine if the iBB influenced other later BBs. The attributes of the linking arrows depend on the status of the relationship at the time the arrow is drawn. Use status arrows of appropriate shapes or colors to describe the relationship found.

Figure 5. Creating initial linkS between BBs

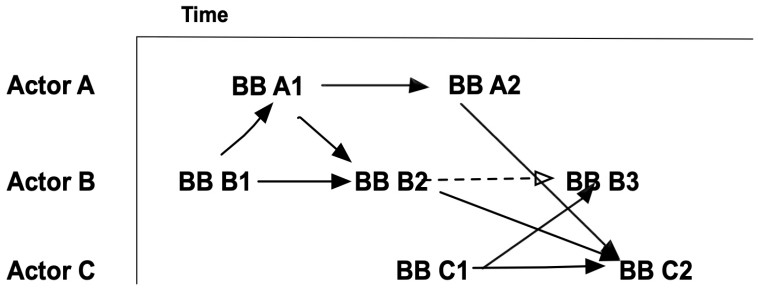


1. Select two BBs on the array as the array is evolving (B1 and A1 for example)
2. Was earlier B1 a necessary input for later A1 to occur as it did?
3. If so, LINK B1 to A2 with a incomplete arrow to show an I/O relationship between the two BBs
4. Repeat step 2 for other BBs on the array, drawing incomplete links if related
5. The do same for each BB as it is created.

After the initial necessary relationships are established, the linked BB pairs are examined to determine whether the linked iBB is the only input required for an oBB to occur as it did, or a *sufficient* input. See Figure 5a. If not sufficient, identify the every other iBB that must have occurred for the oBB to have occurred as it did, and link it or them to the oBB. After all necessary and sufficient iBBs are linked, and the link status updated, reexamine the links to determine if the linked iBB(s)s will always produce the oBB as it occurred. Do not permit any

backward arrows! This procedure takes more time to describe than to perform. The task chart in Appendix A illustrates the procedure.

Figure 5a. Updating BB links during investigations



1. Select two tentatively linked BBs on the array as the array is evolving
2. Was earlier linked BB *sufficient* input for later BB to occur as it did? If yes, show complete link., as between A1-A2, B1-A1, B1-B2,C1-C2
3. If not, locate or add additional BB(s) as required to produce later BB until all n/s input BBs are identified (B1+A2->B2 for example) and complete links are shown.
4. Remaining incomplete link from B2 to B3 indicates situation that needs to be resolved or perhaps unresolvable gap.
5. Do same for all BB pairs as they are created.

This is the core of the data integration function. It will reveal the specific data required to document additional BBs needed to complete the linking of all the BBs on an array, thus steering the investigation's data search, retrieval and documentation efforts. Repeat this process until the investigation has exhausted all available and relevant source data from which to document BBs.

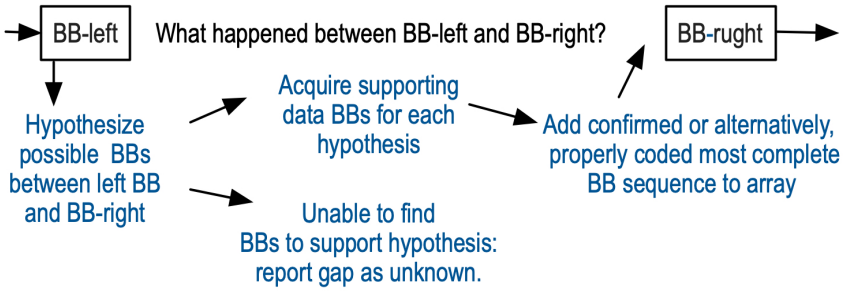
Note that analysts can use this same progressive procedure for the sequential examination of linked BB pairs and sets to identify candidate problem BBs or BB pairs, sets and patterns to support a problem definition. *This systematizes the problem discovery and definition function tasks that need to be completed before proceeding with the development of problem solving response actions or recommendations*, contributing to more rational management of responses to incidents.

6.4 Closing gaps among unlinked BBs

As the investigation progresses, and no direct link is found from some BBs or to some BBs; that creates a gap in the flow of events in the scenario being developed. Gaps can also exist in the sequence of actions by an actor on an actor row. Draw incomplete links between suspected coupled I/O pairs using a place holder (?) on the link to indicate a gap needing attention. Often needed data can be found by tracking the actions of the actor or actors on both sides of a gap in greater detail or by breaking down their actions during the time indicated by the BB row positions on the BB array.

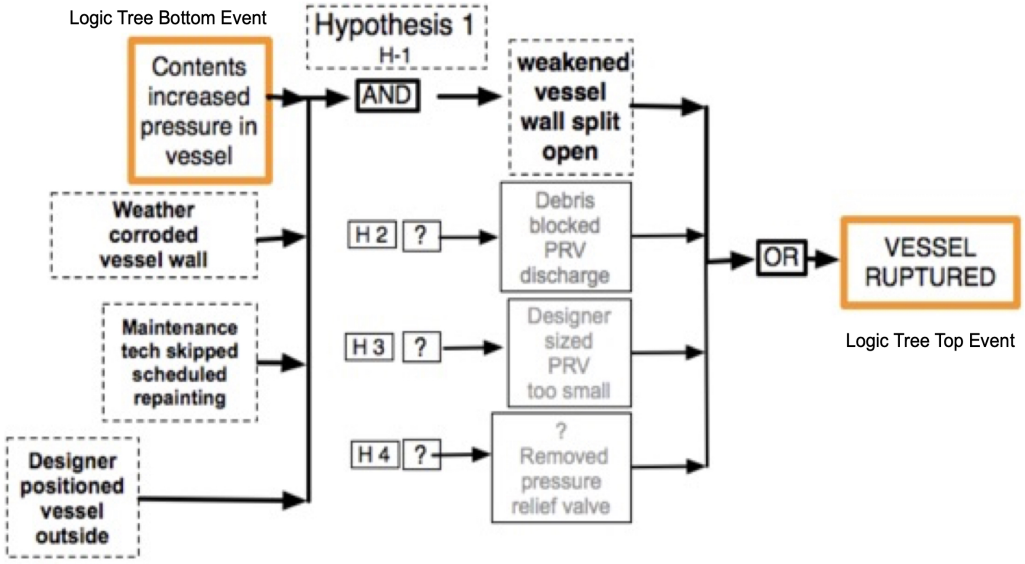
When that does not fill a gap, generate potential bounded hypotheses to theorize possible BBs needed to fill the gap, and try to acquire them.xv [15]This may or may not be successful. If unsuccessful, see Figure 6.

Figure 6. Link Gap Filling Procedure



Development of such hypotheses takes the form of bounded logic trees,xvi[16] with the top event the later oBB and the bottom event the earlier iBB, and speculated possible BB scenarios between the two. The speculated BBs define the data needed to determine if a hypothesized scenario is true, possible or unlikely. For example, if during an investigation a data source indicates internal pressure in a container was rising before it ruptured, several hypotheses might be developed about events that led to the rupture. See Figure 6a for an example of one of four potential hypotheses, each of which could be explored in a pressure vessel rupture.xvii[17]

Figure 6a. Example of gap-filling hypothesis development



6.5 Truth testing of finished array.

Several kind of objective quality assurance tests can be performed on the completed array of linked BBs to determine the validity and completeness of the displayed explanatory description of how it happened.

1. Verify validity of each BB against its source and documentation rules, if not already completed.
2. Perform BB column placement tests to ensure correct spatial and temporal sequence and timing of every BB displayed on every array row.
3. Perform row continuity test to ensure the completeness of description of where each actor was and what each actor did during the occurrence.
4. Perform input/output relationship, necessary, sufficient counterfactual logic validation and status tests among linked BB pairs and sets after column and row tests.
5. Verify validity of excluding documented BB data inputs that not used in the array.
6. Document explanations for remaining investigation unknown or uncertain relationships, for inclusion in the report.

6.6 Reporting explanatory descriptions.

A properly tested and validated graphic array of linked event building blocks will describe and explain what happened, to the maximum extent permitted by surviving data sources. When combined with descriptive data about the beginning state of each actor the linked BB array, and explanations of remaining gaps and uncertainties, the array will provide a readily communicated explanatory description of what happened for all users.

If a narrative textual description is mandated, the array provides an outline to guide the preparation of the description of what happened in narrative format.

Analyses and other uses of the descriptions can then be based on data and relationships validated by tests of each element and relationship.

7 Supplemental information about the data integration function

A decision process chart for creating links among BBs in arrays is shown in the Appendix A.

I/O thinking during the integration function has the advantage of enabling the logical coupling of *influences* to something that happened and their context, which is beyond the ability of the binary cause-effect thinking and causal statement or factor creation. Guidance for investigators to develop *influencing data* for people, object or energy actions is available at http://www.iprr.org/proj/humdecn.html.

The use of question marks (?) as placeholders during investigations to indicate unfinished data acquisition in BB content, or linking gaps, can help remind investigators of remaining tasks. The attachment of reminder notes about investigation tasks to BBs during investigations can also be helpful.

Arrows with arrow shafts as solid lines and solid arrow heads indicating confirmed links between all BBs on an array, are the desired goal of the integration function. However, the goal may not always be achievable due to source destruction of or changes during succeeding stages of the incident, or other reasons. In those circumstances, the inability to fully link all BBs should be explained to keep the description trustworthy.

7.1 Task guidance

Appendix B contains guidance for the input data processing functions

8 What the data integration function can produce.

The competent execution of the BB data integration function in the actor/action graphical matrix framework will produce numerous beneficial results. A primary reason for executing the data integration function during an investigation is its role in supporting the efficient management of incident investigations to produce timely actionable explanatory descriptions for incident data users. The function helps investigators define data still needed as the investigation evolves, to efficiently create the most complete possible explanatory description of the episode being investigated. Properly executed, the data linking results will produce:

1. the most complete, logical, timely and efficient processing of relevant input data from surviving sources during investigations, including inputs that influenced or "programmed" behaviours of involved entities;
2. a readily communicated, quality tested scenario describing what happened in the form of a detailed flow chart of interacting events and influences which started the incident and produced he outcome;
3. the most specific description of individual actions by each person, object or energy involved in the production of the episode's outcome to identify actions to change;
4. clear delineation of multiple and concurrent, necessary and sufficient interactions and influences during the episode, from which a "mental movie" of the episode can largely be visualized;
5. continuous investigation status information for timely investigation management actions;
6. the context for each successive action and interaction during the episode;
7. expunging of irrelevant, misleading, speculative, ambiguous or bogus data in reported explanatory descriptions;
8. full disclosure of unknowable unknowns and unresolvable uncertainties in descriptions of an incident; and
9. data structured to enable *systematic* sequential identification and definition of specific candidate iBB/oBB relationship problems, to guide the formulation of all available lessons learned and response actions by users.

9 Precautions to avoid flawed links.

One idea behind the integration function is that actions among individuals, objects or energies produced the outcome. Sequential tracking to state what each did to produce the outcome is enabled by focusing on actions and the linking of action inputs to action outputs on matrix data arrays. Each unlinked BB indicates a gap in the flow of actions by an involved actor.

Execution of the integration function can be flawed. The most frequently observed flaws in linked arrays like Events and Causal Factors Charts, Failure Mode and Effects charts, logic trees, fishbone nets and similar arrays are the tendency to add links between dissimilar building blocks, and the lack of timing relationships among linked BBs. Other indicators include links from a compound actor like firefighters as the input to an output that are invalid, because the investigator still does not know who did what, or what influenced the action. Backward links are irrational, and confuse I/O relationships.

Links from states to actions may seem questionable, because states do not make any output happen; changes to states are created by actions. It is the actions that produced their occurrence, and actions that influenced how they happened which were necessary inputs for the output states recorded. In some circumstances states may influence how an oBB happened.

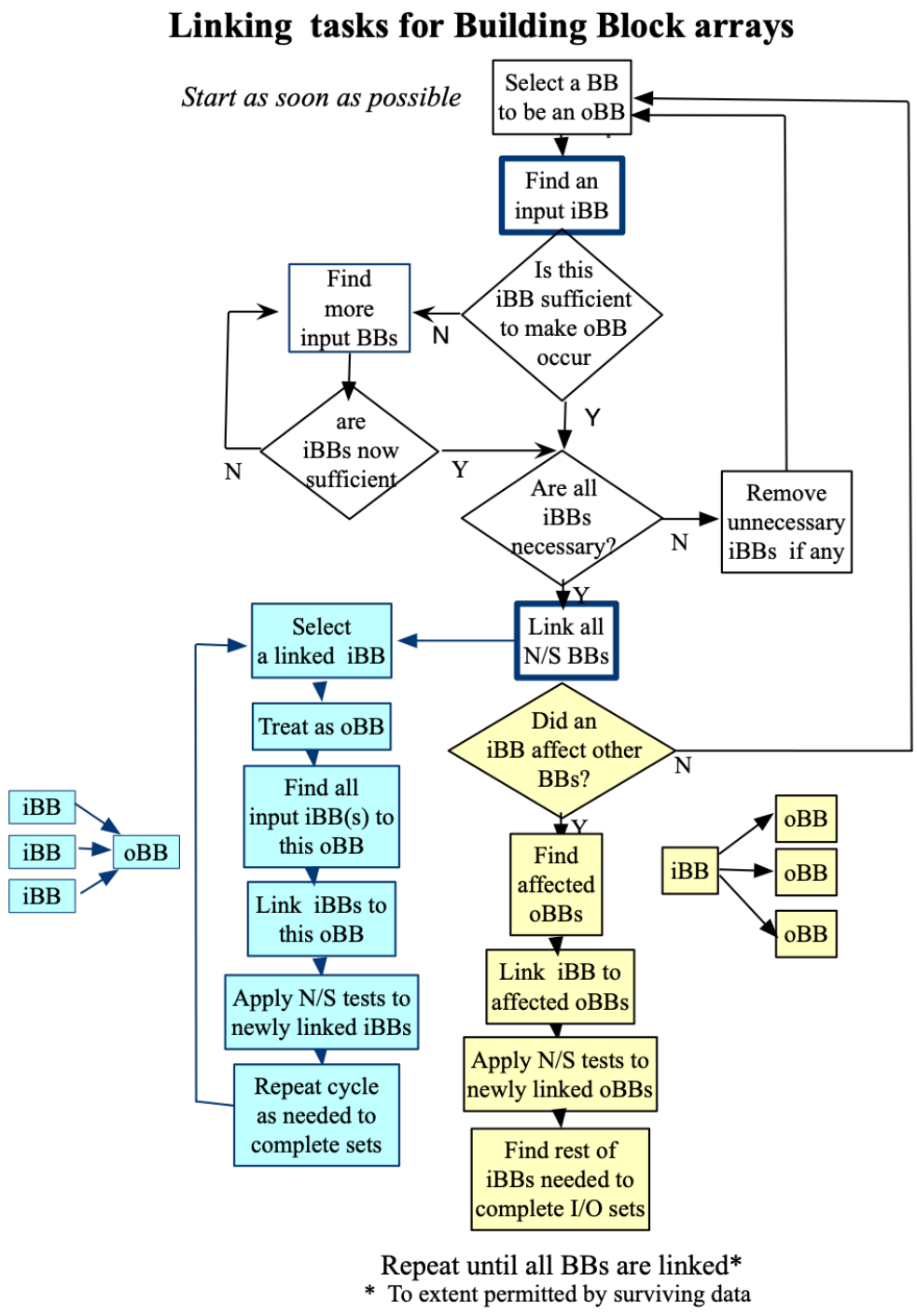
Trying to link a "did not" or "failed to" input to an output to can be suspect if they are a conclusion based on expectations of the investigators or hindsight analyses. What did the actor do that would account for the omission? This can turn out to be something like the actor was occupied doing something else, or interpreted a warning signal differently but understandably, a warning signal that didn't attract attention or was ambiguous, or there was nothing to react to.

Another flawed execution indicator is to leave gaps when tracking what a person or object did during the phenomenon.

References

1. Hendrik, K. and Benner, L., Investigating Accidents with STEP, Marcel Dekker, New, York, NY 1987 p. 77-78
2. Perrow, C., Normal Accidents, Princeton University Press, Princeton N. J. 1999, pp 89-94
3. Beach, D., Process Tracking Method in Social Science, Oxford Research Encyclopaedias, DOI: 10.1093/acrefore/9780190228637.013.176. 2017, p1
4. Investigation Process Research Resources (IPRR) 2019, http://www.iprr.org/research/AI_Methods_db.pdf
5. Benner, L.,Standardizing Safety Investigation Inputs to Reduce Risks, 45th ESReDA Seminar, Oporto, Portugal October 23-34, 2013
6. Dekker, W. A., "Reconstructing human contributions to accidents: the new view on error and performance"in Journal of Safety Research 33 (2002) 371–385

Appendix A


Linking tasks for Building Block arrays
Start as soon as possible
Select a BB to be an oBB
Find an input iBB
Is this iBB sufficient to make oBB occur
N
Find more input BBs
Y
are iBBs now sufficient
N
Y
Are all iBBs necessary?
N
Remove unnecessary iBBs if any
Y
Link all N/S BBs
Select a linked iBB
Treat as oBB
Find all input iBB(s) to this oBB
Link iBBs to this oBB
Apply N/S tests to newly linked iBBs
Repeat cycle as needed to complete sets
Did an iBB affect other BBs?
N
Y
Find affected oBBs
Link iBB to affected oBBs
Apply N/S tests to newly linked oBBs
Find rest of iBBs needed to complete I/O sets
iBB
iBB
iBB
oBB
iBB
oBB
oBB
oBB
Repeat until all BBs are linked*
* To extent permitted by surviving data

Appendix B

Input Data Processing Guidance

B1. Data Sources

1. Concentrate on data generated by the occurrence
2. Cite only incident sources that can be accessed, retrieved or reproduced
3. Cross-reference any codes used to identify sources
4. Show more than one source for BB when available
5. Try to maintain a chain of custody for all source objects, documents and media used

B2. Data selection and acquisition

1. Everyone and everything has to be someplace, doing something during accident process: track their actions
2. Force yourself to think "who or what did what when" during process
3. Look for the actor + action in Appendix B
4. Give each actor a name and always use only that name
5. Give priority to tracking the change makers that changed states
6. Be alert for physical, mental, sensory or "programmer" actions
7. Break down (decompose) actors or actions to clarify what happened
8. Let data, not experience or method, drive search for data
9. Observe the "Do no harm" rule with witnesses and objects
10. Get permissions before recording witness interviews
11. Actions change conditions: read conditions to infer actions
12. Quantify actions where possible
13. Build yourself a mental movie frame by frame as BBs are created
14. Focus on "dids" instead of "did nots" which are conclusions

B3. Tips for Test Plans for retrieving input data from things

1. Whoever Owns the Ball Calls the Game. (If its your money, you are in charge!)
2. NO PLAN, NO TESTS! (one of the basic commandments for Investigation, especially if you own what is to be tested!)
3. Don't destroy it before you get the data it holds now
4. Keep Test(s) relevant to purpose. (i.e., get BBs)
5. Scale the Plan to the value of the data it will produce. (Are BBs worth cost?)
6. Progressive destruction demands priorities

B4. Documenting Data Building Blocks (BBs)

1. An "event" = 1 actor +1 action, with related dimensional attributes
2. Transform observed data into actor + action formatted Event Building Blocks (BBs)
3. Always record Actor first, then action
4. Use ? as placeholders until you get needed data
5. Use one specific and unique name for each actor
6. NEVER ever put two actors or actions in an BB
7. Use consistent grammatical tense
    - a. Past tense for past occurrence
    - b. Present tense for planned or operating systems analysis.
8. Create glossaries for consistent actor and source entries if possible
    - Avoid poison words like pronouns - she, he, they
    - plural nouns - crew, group, squad
    - passive voice- was, were,
    - conjunctions - and, or, but,
    - ambiguous terms, jargon, acronyms, categories, factors
9. Avoid judgmental or opinion words like unsafe, inadequate inadequate, poorly, faulty, unsafe (subjective conclusions)
    - did not (implies error, masks process)
    - failed to or violated (accusatory judgement)
    - the cause (subjective attribution)
    - root cause (limiting attrtbution)
10. Record at least one source for every BB
11. Keep your experience, other external data sources out of BBs
12. Confirm only observed times as factual; add “e” for estimates

B5. Organising BBs

1. Crete a blank time/actor matrix for integrating BBs into a flow chart describing what happened
2. Add each BB to the matrix as it is created
3. Align each new BB along actor row in temporal and spatial sequence relative to all existing BBs
4. Actor row should contain BBs describing everything the actor did during the process. Gaps help identify and define unknown unknowns and data to pursue s

B6. Linking BBs

1. Use input/output logic flows to define links: do not assume or guess or rely on intuition
2. Use solid arrows to show validated input/output links in interactions
3. Use dashed arrows to show tentative links and then confirm tentative links with data if possible
4. Strive for solid black arrow links
5. Key logic test: will linked input behaviors ALWAYS produce the resulting action(s) 6. Use logic trees to bridge gaps to define additional data needed to confirm hypotheses

B7. Matrix validation (quality assurance)

1. Review logic flow of BBs on Matrixes when completed
2. Have disinterested third party review completed matrix for logic flow
3. Verify accessibility of all sources cited
4. Explain reason for all remaining ? and gaps in linkages (uncertainties)
5. Remove extraneous BBs and comments to finish Matrix
6. Title and Sign Matrix if required.

B8. Problem Definition

1. This is an **analysis** task.
2. Examine sequentially every linked BB pair and set, and their links on the finished matrix array
3. Determine whether interaction is a problem that should be addressed
4. Prepare list of identified problems or lessons Learned

B9. Investigation report

1. Use the matrix content to define the description reported
2. if permitted, separate the description of what happened on the matrix from analyses of that description, cause statements and other less reproducible assertions.

Endnotes

[i] For a list of investigation and analysis methods, and information bout each, including differences among them, see the sections of an Accident Investigation and Analysis Methods Database at http://www.iprr.org/research/AI_Methods_db.pdf

[ii] This analysis provides safety investigation procedures to implement the new view of human error presented in "Reconstructing human contributions to accidents: the new view on error and performance" by Sidney W. A. Dekker in Journal of Safety Research 33 (2002) 371–385 That document should be viewed as part of this analysis, for its discussion of investigation challenges, addressed by this analysis.Last viewed June 23,2021. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.411.4985&rep=rep1&type=pdf

[iii] Problems with using legal constructs in safety investigations are described in https://safetydifferently.com/wp-content/uploads/2014/08/Is-It-Time-To-Purge-Legal-Constructs-From-Safety-Investigations.pdflast last viewed June 23, 2012

[iv] See archives of author's prior works at http:/www.ludwigbener.org

[v] These definitions can be found in reference 1, Hendrick, InvestigatingAccidents with STEP.

[vi] Lat viewed February 7, 2020

[vii] Views of complete articles in which the illustrations were described are in m most cases kept from practitioners because they do not have or can not afford academic's access to the digital journal libraries in which they reside.

[viii] See Appendix A for BB creation guidance.

[ix] See Section E of Methods Databse at http://www.iprr.org/research/AI_Methods_db.pdf

[x] For a discussion of the problems this creates, see 'Accident Investigation Data: Users' Hidden Challenges" DOI 10.1016/j.ssci.2019.05.021

[xi] actor is sometimes called "agent" but that term is not definitive enough for defining whose actions were or contributed to state-changing events.

[xii] See Accident Investigation: An analysis of Causal Statements in Accident Descriptions; by author. Work in process; contact author for working draft of report.

[xiii] See Accident Investigation: An analysis of Causal Statements in Accident Descriptions. by author. Work in process; contact author for working draft of report. "

[xiv] This format evolved during the development and testing of versions of software designed to implement the STEP investigation system, concatenate data into databases, and produce various outputs of linked BB input/output pairs and sets. See source of software and user guidance at www.investigationcatalyst.com, and open source code at https://code.google.com/archive/p/meslib/

[xv] This is the *only* stage of an investigation when hypotheses should be initiated during the development of the description of what happened in a data-driven investigation process. If initiated before that stage, a hypothesis and theorized explanation can mislead investigators to seek irrelevant data during the investigation.

[xvi] Called BackSTEP and described in Hendrick 1987, op sit

[xvii] Each hypothesis should fill gap in part of of the linked events constituting the scenarioscenario a

Safety knowledge: the challenge of action

Professor Jan Hayes, RMIT University, jan.hayes2@rmit.edu.au

Associate Professor Sarah Maslen, University of Canberra, sarah.maslen@canberra.edu.au

Abstract

The safety literature has a lot to say about different forms of safety knowledge generated from major disasters, to minor incidents. As the call for papers for this conference illustrates, knowledge is seen to be closely connected to effective management of risks and threats. Much of the writing on this topic treats knowledge as a disembodied object, a 'thing' and yet knowledge has no agency. Perhaps the key to better organisational learning for safety is to focus on knowing, rather than knowledge, remembering rather than memory.

Recasting what we know about safety as a need for professionals to know and remember shifts the focus to improving professional practice – a new perspective on the knowledge problem. Stories have a critical role in knowing, remembering and collective knowing in support of safety excellence.

1 What is safety knowledge?

The organisers of this conference have asked us to consider challenges and practices for using knowledge in risk management and governance regarding safety in hazardous industry. In order to address this, we must first have an understanding regarding the nature of knowledge itself.

What is knowledge? In the context of safety, knowledge is often framed as comprising the facts that need to be applied to prevent accidents from occurring. This kind of abstract, technical knowledge is indeed important. Without it, accidents happen. One example that illustrates the importance of technical, factual knowledge is the major release of LNG that occurred in La Spezia in Italy in 1971 (1). LNG was being unloaded from a carrier vessel into a large onshore storage tank via bottom filling. The LNG was slightly warmer than the contents of the tank and the contents remained stratified with little internal mixing. Approximately 30 hours after unloading began, the contents of the tank 'rolled over' due to the density difference and large quantities of vapour were generated, causing the tank relief values to lift. The large vapour cloud drifted offsite but did not ignite. No-one was injured as a result of the incident, but the potential was significant. This was the first case of LNG tank rollover to be widely reported and the design and operation of LNG storage tanks changed as a result to minimise the potential for such events.

This incident is one of few in the disaster records that shows an accident caused by a new technical phenomenon. Even here, we have to say that this was the first such case reported and widely discussed. It is always possible that some people knew about this prior to La Spezia due to their own local knowledge and experience of a perhaps smaller example of the same phenomenon. We don't know for sure but certainly there was no general understanding of this technical phenomenon prior to this accident. After the accident, models were developed, and standards updated with new general requirements to address this hazard.

Downer calls such cases 'epistemic accidents' (2). Much more commonly, investigations into accident causation find technical issues, which are generally well known, but not managed appropriately in the specific accident case. The necessary knowledge did not find

its way to the right places. Think of Deepwater Horizon in the offshore oil and gas sector or the recent 737 MAX crashes in aviation. In cases such as these, accidents happen because individuals fail to make the connection between what they are doing and the generally known potential for disaster. Knowledge was available but it was not applied. The list of cases such as these is much longer than the list of cases where new scientific phenomena have been revealed. This implies that the existence of knowledge in the form of technical facts is not sufficient for safety. There are other critical factors related to knowing as well as the knowledge itself.

The same concept is present in the definition of a black swan event (although many readers apparently fail to notice it). A black swan is an event, which is not expected and has an extreme impact. Most importantly, the concept implies an event could not be predicted by those in control based on their available knowledge (3). The situated nature of the definition is key: it is about limitations to current knowledge held by a specific individual or group who have the power to change outcomes. In the case of Taleb's key examples such as the global financial crisis, important information existed and yet was not brought to bear in such a way as to prevent extreme outcomes. The notion that knowledge may exist and yet may not be immediately available to those with the power to prevent accidents has resonance with the safety too as our long roll call of major disasters illustrates.

2 Collective knowing and the implications for learning

The Oxford English Dictionary (OED) offers several definitions of knowledge including the idea that knowledge can be defined as objective truth, but it is also much more than that. Knowledge means understanding of a situation or state of affairs grasped through experience, intuition, and the senses. There is also an acknowledgment that knowledge can be acquired through instruction, study, or practice (i.e. that it is learnt), and that it is a matter of competence or expertise in a subject or skill.

When it comes to knowledge in a social context such as within a profession or organisation, recent scholarship has moved from a focus just on formalized and theoretical understandings towards a vision of knowledge as messy, located in space and time (4), specific to small social groups (5, 6), much of it as less than conscious or difficult to put into words (7, 8). These researchers and others have encouraged thinking about knowing as an active and collective undertaking for professional groups, workplace teams and organisations more broadly (9).

A key shift driven by this literature is a move from an appreciation of learning in professional fields as knowledge 'transmission' through training courses and seminars (10, 11), to an acknowledgement that knowing is developed through alternative mechanisms like working alongside colleagues, hearing their stories, getting feedback, and on-the-job experience (6-8, 12-14). Vitally, tacit knowing has been identified as essential to accurate and responsive expert decision-making (7, 15-18).

Development of expertise has been a key interest in recent knowledge scholarship. Research has focused on understanding what distinguishes experts from novices (15, 19), how people become expert (6, 7), what expertise offers organizations (7, 20, 21), and the organizational conditions of expertise development (8, 22). This interest in expertise has bought with it heightened discussion of tacit ways of knowing that are vital to the decision making of experts who work in challenging, critical, and time pressured contexts (7). A defining feature of such knowing is that it is located 'in' individuals, and further, that it is 'sticky' (23), and thus difficult for professional and bureaucratic models of organization to manage in the sense of extracting and sharing it (8). Despite these challenges, significant stock is placed in expertise. In our case of hazardous industry, it is the factor that allows complex technologies to be managed safely (24, 25). Conversely, it is found to be missing where things go wrong (26, 27).

The safety literature generally does not address knowing but there is a significant literature on the precursor to knowing: learning. Various researchers have studied aspects of learning in the context of accident prevention including the importance of learning from incident investigations (28), how best to present data for learning (29), the role of team leaders in group learning (30), and reasons why organizations fail to learn (31). For all of this, a key issue that this literature does not explicitly address is the collective status of such knowledge and there is a strong focus on the knowledge itself rather than the process of knowing.

3 Knowledge in the form of generalised truths

Returning to the idea of knowledge grounded in objective truth, knowledge in the form of generalised truths that must effectively be learned by rote as context-free absolutes remains critical for safety. Accidents sometimes happen due to ignorance of specific facts and we must always ensure that those doing specific jobs have the right technical knowledge for the tasks at hand.

Having said that, it is important to move beyond generalised truths when it comes to expert practical application. As Dreyfus and Dreyfus (19) explain, in the early stages of learning, adults follow generalised, context free rules feeling little responsibility for the outcome of their actions, only in their competence in following the rules. In the context of driving safe outcomes in hazardous industry, this means that novices may not be able to specifically link their work to the potential for hazardous outcomes. They may be broadly aware of the hazardous context and will prefer that tasks are done in accordance with a defined process that leads to a clear specific outcome. Knowledge means knowing which process to follow.

As skill level increases, a competent person has a specific goal in mind and selects context-specific information that seems to be relevant to augment their decision making. A competent person still uses rules to determine how best to tackle the problem at hand and select the best course of action. Whilst the course of action is chosen rationally (i.e., by analysis and application of rules), the decision maker now feels responsible for the outcome. Experts take this approach even further, especially when it comes to unstructured problems i.e. those where there is a potentially unlimited set of relevant information and actions and the way they interact to determine outcomes is unclear. For an expert in uncertain situations, both problem recognition and action selection are intuitive and specific. An expert just acts.

This evolution from abstract to concrete decision making contexts, reverses childhood learning sequences that require understanding of concrete examples before progressing to abstract reasoning. But specific examples are still needed for adults to build expertise. Such examples can come from an individual's personal experience but also can be drawn from the collective experience in a sector, profession or organisation (32).

4 Learning from experience

Learning from experience is complicated when it comes to preventing rare, catastrophic events as experiencing disasters directly is relatively rare and undesirable. The key comes in learning from the experience of others in the form of accident cases or stories. As our past work in this area has shown, cases are critical for expert learning to prevent accidents.

Stories that matter take three forms 1) experts use stories as parables to nurture their ability to imagine possible outcomes and maintain a safety imagination; 2) stories are also embedded in work practices to support decision-making in the moment and 3) stories are strongly linked to organisational learning for experts as a group and in mentoring less-experienced colleagues (32).

When it comes to recording and sharing stories of small faults and failures, incident reporting schemes are important tools. Unfortunately, they tend to focus on reporting and learning without fundamentally considering what people need to know to play their part in

accident prevention. A focus on collective knowledge and knowing redirects our attention to functions beyond repair of individual failures to how such systems can synchronise knowing within professional groups and mediate knowing between professional groups (33).

Major disasters are also key sources of knowledge in the safety context but as our study using the Buncefield incident as a case study shows, stories are often overlooked in incident investigations focused on liability. Despite this, they are critical for general readers in linking the everyday to the disastrous and so in developing safety expertise (34).

Developing material on disasters into effective cases for learning purposes requires detailed consideration of how adults learn. An effective case offers a concrete experience, an opportunity for reflective observation and abstract conceptualization in group discussion, and space to experiment with and apply lessons to participants' own sector completing the learning cycle (35). In fact, experts use other stories as a key part of their reasoning processes to link a disaster case to their own professional experience (36). They are also adept at drawing lessons for their professional practice from disaster in sectors other than their own (37).

5 Conclusions

It is a truism to point out the importance of knowledge but what is even more important is knowing as a practical accomplishment. Here are three points to consider when next you are responsible for a knowledge-transfer activity in your organisation.

— Think about knowing as well as knowledge

When you are thinking about lessons from accidents, whether this means sharing information about major disasters or designing system from sharing information about near misses, start by considering your audience and who need to know what. How do lessons link to day to day activities of various professional groups?

— Learning needs to go beyond 'the facts'

Technical people tend to think of knowledge as generalised models or concepts and hard scientific facts. Aristotle called this episteme. He knew that other kinds of knowledge are also important. We have emphasised here the role of phronetic knowledge – practical wisdom linked to ethics and learned from experience. Please don't forget about phronesis!

— Remember that novices find stories confusing but experienced people love them

Adult beginners like rules and models. Stories can be confusing because they deal with the complexity of the real world rather than having the clarity of a step by step process to achieve a short-term goal. For people trying to develop or maintain expert professional practice, stories are invaluable precisely because they deal with complexity. Think about this when next you are seeking to support knowledge transfer in your organisation.

References

1. Sarsten JA. LNG stratification and rollover,. Pipeline and Gas Journal. 1972;199(September, 1972):37.
2. Downer J. "737-Cabriolet": The Limits of Knowledge and the Sociology of Inevitable Failure. American Journal of Sociology. 2011;117(3):725-62.
3. Taleb NN. The Black Swan. New York: Random House; 2007.
4. Turnbull D. Masons, Tricksters and Cartographers: Comparative Studies in the Sociology of Scientific and Indigenous Knowledges. Amsterdam: Harwood Academic Publishers; 2000.
5. Knorr-Centina K. Epistemic Cultures: How the Sciences Make Knowledge. Cambridge and London: Harvard University Press; 1999.

6. Wenger E. Communities of Practice: Learning, Meaning, and Identity. Cambridge: Cambridge University Press; 1998.

7. Klein G. Sources of Power: How People Make Decisions. Cambridge, Massachusetts: MIT Press; 1998.

8. Lam A. Tacit Knowledge, Organizational Learning and Societal Institutions: An Integrated Framework. Organization Studies. 2000;21(3):487-513.

9. Hecker A. Knowledge Beyond the Individual? Making Sense of a Notion of Collective Knowledge in Organization Theory. Organization Studies. 2012;33:423-45.

10. Brown J, Duguid P. Organizational Learning and Communities of Practice: Toward a Unified View of Working, Learning, and Innovation. Organization Science. 1991;2(1):40-57.

11. Gherardi S, Nicolini D. Learning the Trade: A Culture of Safety in Practice. Organization. 2002;9(2).

12. Legat A. Walking Stories; Leaving Footprints. In: Ingold T, Vergunst JL, editors. Ways of Walking: Ethnography and Practice on Foot. Surrey: Ashgate; 2008. p. 35-49.

13. Nyiri J. Tradition and Practical Knowledge. In: Nyiri J, Smith B, editors. Practical Knowledge: Outlines of a Theory of Traditions and Skills. London, New York, Sydney: Croom Helm; 1988. p. 17-52.

14. Polanyi M. The Tacit Dimension New York: Doubleday; 1967.

15. Collins H, Evans R. Rethinking Expertise. Chicago: University of Chicago Press; 2007.

16. Groopman J. Second Opinions: Stories of Intuition and Choice in the Changing World of Medicine. New York: Viking Penguin; 2000.

17. Ingold T. The Perception of the Environment: Essays on Livelihood, Dwelling, and Skill. . London and New York: Routledge; 2000.

18. Vervoorn A. Mountain Solitudes: Solo Journeys in the Southern Alps of New Zealand. Nelson: Craig Potton Publishing; 2000.

19. Dreyfus HL, Dreyfus SE. Mind over Machine. New York: The Free Press; 1986.

20. Maslen S, Hayes J. Experts under the microscope: the Wivenhoe Dam case. Environment Systems and Decisions. 2014;34(2):183-93.

21. Weick KE, Sutcliffe KM, Obstfeld D. Organizing for High Reliability: Processes of Collective Mindfulness. In: Sutton RI, Staw BM, editors. Research in Organizational Behavior. 21. Stamford: JAI Press Inc.; 1999.

22. Maslen S. Learning to prevent disaster: An investigation into methods for building safety knowledge among new engineers to the Australian gas pipeline industry. Safety Science. 2014;64:82-9.

23. Lam A. Embedded firms, embedded knowledge: Problems of collaboration and knowledge transfer in global cooperative ventures. Organization Studies. 1997;18(6):973-96.

24. Hayes J. Operational Decision-making in High-hazard Organizations: Drawing a Line in the Sand. Farnham: Ashgate; 2013.

25. Roe E, Schulman PR. High Reliability Management: Operating on the Edge. Stanford: Stanford University Press; 2008.

26. Hopkins A. Disastrous Decisions: The Human and Organisational Causes of the Gulf of Mexico Blowout. Sydney: CCH; 2012.

27. Snook SA. Friendly Fire: The Accidental Shootdown of US Black Hawks over Northern Iraq. Princeton: Princeton University Press; 2000.

28. Carroll JS, Rudolph J, Hatakenaka S, Wiederhold T, Boldrini M. Learning in the Context of Incident Investigation: Team Diagnoses and Organizational Decisions at Four Nuclear Power Plants. In: Salas E, Klein G, editors. Linking Expertise and Naturalistic Decision Making. Mahwah, NJ: Lawrence Erbaum Associates; 2001.

29. Chevreau FR, Wybo J-L, Cauchois D. Organizing learning processes on risk by using the bow-tie representation. Journal of Hazard Management. 2006;130:276-83.

30. Edmondson AC. Speaking Up in the Operating Room: How Team Leaders Promote Learning in Interdisciplinary Action Teams. Journal of Management Studies. 2003;40(6):1421-52.

31. Pidgeon N, O'Leary M. Man-made disasters: why technology and organizations (sometimes) fail. Safety Science. 2000;34:15-30.

32. Hayes J, Maslen S. Knowing stories that matter: learning for effective safety decision-making. Journal of Risk Research. 2015;18(6):714-26.

33. Maslen S, Hayes J. Preventing Black Swans: Incident reporting systems as collective knowledge management. Journal of Risk Research. 2016;19(10):1246-60.

34. Hayes J, Maslen S. Buncefield stories: organizational learning and remembering for disaster prevention. In: Gephart R, Chet Miller C, Helgesson KS, editors. The Routledge Companion to Risk, Crisis and Emergency Management Routledge; 2018.

35. Maslen S, Hayes J. Case based learning among practicing engineers: design, facilitation and lessons learned. Cognition, Technology and Work. 2020;22:307-19.

36. Maslen S, Hayes J. "This is How we Debate": Engineers' Use of Stories to Reason through Disaster Causation. Qualitative Sociology. 2020;43:191-212.

37. Hayes J, Maslen S. Finding the parallels: Practitioner learning from cross sector disaster cases Safety Science. 2020;131.

Learning from creeping changes

Zsuzsanna Gyenes PhD, IchemE Safety Centre, zgyenes@icheme.org

Abstract

Past tragic events such as the fatal explosion and crash of Nimrod XV230, Space Shuttle Challenger or Columbia disasters, SHELL Moerdijk explosion, Herald of Free Enterprise, Kings Cross fire, and Texas City refinery explosion occurred in entirely different areas or industry sectors. There is, however, an aspect which is common in these cases, namely the phenomenon known as creeping change. The IChemE Safety Centre has recently addressed this topic, presenting a case study in its quarterly publication, the Safety Lore. They also provided practical tips to managers, process safety engineers, supervisors, and operators of industrial sites to learn how such major incidents involving creeping changes can be avoided. This paper demonstrates the phenomenon of creeping changes via two case studies from two different sectors. In addition, it suggests lead metrics associated with these events to help monitor the changes. Finally, it provides ideas to managers, supervisors, process engineers, and operators of how to address those changes in their work.

Introduction

Creeping changes are the accumulation of minor changes which often are ignored or accepted as the new norm, but which over time can add up to a big change and ultimately lead to a major incident (Goff, 2017). For example, the well-known phenomenon, "normalization of deviance" fits into this category too. It means "that people within the organization become so much accustomed to a deviant behaviour that they don't consider it as deviant, despite the fact that they far exceed their own rules for the elementary safety" (Vaughan, 2008). Past events, such as the fatal explosion and crash of Nimrod XV230 (Cave, 2009), Space Shuttle Challenger and Columbia disasters, SHELL Moerdijk explosion (Dutch Safety Board, 2015; Leveson, 2017), Herald of Free Enterprise or Kings Cross fire (Fennel, 1998) suggest that creeping changes occur with a disturbing frequency. The theory behind creeping changes is that no industrial sites are static, there are changes made to the original design or there are changes due to ageing and degradation of equipment over time, together with organizational changes that can affect plant integrity. Creeping change was noticed as an issue at the UK Health and Safety Executive's Key Programme 4 (HSE, 2014) on ageing and life extension in the offshore oil and gas industry. The Energy Institute also published its report on creeping changes and a modified hazard identification method called CCHAZID to support better understanding of how these creeping changes can be recognized during the hazard identification phase.

The IChemE Safety Centre has recently analysed creeping changes through a case study in its quarterly publication, the Safety Lore. It also provided practical tips to managers, process safety engineers, supervisors, and operators of industrial sites to learn how such major incidents involving creeping changes can be avoided. This paper presents two cases to identify aspects of creeping changes. Then it discusses leading metrics that could be associated with the events to monitor subtle changes, applying the ISC process safety lead metrics guidance document (ISC, 2015).

1 Case histories

A possible method to track creeping changes is by presenting the phenomenon through the story of past events. Those cases demonstrate how subtle changes to the system can contribute to accidents. It is then possible to develop techniques for managing these changes in the future. Creeping changes are difficult to capture based on their nature of initially being hidden and small modifications. One should not forget that all industrial sites, the organization itself and the environment constantly change; nothing remains static. Therefore, it is inevitable that any modification to the system, the original design, or procedures and roles within the organization can lead to an accumulation of creeping changes over time. The following two case studies may provide some further thoughts of what creeping changes are and how they can be captured. The first case is the 1987 tragedy of the Herald of Free Enterprise and the second is the industrial incident which occurred in an oil refinery in 2000.

1.1 Case 1 –The Herald of Free Enterprise

The tragic event of the Roll on-Roll off (Ro-Ro) ferry, the Herald of Free Enterprise, took the lives of 193 when it sank off the port of Zeebrugge, Belgium on 6 March 1987. Most of what happened was described in Kletz's book (Kletz, 2001) and the investigation report was written by the Department of Transport (Department of Transport,1987). The ferry was leaving the harbour of Zeebrugge en route for Dover on 6 March 1987 when water entered the hold and car decks via the open bow door. The Herald was manned by a crew of 80, together with 459 passengers, 81 cars, 47 freight vehicles, and three other vehicles. She passed the port at 18:24 o'clock and capsized approximately four minutes later. Even though the ferry did not sink entirely, as it was in shallow water above a sandbank, there was not enough time for passengers and crew to escape which contributed to the large loss of life.

1.1.1 Creeping changes associated with the case

The bow door, which was left open on the Herald, was used for loading vehicles. The ferry did not have bulkheads within the car decks; therefore, it was easier to load more vehicles faster. It was a normal practice on Ro-Ro ferries. However, it meant that when water entered the ship it then moved to one side of the deck and the ship became unstable. Even though the Parliament passed an act requiring iron ships of over 100 tons to have divided hulls, the shipping lobby got the act repealed. Most ships had divided hulls, but Ro-Ro ferries tended not to because of the difficulties of loading their cargo and the desire to maximise loads. This is a change which fundamentally seems like nothing was changed since the bulkheads remained non-applicable on these ferries. However, it also means that these ships followed a practice which eventually had been altered from the new regulations, lobbying for, and then applying their own old rules.

The Assistant Bosun, whose job it was to close the bow doors as the ship left harbour, had fallen asleep on his bunk and missed the loudspeaker warnings that they were about to depart. The Bosun was on the main deck but he did not consider it his duty to close the doors or to ensure that there was someone to do it. The Captain assumed that everything went well and proceeded to set sail. Leaving the port without making sure of the status of the bow door was a bad practice which was repeated from time to time. That highlights the aspect of normalisation of deviance.

The first ferries had had so-called visor doors that lifted so that the Captain could see from the bridge the status of the doors (open/closed). The door design had been changed to a clam type and the doors were not visible from the bridge anymore. This change never went through a management of change process and, therefore, risks associated with the new design were never revealed.

The investigation report found that on several previous occasions ships had left harbour with their doors open and that several captains had asked for indicator lights to be installed; but their requests had been ignored. That aspect shows normalization of deviance up to a certain extent because captains knew they would leave the port again with open doors. The fact, that they had informed the management about the problem may have given the impression that the issue would be or was solved; thus, the unsafe behaviour was sustained.

The holding company had only owned the company for a few months before the accident. That fact qualifies as an organizational change, which is yet another form of creeping change.

Three crews and five sets of officers were employed in manning the Herald. Consequently, the officers did not always have the same crew. There was a lack of consistency in the duties of each set of officers and of the members of each crew. This aspect can be considered as creeping change due to the lack of consistency, a subtle variation of modus operandi which eventually contributed to the accident.

1.2 Case 2 –Oil refinery fire

The Fluidised Catalytic Cracker Unit (FCCU) was shut down on 29 May 2000 following the power distribution failure and was being restarted after an 11-day shutdown. On 10 June 2000, during start-up, a significant leak of hydrocarbons was discovered, creating a vapour cloud which ignited, resulting in a serious fire. Workers escaped before the blast, and no one was injured in the incident (HSE, 2000).

1.2.1 Creeping changes associated with the case

The leak was a result of the failure of a tee-piece connection at the base of the debutaniser column which found a source of ignition nearby. The tee-piece connection, which had originally been installed in the 1950's, was correctly specified but incorrectly fitted, and then hidden by lagging. There was no subsequent amendment to the plant layout drawings to identify that change.

Since the 1950's, sections of the FCCU had been significantly modified. Prior to the modifications in 1986, changes had been made to the pipe work at the base of the column and a valve had been removed. This resulted in there being inadequate support for the remaining pipe work and the tee-piece connection. Between 1996 and 1998 the FCCU had been experiencing considerable difficulties and did not operate consistently. This resulted in an increase in the number of start-up/shutdown cycles for the plant and pipe work.

An incident occurred in 1999 during a prolonged start-up on the FCCU, which resulted in an ignition of a torch oil vapour cloud. Contrary to plant operating instructions in the master operating manual, the torch oil had been admitted to the regenerator when the unit was at too low a temperature. The plant had solid procedures in place, yet the operating procedure was ignored by the staff. As a result, ignition of the torch oil did not occur in the regenerator. Although ignition had not been verified, a considerable further quantity of torch oil was injected, and it is believed that hot spots in the slumped catalyst bed vaporised the torch oil. The provision of a temperature interlock had previously been considered and discounted, as it was decided that operating procedures alone provided enough control. This decision shows alteration from the original design that would have been required but then was excluded. The change was made based on an assumption rather than on a risk assessment.

In the eleven weeks preceding the incident in 2000, nineteen start-up attempts had been made and only seven were successful. Failure of the tee-piece connection pipe work was probably caused by a combination of the incorrectly fitted tee-piece connection, the inadequately supported pipe work, and the cyclic stresses/vibration caused by the increased number of start-up/shutdown activities on the plant. Eventually they led to fatigue failure of the pipe work in the vicinity of the welded connection. These are the subtle changes that had gone unnoticed for a long time before they were discovered.

The safety report failed to reflect the reality of the condition of the FCCU. The 1997/98 revision concluded that "hardware and software controls in place on the FCCU are adequate to prevent the occurrence of a major accident". Incidents with vibration of the transfer line had occurred over the two years prior to the explosion. These events were not reported or investigated, which resulted in changes going unnoticed.

On the 25th May a cable-laying operator from the cable-laying contractor hired by the company observed a damaged tile and cable in preparation for laying a cable. However, he did not report the damaged cable in the belief that it was dead, and it had already been reported. When such a failure is not reported to the management it is a missed opportunity to identify a creeping change that could lead to a catastrophic event.

2 Lead process safety metrics identified with the case studies

In 2015 the IChemE Safety Centre published a guidance document on process safety lead metrics. The guidance document states that: "Tracking process safety metrics is vital, to help us understand the state of our facilities and systems, as well as providing us with an indication of impending issues. Importantly, while lagging process safety metrics will inform you of history, which can be used to monitor improvement, they will not necessarily predict future loss-of-control events. While leading metrics are proactive and provide the opportunity to manage developments, they are also not predictive of the future". The layout of the guidance was developed along the lines of the ISC functional elements of process safety (ISC, 2014).

The six functional elements, with leadership across all of them are as the followings:

- knowledge and competence,
- engineering and design,
- systems and procedures,
- assurance,
- human factors, and
- culture.

In total, 21 lead process safety metrics were identified in the guidance document around the six functional elements, as it is shown in Figure 1.

Figure 1. Lead process safety metrics.

Elements	Metrics
Knowledge and competence	Conformance with Process Safety related role competency requirement
Engineering and design	Deviations to safety critical elements (SCE) Short term deviation to SCE Open management of change on SCEs Demand on SCE Barriers failing on demand
Systems and procedures	SCE Inspections Performed Versus Planned Barriers fail on test Damage to primary containment detected on test/inspection SCE maintenance deferrals (approved corrective maintenance deferrals following risk assessment) Temporary operating procedures (TOPs) open Permit to work checks performed to plan Permit to work non-conformance Number of process safety related emergency response drills to plan
Assurance	Number of process safety related audits to plan Number of non conformances found in process safety audits
Human factors	Compliance with critical procedures by observation Critical alarms per operator hour (EEMUA, 1999) Standing alarms (EEMUA, 1999)
Culture	Open process safety items Number of process safety interactions that occur

Source: ISC, 2015.

2.1 Lead process safety metrics identified related to Case 1

Relating to the case of the Herald of Free Enterprise, a strong lead metric would be the Conformance with Process Safety related role competency requirements. This metric measures the overall capability of personnel to consistently manage and implement work activities in accordance with company requirements and expectations (including behaviours). In this case, personnel were overworked; the investigation revealed that the officers were required to work 12 hours on and not less than 24 hours off. In contrast, each crew was on board for 24 hours and then had 48 hours ashore. Also, they simply could not implement work activities in accordance with company requirements because the company lacked any procedures.

An additional metric associated with the case is linked to safety culture. For example, during the interviews after the accident, the Bosun stated that it was not his duty to check whether the doors were open or closed. Another problem the investigation discussed was the fact that the management ignored the advice of their experts regarding various problems with the ferries. There were numerous events when onshore management did not listen to the advice of their well-qualified ships' masters. These included requests for bigger ballast pumps, fewer passengers, and complaints that draught marks were hard to read, in addition to the requests for indicator lights.

Barriers failing on demand is a metric that could be identified in this case. A high number of failures upon demand would indicate either an engineering design issue or the need for improvement in the effectiveness of the inspection and maintenance of the barrier to

determine whether the demand frequency matches the design of the protection loop. The lack of divided hulls is a significant barrier failure which, if corrected, could have prevented the ship from becoming unstable and moving to one side of the deck and finally overturning.

Safety critical elements (SCEs) inspections were planned but were not performed. This metric identifies the level to which SCEs are not being inspected or tested within the required inspection period. The metric will indicate problems related to planning, resourcing requirements, or culture relating to the acceptability to allow SCEs to remain in service after required inspection periods have lapsed.

Albeit indirectly, Open Management of Change (MoC) on safety critical elements is a metric that can also be identified in this case. The change in the design of the visor doors would have required an MoC process. When a new hazard is identified as part of an incident and requires an instrumented system to be installed. The same metric could be applied considering the several occasions when ships had left harbour with their doors open and several captains had asked for indicator lights to be installed.

The metric of compliance with safety critical procedures by observation is a critical indicator in this case. It tracks compliance with safety critical procedures at all levels of the organisation, those related to the processing facility safety critical elements and tasks where failure to follow the procedure correctly could lead to a process safety incident. Apparently, the Herald of Free Enterprise lacked operating procedures. The situation got worse with officers not having the same crew which resulted in the lack of uniformity in the duties of each set of officers and of the members of each crew.

In terms of assurance, there were no audits carried out, which could have highlighted the lack of hazard analysis, missing procedures, and other non-conformances in the operation of the ferry, such as carrying an excessive number of passengers; occasionally even 10-20% more than the limit.

2.2 Lead process safety metrics identified related to Case 2

In this incident, lead process safety metrics are simpler to identify compared to the case of non-process safety incidents, such as the Herald of Free Enterprise. However, many of the past events show that there is still a lack of proper implementation and understanding of what lead metrics are and how to monitor them. This section of the paper shows examples of process safety lead metrics that could have been in place in this oil refinery.

The tee-piece connection played a significant role as a safety critical element; therefore, the metrics in connection with SCE's should be identified, especially relating to the ISC functional element "Engineering and design". For example, the increased number of start-up/shutdown cycles for the plant and pipe work could be monitored by implementing the metric Demand on SCE's which monitors the frequency when safety systems are called to function. The increased number of start-ups and shutdowns would have been tracked applying this metric.

The metric "Compliance with safety critical procedures by observation" could have revealed whether critical procedures, such as start-up procedures, are correctly followed. In this case, an incident occurred in 1999 during a prolonged start-up on the FCCU which resulted in an ignition of a torch oil vapour cloud. Contrary to plant operating instructions, the torch oil had been admitted to the regenerator when the unit was at too low a temperature.

Open management of change on SCE's can be identified relating to the modification of the plant, particularly the removal of a valve on the pipe work, at the base of the column which supported the pipe work and the tee-piece connection.

Incidents with vibration of the transfer line had occurred over the two years prior to the explosion. These events were not reported or investigated, which resulted in changes going unnoticed. Also, the company reviewed the FCCU to find out why it did not operate properly

but the findings were never implemented or communicated properly. These are aspects that illustrate the absence of lead metrics monitoring culture.

The safety report failed to reflect the reality of the condition of the FCCU. The 1997/98 revision concluded that "hardware and software controls in place on the FCCU are adequate to prevent the occurrence of a major accident". The metric called "Number of non-conformances found in process safety audits" could have provided further insights of this mishap. It could have been a valuable indicator both to the company and to the competent authority. This metric provides assurance to the board and the senior management that process safety systems are implemented and effective in the plant. The purpose of having process safety auditing as a safety metric is to provide assurance of the quality of activities associated with other process safety lead metrics.

3 What can you do?

In addition to the lead metrics recommended, along with the case studies, the following tips to managers, supervisors, and operators could be listed to tackle creeping changes more effectively. Tables 2-4are an extract from the ISC Safety Lore (ISC, 2019) showing the list of the responsibilities for managers, supervisors, and process engineers and operators.

3.1 What can managers do about creeping changes?

Table 1. Responsibilities of managers.

Management
Be aware that changes in management or ownership can have large consequential hazards; therefore, make sure that organisational changes go through a Management of Change (MoC) procedure.
Incidents often occur after some change in the system. Make sure that changes as a result of adoption of new or altered processes, loss of skills, and new knowledge brought into the operation are addressed in the MoC process.
Ensure that audits address changing behaviour to check that the process is carried out as designed.
Every system and its environment change over time. Make sure to apply strategies to adapt to changing environment and/or changes in the safety management system.
Have the safety case or safety report kept as a living document that needs constant review to follow up the changes that might occur over the years.
There can be significant differences between the designed and the built system. If an incident scenario is not considered in the design phase but that scenario is possible, then it needs to be incorporated into the leading metrics programme.
Signs of change are difficult to detect; therefore, consider implementing a system and structured process for identifying them, detecting how the process should operate, and what the current status is.
Make sure that leading metrics are implemented in the risk management programme and that responsibilities are assigned for checking the metrics and following them up in case problems are found.
Have an action plan in place to ensure that leading metrics exist and that they indicate when and how they will be checked and have an action associated with them. Periodically review and update the list of leading metrics.

Make sure that near miss events are identified and investigated as they can be precursors of a major incident. Pay attention to cumulative causes that help to identify dramatic changes that may have been overlooked.
Ensure that change is detected and even small changes to the system are documented in the incident investigation reports instead of simply focusing on proximal events.
In case of an incident, check whether leading metrics are in place and why they failed to identify the problem to prevent the incident, or, if they did, why effective action was not taken.
Make sure that cost cuts do not impact safety and they do not threaten plant integrity.
Make sure that process knowledge is maintained and transferred.
Make sure that you record trending of the leading metrics; ensure that the process functions as it is intended based on the original design.
Ensure that you document all changes, particularly safety critical ones and near misses immediately and that these records are incorporated into the plant operating procedures.
Starting up a process unit results in significant changes (operating temperature, pressure) on the pipe work and vessels as they are brought up to the required operating conditions from ambient. Be aware that increasing the frequency of start-ups results in fluctuations in conditions and increased cyclic stresses on mechanical systems.
Pay attention to the signs of normalisation of deviance where operators might alter from the original procedures, to make sure that safe operation is in place.
Have up-to-date plant layout drawings and maps to follow up changes and keep record of the original design layouts.
Report and investigate all cases of violations, unauthorised changes and workarounds in the system.
Make sure that you follow the operating, maintenance and emergency procedures and do not deviate from them.
Report any damage or irregular event immediately to the supervisor.
If the procedures cannot be followed, report the situation to your supervisor for investigation and resolution.

Source: ISC, 2019.

3.2 What can supervisors and process engineers do about creeping changes?

Table 2. Responsibilities of supervisors and process engineers.

Process Engineer/Supervisor
Make sure you record trending of the leading metrics; ensure that the process functions as it is intended, based on the original design.
Ensure that you document all changes, particularly safety critical ones and near misses immediately and these records are incorporated into the plant operating procedures.
Starting up a process unit results in significant changes (operating temperature, pressure) on the pipe work and vessels as they are brought up to the required operating

conditions from ambient. Be aware that increasing the frequency of start-ups results in fluctuations in conditions and increased cyclic stresses on mechanical systems.
Pay attention to the signs of normalisation of deviance where operators might alter from the original procedures, to make sure that safe operation is in place.
Have up-to-date plant layout drawings and maps to follow up on changes and to keep a record of the original design layouts.
Report and investigate all cases of violations, unauthorised changes, and workarounds in the system.
Make sure that you follow the operating, maintenance, and emergency procedures and do not deviate from them.
Report any damage or irregular event immediately to the supervisor.
If the procedures cannot be followed, report the situation to your supervisor for investigation and resolution.

Source: ISC, 2019.

3.3 What can operators do about creeping changes?

Table 3. Responsibilities of operators.

Operator
Make sure that you follow the operating, maintenance and emergency procedures and do not deviate from them.
Report any damage or irregular event immediately to the supervisor.
If the procedures cannot be followed, report the situation to your supervisor for investigation and resolution.

Source: ISC, 2019.

4 Conclusions

The cases presented in the paper show how even subtle but gradual changes to the system can contribute to accidents. This paper demonstrates the phenomenon of creeping changes, taking two case studies from entirely different sectors. In addition, it suggests a variety of lead metrics which could be associated with each event. Lead metrics are helpful tools for any organisation to monitor processes and changes. If they are applied with appropriate knowledge and understanding of what we want to achieve and why, they can help to prevent tragic events. Every organisation can benefit from implementing lead metrics, regardless of the profile of the industry. To be able to capture creeping changes relevant to the job, and make relevant stakeholders aware of their own responsibility, the paper provides advice to managers, supervisors, process engineers, and operators. Creeping changes are difficult to identify based on the nature of them being initially hidden, small, and subtle modifications. However, with the necessary care and vigorous monitoring of the system, these changes can be captured in time to prevent a major incident.

References

1. Department of Transport,1987 Formal Investigation Herald of Free Enterprise, Report of Court No. 8074. ISBN 0 11 550828 7 Crown Copyright, 1987

2. Dutch Safety Board, Explosions MSPO2 Shell Moerdijk, The Hague, 2015
3. Fennell, D. (1998), Investigation into the King's Cross Underground Fire, London: The Stationary Office
4. Haddon-Cave, C. (2009), An Independent Review into the Broader Issues Surrounding the Loss of the RAF Nimrod MR2
5. HSE (2000), BP Grangemouth. Major Incident Investigation Report. Crown copyright 2003. Retrieved 12 April 2021 from "http://www.hse.gov.uk/comah/bpgrange/images/bprgrangemouth.pdf"
6. HSE (2007), Key Programme 3 (KP4): Asset Integrity Programme http://www.hse.gov.uk/offshore/kp3.pdf accessed at 5 May 2021
7. HSE (2014), Key Programme 4 (KP4): Ageing and Life Extension Programme. Retrieved 9 May 2021 from http://www.hse.gov.uk/offshore/ageing/kp4-report.pdf
8. ISC (2014) IChemE Safety Centre framework at https://www.icheme.org/knowledge/safety-centre/framework/ accessed at 10 May 2021
9. ISC (2015) IChemE Safety Centre Guidance Lead Process Safety Metrics - selecting, tracking and learning. Retrieved 10 May 2021 from "https://www.icheme.org/media/14928/safety-centre-metrics.pdf
10. ISC (2019) ISC Safety Lore Issue 5 Key lessons from incidents relating to creeping changes. Retrieved 10 May 2021 from "https://www.icheme.org/media/10952/isc-safety-lore_issue-no5.pdf
11. Kletz (2001) Learning from accidents. Chemical, Petrochemical & Process Referex Engineering. 075064883X, 9780750648837. Routledge, 2001
12. Nancy G. Leveson (2017) CAST Analysis of the Shell Moerdijk Accident Retrieved 4 May 2021 from http://sunnyday.mit.edu/shell-moerdijk-cast.pdf
13. Richard J. Goff (2017) What to do about creeping change, The Chemical Engineer Issue 917. 2017
14. Vaughan (2008), Interview: Diane Vaughan Sociologist, Columbia University. Retrieved 17 May 2019 from http://www.Consultingnewsline.com/Info/Vie%20du%20Conseil/Le%20Consultant%20du%20mois/Diane%20Vaughan%20(English).html accessed at 17 May 2021

Safety: Old School or New School, myths or questions?

John Stoop, stoop@kindunos.nl

Sverre Roed-Larsen, sverre.rl@wemail.no

Abstract

In this paper, a plea is made for reflection on present debates about an assumed primacy of either an Old School or New School in safety thinking. Taking into account the very nature of socio-technical systems, such a debate is fruitless and reinforces the dialectic stall that has already dominated the debate on safety notions for decades. Rather than continuing this debate, the legacy and nature of socio-technical systems is explored. In order to cope with the dynamics and complexity of modern high energy density systems such as the maritime, rail and aviation, new notions such as resilience and foresight are introduced. Both notions deserve thorough consideration in their validation by verification or falsification. Based on the Ultra Large Container Ship MSC Zoe case, a proposal is formulated to combine the goods of both developments into a new school of safety thinking. Such an evidence and knowledge based school could be coined a Smart School of Safety Thinking. Heading towards a Smart School of Safety Thinking: knowledge based in the design, evidence based in investigations, value based in communication and cooperation.

1 Introduction

In recent discussions on safety, the tradition of coining conflicting notions has reached a new level of disagreement. Over the past decades, controverses have been created between notions, challenging each other as more modern, valid or theoretically correct in a scientific manner or in a socio-organisational and economical context. Such debates have focused on occupational versus process safety in a context of corporate values, static versus dynamic risk modelling under conditions of scientific uncertainty, internal versus external environmental safety, technical versus social managerial controllability, deterministic versus probabilistic risk acceptance considerations, normal versus non-normal operational conditions and Safety 1 versus Safety 2 as feedback or feedforward learning loops. Nowadays, not only a controversy between safety notions is debated, but the validity of safety as a science is questioned as being superfluous to already existing disciplines in the socio-psychological and organisational domain (Safety Science 2014, Stoop, De Kroes and Hale 2017). This debate on different schools of safety thinking focuses on a paradigm shift rather than differences in safety notions. This New School emphasizes a recovery from unanticipated consequences instead of hazard identification and precaution, developing coping strategies of a governance and operational control nature versus application of system engineering design and certification principles. This School profiles itself as Resilience Engineering, with their own socio-psychological interpretation of technological notions from the system engineering domain such as elasticity, adaptivity, functional interferences and resonance and oscillation of system Eigen Value vectors. It introduces a new, exclusive expert language, interpreting and contradicting existing notions in a new context. Such a language hampers communication with Old School thinkers, making the debate non-conversant with system engineering design disciplines (Rayo 2021). In this debate, several myths are cultivated about 'Old School' of safety thinking as being reactive, retrospective or even obsolete. In the 1990's this 'New School ' of thinking emerged as a response to the Reason/Rasmussen socio-psychological school of thinking. Some 'New School' thinkers claim that 'we' cannot learn from failure, but

should rather learn from success. Safety should be based on learning from emergent properties in practice, as outcomes of complex socio-technical systems which are by definition incomprehensible. Such learning should be based on a shared responsibility of both management and first line operators in solving discrepancies between Work as Intended and Work as Done. In this New School thinking there is an almost unnoticed transition from a socio-technical towards a socio-organisational paradigm. In analysing complex systems, a hierarchical and vertically layered system architecture is gradually replaced by a heterarchical (e.g. based on cooperation and consensus), open and horizontal network construct. This new school claims a new construct of 'Resilience Engineering' that should provide the ability to recover from unanticipated and unprecedented events during operations with a focus on governance and managerial control, rather than identifying hazards during the systems engineering design and certification process.

There is no evidence however, that such 'New School' thinking has superior qualifications and achievements. There is no proof of concept (yet). According to New School thinkers, a lack of acceptance of this New School should be attributed to cognitive stubbornness and reluctance to change in high tech sectors such as aviation and maritime (Zimmermann et.al. 2011). Such claims raise a more fundamental question: does this New School thinking comply with needs and constraints of socio-technical complex systems in their efforts to create disruptive and prospective adaptations to modern times?

2 Research questions

So far in practice, this New School is not accepted by high tech industries such as aviation and maritime, because reality is harsh. This New School debate does not acknowledge all efforts, resources, experiences, expertise and knowledge that have been devoted over decades in what nowadays is called legacy systems. Aviation and maritime have become - by definition of the 10e-7 failure rate asymptote - Non-Plus Ultra-Safe systems, decades before this safety debate on Resilience Engineering started. A legitimate question therefore is: how did aviation and maritime become so safe if they were grounded on apparent deficient principles of Old School thinking? What were the driving forces and change agents that lead to an unsatisfactory perspective of reaching an asymptote that cannot be superseded? Is the Old School unable to identify and accept a more disruptive safety approach in adhering to its Old School thinking?

The basic research question in this paper is: are the New School claims and assumptions true? Does this school really has added value? Is there a proof of concept?

In order to accept New School thinking, three showstoppers can be identified and analysed:

1 Theoretical vulnerabilities in assumptions. In old school thinking, complex and dynamic systems with a high level of technological sophistication, such as aviation and the maritime, require an integral systems approach throughout life cycles and aspects, starting in its conceptual design, operational specifics and conditional limitations as expressed by the systems operating envelope up to the phase of rescue, recovery and reconfiguration. Such a systems approach recognizes several system state transitions, producing specific generations of technology, organisation, governance and institutional control. In contrast, in their desire to proclaim a paradigm shift in a New School thinking, resilience engineering advocates specifically focus on generic operational conditions, organisational aspects, managerial competences and public governance. In shifting their focus, they prefer different optimization rationales and control assumptions. In their approach, technology is considered evolutionary, almost a constant, while operating in a steady -normal- system state. There is no substantive distinction between derivative and disruptive adaptation of systems, which are considered to be triggered by 'emergent', rather than by inherent properties of such high energy density systems. Exploration of assumptions in both schools seems inevitable.
2 External interferences in the debate. First, in socio-organisational literature, limited assumptions on systems architecture and dynamics prevail. System concepts

seldomly focus on stability and control of a higher level than the human operator in its organisational context, feeding back information and experiences from reality into technical system adaptations and organisational change, emphasizing compliance with optimal performance standards rather than to cope with unforeseen situations and system state transitions that require problem solving competences at a higher cognitive level. Second in a wider context than the actual operating environment, New Economy paradigms interfere with scientific modelling of managerial control and governance change agents. The paradigm shift in New Economic thinking has prioritized process over content, market over knowledge. New Economy considers technology as unjustified 'unruly', to be reformatted and submitted as 'ruly', based on prescriptive conditions, hierarchically controlled at a governance level. Deregulation and privatisation should enable a free market business model, facilitated by 'unruly' organisational conditions. As a consequence, such a system architecture reflects the chaotic and unforeseeable nature and behaviour, creating 'emergent' behaviour. Anomalies, disruptions, change triggers and change agents have become the subject of scientific exploration and research by prominent academics of a variety of scientific disciplines (Minsky 1986, Vincenti 1990, Berkhout 2000). To distinguish between technological complexity and socio-organisational complexity, the Cynefin model is introduced: technological complexity should be of a lower order -called complicated systems- than socio-organisational complexity -called complex systems (Snowden 2007). Such socio-organisational systems have the potential to drift into chaotic systems if governance and control mechanisms are not adequately organised. In such cases, properties cannot be longer identified and analysed as inherent, but should be emergent; only perceivable and understandable in hindsight. Or, with the paraphrasing of Rumsfeld, become opaque and intangible as 'Unknow Unknows'. This, however, does not discredit emergent properties and serendipity. Due to gradual changes and graceful adaptations, systems may encounter occurrences as 'serendipities': accidents that could not have been observed before (Arslanian 2011).

3 Myths or proof of concept? In arguing the need for a new paradigm, four beliefs are articulated in favour of such a change. They argue the need for a radical new school of thinking. However, such beliefs should either be substantiated or falsified. First; according to Amalberti, a theoretical asymptote of 10e-6 should exist beyond which no further progress should be possible. The existence of such an asymptote has never been proven. In contrast, in 2019, the international commercial aviation community suffered no fatalities, achieving Zero Accidents. Consequently, this result falsified this belief as a theoretical limit which could not be crossed. Second; derivative and disruptive adaptations should be indiscriminate. Unfortunately, derivative evolution hardens the belief and even reliance on the fundamental assumptions in a system design. Disruptives however, challenge such assumptions, creating new options and exploring opportunities of a different nature. According to the research on disruptives of Vincenti (1990), Berkhout (2000) and Snowden (2007), such system state transitions and anomalies have a radically different safety impact on system performance levels. Such differences also require different testing and reveal deficiencies in certification regimes, as demonstrated by the Boeing 737MAX case. Thirdly; while individual risk is defined as the product of probability times severity, the systemic risk exposure is also determined by the size of the population at risk and the overall number of events and occurrences. This belief is related to the linearity in system growth and validity of extrapolating existing assumptions. In reality, there are limitations to growth, accompanied with sudden changes; systemic perturbations and tripping points. Finally, the New School of thinking relies on a belief in dominance of operator variance: operational feedback should drive out feedforward restrictions in qualified operational performance. Operational experience, tacit knowledge is as valid a source of information as design assumptions on operational performance and cognitive modelling of operator behaviour. Combining the two sources of feed forward and

feedback information complies with the theoretical Full Information Paradigm of Klir (1987).

3 Analysis into the nature of legacy systems

Before safety analysts can embrace this New School thinking, the nature of legacy systems should be clarified to see whether there is a need for surpassing deficiencies in Old School thinking, to be inevitably replaced by a New School thinking. Scanning the legacy of the maritime sector as a socio-technical system, several characteristic properties can be identified:

- The dual nature of a socio-technical stability, based on both technical design of vessels and their navigational equipment, certification and governance control by supra national institutes and regulations such as the International Maritime Organisation IMO
- Technology as a flywheel for progress; an unruly regime for vessel design is combined with vessel/fairway harmonisation of dimensions and operational conditions
- Derivative adaptations by reliance on parent vessel design principles, creating safe and reliable variation selection and certification regimes
- The principle of Good Seamanship, delegating and distributing final responsibility for safe and sound conduct, guaranteeing survival of passengers, crew, cargo and vessel
- Feedback from operational practices by disciplinary actions, institutionalized in Maritime Courts, Codes of Conduct and crew qualification standards.

This legacy nature of the maritime community is challenged by changes in the international operational context and conditions, compliant to requirements of Neoliberalism:

- Deregulation and privatization erode governmental institutions and state oversight
- Economy of scale jeopardizes harmonization of vessel dimensions and fairway limitations, such as VLCC's, cruise vessels, ferries and ULCS container vessels
- Flag State policies promote flagging out to Flags of Convenience, lowering the level of the safety playing field
- Traffic Separation Schemes, mandatory routing optimization and routeing restrictions create dense traffic flows in shallow waters and narrow sailing areas
- Managerial pressure on logistic chain handling by Just in Time requirements erode defences regarding aggravating sailing and weather conditions, pushing operations in the margins of the performance envelope.

In the Old School logic, defences were established to such challenges by investigating the events in order to understand the system, thinking along lines of system life phases of design, operations and emergency handling. To prevent a drift into chaotic systems behaviour, higher system orders are analysed, dealing with system properties, principles and systemic stability and control. On a regular basis, additional regulations became mandatory under the umbrella of IMO Regulations. Such regulations were not seldomly triggered by maritime disasters and their subsequent recommendations to improve the safety performance of the maritime system. The general motto is: by exploring the system functioning in hindsight, gain insight in order to achieve oversight for the sake of foresight.

In conclusion: this Old School analytical thinking complies with the architecture and needs of the maritime sector and serves as the driver for change and innovations. Such thinking serves to clarify system design assumptions, operating limitations and restrictions in operator system state awareness. Such thinking serves as a knowledge provider of awareness and understanding of the various states a system may demonstrate in previously unanticipated situations, unforeseen interrelations and deviating dynamics.

4 The MSC Zoe case, perspectives and findings

In a debate between Old School, New School advocates claim that differences in perspectives shed new insights on accident causation. A basic claim that should be either proven or falsified is whether or not New School thinking enables to learn from what went right, making learning from what went wrong oblivious.

Figure 1. The Ultra Large Container Ship MSC Zoe.

In the investigations of the MSC Zoe case, two different perspectives can be identified:

- A **socio**-technical case perception, where data collection and interpretation is based on newspaper analysis, social media, operational expert opinions
- A socio-**technical** case description, based on the official report of the Dutch Safety Board supported by recommendations to enhance the systemic performance.

1. The **socio**-technical case perception is based on information feedback from the operational phase, such as crew and operator perceptions and observations, newspapers, social media, expert opinions, scientific literature and applied maritime journals. Such information is not necessarily related to the specifics of the MSC Zoe case.

- Known issue: annual loss of 1700 containers worldwide
- Safe draught was known as compromised by sea and weather conditions
- Shortest route for economic reasons, short port stays for container handling
- Just In Time deliveries, 24/7 operations,
- Additonal warnings included in regulations
- Black box malfunctioning known deficiency
- Vessel experienced violent manoeuvring due to sea conditions
- Likelyhood of grounding excluded in shallow Southern Traffic Lane
- Green water impact excluded due to size and robustness of vessel
- Crew fatigued and fire safety known as compromised
- Harsh competition, small margins, hardly port authority inspections
- No info on container content based on confidentiality and competiveness

- Legal and financial claims rise into millions of Euros
- Involvement of inspectorate, parliament, local authorities, Dutch investigation Board
- Everybody responsible, nobody accountable
- Advocacy for smart container track and tracing devices

2. The socio-**technical** case description deals with a factual and evidence based reconstruction of the event by an investigative authority. This reconstruction focuses on the specifics, context and operating conditions of the MSC Zoe in particular and is condensed in a formal safety investigation report (Dutch Safety Board 2020).

- The 400 m MSC Zoe loses 342 containers in the Southern TSS Terschelling-German Bight due to violent roll at Bft 9 wind. Loss of cargo and environmental damage causes major public concern because of the Wadden as Unesco World Heritage. Due to the size, vessel motions, night and seagoing conditions, the crew did not notice 5 out of 6 losses. The crew was appropriately qualified.
- Transverse accelerations and forces relate to stacking heights and GM (metacentre) stability and length of the vessel, exceeding CSS Codes of lashing and storing calculations and their validity range. The applied computer software was not transparent in the calculation details and design accelerations. A reduction of stack mass and heights should have been effected.
- Deformation of the vessel increased the loads and accelaration levels with 40-50% by its flexible response due to elasticity issues.
- A series of new and unexplained issues reduced safety levels: container stack dynamics increased 200% over static calculations. This was triggered by insufficient roll damping due to high stability and GM values, combined with wave resonance. Sea conditions in shallow waters and the beam sea scenario interfered with vessel dynamics, causing a continuous rolling.
- Soft contact with the bottom, green water, impulsive wave loads, tidal situations and slamming created large accelarations, forces and vibrations causing a repeated loss of containers. The combined impact of these 4 phenomena is unknown.
- The southern routeing of the Zoe was optional and complied with fuel economy and time scheduling requirements unlike tankers and hazmat transport mandatory routeing along the northern fairway. The Zoe did not have information available on restrictions for this passage. This safety risk was not recognised and formalised by IMO. Due to instrument restrictions, the crew did not have insight of the actual forces and accelerations, or indication of the actual rolling angle.

Based on understanding the system architecture, arrangements, institutions and organisations, disruptive **design interventions** beyond Old School and New School solutions were formulated. These interventions are generated by subject matter experts, such as maritime safety experts and naval architects:

- No longitudinal but transversal stacking, track and trace of lost cargo, limitations on operational GM levels
- Good Seamanship decision making, ICT supported situation awareness, crew training and guidelines
- State Oversight, IMO Code revision, design limit adjustment to sea and weather conditions, industry standards
- Innovate vessel design by hull and lashing system adaptation.

5 Case based conclusions

What do these two perspectives learn us? Despite numerous precautionary measures to guarantee a nominal performance -and due to aggravated weather conditions, an apparent rough journey- an almost unnoticed major loss of containers occurred. Only during the last of 6 occasions, the crew noticed the loss of containers. The first 5 losses were out of their sight and masked by darkness, bad weather, sea wave noise and vessel movements. In their view, the crew did everything right and did not incline to take irresponsible risks and

complied with all regulations. What did they then learn from what they thought went right? They were not in a position to notice the magnitude and progress of the disaster.

Based on the MSC Zoe cases, some of the triggers for change to adapt to modern times are identified as higher system order properties and principles. In this analysis we surpass the level of individual resistance to change and adopt new cognitive models of human operator performance. An unwillingness to accept new concepts of thinking -in particular resilience engineering- goes beyond cognitive stubbornness, a reluctance to change or preferring best practices over scientific theories. Apparently, New Economy constraints, algorithmic optimizations, and 'performance excellence' by operator variance have to be explored. Properties of legacy systems dominate the potential to adapt, to change principles and to anticipate disruptive anomalies in a system architectural development.

Two of these properties and principles are explored more in detail, clarifying vulnerabilities, sensitivities and emergent deficiencies in this New School of safety thinking for aviation and maritime systems.

First: Could the crew have learned from what went right? What were the indicators and observables:

- The captain and crew were fully qualified, experienced and proficient to their task
- Mandatory trip and operating conditions info was on-line available
- Loads and acceleration calculations complied with software modes of operation
- The shipping lane authorization complied with regulations
- The vessel was technically 'ship shape'

But beyond their window of observations, operating experience and risk perception, a disaster developed:

- 342 containers were lost in aggravated sea and weather conditions
- Millions of Euros of recovery costs and environmental damage occurred
- There was a huge loss of public confidence
- Identification of design knowledge deficiencies and flawed regulatory limitations only emerged in the aftermath of the disaster'

Second: Questions are raised whether or not:

- Resilience could have contributed more to this understanding
- there was an opportunity to prevent the loss of cargo or to save human lives
- could inherent or emergent properties and deficiencies be identified beforehand
- were there any early warning signals of operational feedback for the operators
- was there an understanding of higher system order stability and control
- could they discriminate between derivative and disruptive adaptations?

Were they in a position to change course to the Northern fairway, ride out the storm or take equivalent evasive actions and consequently avoid the loss of 342 containers? Was this event preventable, based on theoretical grounds according to Resilience Engineering principles? What does Resilience Engineering theory say about this?

Two deficiencies in Resilience Engineering theory are identified:

- Overarching socio-economic theories on New Economy principles in the Anglo-Saxon hemisphere, expel foresight from the safety analytical toolbox at a governance oversight and control level, reducing intervention and adaptation to an 'after the event' safety enhancement strategy at the corporate level
- Ignorance about the safety consequences of a simultaneous introduction of disruptive anomalies in both technology, organisation and business models, creating chaotic and unstable systems by focusing on the operational rather than the engineering design phase without discriminating between derivative and disruptive adaptations.

Transitions in socio-economical markets and technological innovations introduced vulnerabilities and higher order sensitivities in legacy systems that are not taken in account in the New School thinking. Such ignorance in New School thinking hampers understanding of how legacy systems developed into their present level of safety performance and disguises their actual change potential in both derivative, disruptive and prospective approaches.

6 Towards a Resilience Engineering 2.0?

The emergence of Resilience Engineering is part of a natural process of thougth development, responding and reflecting on proven deficiencies in existing and dominant theories. The theory of Vincenti about disruptive anomalies indicates that also for scientific theories, under new conditions, new theories may perform better than existing ones. As stated in the beginning of this paper, the emergence of Resilience Engineering elevates the debate from a dialectic stall on conflicting notions to the level of paradigmatic change. But like any other new theory, validation and falsification are essential elements in its development. A proof of concept is required to demonstrate the validity of the new paradigm. It is likely to indicate adaptations and improvements to earlier concepts.

1. *The value of a new approach*

Resilience Engineering contains powerful notions such as learning, responding, monitoring, and anticipating. Beyond these notions the paradigm upgrades the analytic potential to the level of functional analysis. It combines socio-psychological concepts with basic notions of systems engineering, derived from the technological domain. Finally, it explicitely introduces the dynamics of system performance as a principle asset of the concept. Like any other new concept, it also relies on assumptions and simplifications in order to describe reality. Such assumptions should be open to verification and falsification:

> Assumption 1: complexity superseeds complicated, learning from what went right. This assumption raises questions about whether a difference between complicated and complexity really exist? Or is it a construct to legitimise the new approach?
> Assumption 2: Can learning from what went right replace learning from what went wrong? This assumption raises questions about how we can learn, from which perspective and from what observations.

According to Woods (2019), answering these questions requires recognition of sharing values and perspectives with respect to:

- Bottom-up participation of expertise and experience
- Communication across stakeholders
- Commitment and shared responsibility of all parties involved
- Recognitions of system long term dynamics, a cyclic nature of innovation and continuous adaptation.

Based on these insight, Woods (2019) proposes to incorporate two additional notions in validating Resilience Engineering thinking to accommodate communication and information exchange:

- Initiative
- Reciprocity.

Answering such questions also should be based on theoretical notions to understand system architecture and dynamics. Such a reflection has also been the subject of research in the ESReDA Project Group Foresight in Safety (ESReDA 2020).

This research has committed itself to explore:

- The Full information paradigm: feedback and feedforward (Klir 1987)
- The counterpart of complexity: transparency rather than simplicity (Arslanian 2011)
- Full range of achieving understanding: hindsight, insight, oversight and foresight
- Democratic participation of all knowledgeable and qualified parties involved.

A basic finding in the ESReDA research has been how to deal with opiniators, influencers, social media and spin doctors. Is their participation knowledgeable, evidence based or merely speculation, interpretation or perception? Are they falling into the trap of confirmation bias? Should policy analysts and risk managers disqualify them and exclude them from participation in the communication process? Should managerial perspectives drive out understanding of technological complexity?

However, to achieve credible , plausible and consistent conclusions after analyzing system complexity and dynamics, the experience, expertise, perspectives and values of all knowledgeable participants are indispensable to gain oversight as a basis for foresight (ESReDA 2020).

2. *Or towards a synthesis of new concepts: a Smart Safety School of Thinking?*

In this paper, we have explored opportunites to learn from each other: representatives of two emerging new schools of safety thinking should not catch each other in a next dialectic stall, however on a paradigmatic basis. They could compare their mutual observations, interpretations and underlying scientific disciplinary paradigms. If we talk about socio-technical systems, there should not be a hierarchy of an either technological or socio-organisational nature, but the legacy and nature of the systems under scrutiny should be leading. Each school contains necessary but not sufficient conditions to introduce a new paradigm in safety thinking. There is an opportunity for sharing insights and an added value in a combined approach.

Combining the good of two worlds means incorporating two aspects of socio-technical systems, being a Reliability Engineering and a Resilience Engineering perspective by:

- Applying the Full Information Paradigm
- Incorporating operator participation and feedback
- Considering Normal and Non-normal operationg conditions
- Discriminating between derivative as well as disruptive adaptations
- Acknowledging legacy, nature and system architecture
- Integrating precaution, salvage, rescue, *and* resilience
- Providing proof of concept and added value of new approaches
- Not replaceing but reinforcing safety enhancement strategies
- Mobilizing new scientific domains in order to cope with knowledge deficiencies.

7 Overall conclusions

Legacy systems such as aviation and maritime nowadays operate under New Economy conditions in which process has driven out content and market has driven out knowledge. These operating conditions have reduced the knowledgeability on their behaviour and contributed to the opaqueness and unforeseeability. Their behaviour has become more emergent. Simultaneously, by introducing new technologies and a system of systems interconnectivity, they have evolved into complex and dynamic systems of a high energy density nature. Based on their legacy, they evolved into Non-Plus Ultra-Safe systems.

Failures in such systems have created catastrophic events of a nature and size that are technically, economically and socially unacceptable and that can propagate through systems rapidly, but unnoticed. Such catastrophies should be foreseen before they can manifest themselves as emergent properties. The systems should be able to resile and recover from such immanent manifestations and their stability and control options should be foreseeable and manageable. Safety thinking about such systems can benefit from the theory of Vincenti on disruptive anomalies, technological innovation and system adaptation.

From the analysis of the MSC Zoe case, it is concluded that a system wide understanding of safe states of legacy systems is hampered by a lack of cohesion between hindsight -by legacy-, insight -by safety investigations, oversight -by governance and knowledge based interpretation of unanticipated phenomena and foresight -by anticipating on future consequences of disruptive anomalies and adaptations.

This paper claims that, based on both system architecture design principles and foresight theory and practices, phenomena such as the MSC Zoe and similar cases already could have been foreseen by Old School thinking. A New School of thinking on learning exclusively from successes could not have made a difference in preventing the loss of 342 containers or unprecedented major damage to a coastal environment. In practice, early warnings of experts and operators on unsafe performance were excluded from the system control, stigmatising the messengers as whistle blowers.

Both perspectives are basically complimentary, not competitive or successive.

References

Arslanian P.L., 2011. Acknowledgement speech ISASI's Jerome Lederer Award 2011. ISASI Forum, October-December 2011 p12-13

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

Dutch Safety Board, 2020. Loss of containers overboard from MSC Zoe 1-2 January 2019. Panama maritime Authority, Dutch Safety Board and Bundesstelle fur Seeunfalluntersuchung. June 25th 2020

ESReDA, 2020. Enhancing Safety: The Challenge of Foresight. ESReDA Project Group *Foresight in Safety* EUR 30441, Joint Research Centre, European Safety, Reliability and Data Association

Klir G., 1987. The role of methodological paradigms in systems design. Dept. of Science. Thomas J. Watson School of Engineering. State University of New York ai Binghamton, New York

Minsky H., 1986. Stabilizing an Unstable Economy. McGraw-Hill Companies

Rayo M., 2021. A word from this issue's editor. REA Newsletter, June 2021.

Safety Science 2014. Special issue on the foundations of safety science. Vol 67, August 2014, pp 1-70

Snowden D., 2007. The origins of Cynefin. Cognitive Edge Pte Ltd. www.cognitive-edge.com

Stoop J., De Kroes J. and Hale R., 2017. Safety science, a founding father's retrospection Safety Science 94 (2017) 103 - 115

Vincenti W., 1990. What Engineers Know and How They Know IT. Analytical Studies from Aeronautical History. The John Hopkins University Press

Woods D., 2019. Essentials of resilience Engineering revisited. https://www.researchgate.net/publication/330116587

Zimmermann K., Paries J., Amalberti R. And Hummerdal D., 2011. Chapter 18: Is the aviation industry ready for resilience? Mapping Human Factors Assumptions across the Aviation Sector. In: Hollnagel et.al. 2011, Resilience Engineering in Practice

How Knowledge is Knowledge Enough for Managing Risks

Dien Yves, Collectif Heuristique d'Analyse Organisationnelle de la Sécurité – CHAOS, yves.dien@hotmail.fr

Paul Sever, Agentia de Investigare Feroviara Româna - AGIFER, sever.paul@agifer.ro

Abstract

"Operational feedback" approach specially aims to gain knowledge about flaws of sociotechnical systems in order enhance their safety thanks to analyses of events which occurred. Unfortunately, despite decades of operational feedback systems running, progress seems terribly slow. In numerous industrial accidents warning signs were not considered. Several reasons explain why an organisation is blind to warning signs. Overcoming current weaknesses in operational feedback is an organisational issue that will require a dramatic cultural shift.

1 Introduction: The Issue

One important pillar for safety management is "operational feedback" (O.F.). Its goal is to identify the causes of an event, learn from those and then define and implement corrective measures so that such event never occurs again. In other words, O.F. can be seen as a tool for gaining (new) knowledge about the process and its (mal)functioning. That is why, since decades, many companies, and especially the ones belonging to high-risk industries, set up O.F. systems as part of their risk management processes: event analyses must lead to safety enhancements. Huge and numerous efforts are made to run and improve O.F. systems. "Yet despite these substantial efforts, after several years of running O.F. systems, many managers and experts share the view that progress is terribly slow or has come to a halt. It is getting harder to establish convincing corrective action plans. In particular, the same human errors or series of similar technical breakdowns seem to recur" [1]. Thus, from one year to the next, the results in terms of safety are either a little better or a little less good: which led Claude Frantzen to state that we are "dancing tango on an asymptote" [2].

If increasing knowledge, thanks to results figured out through O.F. analyses, is parallel to increasing safety, why do we face these stagnant results while, at the same time, knowledge and knowledge management become central issues in domain of risks management?

The O.F. process comprises several stages. Amongst them, the two last stages are [3]:

- the memorizing of elements "surrounding" the event and its analysis (i.e., recording the method used for analysis, lessons learned, corrective measures defined, follow-up of their implementation).
- the communication and sharing of the lessons to be learned for stakeholders and potentially interested parties.

These stages should be those that favour increasing knowledge of system functioning, and therefore its safety once corrective measures are implemented. Nevertheless, it seems that we cope with a paradox, if not a contradiction. On the one hand, we can note that tools are nominally increasing knowledge (O.F. systems) with the goal of enhancing safety; on the other hand, the results obtained do not match the investments made since there is no convincing improvement.

In this article, we are going to discuss some cases of accidents that could have, perhaps, been avoided if the knowledge of how the process is working had evolved according to new "data" available. Then, from these weaknesses or failures of learning, we will analyse their causes and propose a few potential paths for improvement.

2 Failures of (in-time) Learning

We will not do, in this paragraph, an in-depth analysis of the accidents that we are taking as examples. We will content ourselves with exposing the direct and immediate causes of the event while being aware that its occurrence is multicausal. These events are well documented and those who require further information can refer to the detailed analyses (see References).

2.1 Core Meltdown in A Nuclear Power Plant

2.1.1 Event synopsis

On 28 March 1979, at unit 2 of Three Mile Island Pressurised Water Reactor (TMI PWR) nuclear power plant, near the city of Harrisburg in Pennsylvania (USA), while the plant was at full power, a shutdown of the water supply pumps for the steam generators resulted in a shutdown of the turbine driving the alternator "producing" electricity. As result, an increase in primary pressure (7 bar above nominal pressure) led to an opening of the pressurizer relief valve (which is designed to work this way in order to decrease primary pressure). Reactor scram occurred 8 second later. 13 seconds after their opening, the I&C system " commanded" closure of the valve. It remained blocked open (mechanically), while information given in the control room indicated the order and not the actual position of the component. Unit 2 found itself in a so-called LOCA (Loss of Coolant Accident) situation which was considered in the design of the plant. So, in order to compensate loss of water – through the open valve – the emergency water injection system – a safety backup system – started automatically. Due to wrong information (pressurizer level) and misleading information (display of the I&C order rather than equipment's actual position), operators in the control room did not clearly identify the situation and stopped the water emergency supply[1] [5], [6].

As consequence of the event, the reactor core partially melted, a small amount of radioactive gas was released in the atmosphere and TMI unit 2 definitively closed[2].

This accident was classified at level 5 (out of 7) on the International Nuclear Events Scale (INES).

2.1.2 Unpredictable Event?

The official investigation report stated that "*the major factor that turned* [a common operating] *incident into a serious accident was inappropriate operator action*" [5, p. 11]. Numerous analyses have drawn this conclusion, while forgetting the rest of the statement: "*therefore – whether or not operator error 'explains' this particular case -- given all the above deficiencies*[3]*, we are convinced that an accident like Three Mile Island was eventually inevitable*" [5, p. 11].

Was the accident that unpredictable?

[1] The concept of "*human /operator error*" stems from analysis of this event. Even if it is disputed today, it is still popular amongst industrialists (as an explanation of event occurrence) [4].
[2] First reactor criticality in March 1978, power plant commissioning on 30 December 1978.
[3] Deficiencies in training, lack of clarity in operating procedures, failure of organisations to learn the proper lessons from previous incidents, and deficiencies in the design of the control room.

- On 24 September 1977, at Davis Besse nuclear power plant, a twin sister of TMI[4], the same (initiating) event occurred: the relief valve failed to close after the reactor shut down, due to a malfunctioning of the feedwater system. Operators quickly noticed (i.e., in time) that the valve had stuck open and closed it. That "transient"[5] was deeply analysed by designers and Davis Besse engineers but no result was shared with the TMI power plant (nor to other plants) [5], [6].
- On 20 August 1974, a similar event as at TMI occurred at a Westinghouse design reactor in Beznau (Switzerland): a valve stuck open giving misleading information. For Westinghouse, this event proved the validity of one of its earlier studies that considered that operators would have enough time to react and to recover the situation. Furthermore, the Nuclear Regulatory Commission (NRC), the U.S. safety authority, was never informed because, at the time of the event, it was not mandatory for the designer / manufacturer to notify the safety authority about events that occurred at foreign reactors [6].
- In 1977, an engineer, consultant for an NRC Department, took the initiative to carry out a study for checking what would happen in a Babcock & Wilcox reactor if a small break occurred in the top of the pressurizer (TMI scenario). In January 1978, the study was reviewed within the NRC. Based on the concerns raised in the study and the Davis Besse event, the reviewer concluded that operators could be misled into turning off the water emergency injection system. The conclusion memo was not broadly circulated and eventually was simply filed away without arousing any other interest [6].

So, it would seem that some elements of knowledge were present before the TMI accident. If they had been treated at their fair value, perhaps the TMI event would not have had the same consequences.

2.2 Head-on Collision of Two Trains

2.2.1 Event synopsis

Information of this section comes from [7].

On 5 October 1999, a head-on collision of two trains occurred at Ladbroke Grove Junction, a few kilometres from Paddington station in west London. A turbo train of the company Thames Trains passed a signal at danger (SPAD[6]). Signallers in the Control Centre failed to respond as required: they did not call the turbo train driver to tell him to stop or, if they did, it was too late. The turbo train went on the same track as a high-speed train of the company First Great Western which was moving in the opposite direction.

We can be sure that the accident was not due to a physical failure of the turbo train driver (e.g., heart attack) because he had actions of driving the train (acceleration as well as emergency braking) after he passed the signal at red. The hypothesis of suicide can also be ruled out. Indeed, his colleagues described him as enthusiastic and dedicated; he was not depressed. Furthermore, on the day of the accident, he was celebrating the birthday of one of his two young sons.

The accident resulted in the death of 24 people in the turbo train out of the 148 passengers and seven of the 422 passengers in the high-speed train. The two train drivers died. Furthermore, 400 persons were injured, some seriously. The crash was made worse by a fire due to an oil leak from the turbo train. Fortunately, rescue teams were efficient.

[4] Both plants were designed by Babcock & Wilcox.
[5] "*as such events are called when they do not result in accidents*" [6, p. 33]!
[6] "**S**ignal **P**assed **A**t Danger" i.e., a signal passed when it is red.

2.2.2 Unforeseen Event?

The head-on collision of two trains is such a rare case that it is difficult to imagine. However, was this accident a thunderclap in a serene, all blue sky? Here are some considerations:

- The signal that was passed at danger and that led to the catastrophe in October 1999 had already been passed eight times between August 1993 and August 1998. It means that the likelihood of this specific signal being passed at danger once a year is 0.86 (86%). It also leads to a likelihood of a crash of 0.072 (7.2%). In other words, one crash every 14 years. The company in charge of the British rail network management acknowledged that this specific signal was a "black spot": it was one of the 22 signals for which the highest number of SPADs had taken place.
- More generally, from 1993 to 1999, 46 SPADs occurred in the zone supervised by the signallers' control centre. There was no O.F. regarding SPADs, no analysis, no debriefing about SPADs.
- The issue of SPADs was a concern for the rail sector. Several working groups had been set up: they worked in parallel with only a few information exchanges. They did not promote a global approach, only proposals of specific solutions.
- In February 1998, SN 109[7] was passed at danger. Six months later, another SPAD occurred with the SN 109. The Operations and Safety Director of the company First Great Western was concerned by this succession of errors. Between 26 August 1998 and 9 June 1999, she wrote three letters to different chairpersons of working groups dealing with SPADs in order to know what was supposed to be done (and when) for solving the problem. The letters had no effect: either she had no response or the recipients had a new position and had not followed up, or promises, of studies were made to her, but never kept.

2.3 Disintegration of a Space Shuttle

2.3.1 Event synopsis

After the loss of the Space Shuttle Challenger in January 1986, NASA[8] had a second "big one" on 1 February 2003. During its atmosphere **re-entry** phase, after a 16-day mission, the Space Shuttle Columbia disintegrated. The seven crew members were killed**.** It was the 113th launch for a space shuttle and the 28th mission for Columbia.

81.9 seconds after the Space Shuttle lift-off, a piece of insulating foam separated from the left bipod of its External Tank. It struck the edge of the left wing and made a breach in the Thermal Protection System of the shuttle. Neither Columbia crew nor NASA ground staff were aware of the damage at the moment it occurred[9]. During atmosphere re-entry, the breach was large enough to allow superheated air - temperature of around 2760° C - to enter "inside" left wing internal structures and to melt the aluminium spars (melting temperature: 660° C). The Shuttle broke apart over east Texas, south of Dallas, 10 minutes before its scheduled landing at Kennedy Space Centre, Florida. [8].

[7] "Code" of signal passed at danger before the accident.
[8] **N**ational **A**eronautics and **S**pace **A**dministration
[9] Day 2 of the mission, after analyses of launch photos and films, an informal group "self-set up" in order to assess the effects of debris impact on the integrity of the Orbiter. Unfortunately, with the data they had, the group members were unable to draw any conclusions. They thought that consequences "*may have a widespread ranging from acceptable to not-acceptable to horrible, and no way to reduce uncertainty*" [8, p. 151]. So, the group requested better images to get a better view on the impact area – a satellite of the Department of Defence could have taken photos of the shuttle. Eventually, the request was rejected by the Mission Management Team who believed that there was no flight safety-related problem due to debris strike.

2.3.2 Thinking and Acting Before the Event?

The shedding of foam was a problem that violated design requirements. Nevertheless, it was a known issue. Indeed, incidents of foam loss were frequent: "*Foam loss has occurred on more than 80 per cent of the 79 missions for which imagery is available, and foam was lost from the left bipod ramp on nearly 10 per cent of missions where the left bipod ramp was visible following External Tank separation*[10]*. For about 30 per cent of all missions, there is no way to determine if foam was lost*" [8, p. 53]. The CAIB[11] investigation committee identified 14 Shuttle flights that had significant thermal protection system damage or major insolating foam loss. The fifth important event was labelled as "safety of flight issue" by NASA. The sixth significant event was the first time that the following mission was launched without the debris in-flight anomaly closed. NASA defined the third known bipod ramp foam event (the eighth significant event) as an "accepted risk". The 10th important event was called "within experience base" and considered "in family". The 12th significant event involved damage to the Orbiter thermal protection system and tests to resolve foam-shedding, but the foam fix was ineffective. The in-flight anomaly was eventually closed as an "accepted risk". The 12th significant event (three months before loss of the Columbia) was the s sixth known left bipod ramp foam loss. For the first time, a major debris event was not categorised as an in-flight anomaly.

2.4 Atypical Events?

Thanks to the efficiency of O.F. systems put in place in every (at-risk) industry, we could have believed that situations in which early warning signs are poorly or not treated are very rare.

On the other hand, we could have referred to the McDonnell Douglas DC-10 crash into the Ermenonville Forest, outside Paris on 3 March 1974 resulting in the deaths of all 346 people on-board. This Turkish Airlines flight was scheduled to go from Istanbul to London Heathrow, with a stopover in Paris. The cargo door at the rear of the plane, incorrectly closed at Paris airport, burst open a few minutes after take-off. It led to an explosive decompression that collapsed the floor of the passenger cabin which severed critical cables necessary to control the aircraft [9], [10]. This disaster should not astonish: an explosive decompression had already occurred during tests for the design of the DC-10 in the 1970s; a similar event happened in June 1972 over Windsor, Canada for a commercial flight from Los Angeles to New York via Detroit and Buffalo. Fortunately, this "only" caused a partial collapse of the passenger cabin floor and thus did not cut all of the electrical cables allowing the pilots to make an emergency landing [10], [11]. A few days after this event the Director of Product Engineering of a subcontracting company for McDonnell Douglas wrote a memorandum in which he claimed serious concerns about safety and made some proposals for improvements [11]. He ended it by a premonition: "*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*" [12, p. 234]. The only reaction of top management was to ask who will pay for upgrade immobilization of the DC-10 fleet [11]. Furthermore, in a six-month period, from September 1976 to February 1974, with of fleet of a little fewer than 100 planes in the USA, the DC-10s suffered 167 door defaults, 254 electrical faults and 254 faults in door seals.

And what should we think of the shipwreck of the roll-on/roll-off ferry "Herald of Free Enterprise" which capsized on 6 March 1987 just after having moved away from the port of Zeebrugge (Belgium)? There were 459 people on board and 193 died. When the boat left the harbour, it had the bow door open, and the sea immediately flooded the decks. Within minutes, it was lying on its side in shallow water. It appears that the management of the company did not pay attention to warnings from the masters of the vessels regarding

[10] "*the total known left bipod ramp shedding events to 7 out of 72 missions for which imagery of the launch or External Tank separation is available*" [8, p. 55].
[11] **C**olumbia **A**ccident **I**nvestigation **B**oard.

suggestions for the fitting of warning lights on the bridge to indicate whether the doors were open or to other suggestions (e.g., carrying passengers in excess of the permitted numbers, problems over reading the draughts of the vessels, …) [13].

And what about the BP refinery accident at Texas City (USA) that left 15 dead and 180 injured on 23 March 2005? Due to a deviation from the procedure, a triggering event led to overfilling a raffinate splitter tank during the start-up of an isomerisation unit, which led to release of a flammable liquid causing explosions and fires when it met a hot spot [14], [15]. Between 2000 and 2005, out of 19 start-ups of the isomerisation unit, the "phenomenon" of procedural deviation was observed 18 times: however, no analysis was ever carried out. Furthermore, there were more than 80 hydrocarbon releases in the 2000-2001 period [14]. Regarding safety records, the Texas City managers confused occupational safety and process safety [16].

Many other examples could be given. That is why, we think that weakness of O.F. is a major issue regarding process safety. We labelled it "Pathogenic Organisational Factor" [4].

3 Requested Level of Knowledge for Acting in Time

The correctives measures defined and implemented after an accident have to be noted at the level of the company and / or at the level of the industrial sector[12]. Everything happens as if the early warning signs were not detected or seen as symptoms of safety degradation. It may be due to a management policy that lives in a approach "so far so good": it is what we can call the "syndrome of the one who falls from the top of a skyscraper"[13].

There are two visions for the occurrence of an event:

- It is seen as a surprise (an exceptional unfortunate chain of circumstances). In this case, managers (the organisation) consider(s) that everything reasonably achievable is done for ensuring a high level of safety: there can be a smugness towards current achievements. It leads to a **reactive O.F.** which mainly, not to say only, deals with past events. According to Michael Lewis [17], people are good for managing an event that just happened because they think that it could reoccur, and they prepared for it. On the other hand, they are not as good for imaging an event and for defining the mitigating measures before it occurs for the first time.
- Or managers (the organisation) consider that the situation must be seen as an "accident waiting to happen" situation. The questions become: what did we not do? what do we need to do more for ensuring a high level of safety? It is a **proactive O.F.** which also treats, in addition to past events, the early warning signs of level of safety degradation (malfunctioning, near misses, weak signals). We assume this approach helps us to gain better knowledge about maintaining and enhancing safety because it brings about an in-depth knowledge of actual process functioning.

The confusion between safety and reliability is detrimental to safety. For example, both investigation commissions after the loss of shuttles Challenger and Columbia have considered that success of past flights was taken as evidence of safety: "*reliance on past success* [can act] *as a substitute for sound engineering practices*" [8, p. 177]. This confusion can induce new organisational practices and become a break in gaining knowledge. If "reliability" and "safety" are indeed two fundamental functions of socio-technical systems at risk, they cannot be merged [18]. A side effect of this confusion is the normalisation of deviance, i.e., a process by which deviation from proper behaviour concerning safety becomes normalised in a corporate culture, and so, allows some defaults and malfunctions to continue functioning [19].

[12] It is the case for events we briefly presented. We will not discuss about efficiency of the measures.
[13] At floor 100 he/she can say ""so far so good"; same at floor 75; same at floor 70; … without acknowledges that risk is approaching, and that the disaster is close.

Bureaucratic behaviour does not ease evolution of knowledge because it blocks open fluid communication. It goes hand in hand with an attitude of compliance with rules and regulation: the goal is not to be as safe as possible but to be as close as possible to regulation. It will lead to a "tick-box mentality", which hinders initiatives.

Another phenomenon that does not help in gaining knowledge about safety is differences between managerial speeches ("safety first") and managerial decision-making, which, very often, results in resistance to what can adversely affect performance (production pressures [20]). This is especially true in "grey zone" situations, in which it is not obvious that safety is at stake and (too much) favouring it could significantly impact production.

Risk identification is based on "dated" (i.e., past) scientific knowledge. So, knowledge become cultural beliefs instead (with time). If we refer to the Barry Turner's model [21], this is the first stage (out of six) of the development of a disaster. Norms, codes of practices are associated to the beliefs. Stage 2 is an incubation period during which there is an accumulation of unnoticed events at odds with the (shared) belief about the way to manage safety. Due to these beliefs, it is difficult to detect and to label as meaningful the events not in line with them. So, detection of negative trends also fails and coping with new situations becomes harder.

Very often organisations act with a NIMBY[14] attitude / behaviour: events that occur in other identical or similar plants or in other industrial sectors are not considered, not analysed. Feeling is that there no lesson to be learned from "outside".

Managers show a lack of reflexivity: they feel difficulties for judging their own actions and decisions, especially when they caused a catastrophe.

Whistle-blowers, persons who commit themselves to raise concerns about safety degradation, are ignored [22]. There is no debate, no discussion with them[15]. On the contrary, they are often isolated or harassed by managers and / or colleagues.

The engineering background and culture lead to a favouring of quantitative rather than qualitative approaches and methods. As a result, event analyses lose their richness. It is one cause of the weakness of event analyses which are still, too often, put down to human error.

In this context, here is a long quote from the CAIB report [8, p. 97]: "*Many accident investigations do not go far enough. They identify the technical cause of the accident, and then connect it to a variant of "operator error"* […]. *But this is seldom the entire issue. When the determinations of the causal chain are limited to the technical flaw and individual failure, typically the actions taken to prevent a similar event in the future are also limited: fix the technical problem and replace or retrain the individual responsible.* ***Putting these corrections in place leads to another mistake – the belief that the problem is solved***"[16].

[14] **N**ot **I**n **M**y **B**ack **Y**ard.

[15] Examples: **(i)** Roger Boisjoly, mechanical engineer who warned about problems with space shuttle O-ring in 1995, a few months before its fatal mission and tried to delay the flight the day before its launch; **(ii)** George Galatis, nuclear engineer who warned about refuelling procedures at Millstone Nuclear Power Plant -1996-; **(iii)** All along the end of the 80s , Dr Irène Frachon, a pneumologist has alerted about misuse of a drug (to be prescribed for cases of non-insulin-dependent diabetes, but also mainly used as an "appetite suppressant"). She was harassed and prosecuted by the Lab manufacturing for which this drug was one of its most sold (between 1500 and 2100 people lost their lives because of this drug). [23].

[16] Emphasis added.

4 Conclusion: Path for Improvements

We have shown that there are a lot of obstacles that impair an increase in knowledge of how to improve safety.

Efficient risk management needs, among other things, an improvement, not to say a drastic, fundamental change of its paradigm(s), thank, especially to enhancement of knowledge from operational feedback.

Nevertheless, overcoming current weaknesses in operational feedback is an organisational issue.

Will it be easy to jump over the obstacles so that risk management and process safety improve?

The likelihood of succeeding in the development of new concepts, approaches, behaviours in order to really learn lessons after an event, to increase knowledge and improve risk management, will require a dramatic, but necessary cultural shift.

References

1. Dien, Y. & Llory, M. (2004), Effects of the Columbia Space Shuttle Accident on High-Risk Industries or: Can We Learn Lessons from Other Industries? *Hazards XVIII: Process Safety - Sharing Best Practice*, –23-25 November, Manchester pp. 36-50, Icheme Northwest Branch.
2. Frantzen, C. (2004), Tango on An Asymptote, *13th Annual Meeting of SRA Europe*, 15-17 November, Paris.
3. Dechy, N., Dien, Y., Marsden, E. & Rousseau, J-M. (2018), Learning Failures as the Ultimate Root Causes of Accidents, In: Jan U Hagen (Edit), *How could this happen? - Managing errors in organizations*, pp 105-128, Palgrave Macmillan.
4. 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
5. 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. & 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.
6. Rogovin, M. & Frampton, G. (1980), *Three Mile Island - A Report to the Commissioners and to the Public*, Nuclear Regulatory Commission Special Inquiry Group, GPO Sales Program, Division of Technical Information and Document Control, U.S. Nuclear Regulatory Commission.
7. Cullen, W. D. (2000), The Ladbroke Grove Rail Inquiry, Part 1 Report, HSE Books, Her Majesty's Stationery Office, Norwich.
8. CAIB (2003), Report Volume 1, National Aeronautics and Space Administration and the Government Printing Office
9. Journal Officiel de la République Française (1976), *Rapport final sur l'accident de l'avion D.C. 10 TC-JAV des Turkish Airlines survenu à ERMENONVILLE le 3 mars 1974,* Année 1976 n°27, Édition des Documents Administratifs
10. Eddy P., Potter E., & Page B. (1976), *Destination Disaster: From the Tri-Motor to the DC-10 - The Risk of Flying*, Times Books.
11. NTSB (1973), *AIRCRAFT ACCIDENT REPORT, AMERICAN AIRLINES, INC. MCDONNELL DOUGLAS DC-10-10, N103AA, NEAR WINDSOR, ONTARIO, CANADA, JUNE 12, 1972*, Report n° NTSB AA R. 73-2

12. Johnston, M. (1976), *The Last Nine Minutes: The Story of Flight 981*, William Morrow and Company Books.

13. Sheen, J. (1988), *The Merchant Shipping Act 1894, mv Herald of Free Enterprise*, Report of Court n° 8074 Formal Investigation, Department of Transport, 3rd edition, Her Majesty's Stationary Office.

14. U.S. *Chemical Safety and Hazard Investigation Board* (2007), Investigation Report, Refinery Explosion and Fire, BP – Texas City, Texas, March 23, 2005, Report N°2005-04-I-TX

15. Hopkins A. (2015,) *Failure to Learn - The BP Texas City Refinery Disaster*, CCH Australia Limited

16. Baker J., Bowman F., Erwin G., Gorton S., Hendershot D., Leveson N., Priest S., Rosenthal I., Tebo P., Wiegmann D. & Wilson L. (2007), *The Report of the BP U.S. Refineries Independent Safety Review Panel*, http://www.csb.gov/assets/1/19/Baker_panel_report1.pdf.

17. Lewis M. (2018), *The Fifth Risk: Undoing Democracy*, W. W. Norton & Company.

18. Llory, M. & Dien Y. (2006-2007), Fiabilité et sécurité des systèmes sociotechniques à risques, *Performance*, Part 1, n°30-septembre - octobre 2006, Part 2, n°31-novembre - décembre 2006, Part 3, n°32-janvier - février 2007.

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

20. Perrow, C. (1984), *Normal Accidents. - Living with High-Risk Technology*, Basic Books.

21. Turner, B. & Pidgeon, N. (1997), *Man-Made Disasters*, 2nd edition, Butterworth Heinemann, Oxford [1st edition: Turner, B. (1978), Wykeham Publications].

22. Dien, Y. (2014), Les signaux faibles à l'aune des lanceurs d'alerte, *Congrès IMDR λμ19, Décider dans monde incertain : enjeu majeur de la maîtrise des risques*, Dijon 21–23 octobre.

23. Dien, Y. Maia, P., Paul, S, Røed-Larsen, S., Stoop, J. & Marsden, E. (2021), The Whistle-Blowers: Active Actors in Foresight for Safety - Chapter 11, In: *Enhancing Safety: The Challenge of Foresight*, (Edit) ESReDA project group Foresight in Safety, https://www.esreda.org/wp-content/uploads/2021/01/ ESReDA-f oresight-safety-chapter11.pdf.

Safety I outdates learning and knowledge from failures and accidents: is it relevant?

Nicolas Dechy[1,2], Yves Dien[3], Michel Llory[3], Alexandre Largier[1], Jean-Marie Rousseau[1]

[1.] Institut de radioprotection et de sûreté nucléaire ;
[2.] LEMNA, IMT Atlantique ;
[3.] Collectif heuristique pour l'analyse organisationnelle de sécurité
Contact : nicolas.dechy@irsn.fr

Summary

Two new coin words and conceptual proposals appeared in safety management thinking a few years ago "Safety-I" and the related "Safety-II" especially with a white paper issued by Eurocontrol in 2013, co-authored by E. Hollnagel, J. Leonhardt, T. Licu and S. Shorrock and a book of E. Hollnagel in 2014.

It invites to change of definition of safety, with Safety-I defined as a condition with as low as possible of adverse events and Safety-II as a condition with the number of successful outcomes as high as possible. Safety-II invites to change the focus of the work to enhance safety, by trying to make sure that things go right, rather than by preventing them from going wrong.

In other words, safety management requires more than the prevention of incidents and accidents, and learning and knowledge management for safety management should rather understand the influence factors of success rather than those of failures.

Thus, to defend the transition towards safety-II, Safety-I is looked as 'old fashioned' with references to old paradigms that did not address complexity, to history of safety development linked to the sixties to eighties, and with several comparison effects associated with critiques. In this case, is learning from events outdated? Is learning from work-as-done easy?

Our work is in progress and with this communication we aimed to raise questions and to invite safety researchers and practitioners to undertake a critical review process of these new approaches, as promoted in science when new proposals are made, especially when they claim a paradigm change. This is not new in safety and risk management sciences, where different worldviews of what constitutes safety have competed (e.g. Wilpert and Fahlbruch, 1998) and continued to be enriched by new proposals such as Resilience engineering (Hollnagel et al, 2006).

More specifically, some issues and debates have already animated the safety community on very close topics with the High-reliability organizations researchers (e.g. Roberts, 1990) counter-proposals to the traditional study of accidents reports and failures and 'normal accident theory' (e.g. Perrow, 1984). The researchers in HRO proposed to study the daily operations to understand how people and organizations achieved reliable performance despite the high-risks. This kind of debates is still up-to-date with the Safety science journal that issued in 2019 a special issue that invited for comparing HRO and Resilience engineering proposals.

Similarly, our aim is to invite researchers and practitioners to consider the benefits, limits and critics addressed to the opposite research practice of studies of learning from several accidents undertaken by several scholars (Turner, 1978; Llory, 1996; Reason, 1997; Rasmussen, 1997; Hopkins, 2010; Hayes and Hopkins, 2015) and the theories of the 'gift of failure' (attributed to Wilpert, Carroll and Fahlbruch, 2011), the 'royal road' of accidents (Llory, 1996) and 'knowledge of accidents' (Dechy et al., 2010, 2016).

The discussion of the benefits, biases and limits of the two approaches for developing knowledge and practices for prevention of accidents and safety management should be organized at two levels, theoretical and empirical. One should notice that Hollnagel et al. (2013) carefully nuance their conclusions by recognizing that the two ways of thinking should be seen as complementary views rather than conflicting.

References

Carroll, J. S., Fahlbruch B. (2011), The gift of failure: New approaches to analyzing and learning from events and near-misses, Safety Science, 49 1–4.

Dechy, N., Dien, Y., Llory M. (2010), Pour une culture des accidents au service de la sécurité industrielle, Congrès lm17 de l'IMdR, La Rochelle, 5-7 Octobre

Dechy N., Rousseau J.-M., Dien Y., Llory M. Montmayeul R., (2016) Learning lessons from TMI to Fukushima and other industrial accidents : keys for assessing safety management practices, Proceedings of the IAEA International Conference on Human and Organizational Aspects of Assuring Nuclear Safety –Exploring 30 Years of Safety Culture, 22-26th February, Vienna, Austria

Hayes J., Hopkins A., (2015) Nightmare pipeline failures, fantasy planning, black swans and integrity management, CCH Wolters Kluwers.

Hollnagel, E., Woods, D. D. & Leveson, N. C. (Eds.) (2006). Resilience Engineering: Concepts and Precepts. Aldershot, UK: Ashgate

Hollnagel E., Leonhardt J., Licu T. and Shorrock S. (2013), From Safety-I to Safety-II: A White Paper, Edited by Eurocontrol

Hollnagel E. (2014), Safety-I and Safety-II, The Past and Future of Safety Management, Ashgate.

Hopkins, A. (2010). Failure to learn: the BP Texas City refinery disaster, CCH Australia Ltd. Wolters Kluvers.

Llory, M. (1996). Accidents industriels : le coût du silence, Opérateurs privés de parole et cadres introuvables, Éditions L'Harmattan.

Perrow, C. (1984). Normal accidents, living with high risk-technologies, Princeton Uni. Press.

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem, Safety Science, 27 (2-3), pp 183-213.

Reason, J. (1997). Managing the Risks of Organisational Accidents, Ashgate, Aldershot.

Roberts, K. H. (1990). Some Characteristics of High-Reliability Organizations. Organization Science, 1, 160-177

Turner, B. (1978), Man-Made Disasters, Wykeham Publications

Wilpert, B. & Fahlbruch, B. (1998). Safety Related Interventions in Inter-Organisational Fields, in: A. Hale & M. Baram (Eds), Safety Management – The Challenge of Change, Pergamon, Elsevier Science Ltd, pp 235-248.

The Accident Analysis Benchmarking Exercise (AABE)

Lee Allford, Halcyon Safety Associates, leeallford@btinternet.com

Maureen Wood, Major Accidents Hazard Bureau (MAHB) Maureen.WOOD@ec.europa.eu

Abstract

Accident investigators face several challenges with major accidents. These can include understanding the strengths and weaknesses of various accident analysis methodologies and selecting the optimal tool, given the objectives of the investigation, the nature of the accident, and the limits of the resource. The accident investigation community seemingly has many different methodologies at its disposal but often inadequate resources to test and explore the merits and drawbacks of each tool. In a similar vein, the challenge facing competent authorities and industry, especially smaller sites and more generally small to medium enterprises, is identifying and applying accident analysis and investigation methods that are suited to their resources, competences and objectives. For this reason, the Major Accident Hazards Bureau (MAHB) of the European Commission's Joint Research Centre (JRC) engaged a cross-section of competent authorities, researchers, institutes, OECD representatives and third parties to take part in an exercise to look at how different methods could be useful in different investigation contexts. The objective of the first phase of the Accident Analysis Benchmarking Exercise (AABE), was to compare the results produced by application of methods to analyse a defined set of accidents and evaluate the use of the methods against agreed criteria. The paper summarises in part the activities and results of the first phase of this project and the direction proposed by the group for the second phase.

1 Introduction

The Accident Analysis Benchmarking Exercise (AABE) was originally conceived by MAHB and further developed by participating experts in a launch workshop hosted by the MAHB on 5-6 November 2015. MAHB engaged a cross-section of competent authorities, researchers, institutes, OECD representatives and third parties to take part in the workshop with the aim to encourage participation in the exercise.

The main objective of the exercise was to compare the results produced by application of different accident analysis methods (selected by participants) to analyse a past accident (or possibly, more than one accident, evaluate the use of the methods against agreed criteria and more broadly to gather the experiences of the analysts.

2 The Approach

At the launch workshop the participants agreed to analyse selected past accidents using investigation reports, many of which are publicly available. The primary objective of the exercise was to compare the results produced by application of different accident analysis methods. It was not intended to recommend a best single method. The operational aspects of the exercises and further elements (selection of methods and criteria for selection, accident(s) studied, etc.) were determined by the participants.

It was decided to break down the analyses into three explicit phases and use appropriate methods for each phase as below.

Phase 1: Chronology e.g. Step/ECFA

Phase 2: Causal e.g. Bow Tie, Change Analysis

Phase 3: Underlying causation e.g. Accimap, MTO

Teams were tasked to work through an accident analysis starting with a chosen method from Phase 1, accident chronology, then progressing to Phase 2, accident causation and then finally to Phase 3, underlying causation.

3 Accident analysis methods and study teams

There are numerous accident analysis models for examining accident data and producing conclusions and recommendations. These models are simplified representations of accidents and each model emphasises different aspects of an event, its causes and contributing factors. Accident models are closely related to risk analysis methods as well as accident investigation methods, the difference being mainly timing (before or after an accident). During the exercise a total of eighteen accident analysis methods were used across the study teams.

Six teams managed to complete their chosen analyses and report the results to MAHB (out of the original eleven teams).

Table 1. Study teams and choice of historical accident and analysis methodology.

Study team	Accident	Methods
1	Shell Moerdijk (2014)	Storybuilder
3	Toxic cloud in Belgium	BARPI's Method – ARIA 3
4	BP Texas City (2005)	Organisational Analysis of Safety
6 Nuclear	Fukushima (Natech)	Fault Tree, Event Tree
6 Chemical 1	Cosmo Refinery (Natech)	STEP, Event and Causal Factors Charting, Barrier analysis on a Tier-based sorting
6 Chemical 2	JX Refinery (Natech)	STEP, Fault Tree, Event Tree, MTO
7	Buncefield (2005)	STEP, Tripod Beta, Accimap, CAST
8	Tianjin (2015)	Bow Tie, Accimap

4 Results of the Benchmarking Exercise

An important objective agreed at the launch workshop was the evaluation of the selected accident investigation methods based on evaluation criteria as described in Table 2. The study teams assessed the accident analysis methodologies against the criteria and these have been captured in Table 3 (not all teams reported their assessments in full)

Table 2. Description of evaluation criteria.

Criteria	**Description**	**Range of possible responses**
Self-supporting	Some methods intend to cover the whole event analysis process whereas others could be (are) used as input for other analysis methods	Yes/No
Graphical output	Some methods propose a diagram of the accident sequence (graphical representation of the scenario).	Yes/No
Accessibility	For some methods documentation is freely accessible while for others documentation incurs a charge.	Yes/To some extent (TSE)/No
Learning easiness	Can method be used with no "extensive formal accident analysis training" and/or with no "deep" knowledge about some scientific domains (e.g. sociology, engineering science…)	Yes/To some extent (TSE)/No
Scope of analysis	A method will address different levels of the sociotechnical system.	1. work and technological system 2. staff level 3. management level 4. company level 5. regulators and associations 6. government level
Duration	According to method used duration of an analysis could differ	Days/Weeks/Years
Replication	Even if an analysis method allows some flexibility, it needs to be sufficiently robust so that its results/outputs do not depend on the analyst(s) [different analyst(s) would reach (more or less) the same result applying the same method on a specific event]	Yes/To some extent (TSE) /No

Table 3. Methods used and evaluated by different teams.

Method	Team	Phase	Self-supporting	Graphical Output	Accessibility	Learning easiness	Scope of investigation	Duration	Replication
Storybuilder	1	1,2,3	No	Yes	Yes	Yes	1->4	Days	TSE
ARIA 3 (BARPI method)	3	1,2,3	No	Yes	TSE	Yes	1->4	Days	Yes
Organisational Analysis of Safety	4	1	Yes	No	Yes	TSE	NA	Weeks	TSE
		2	Yes	No	Yes	TSE	1->2/3	Weeks	TSE
		3	Yes	No	Yes	TSE	3->6	Weeks	TSE
ECFA	4	1	No	Yes	Yes	Yes	1	Days	
ETBA	4	2	Yes	No	Yes	Yes	1	Days	
MORT	4	3	No	Yes	Yes	TSE	1->4	Weeks	
ESReDA Cube	4			Yes	Yes	No	1->6	Weeks> Months	TSE/No
MTO	6	2,3	No	Yes			1->6		
ECFC	6	2,3	No	Yes			1->6		
Chronology Description	6	1	No	No	Yes		1->6	Weeks	TSE
Barrier Analysis	6	1,2,3					1->6		

Method	Team	Phase	Self-supporting	Graphical Output	Accessibility	Learning easiness	Scope of investigation	Duration	Replication
Root cause on tiered sorting basis	6	2,3					1->6		
Event Tree	6	3	Yes	Yes	TSE	No	1->2	Months	Yes
	6	2,3	No	Yes			1->6		
Fault Tree	6	3	Yes	Yes	TSE	No	1->2	Months	Yes
	6	2,3	No	Yes			1->6		
STEP	6	1,3	No	Yes			1->6		
	7	1	Yes	Yes	Yes	Yes	1->4	Days	Yes
Tripod Beta	7	2,3	No	Yes	No	No	1->4	Days	
CAST	7	3	Yes	Yes	TSE	TSE	2->4	Days	
Accimap	7	3	Yes	Yes	Yes	Yes	1->6	Weeks	Yes
	8	3	Yes	Yes	Yes	Yes	1->6	Weeks	Yes
Bow Tie	8	2	No	Yes	No	Yes	1->4	Days	Yes

5 Future Work

The results of the exercise were shared at a participant workshop organised by MAHB in December 2018. It was agreed to follow up this work with the development of an accident investigation handbook more broadly scoped towards the investigation process and geared primarily towards the needs of the Seveso inspector. The draft of the handbook is to be shared with participants for review over the summer of 2021 and published later in the year.

A full report on AABE has been published with the details below

Allford,L. and Wood, M., Accident Analysis Benchmarking Exercise, EUR 30564 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-28605-9, doi:10.2760/08034, JRC123513.

References

Rasmussen, J. (1997), Risk management in a dynamic society: a modelling problem, Safety Science, Vol. 27, N° 2/3, pp. 183-213.

Munson, S. (2000), Assessment of accident investigation methods for wildland firefighting incidents by case study method. Theses, Dissertations, Professional Papers. Paper 1616, The University of Montana, USA.

Sklet, S. (2002), Methods for accident investigation, ROSS (NTNU) 200208, NTNU, Trondheim, Norway.

Guide to safety analysis for accident prevention (Harms-Ringdahl, 2013)

Root cause analysis: Literature review. Contract research report 325/2001. (HSE, 2001)

The online eMARS reports are available at https://emars.jrc.ec.europa.eu and are maintained by the Major Accident Hazards Bureau (MAHB) of the European Commission Joint Research Centre.

One Sort of Challenge for Safety Management in Small or Medium Enterprises

Milos Ferjencik, Faculty of Chemical Technology, University of Pardubice, Pardubice, Czech Republic, milos.ferjencik@upce.cz

Abstract

Safety management consists of two parts: the long-term part and the fast-responding risk control. Two examples from small or medium enterprises (SMEs) - thermal explosion in Jacksonville and AN detonation in West - confirm that failures in the long-term part may be substantial. Cause analyses of both accidents show that their common feature was the contribution of regulatory bodies, which failed to provide both SMEs with a stimulus sufficient to make them aware of the presence of reactive hazards.

The author believes that both accidents can be considered not only as a failure of safety management, but also as a result of failure of knowledge management. He describes the process of adaptation of a SME to a hazard and emphasizes the importance of the transfer of knowledge across the boundary between the industry environment and local safety management of SME. He concludes that supporting the process of adaptation to hazards is one sort of challenge to both safety and knowledge managements in SME.

1. Introduction

Serious accidents can occur in small or medium enterprises (SMEs). The author examines in [1] the implementation of safety management (SM) v SMEs. He emphasizes that it does not start in a general description of local safety management system (SMS). SM in SMEs grows out of the vigilance against hazards. Harms-Ringdahl [2] states that SM is usually 'informal' in such companies, which may mean that the competence and working time available for safety management are very limited. Frequently, people hope together with Gowland [3] that SMEs are helped with this task by industry bodies.

Article [1] shows that complete and practical SM procedure consists of two parts. The long-term part is matter of permanent vigilance and openness. It requires to be permanently ready to indicate new symptoms of hazards in local process/system. The second part of the procedure is the fast-responding risk control/ risk management strategy. The long-term part is indispensable since it sets the fast-responding part into motion.

Article [1] states that two examples of real accidents in SMEs (West and Jacksonville) point out that the above-mentioned vigilance and openness is an essential part of SM.

In this article, the author wants to show that both accidents also represent a certain challenge for knowledge management. The knowledge needed to prevent such accidents exists within the industry, but has not been implemented as part of the SM in the above-mentioned SMEs. Both examples show the existence of a communication barrier that can hinder the implementation of successful risk management much more frequently than just two examples suggest.

An analysis of the causes of both accidents shows that difficulties arise in the transfer of knowledge from the industry environment across the local SM boundary. Following this, the process of knowledge transfer across this boundary and the adaptation of SMEs to new knowledge is described. The process is divided into five steps. It turns out that if the relevant knowledge is to cross the local SM boundary and be implemented in SME

practice, vigilance and openness on the part of the SME is not enough, but a certain helpfulness and persuasiveness on the part of industry bodies is also necessary. Knowledge management requires effort on both sides of the indicated boundary.

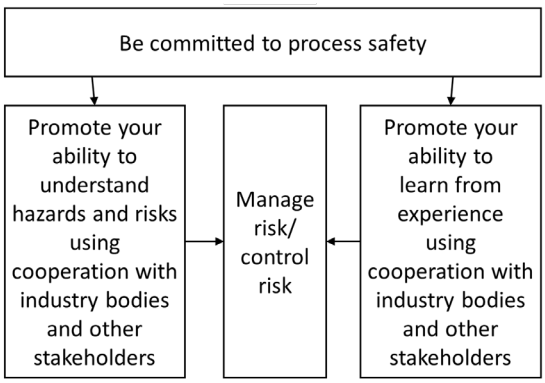
2. Safety Management in Small or Medium Enterprises

2.1 Elementary Safety Management

Harms-Ringdhal in [2] reduces the definition of SM to simply: Safety management is a way of managing the hazards (safety risks) of a company.

Safety management contains activities, which cannot be included in risk control/ management. At least commitment, learning, and part of understanding lies outside the term risk control. Aware of this description and the fact that risk originates in hazards, findings can be incorporated into Figure 1. According to this figure, Elementary Safety Management (ESM) includes three other groups of activities in addition to risk control/management. These three groups of activities precede and stimulate risk control. Since in any organization and especially in SME it cannot be expected that understanding and learning will be based only on internal experience, external sources of experience are mentioned. This refers to hope that 'SMEs are helped by industry bodies'.

Figure 1. Elementary Safety Management.



The ESM diagram in Figure 1 shows that risk management only starts after safety management has worked successfully. Simply put, risk management starts only after the SME manager takes note of his commitment to process safety, becomes interested in hazards in his SME (either on the basis of his own understanding or using tools such as [4] or on the basis of experience, perhaps in cooperation with external industry bodies or other stakeholders) and recognizes that hazards exist within the enterprise that deserve risk control.

2.2 Elementary Risk Control

When an enterprise turns out to contain hazards for the community, the SME manager asks: In what ways do I get those hazards under control to satisfy the local community and maintain the best economic efficiency of my enterprise? SME manager looks for the simplest strategy that will lead from the initial milestone - identification of hazards, to the target milestone - optimal control measures.

Two milestones mark the way from hazards to controls: scenarios and causal events. Elementary Risk Control within Elementary Safety Management can be condensed into three sentences representing a safety trivium:

1. Identify and control your hazards;
2. If impossible, identify your scenarios and control initiating events and/or consequences.
3. If impossible, optimize your controls based on your causal events.

The article [1] expresses the opinion that Elementary Safety Management with risk control described as Elementary Risk Control condenses the minimum contents of safety management which should be present in the mind of the SME manager. It provides the SME manager with assistance for communication and management of procedure from hazards through causal events to necessary and sufficient controls.

2.3 The role of industry bodies and other stakeholders

It has been mentioned several times that SMEs are expected to receive assistance from industrial bodies. The American Institute of Chemical Engineers (AIChE) is such a body that publishes guidelines providing instructions for risk management in the chemical and process industries. These books (e.g. [4] - [9]) are potentially useful outside the chemical/process industry, too. However, two problems can be identified.

First, there is a problem with using AIChE guidelines within SMEs since these guidelines place relatively high demands on the special training of those using them. Unfortunately, SMEs cannot be expected to use the full range of AIChE tools. To ensure that SME managers at least communicate within the framework in which these tools are used, risk management has been boiled up into a small number of basic rules.

Second, AIChE assistance in the ESM scheme focuses primarily on risk control. In addition, AIChE also offers assistance for learning from experience, understanding hazards and risks, and even for commitment to process safety (see publication [5]). In all cases, however, it focuses on theoretical concepts and descriptions of proper activity or behaviour. The AIChE guidelines cannot provide SMEs with motivation for SM, or even for vigilance and openness which is an essential part of SM. At the same time, the further we are in Figure 1 from the central box 'risk control', the more important is the role of motivation. Other stakeholders mentioned in Figure 1 (e.g. municipalities, civic activists, as well as regulatory bodies) should promote motivation, vigilance and openness.

3. Two Examples to Be Studied

3.1 The question solved in this paper

As it is shown above, the approaches to risk management can be boiled up into a small number of basic rules and set into the environment of SM. Then a question can be asked which elements of these approaches seem to be accepted in SMEs and which are visibly absent. This is the main objective of this section: Where can challenges for safety management in SMEs be identified?

Such a result can only be useful if it is based on the examination of real safety management failures. This paper is based on an analysis of two accidents in small or medium enterprises.

3.2 Two example accident stories

Two accidents were selected for the analysis: the explosion in T2 Laboratories, Jacksonville ([10], [11]) and the detonation in West Fertilizer Co. ([12], [13]). Introductory information on these accidents is provided in Table 1.

Table 1. Two examples of real accidents in SMEs.

What happened in Jacksonville on December 19, 2007? [10], [11]	A tremendous explosion shocked the northern Jacksonville, Florida region. Tons of sodium, hydrogen, and organics exploded into the surrounding environment via a reactor rupture and caught fire. The explosion occurred at a chemical producer called T2 Laboratories. Four people lost their lives. Thirty-two people within the vicinity suffered injuries. The power of the shock wave was felt 15 miles away. The plant manufactured methylcyclopentadienyl manganese tricarbonyl, a gasoline antiknock additive, for a third party distributor.
What happened in West on April 17, 2013? [12], [13]	A chemical storage and distribution facility owned by West Fertilizer Co. caught fire followed by the explosion of around 30 tons of ammonium nitrate while the emergency responders were trying to extinguish the fire, leading to 15 fatalities and numerous buildings, businesses and homes destroyed or damaged. This incident resulted in devastating consequences for the community around the facility, and shed light on a need to improve the safety management of local small businesses similar to the West facility.

There are three good reasons for choosing these two accidents for cause analysis according to [14]. First, these accidents occurred in SMEs. These were exactly such accidents that, when they occur, the question arises to what extent modern approaches to safety are being promoted in SMEs that work with hazardous materials.

Second, these are large and surprising accidents that have aroused great media response, have received a lot of attention, and high-quality descriptions and analyses are available for them.

Third but not the least, the examples we have selected represent the accidents that occurred in the type of hazard which identification is considered to be the most difficult. Typically, hazards in SMEs may have three forms:

1. A presence of volumes of substances with hazardous properties;
2. A presence of accumulated energy; or
3. A possibility of realization of an undesirable chemical reaction.

The identification of hazards of type 3 (reactive hazards) is the most difficult, because undesirable chemical reactions can be of very different origins. In both cases we have selected, the accidents occurred in hazards of type 3. The examples illustrate vividly what hazards in processes remain undetected and therefore lack proper control measures.

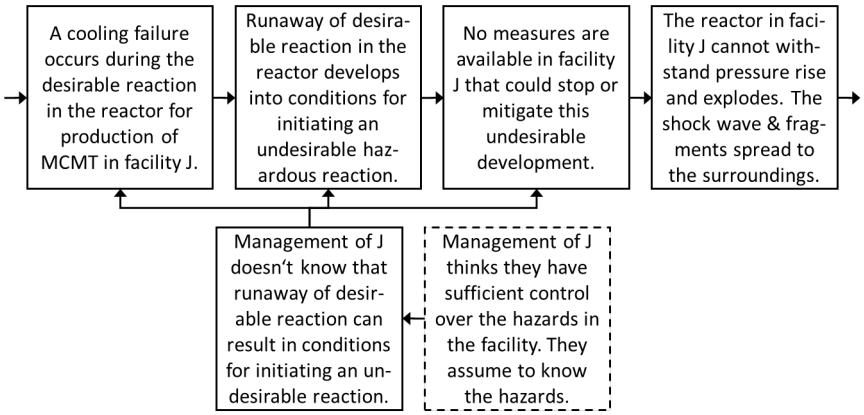
Names of enterprises where accidents occurred, will be often shortened to J and W. So, we will write about facilities J and W, accidents in J and W and managements of J and W.

3.3 Accident in Jacksonville

The explosion occurred in a batch reactor of about 9 m3 located in the open air in an industrial zone on the outskirts of Jacksonville. The explosion occurred in the first step of the production process (metalation). In the experience of management of J, metalation was "slightly" exothermic. Therefore, the obligation was introduced into the production procedure to maintain the temperature in the reactor at 177 °C by switching off the heating and supplying water to the duplicator. The reactor was intensively cooled by boiling water and discharging steam to the surroundings. The safety measures were in line with the idea that, if cooling failed, a rise in temperature would at most degrade the product.

Management of J did not know that when the reactor reaches about 199 °C, an unwanted decomposition reaction of sodium with diglyme starts, releasing several times more heat.

Figure 2. Diagram describing the most substantial part of development of accident in J.



Management of J did not know about this hazard because they did not subject the production process to any systematic reactive hazard testing. There could be several reasons for this: The manufacturing process was based only on patents, which do not necessarily inform about hazards. Management of J could assume that the information on exotherm collected during the start-up of production was sufficient for safe operation. They did not learn during their education that hazards as a possibility of undesirable dangerous reactions may be present. They might not even know that experts can detect these hazards routinely.

Therefore, it happened that the accident revealed a fact that could be detected in advance: if a temperature above 199 °C is reached in the first stage of the manufacturing process, then an undesirable highly exothermic chemical reaction will start, which will cause the reactor to explode. Figure 2 summarizes the evolution of the accident from the loss of temperature control in the reactor to the explosion.

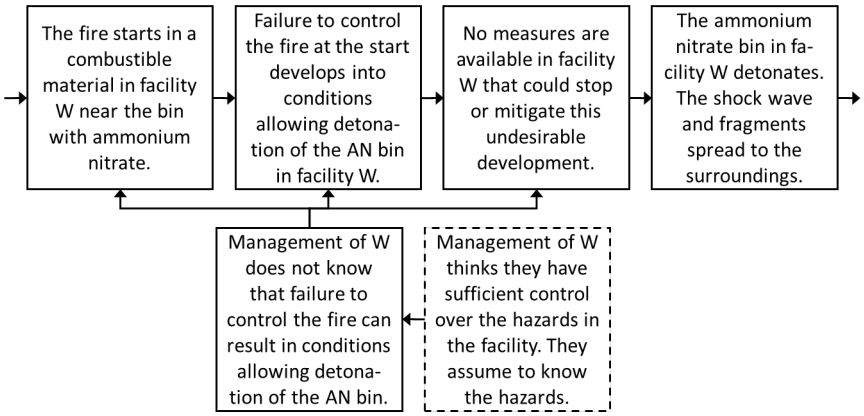
3.4 Accident in West

The detonation took place in an AN bin located in a wooden building of a bulk fertilizer store. The AN bin was made of plywood on a wooden structure, was about 9 m high and had a volume of about 130 m3. The bucket elevator from the storage pit was used to fill it. A considerable amount of combustible substances, such as hay seed, was stored on pallets near the AN bin. The fire probably started in the seed. It developed rapidly and soon engulfed the entire northern part of the bulk fertilizer store. Twenty minutes after the fire was reported, an explosion broke out, sweeping away firefighters and their vehicles.

Anhydrous ammonia tanks (total capacity 50 t) stood in the open air next to the store building. A few years earlier, management of W had been forced by regulatory body to accept that storing anhydrous ammonia was a hazard. Risk control in facility W was focused on ammonia. Anhydrous ammonia tanks did not fail neither in the event of fire nor in case of subsequent explosion.

However, no one drew attention to the dangers associated with AN. Even local firefighters were not aware of the danger of AN. They lacked training in the event of an AN accident.

Figure 3. Diagram describing the most substantial part of development of accident in W.



AN is considered a substance that is difficult to detonate. Factors such as strong shock, high temperatures, confinement, and contamination (by e.g. chlorides or powdered metals) can contribute to detonation. These factors combined in the store under fire condition. The possibility of detonation of AN is evidenced by numerous events that have taken place in the world, of which at least the regulatory bodies are informed.

Therefore, it happened that the accident revealed a fact that could be detected in advance: if the fire will surround the ammonium nitrate bin in the fertilizer store, then a violent exothermic reaction may develop which will lead to the detonation of the bin contents. Figure 3 summarizes the development of the accident from the loss of control of a store fire to the detonation.

4. Analysis of Causes

4.1 General timeline and causal events

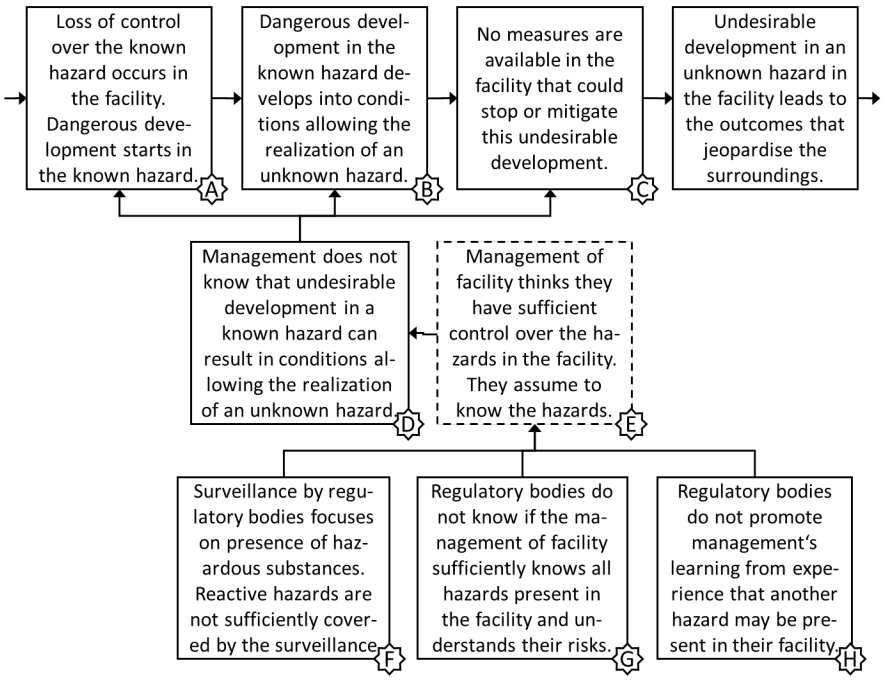
The development of both events is very similar in the most important features. In both accidents, a key role is played by the fact that management knew some hazards and focused on the risk control associated with them, but was not aware of the existence of another hazard, and therefore neglected the risk control associated with it. In addition, the realization of that unrecognized hazard followed the unmanaged realization of one of the known hazards. The problem in safety management did not arise because the risk control was not used, but because one hazard could not be identified. All indications testify that Elementary Risk Control was used in both SMEs, but there was a failure in the first step of the safety trivium.

In both cases, a reactive hazard has not been identified, i.e. a hazard that is often too difficult for SME staff to identify. It can be understood that management of J did not have to realize in itself that there was a risk of an unwanted reaction with the solvent, just as management of W did not have to realize that an unwanted detonation decomposition of AN could start in a fire. In both cases, however, the knowledge existed within the reach of the management of both companies that would help both hazards to be detected in time. It was only necessary for other stakeholders having this knowledge to speak and be heard.

Published analyses of both events pay attention mainly to one of all possible other stakeholders. They discuss how the various agencies, which we summarize here as regulatory bodies, could have helped to prevent both events. Their role is not described identically in both cases, but it can be summarized with some simplification into three sub-events written in the third line of the generalized diagram of accident in Figure 4.

Figure 4 describes the generalized timeline of both accidents and features a total of eight causal events. Causal events A to C represent facilities-level failures and will not be discussed in more detail here. Their common underlying cause is the lack of knowledge at the level of management of facilities J and W. The fact that management does not know about undesirable development is called causal event D. In addition, management was satisfied to remain ignorant, which we call causal event E. Existence of this complacency (= a feeling of contented self-satisfaction, especially when unaware of upcoming trouble) is not explicitly stated in the available analyses, therefore the dashed line delimits the causal event E. Such complacency may be present in long-term successfully operated SMEs and was almost certainly present in J and W. It prevented fruitful communication about hazards between management of facilities and other stakeholders, primarily regulatory bodies.

Figure 4. Generalised accident including the role of regulatory bodies.



Some stimulus was needed to break the barrier E. It should encourage either more professional testing in J or acceptance of accident experience in W. But just as the internal creation of this stimulus inside the management of facilities failed, so did the external stimulus creation in regulatory bodies representing all other stakeholders. The reasons are summarized by causal events F to H.

4.2 General underlying causes

The following table identifies the safety management components according to guideline [5] that have visibly failed at the management of facilities and external surveillance levels.

Table 2. Underlying causes of generalised causal events.

Process	**Components of safety management according to [5]**
Management of facilities (causal events D and E)	Commitment to process safety: - Process safety culture - Develop and implement a sound culture - (Maintain a sense of vulnerability & Establish a questioning/learning environment) - Stakeholder outreach - Identify communication and outreach needs - Identify relevant stakeholders Understanding hazards and risk: - Process knowledge management - Maintain a dependable practice - Thoroughly document chemical reactivity and incompatibility hazards - Hazard identification and risk analysis - Identify hazards and evaluate risks - Gather and use appropriate data to identify hazards and evaluate risks Learning from experience: - Incident investigation - Use appropriate techniques to investigate incidents - Investigate causes to an appropriate depth - Management review and continuous improvement - Monitor organizational performance - Strive to continuously improve
Surveillance by regulatory bodies (causal events F to H)	Commitment to process safety: - Process safety culture - Develop and implement a sound culture - (Maintain a sense of vulnerability & Establish a questioning/learning environment) - Process safety competency - (Execute activities that help maintain and enhance process safety competency - Solicit knowledge from external sources) & Evaluate and share results - Evaluate the utility of existing efforts) - Stakeholder outreach - (Identify communication and outreach needs - Identify relevant stakeholders) & (Conduct communication/outreach activities - Identify appropriate communication pathways) Understanding hazards and risk: - Process knowledge management - (Maintain a dependable practice - Thoroughly document chemical reactivity and incompatibility hazards) & (Use process knowledge - Ensure awareness) - Hazard identification and risk analysis - (Identify hazards and evaluate risks - Gather and use appropriate data to identify hazards and evaluate risks) & (Follow through an assessment results - Communicate results externally) Management of risk: - Operating procedures - Identify what operating procedures are needed - Determine what procedures are needed and their appropriate level of detail - Conduct of operation - Develop required skills/behaviour - Promote a questioning/learning attitude Learning from experience: - Incident investigation - Follow through on results of investigations - Communicate findings externally - Management review and continuous improvement - (Maintain a dependable practice - Validate program effectiveness) & (Monitor organizational performance - Strive to continuously improve)

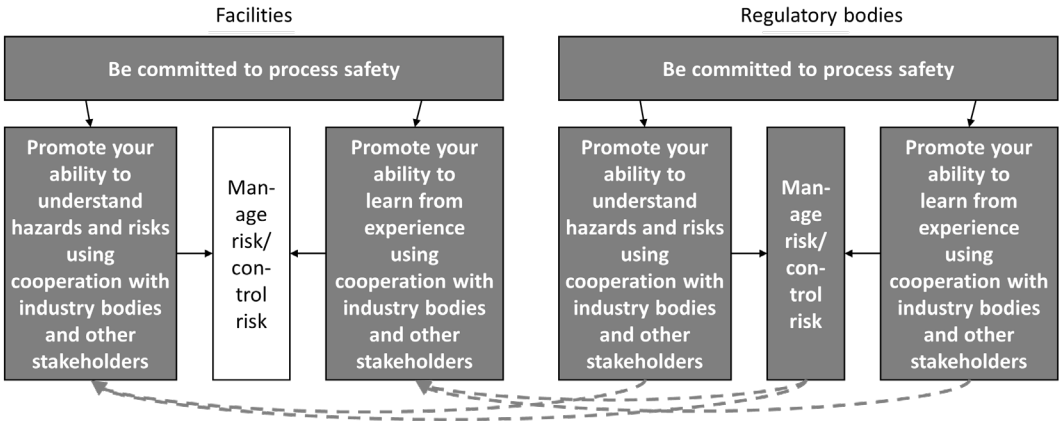
5. A Challenge for Safety and Knowledge Managements

The examples showed SMEs where management had no idea that they were working with a significant hazard. They were not helped by industry bodies. Both accidents occurred because companies lacked knowledge of hazards. Even though knowledge was available within the industry that would lead both to the detection of hazards and the prevention of accidents. The problem was not risk management/ risk control, but blindness to hazards, which in the first simplification can be attributed to a lack of vigilance and openness. The cause analysis confirmed that the deficiencies were present mainly in the long-term part of the SM. Areas of deficiencies are shown in the left part of Figure 5.

At the same time, the analysis also showed that similar deficiencies can be identified in the SM of the relevant regulatory bodies. Their range is even greater. They were joined by deficiencies in risk management (Determine what procedures are needed and their appropriate level of detail; Promote a questioning / learning attitude in conduct of operation) and in information transfer (Communicate HIRA results externally; Communicate incident investigation findings externally). These deficiencies undoubtedly affected the deficiencies in the safety management of SMEs. Everything is illustrated in Figure 5

SMEs have failed to identify hazards, but at the same time it can be stated that the identification of the hazards was not purely their business. External actors (regulatory bodies) were supposed to help them with that. It can be assumed that regulatory bodies are generally better informed about the existence of reactive hazards than SMEs and should draw attention to them. Blindness towards new reactive hazards would be lower in both SMEs if external stakeholders showed higher helpfulness and persuasiveness.

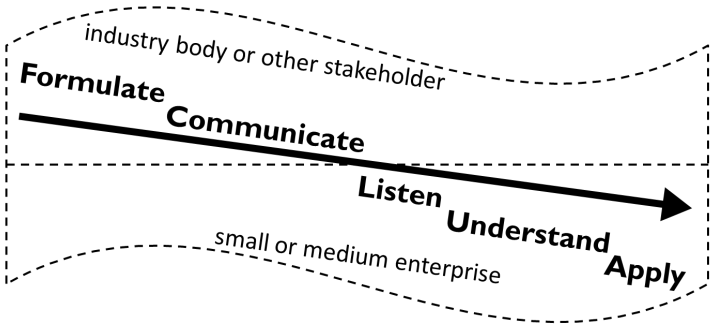
Figure 5. Deficiencies of safety management in SMEs and their regulatory bodies.



Both accidents can be considered not only as a problem of safety management, but also as a failure of knowledge management. Knowledge about new hazards comes to most SMEs from external actors, most often from regulatory bodies. This means that there is some knowledge of hazards among external actors for some time, which has not yet been adapted in SMEs that work with these hazards. This can be understood: SMEs are usually fully occupied with their commercial activities and have only limited competence and working time available for safety management. Vigilance and openness can be required of SMEs, but SMEs cannot be expected to actively seek information on new reactive hazards. On the other hand, it would be appropriate for regulatory bodies to effectively stimulate SMEs in these areas.

The core of SME adaptation to a new hazard is knowledge transfer. It is useful to describe a more detailed idea of how the whole process of adaptation to a new hazard takes place if it is initiated by an industry body or external stakeholder. The author illustrates the description of this process in Figure 6.

Figure 6. Adapt SME to a hazard using cooperation with industry bodies and other stakeholders.



The process of the adaptation of SMEs to a new knowledge is divided into five steps: (1) formulate, (2) communicate, (3) listen, (4) understand, (5) apply. Steps have different actors. The first two steps take place outside the SME: the external actor formulates the name of the new hazard and communicates this information. Difficulties arise in the transfer of knowledge from the broader industry environment across the local SM boundary i.e. between steps (2) and (3).

SME is an actor of steps (3) to (5). The step (3) means be vigilant or be ready to register information about a new hazard from one of the stakeholders with whom you maintain contact. This is the "vigilance against hazards".

6. Conclusions

Much effort has already been made to improve risk control and safety management in SMEs. However, it cannot be relied upon that these modern approaches will be automatically applied in SMEs to hazards that are not generally known, especially reactive hazards. SMEs have too limited capacity for this. They cannot do without outside help, which should also be supported by knowledge management. Careful consideration should be given to how to support the implementation of the five adaptation steps of Figure 6.

The task of formulating and communicating a new knowledge about hazard so that it overcomes the reluctance to listen and complacency and is listened to as effectively as possible is a real challenge for both safety management and knowledge management. This challenge is difficult probably due, at least in part, to the fact that it acts on the boundary between SME and external industry environment. The ability to promote understanding and learning beyond this boundary is very essential. External actors need to be active and trustworthy.

SMEs are expected to be motivated, open, and vigilant. External actors are expected to be helpful and persuasive.

References

1. Ferjencik, M. (2020) *Practical safety management for small or medium enterprises.* Journal of Loss Prevention in the Process Industries 68, 104281
2. Harms-Ringdahl, L. (2004) Relationships between accident investigations, risk analysis, and safety management. *Journal of Hazardous Materials* 111, 13–19.
3. Gowland, R. (1999) Is the Seveso II directive an improvement on its predecessor? A chemical industry safety professional's personal view. *Journal of Hazardous Materials* 65, 15–22.

4. AIChE Center for Chemical Process Safety (2008) *Guidelines for Hazard Evaluation Procedures, Third Edition*. John Wiley & Sons.
5. AIChE Center for Chemical Process Safety (2007) *Guidelines for Risk Based Process Safety*. American Institute of Chemical Engineers, New York.
6. AIChE Center for Chemical Process Safety (2009) *Inherently Safer Chemical Processes, A Life Cycle Approach, Second Edition.* John Wiley & Sons.
7. AIChE Center for Chemical Process Safety (2003) *Guidelines for Investigating Chemical Process Incidents, second ed.* American Institute of Chemical Engineers, New York.
8. AIChE Center for Chemical Process Safety (2001) *Layer of Protection Analysis, Simplified Process Risk Assessment.* American Institute of Chemical Engineers.
9. AIChE Center for Chemical Process Safety (2000) *Guidelines for Chemical Process Quantitative Risk Analysis, Second Edition.* American Institute of Chemical Engineers, New York.
10. U.S. Chemical Safety and Hazard Investigation Board (2009) *Investigation Report T2 Laboratories, Inc. Runaway Reaction.* Investigation Report No. 2008–3-I-FL Sep 2009, Available at: http://www.csb.gov.
11. Willey R.J., Fogler, H.S., and Cutlip, M.B. (2011) The Integration of Process Safety into a Chemical Reaction Engineering Course: Kinetic Modeling of the T2 Incident. *Process Safety Progress* 30(1), p. 39 – 44.
12. U.S. Chemical Safety and Hazard Investigation Board (2016) *West Fertilizer Company Fire and Explosion, Final Investigation Report,* REPORT 2013-02-I-TX, January 2016, 267 pp., available from http://www.csb.gov
13. Laboureur, D.M. et al. (2016) Case study and lessons learned from the ammonium nitrate explosion at the West Fertilizer facility. *Journal of Hazardous Materials* 308, 164–172
14. Ferjencik, M. (2014) IPICA_Lite - Improvements to root cause analysis. *Reliability Engineering and System Safety* 131, 1-13.

On risk management for some complex and highly innovative artefact systems

Dan Serbanescu, Division of Logic and Models in Science Romanian Academy, dan.serbanescu1953@yahoo.com

Abstract

The paper presents results from insights on the risk management for energy systems, as complex and highly innovative artefact systems. The cases considered are related to the nuclear energy systems, as defined for their components (research, design, the whole lifecycle) are at the cross roads of various other technologies.

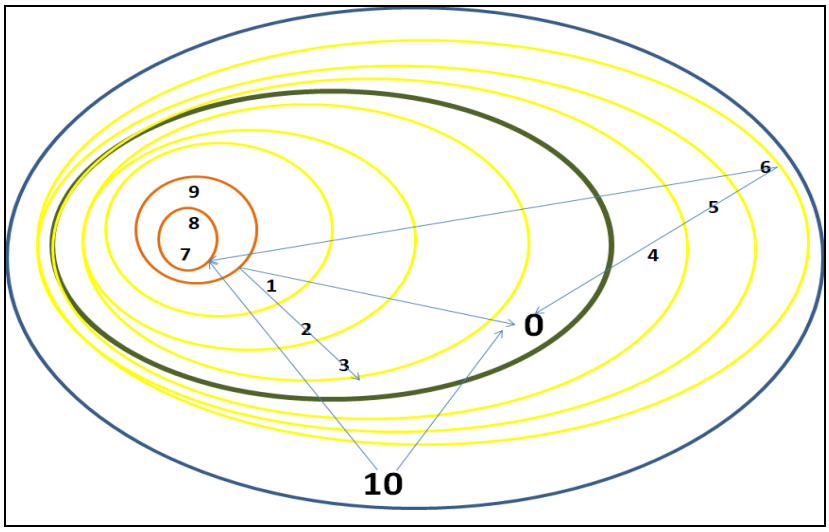
1 Introduction

The paper presents some insights from an on-going project related to the evaluation of interfaces between various technologies. The cases considered so far are related to the energy systems, as they are highly complex and innovative artefacts, interacting / being challenged by other man-made and natural similar systems. The interfaces were considered from diverse facets, by using as a guiding criterion the risk impact of New Technologies, other than nuclear (NT) and Nuclear Energy technologies (NE), in the context of hazardous environments. The evaluation considered the NE as defined for their components and for the lifecycle periods (research, design, operation and end of life. The energy systems considered are illustrated in Table 1 and Figure 1 and described in detail in [1-6] as being Complex Apoietic Topological Systems (CATS), i.e. self-regulating fractal type complex systems, described by topological structures.

Table 1. Energy Systems at various levels.

Type of NE systems	Abbreviation	Notation as per Figure 1
Sub quantic	SQ	7
Quantic	Q	8
Molecular	M	9
Molecular life	ML	1
Planetary	P	2
Planetary life	PL	3
Planetary life intelligent	PLI	0
Galaxy	G	4
Cosmic	C	5
Cosmic life	CL	6
Cosmic Intelligent	CLI	10

Figure 1. CATS from Table 1 representation in a "matrioshka" style.



The systems of CATS type chosen as cases for the evaluation of interface between NE and NT are described by a set of minimal parameters (syzygys) – mass, energy and information (formulas (1) and (2)). CATS are composed of a set of subsystems (k):

$$E^{(k)} \equiv \sum_{l=0}^{8} E_l^{(k)} i_l^{(k)} \quad (1)$$

$$m^{(k)} \equiv \sum_{l=0}^{8} m_l^{(k)} i_l^{(k)} \quad (2)$$

$$\psi^{2(k)} \equiv \sum_{l=0}^{8} \psi^{2}{}_l^{(k)} i_l^{(k)} \quad (3)$$

$$E_{ini}^{(k)}(t) = \sum_{l=0}^{8}((m_l^{(k)}(t) * c^2) * \psi^{((k)^2)} * i_l^{(k)}) \quad (4)$$

where

m - mass

C - speed of light

ψ^2 – entropy; $\psi^2$is expressed in general as information entropy, but being actually a matrix of elements describing the entropies at various levels and for various types of energy systems.

The full expression of the multilevel energy system of CATS type, for any system in Table 1 and Figure 1 is considered as in (5) (details in ...[ ]):

$$\boldsymbol{E^{(k)}} \equiv \underbrace{\boldsymbol{E_0^{(k)} i_0^{(k)} + E_1^{(k)} i_1^{(k)}}}_{01} + \underbrace{\boldsymbol{E_2^{(k)} i_2^{(k)} + E_3^{(k)} i_3^{(k)}}}_{23} + \underbrace{\boldsymbol{E_4^{(k)} i_4^{(k)} + E_5^{(k)} i_5^{(k)} + E_6^{(k)} i_6^{(k)} + E_7^{(k)} i_7^{(k)} + E_8^{(k)} i_8^{(k)}}}_{4\text{-}8}$$

Real energy Complex energy Hypercomplex energy (5)

The transitions from one state to another for a given system and from one system to another take place in accordance with a transformation matrix governed by self-regulating mechanisms described by a general form of cybernetics (Hypercybernetics) (as detailed in [1-6]).

2 Evaluation and results

NE systems described by the CATS type can be also defined as technologies. By *"Technology"* it is understood the *whole set of knowledge from the theoretical sciences (physics, chemistry, mathematics etc.) and their applicative branches to the engineering technological solutions for various energy system*.
On the other side NE are a set of enveloping technologies of two main groups:
— specific dominant technologies (nuclear science and energy related) and
— various other technologies, non-nuclear related (NT).
Examples of the NT considered are:
— Artificial Intelligence (AI), virtual reality, digital computing (High Performance Computing and Quantum Computing) and robotics
— Nanotechnology and various material manufacturing technologies
— Biotechnologies and ecological modelling
— Solutions for the Man-Machine Interface
— Management of specificity of human societies, including those related to the future human generations etc.
The NT plays various roles in relation with NE, from the supporting to challenging ones. The evaluation of the impact of NT on NE from the risk impact point of view is considered ([7-11]) based on a *three facets approach:*
— *FACET I*:Interface between two technologies and the possible use of NT for the existing NE technologies, from hardware and software perspectives, during their lifecycle, in the context of the society/civilization future changes
— *FACET II*:Impact of NT on the fundamentals of nuclear physics and its applications in NE from the perspective of the emergence and then interface of new sciences and technologies
— *FACET III*:Changes in paradigms of knowledge in general, from the energy production and use point of view and from the epistemological perspectives

Technologies are described by objective functions, which are defined by s-curve (technological curve) (6).

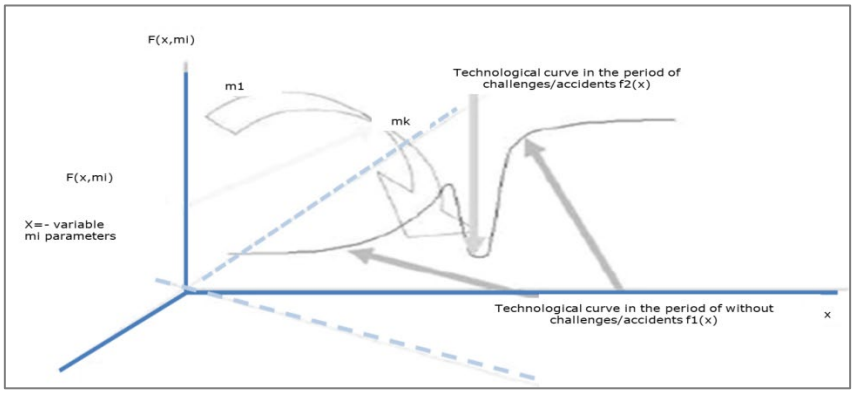
$$S(x) = f_1(x) = \frac{1}{1+\frac{1}{e^{a(x-b)}}} \tag{6}$$

However, in case that an accident takes place or a major technology failure, then the objective fucntion will be under a variation as per formula (7).

$$f_2(x) = e^{-x} \tag{7}$$

Therefore, technologies might be considered as a series of evolutions as per (6) and (7).

Figure 2. S-curve – technological function [1-6].



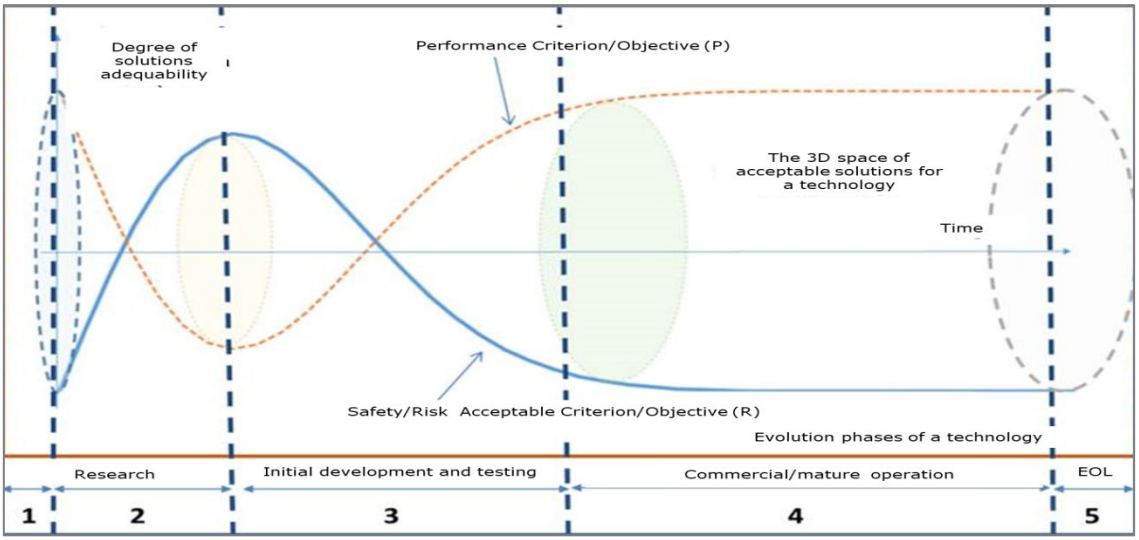
For a given technology the performance function (P, as per the s curve in formula (6)) and the safety margin/risk function (R as per formula (8)) are defined (Figure 3).

$$R = 1 - 2 * x * e^{-x^2} \quad (8)$$

Those functions (P and R) defined above are related to all the lifecycle phases. It is important to mention specific aspects of the startup and end of a technology:

1. The initiation of a technology (phase 1), as a random appearance to solve a well defined need of the society combined with the maturity of the scientific background
2. The end of a technology (Phase 5) is indicated by the impossibility to improve it / make it more complicated without getting into a zone of chaotic behaviour, as they reach the critical level of complexity.

Figure 3. Evolution of the Performance and Risk functions for a technology during its lifetime.

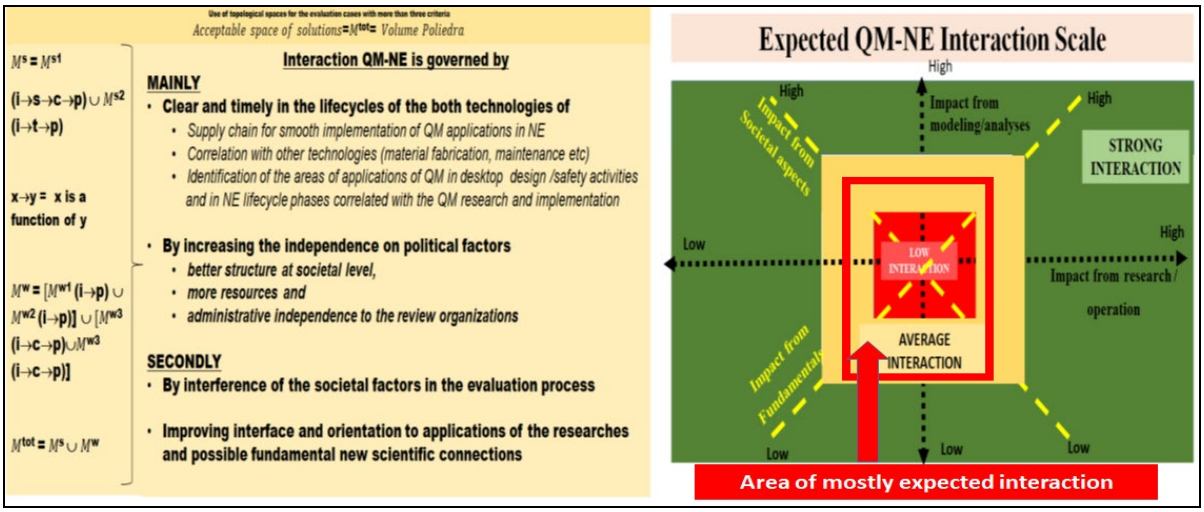


The acceptable solutions for the use of a technology are a space defined by the P and R curves (Figure 3), considering the lifetime evolution of a technology and possible failures of it.

The interference between NE and diverse NT leads to enveloping spaces of possible acceptable solutions and diverse timelines of the validity of NE technology using other technologies. On special interest is the fact that the nuclear science and nuclear energy technologies defining NE systems are human artefacts with long lifecycles, compared to human generations. Therefore, the generation change impact on technologies designed today to operate for 60 to 80 (may be even more) years from now have to seriously consider the generations specifics impact on them.

The evaluation of the interface between NT and NE is performed by using a set of criteria for a triple facets approach [7-11]. Figure 4 illustrates results of the areas identified using such approach for the evaluation of the interface between Quantum Mechanics (QM) technologies (as for instance quantum computing) and NE. It is important to note that the solutions space for long term evaluation is larger if the potential positive impact of supporting technologies of NT is considered.

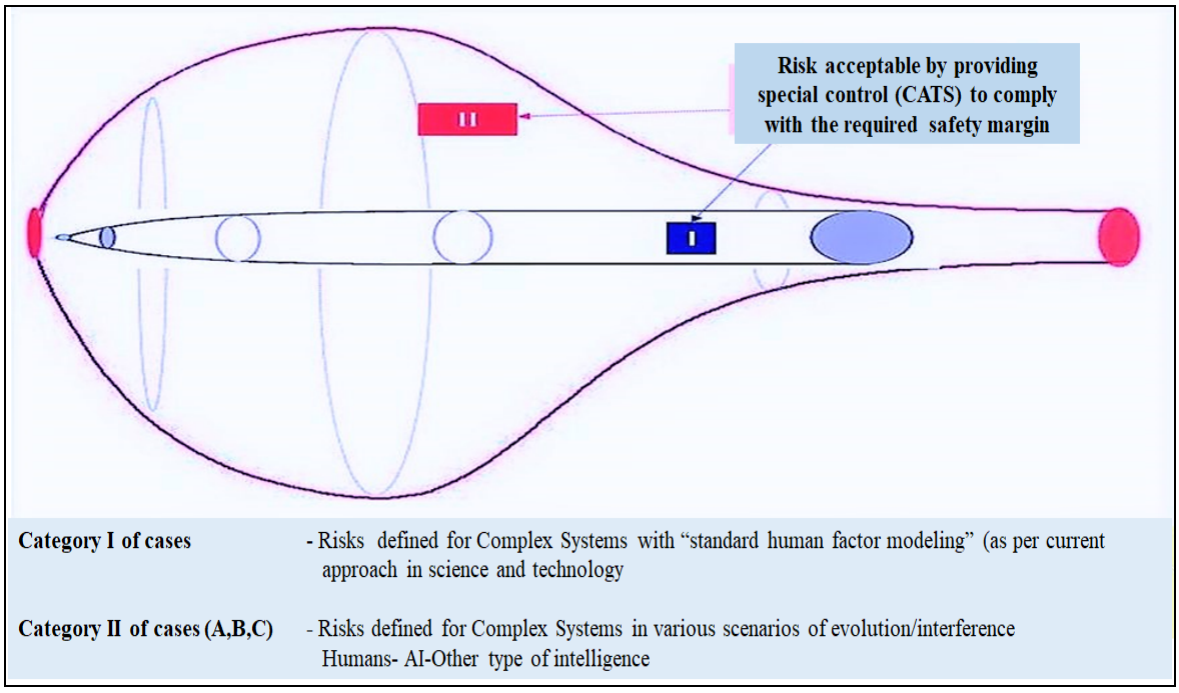
Figure 4. Evolution of the Performance and Risk functions for a technology during its lifetime



It is also important to note the fact that the type of society and human resources are of very high impact on the solutions, as being some of the main governing parameters of a technology. The MCDA (Multi Criteria Decision Analysis) evaluations for the criteria dominant of the triple facets, performed from the perspective of human factors (society, management, type of generations etc.) lead to an envelope of possible solutions having different risk impact for NE. The risk impact categories are (Figure 5):

- CATEGORY I – Risk defined by a standard society and human model (no major changes by comparison with the present situation) and a technology trend for NE and NT as it is now.
- CATEGORY II- Risk defined by different scenarios of human factors evolution (as per Figure 5) and interaction between NE and NT

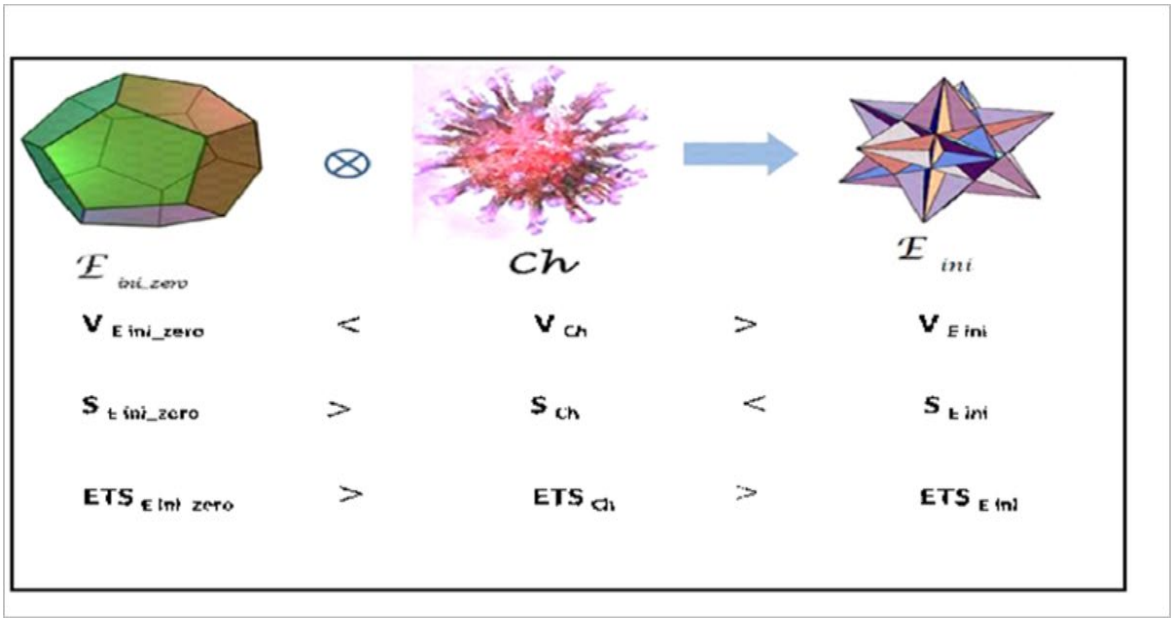
Figure 5. Evolution of the Performance and Risk functions for a technology during its lifetime



The decision tables of MCDA applied for a set of variations of the parameters with impact on the risk classification for a solution lead to the definition of algebric spaces, which can be represented geometrically, too.

The solutions spaces define therefore different polihedral forms (Figure 6). The characteristics of those forms for NE (coded *Eini_zero* in Figure 6) and of the challenging technologies (coded Ch in Figure 6) interfere and lead to a set of final spaces of solutions (coded *E ini*) The characteristiscs of those geometrical forms are the volume (V), the surface (S) and ETS (enantiothopy of a state) as a probability to change the NE/NT states [1-6].

Figure 6. Building the solutions space of optimal risk for technologies interface



The resultant phase for NE technology may be stable or not. In care it is unstable – of very high transition pghase characteristics, the only manner to assure a stable set is to simplify NE and reduce to minimum the impact of other NT.

The main aspects of the expected impact of various technologies NT on NE can be summarized as follows:

- For NE technologies the dominant cathalist of the development by the end of the '50s was the political decision of using nuclear energy in peacefull purposes and the implementation was done by transferring results and achievements in the military area to the civil applications.However, further development of NE technologies on civil peacefull purposes followed the pattern of any technology, as described in this and previous papers [7-11].
- The NE technology, like any other one, is following the pattern described in the paper. However, the NE technology evolution in time is an envelope of the main nuclear energy and engineering set of design, fabrication and operation of a nuclear reactor and of all the other technologies supporting them (material fabrication, instrumentation and control, management systems, operator training etc.). However, for the existing NE generations and for the future developments there are NT like quantum computing, nanotechnology, artificiall intelligence, biology, robotics, virual reality etc of high impact on how a nuclear plant is going to be designed and operated. As illustrated in Figure 7. NE is in correlation with a whole new industrial revolution (Industry 4.0), which means that it will be highly influenced on all stages (research, desiign, operation) by the new NT mentioned before. The impact of this

interaction is in the risk evaluations and performance predictions of the new NE technologies. Risk methods become more flexible to adapted to the complexity of diverse technologies, a set of new methods are expected to cope with combined effects of man made artefacts –biological components-AI- new human generations features (Figure 8). Risk management becomes more complex and the Knowledge Management will rely on extentive trans and interdisciplinary approaches.

Figure 7. NE and Industry 4.0 era

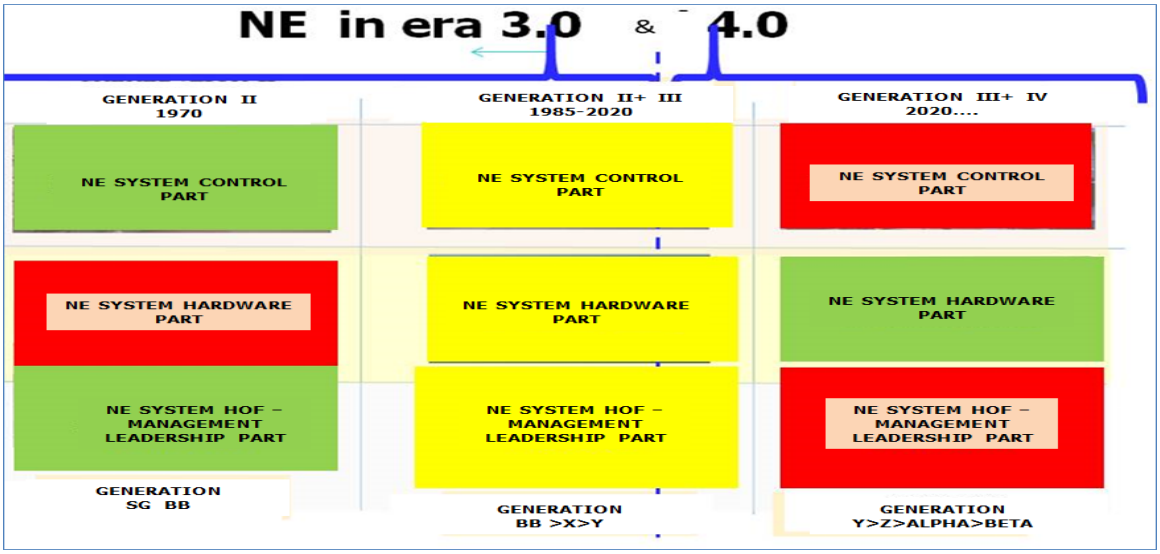
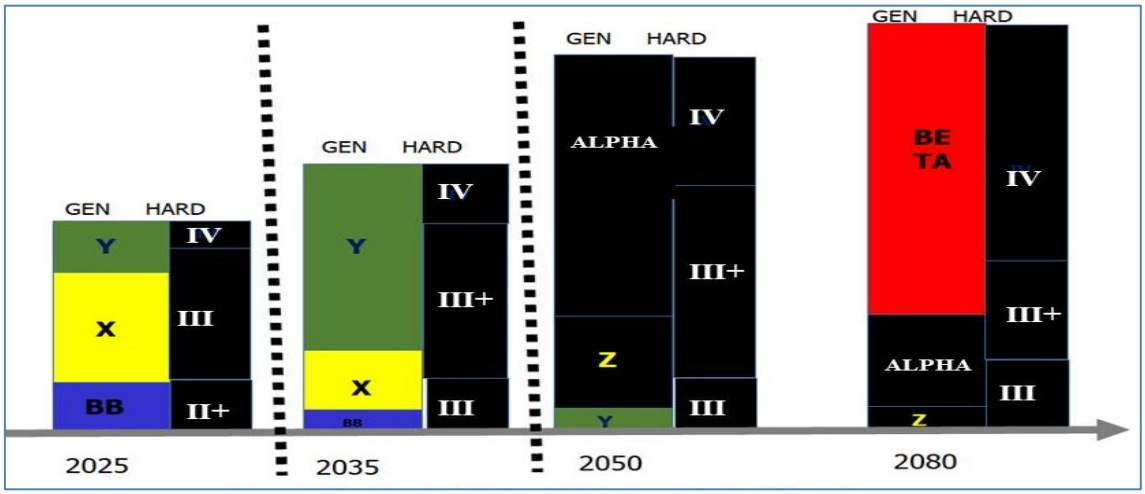


Figure 8. NE and human generations



3 Conclusions

The interface of various technologies on a governing one for a given artefact is evaluated for a special case of energy systems. The results illustrate the importance of considering the effect of interacting technologies while evaluating risk of new products and trying to use a certain risk management approach. For the impact of some NT on NE a set of practical conclusions for the next generations are derived.

References

1. Serbanescu D., Selected topics on safety issues for some complex systems LAP LAMBERT Academic Publishing (2018-03-07), ISBN-13:978-613-4-95529-4 ISBN-10: 6134955299 EAN: 9786134955294
2. Șerbănescu, D*, Discours de la création de la réalité – Manifest pentru un viitor al civilizației pământești*, February 2017, DOI:10.13140/RG.2.2.27889.28002 Conference: Simpozionul aniversar In honorem Mircea Malita 90 Romanian Academy DLMFS
3. Serbanescu, D., Safety paradigm changes and major accidents in nuclear power plants, SIEN 2017, Bucharest.
4. Șerbănescu, D*,On challenges and changes for complex energy systems,* May 2020,DOI: 10.13240/RG.2.2.22359,Cernavoda 24-25 Iunie 2019, DOI: 10.13240/RG.2.2.28998.70401
5. Serbanescu, D., On some issues related to foresight on safety for complex systems - Safety Margin history in nuclear and its systematic research, October 2017 DOI: 10.13140/RG.2.2.19424.58887, https://www.researchgate.net/publication/320394804
6. Serbanescu D., Systematic biases in NPP event reviews and their impact on learning process, June 2016, IAEA Conference
7. Serbanescu, D, Nuclear technologies and the generations - Tehnologiile nucleare și generațiile, Seminar on the dialog between the generations in science and technology, Division of Logic and Models, Romanian Academy, 31 October 2019, DOI:10.13240/RG.2.2.29999.70405,https://www.researchgate.net/publication/336898932
8. Serbanescu, D., On a possible approach for the multi criteria event analysis in complex systems events, 55th ESReDA Seminar on , Bucharest, Romania October 9th – 10th, 2018
9. Serbanescu, D., keynote speech, A triple facets view on some issues on the interface between Quantum Mechanics and Nuclear Engineering, OLC, International conference and Exhibition Quantum Mechanics and Nuclear Engineering, May 21-22 2020, Athens, Greece
10. Șerbănescu, D*, A triple facets view on some issues on the interface between quantum mechanics and nuclear engineering*, LC International – International conference and exhibition on Quantum Mechanics on Nuclear Engineering, 2020 Keynote speaker, Athens, Greece
11. Șerbănescu, D,A View on the Interface between some New Technologies and Nuclear Engineering DOI: 10.13240/RG.2.9.39959

Application of models for the efficiency of maintenance on practice failure data from power plants

Henk Wels, Reliability engineer, retired, formerly DNV GL and DEKRA, the Netherlands, hc-wels@outlook.com

Patrick Wolbers, Reliability engineer, DNV GL, the Netherlands

Abstract

Models for the relation between preventive maintenance and failures are abundant. While conceptually simple, application of p-F intervals for start of the problem to actual failure is almost impossible due to lack of practice data. Expert opinion is often used however it is seldom validated. Promising models in combination with sufficient data from practice are OREDA degradation-incipient-critical failure models as well as ARA (Arithmetic Reduction of Age) models as used by EDF and Grenoble University. An R&D project is envisaged incorporating OREDA, VGB and companies with conventional power plants to investigate the applicability of these models to failure data from practice. It would result in the efficiency of maintenance on specific systems in power plants as well as a prediction for the number of failures when minimal maintenance would be applied. This is essential for fossil power plants being backup facilities if renewable generation is insufficiently present (no sun, no wind). A major amount of preparatory work was already carried out using data available at DNV GL from VGB's KISSY database as well as from OREDA Handbooks. The paper shows preliminary results for boilers and steam turbines as well as a system in the Handbooks. This should help careful decision making on minimal maintenance for fossil power plants and still have sufficient grid reserve generation available.

1 Introduction

For the years to come, fossil fired power plants are to be the backbone for backup if there is insufficient renewable generation (no sun, no wind present) and with coal fired plants phasing out. The economic pressure for minimal maintenance will be large yet maintenance should be reduced cautiously in such a way that when "in the money" and when the plant is needed, the plant should be available. At present, databases for failure data very seldom give clues on the optimum PM interval let alone what would happen with only corrective maintenance (CM) applied. Given this background a VGB Research project is set up based on OREDA data for components offshore and VGB KISSY data for forced availability of power plants. This R&D project is expected to start in 2021. Major preparatory work has already been carried out, which is the subject of this paper. By sharing the knowledge gained from this preparatory work it is hoped to further understand the relation between maintenance and failures and by its application to power plants keep the lights on (have sufficient grid reserve generation available).

2 Methods to assess the relation between preventive maintenance and failures

Maintenance models are abundant. The problem is in the data for validating these models as well as convincing management and maintenance engineers to use these models. Essentially there are 5 ways forward to further optimize maintenance, that is:

1. Condition monitoring, using a p-F interval and assess the time for decision making between first notice of an imminent failure (time p) and the time to take the component

out of operation for economical or safety reasons (F). In English literature delay-time models have been developed by Christer [1], yet their application is still limited as there have been little data for validation. One should gather such data from power plant condition monitoring centres as the time for decision making is dependent on the component and therefore generic data gathering make sense. As the data are lacking and inspection / overhauling is still the dominant way of carrying out preventive maintenance in power plants, this is not the way forward in the proposed VGB Research project. Some "homework" using Licensee Event Reports (LERs) from nuclear power plants in the US did bring insight but not sufficient data to establish p-F intervals.

2. Investigating the relation between incipient, degrading and critical failures. The three failure severities are clearly defined in OREDA [2]. An incipient failure is a problem which, if not attended to, could result in a critical or degraded failure in the future. A degraded failure prevents equipment from operating according to specs. Such failures may develop into a critical failure in time. A critical failure causes immediate and complete loss of equipment capability of providing its output. The general idea is that incipient and degraded failures are in the time trajectory to failure before critical failures and, when resolved by preventive maintenance, will prevent critical failures. The OREDA data are taken into account in the proposed R&D project.
3. Age-reduction modelling (ARA-models) assumes that overhauls and repairs as a function of their efficiency, set the life of equipment back in time (rejuvenate) and limits ageing of equipment. ARA models are extensively dealed with, including calculation schemes and practical examples, in a French literature Handbook [3] as well as, in English, in the ESREDA Handbook on Maintenance Modelling and Applications. The ARA-models are taken into account in the proposed R&D project.
4. In RCM and reliability engineering handbooks the concept of a bathtub curve is shown. In practice one often finds teething troubles in reliability data as per the beginning of the bathtub curve. However it is a mistake to think that an ageing pattern will not arise as KISSY data and data in [4] have shown that due to minimal maintenance, ageing is visible for specific subsystems in boilers and other systems. Many bathtub applications assume that after maintenance, the component is As Good As New (AGAN) and the bathtub is repeated. This is questionable in most components in power plants with the exception of gas turbine blades, coal mill parts and other "wear" components, as most components are not replaced but are inspected and where necessary repaired. Most components are repairable for which a bathtub curve together with AGAN after maintenance does not hold. Therefore a bathtub curve in combination with AGAN is not the way forward in the present project. A component As Bad As Old (ABAO) or AGAN form the outer boundaries in ARA-modelling however.
5. Engineering judgement. It is always possible to use engineering judgement for assessing risks and, when practitioners and/or experts are available, interview them in a systematic way and use for instance Bayesian analysis to incorporate their judgement in a scientific way. Yet, publications on validating such judgement are rare, an example is however a publication on the judgement of airline pilots[1]. Engineering judgement is however not the way forward in the proposed project that is focussing on quantitative data, validating models and knowledge transfer.

In short: the proposed project is to assess maintenance efficiency and to give clues to the effects of minimum maintenance on the availability of subsystems in power plants. Utilities can use this knowledge to reduce costs as well as have power plants available when needed.

[1] 50th ESREDA Seminar, Karanikas and Kaspers, *Do experts agree when assessing risks? An empirical study.*

3 Maintenance efficiency from OREDA data

Haugen ea. [5] while using OREDA data has analysed degraded and critical failures for safety valves. As a safety valve is a component having dormant failure modes that should be found during inspection rather than during operation, an inspection efficiency can be calculated from the frequency of critical versus degradation failures. The inspection interval should be taken into account. Two data sets were used in [5]. The inspection efficiencies ranged from 40 % at a 12 month interval to about 75 % at a 3 month interval.

Haugen ea. in an Internet paper [6] showed also for a 28 MW aero-derivative gas turbine (GT) how to derive a maintenance efficiency from degraded, critical, shock-failures, the detection method and the preventive maintenance (PM) interval. This method will, with some modifications to make the effect of the PM interval more explicit, be used also for the proposed VGB R&D project. Maintenance efficiency is calculated from dividing all non-critical failures by non-critical + critical failures. Average overall maintenance efficiency was calculated as 84%. The failure rate without PM would be a factor 7 compared to that for critical failures with PM. In this number only non-shock failures are included. In shock failures for which many appear to be present at control systems, PM according to the analysis makes no sense as one by definition cannot see a degradation trajectory when shock-failures are imminent.

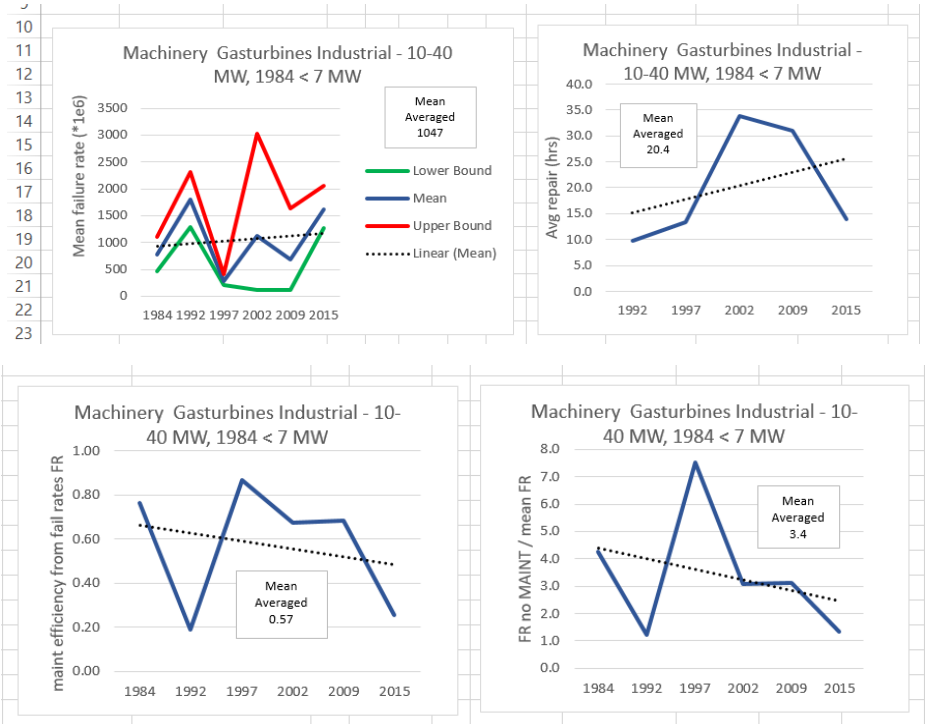
From the tables in the OREDA Handbooks one can easily derive the ratio of incipient plus degraded to critical failures for subsystems which is an indication of maintenance efficiency (as without maintenance all failures will be critical failures). However, the table in the Handbooks for GT maintainable items such as combustor, inlet vanes, etc. does not show degraded nor critical failures nor shock failures, the method of detection or the maintenance interval applied. Such tables should therefore be derived using the OREDA database raw failures.

Data for GTs (no differentiation in size or type) from the 2015 Handbook (Handbook table 1.2), indicate an average maintenance efficiency of 0.56 for the GTs in total. A failure to start on demand is expected to be either a dormant failure found during starting or the result of a human error. Evidently, maintenance efficiency defined by the ratio of degraded to critical failures for starting failures appears to be low and is in the order of 2%.

Using OREDA Handbooks over 1984-2015, maintenance efficiency over the years was calculated for various subsystems. Please note that as the taxonomy or "type indicator" as well as system boundaries change over the years, the different Handbooks are not easily compared. Systems were selected comparable to those in power plants such as gas turbines, pumps, generators, heat exchangers and valves. Preferably the analysis should be carried out on Maintainable Items such as bearings etc. however the amount of failures will be smaller and therefore the results less certain. Also maintenance strategies in power plants generally are per system and subsystem as combined work packages during planned outages are expected to be optimum.

An example of the results for industrial GTs is shown in Figure 1. In the figure trend lines are shown, however it is too early to draw conclusions from these lines as outliers can appreciably influence the trend. Furthermore, the 1997 results for GTs are somewhat strange in the sense that the (statistical) difference between upper and lower bound appears to be minimal. One expects a much larger difference as the average for 25 failures will be uncertain. Similar plots were made for compressors, pumps, heat exchangers and valves.

Figure 1. Trend analysis using OREDA Handbooks.



4 Maintenance efficiency in ARA models

In Procaccia & Ferton [3] a thorough discussion and calculation examples for age-reduction models such ARA[2], ARI, Kijima I/II etc. can be found. Essentially the ARA and Kijima models assume that inspection followed by necessary repair as well as other preventive maintenance such as revision or overhaul of a component reduces the age of that component and subsequently shift the bathtub curve. Also repair after a failure may reduce the age of that component and shift the bathtub curve.

Using log likelihood calculations and failure data from practice, it is possible to arrive at a failure intensity λ, an ageing coefficient β, an characteristic life η and a maintenance efficiency coefficient ρ for corrective (CM) and/or preventive (PM) maintenance as well as a time series for the average (expected) number of failures. The majority of the examples and applications is for $\beta > 1$, yet there is no reason why ARA models cannot be applied for $\beta < 1$[3]. Please note that the definition of maintenance efficiency differs between ARA and OREDA yet one expects that the higher the efficiency, the less (critical) failures,

Given these coefficients one can vary the maintenance interval (more or less age reduction) and the maintenance efficiency (for instance applying more precise measuring techniques at the inspection) and calculate the average number of failures over a period of interest. One can apply estimates for ρ from maintenance engineers / experts together with Bayesian updating when insufficient data are available, however this is not tried in the proposed project as the emphasis is on application to quantitative practice data rather than on engineering judgement.

The essence of Arithmetic Age Reduction (ARA) modelling is therefore setting back the age of the component or (sub-) system by an amount ρ from the last event. This is the ARA1

[2] ARA stands for Arithmetic Reduction of Age, ARI stands for Arithmetic Reduction of Intensity
[3] It makes no sense applying ARA models for $\beta = 1$ as the intensity is constant and independent on age.

model. When setting back the age from earlier events also, the ARA infinity model is present. When only CM is present, the ARA1 formulas are shown below.

$$\lambda(\mathrm{s}) = \alpha\beta s^{\beta-1} \tag{1}$$

$$\lambda_s = \lambda(s - \rho T_{Ns-}) \tag{2}$$

$T_N = \text{last maintenance}$

When both P and CM are present, the formulas are:

$$\lambda(\mathrm{s}) = \alpha\beta s^{\beta-1} \tag{3}$$

$$\lambda_s = \lambda(s - C_k + W_k) \tag{4}$$

$C_K = \text{last MC or MP time before s}$

$W_0 = 0$

$$W_{k+1} = (1 - \rho_c)(T_N - C_K) + W_K \text{ if } T_N = C_{K+1} \tag{5}$$

$$W_{k+1} = (1 - \rho_p)(\tau_M - C_K) + W_K \text{ if } \tau_M = C_{K+1} \tag{6}$$

In the MARS software of EDF and Grenoble University [7], the coefficients α, β, ρC and ρP are calculated using Maximum Likelihood equations. They can in principle also be calculated fitting the coefficients on the cumulative number of failures using least squares or optimisation with Excel Solver, however it was found that the resultant coefficients are not the same. As MARS is the most tested, the public version of MARS was proposed as the main software in the project.

5 VGB KISSY data

5.1 The database

Since 1988 data on the unavailability of power plants are gathered at VGB. This has grown into a modern computerized system called KISSY (Kraftwerk Informations System) By contacting VGB, VGB members or third parties can have raw anonymous failure information downloaded to Excel. Based on inputs by plant engineers and operators, for each event that causes a plant outage or power curtailment, the begin and end of the outage / failure is recorded, together with the sub-system that caused the failure as per the KKS Kraftwerk Kennzeichen System (which is a reference designation system in power plants). The background and consequences of the event are coded with the EMS Ereignis Merkmal Schlüssel system (a coding system for incidents in power plants). The text comments describing the circumstances of the outage or sometimes even its direct or root causes are especially helpful for explanations and further analysis but evidently take more time than analysis of codes.

In VGB R&D project 361 [8], plants were grouped into type of plant, fuel, capacity in MW, age, etc. to make failure data as specific as possible. Also, to assure the quality of data, VGB staff included only plants that had contributed for several years as well as plants where the summed total plant unavailability in the database part "Availability of Thermal Power Plants" was consistent with the KKS-defined sub-system database "Analysis of Unavailability of Thermal Power Plants". For the majority of plants analysed in this R&D project, anonymous data for each plant were available over a 10-year period up to 2011.

DNV GL (at that time DNV KEMA) issued in R&D project 361 a set of standard reports for the 20 % specific subsystems that caused 80 % of the forced unavailability (Pareto's Rule). They were made with spreadsheets that allow for every KKS to calculate the standard reports on a 1, 2 or 3 level KKS-code. For example for KKS = HA (Pressure parts boiler) and aged (> 25 year old conventional plants) the (abbreviated) standard report is shown in Figure 2 to Figure 8. In the standard reports, rather than only presenting the averages for failure rates and repair times, differences between plants are taken into account as per Figure 3[4].

Part of the standard reports is to show dependence on operating time, a short ageing analysis and the distribution of repair times (which is an essential start in a spare parts analysis). From Figure 8 it appears that the more operating hrs. per year, the larger the number of failures for a boiler. Regrettably in VGB 361 the number of starts was not yet present, which is to be bettered in the new VGB Research project as starts and operating hours per year are not unrelated[5]. The cumulative time since first failure often shows tell-tale increases indicating problems being not directly solved and causing a repeat failure or a new failure mechanism. This is dependent on component type as some (for example MAD = ST bearings) are more susceptible to repeat failures.

The dependence on calendar time shows ageing as per Figure 7 which is indicated by the quadratic term. Ageing using the ABAO model is however best described by a Crow-AMSAA model, semi-automatically calculated in the standard spreadsheets rather than by regression on failures[6]. The Crow β-coefficient is 1.78, the corresponding failure intensity is 2.22E-8 per hr. The spreadsheets, not yet part of the standard report, give ageing coefficients per plant using the Crow model. They are shown in Figure 9 for HA (pressure parts boiler) Similar plots can be made for KKS-codes in more detail such as for HAD (evaporator), HAH (superheater(s)) and HAC (economizer(s), etc.

Figure 10, using times since the first failure in the database, shows a different β compared to that using times since start of operation. This is important for the MARS coefficients calculated with time since the first failure in the database, as seldom failure data are present since the start of operation. This time shift appears to result in an apparent lower β and some β's < 1 indicating betterment as a function of time. Were it not that the power plants analysed are over 25 years old, this could be interpreted as teething troubles. It is envisaged during the project to use also younger power plants and study this phenomenon further.

4 Data are colored green when < 50 % of average, red when > 50 % of average.

5 Base load plants have about 8000 operating hrs. per year with say 10 starts, cycling plants can have 2000 operating hrs. per year with 100 starts. When analyzing the effect of operating hours on forced failures, starts is a confounder as per Pearl & Mackenzie, The Book of Why [14].

6 Some plants do not have failures but do have operating time. This should be taken into account in the average (expected) number of failures.

Figure 2. Plant characteristics in VGB 361 (sample from 84 plants)

Coal - Lignite aged > 25 years | KKS Code | HA | Level | KKS2 | Repeated within | 168 | hrs
Pressure system

Plot no	Include	Power Plant Unit	Type of Power Plant	Fuel	Capacity net [MW]	Age [Comm. to 2011]	Average Operating Hours	Years in database
1	1	1	Fossil Block Mono	Lignite	3: 200 - 399 MW	26	7017	10
2	1	10	Fossil Block Duo	Hard Coal	3: 200 - 399 MW	40	4307	10
3	1	11	Fossil Block Mono	Hard Coal	3: 200 - 399 MW	29	4992	10
4	1	15	Fossil Block Mono	Hard Coal	4: 400 - 599 MW	25	6373	8
5	0	16	Fossil Block Mono	Oil	4: 400 - 599 MW	37	470	0
6	0	17	Fossil Block Mono	Oil	3: 200 - 399 MW	38	599	0
7	0	19	Fossil Block Mono	Oil	4: 400 - 599 MW	38	1980	0
8	0	20	Fossil Block Mono	Oil	4: 400 - 599 MW	37	1945	0
9	1	21	Fossil Block Mono	Hard Coal	3: 200 - 399 MW	42	6192	8
10	1	25	Fossil Block Mono	Hard Coal	5: 600 - 999 MW	35	6283	10
11	1	28	Fossil Block Duo	Hard Coal	3: 200 - 399 MW	46	4406	10
12	1	29	Fossil Block Mono	Hard Coal	3: 200 - 399 MW	41	4444	10
13	0	30	Fossil Block Mono	Oil	5: 600 - 999 MW	34	1049	0
14	1	34	Fossil Block Mono	Hard Coal	3: 200 - 399 MW	41	7036	10
15	1	35	Fossil Block Mono	Hard Coal	3: 200 - 399 MW	43	7247	10
16	1	36	Fossil Block Mono	Hard Coal	3: 200 - 399 MW	42	5941	10
17	1	37	Fossil Block Mono	Hard Coal	3: 200 - 399 MW	41	5981	10
18	1	38	Fossil Block Mono	Hard Coal	3: 200 - 399 MW	40	5972	10
19	1	39	Fossil Block Mono	Hard Coal	5: 600 - 999 MW	32	4900	10
20	1	42	Fossil Block Mono	Hard Coal	2: 100 - 199 MW	42	6845	10

Figure 3. Failure data in VGB361 standard report (sample from 84 plants)

Power Plant Unit	Nr of failures in database	Nr of components	Redundant vs Multiple Component(s)	Failure rate (1/hr)	Average repair time (hr)	Average unavail capacity	Unavailability [time based]	Theoretical Unavailability (plant needed)	Unavailability [energy based]	Fraction Repeat in failures
1	42	1	0	5.99E-04	63.8	88%	3.06%	3.68%	3.07%	11.9%
10	70	2	M2	8.13E-04	104.2	51%	8.33%	7.81%	4.73%	15.7%
11	36	1	0	7.21E-04	63.6	98%	2.62%	4.39%	2.75%	5.6%
15	5	1	0	9.81E-05	18.6	86%	0.13%	0.18%	0.13%	20.0%
16	0	1	0				0.00%	0.00%	0.00%	
17	0	1	0				0.00%	0.00%	0.00%	
19	0	1	0				0.00%	0.00%	0.00%	
20	0	1	0				0.00%	0.00%	0.00%	
21	95	1	0	1.92E-03	31.7	88%	4.29%	5.73%	4.24%	12.6%
25	73	1	0	1.16E-03	31.8	89%	2.65%	3.56%	2.64%	13.7%
28	59	2	M2	6.70E-04	49.2	52%	3.31%	3.19%	2.04%	11.9%
29	94	1	0	2.12E-03	69.2	88%	7.43%	12.77%	7.33%	8.5%
30	0	1	0				0.00%	0.00%	0.00%	
34	26	1	0	3.70E-04	39.3	88%	1.17%	1.43%	1.16%	11.5%
35	49	1	0	6.76E-04	43.0	93%	2.40%	2.82%	2.39%	2.0%
36	90	1	0	1.51E-03	36.1	92%	3.71%	5.18%	3.60%	5.6%
37	69	1	0	1.15E-03	56.9	92%	4.48%	6.16%	4.35%	4.3%
38	77	1	0	1.29E-03	36.3	92%	3.19%	4.48%	3.14%	2.6%
39	68	1	0	1.39E-03	39.3	91%	3.05%	5.17%	3.05%	5.9%
42	54	1	0	7.89E-04	46.9	100%	2.89%	3.57%	2.89%	7.4%

244	40	1	0	8.25E-04	88.4	73%	5.04%	6.79%	3.50%	10.0%
246	29	1	0	7.92E-04	96.9	93%	4.01%	7.13%	3.98%	6.9%
247	8	1	0	7.68E-04	68.2	100%	1.04%	4.98%	1.04%	12.5%
252	0	1	0				0.00%	0.00%	0.00%	
253	0	1	0				0.00%	0.00%	0.00%	
	4486			8.33E-04	67.6		4.95%	5.33%	3.51%	11.7%

Figure 4. Full outage data in VGB361 standard report (sample from 84 plants)

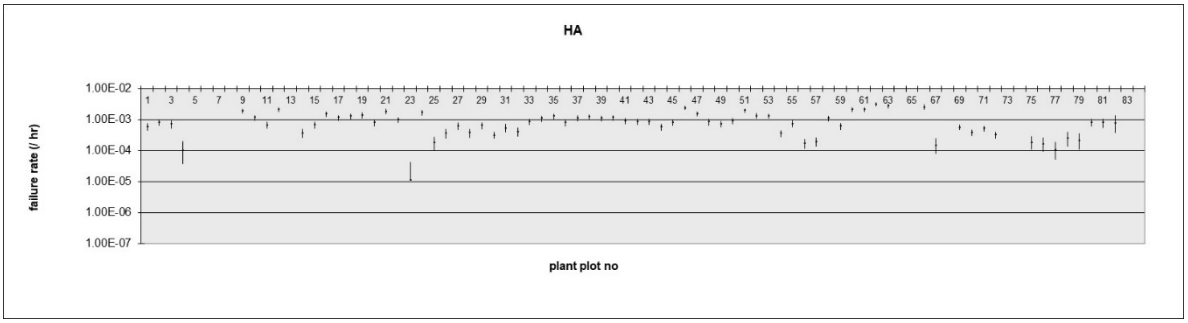
Power Plant Unit	Expected failures (/ yr)	Nr of full outage failures	Fraction full out	Full out Failure rate	Average full out repair time	Nr of automatic grid separations UAGS	fraction UAGS	average duration UAGS
1	5.24	41	98%	5.84E-04	65.3	2	5%	72.8
10	7.12	9	13%	1.04E-04	179.1	0	0%	
11	6.32	33	92%	6.61E-04	68.1	2	6%	51.3
15	0.86	4	80%	7.85E-05	22.8	0	0%	

215	2.14	4	33%	8.15E-05	85.4	2	50%	26.7
216	1.83	2	20%	4.19E-05	80.3	0	0%	
244	7.22	26	65%	5.36E-04	74.1	1	4%	2.3
246	6.94	26	90%	7.10E-04	108.0	1	4%	2.0
247	6.73	8	100%	7.68E-04	68.2	2	25%	39.1
252		0				0		
253		0				0		
	7.30	3444	77%	7.38E-04	62.4	18	1%	21.2

Figure 5. Failure rate and repair time for KKS= HA (VGB361)

Initial estimate for failure rate			uncertainty for homogeneous set of plants
lambda	8.33E-04 / hr	5% lower	8.13E-04
stdeviation	6.84E-04	95% upper	8.54E-04

OREDA multi sampling for non-homogeneous sets			uncertainty for NON-homogeneous set of plants
estimate lambda	9.43E-04	5% lower	1.50E-04 /hr
stdev	6.31E-04	95% upper	2.00E-03 /hr



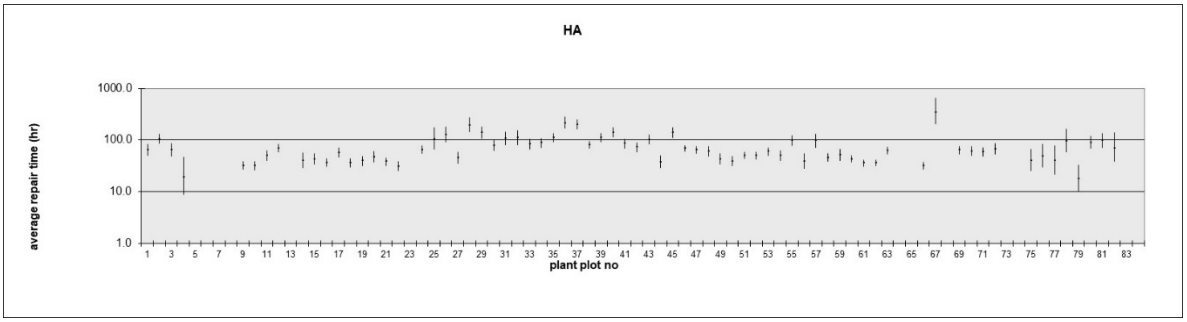


Figure 6. Dependence on operating time

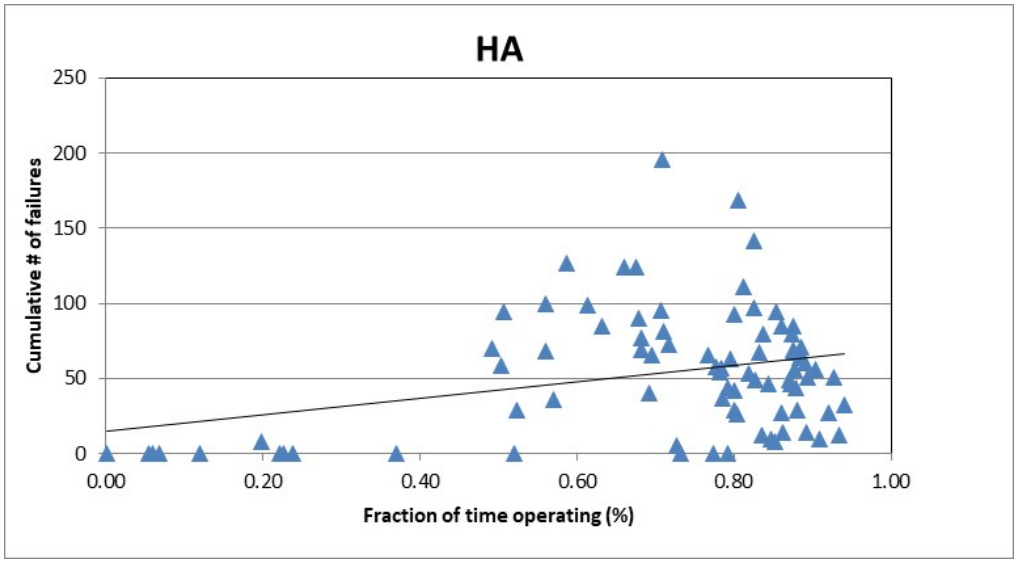


Figure 7. Dependence on cumulative calendar hrs

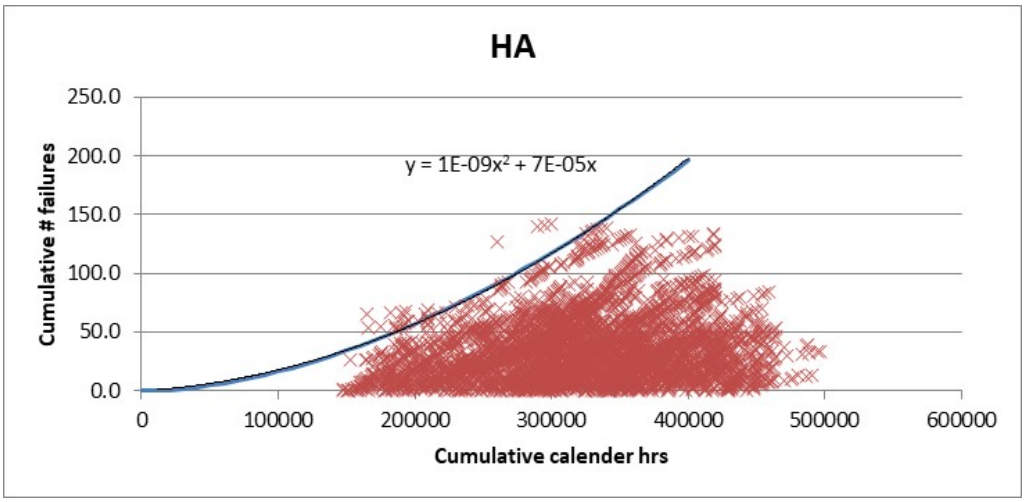


Figure 8. Distribution of repair time

Figure 9. Ageing coefficients Crow model for HA (pressure parts boiler)

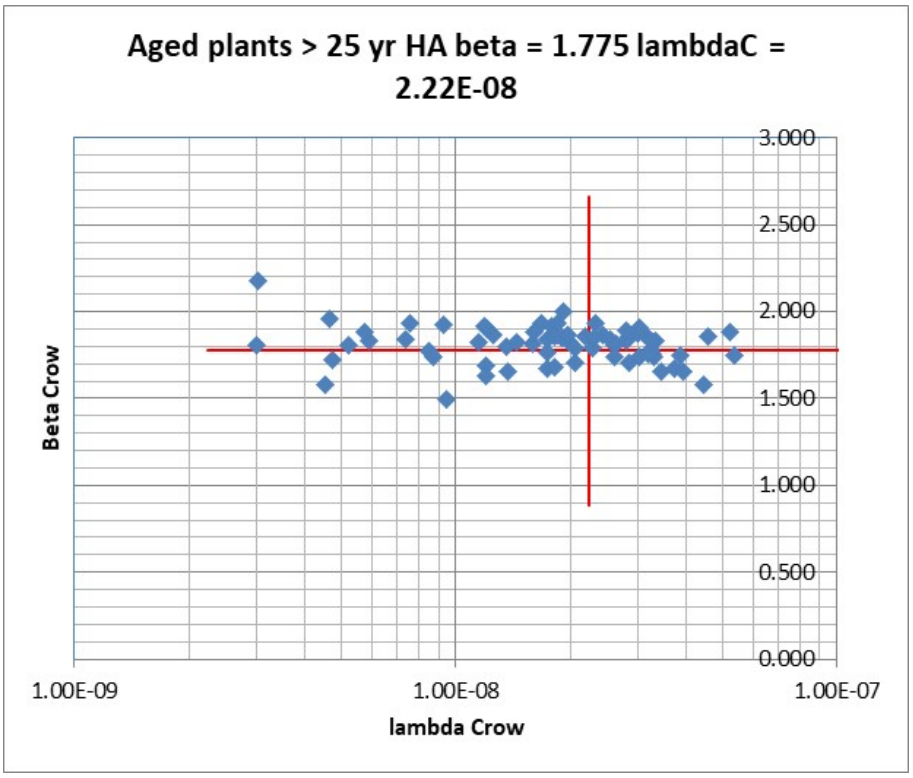
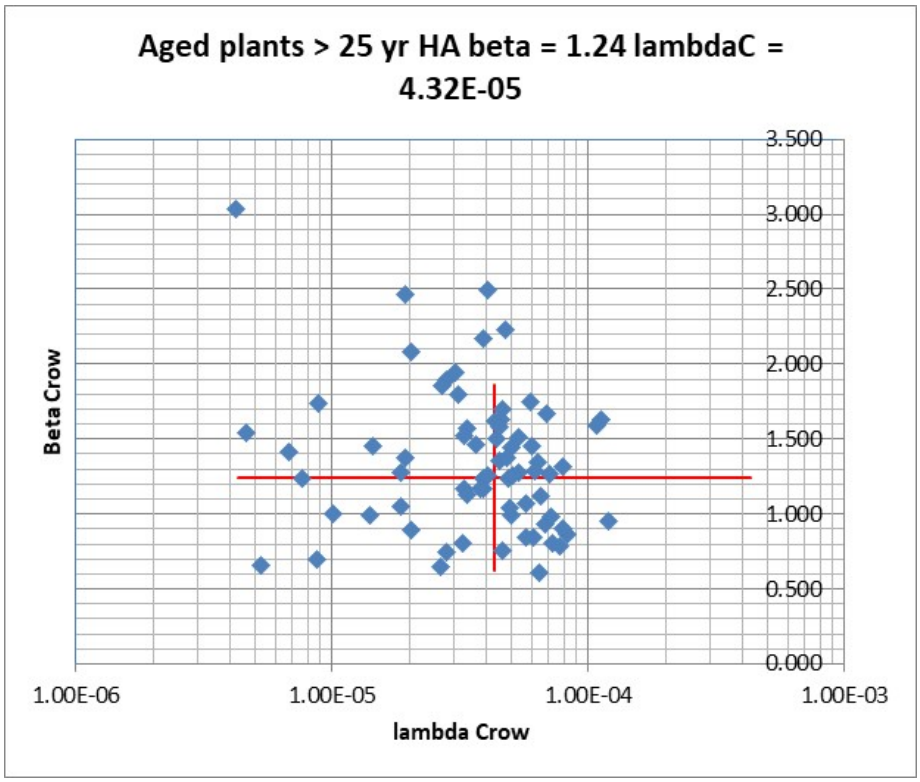


Figure 10. Ageing coefficients Crow model for HA (pressure parts boiler) time shifted since first failure in database



5.2 KISSY data for boilers

Using MARS on VGB 361 data boiler data for aged coal & lignite fired plants, with about 4500 failure data on 82 boilers, the ageing coefficients and maintenance efficiencies were calculated. During analysis it was found that 6 boilers had less than 10 failures which were disregarded as having insufficient information to derive 4 parameters from. For the new VGB Research project, when components have only a few failures, details on why this is the case can be interesting to the partner utilities in the project in order to improve their plants. Contacting such plants is difficult for generic data.

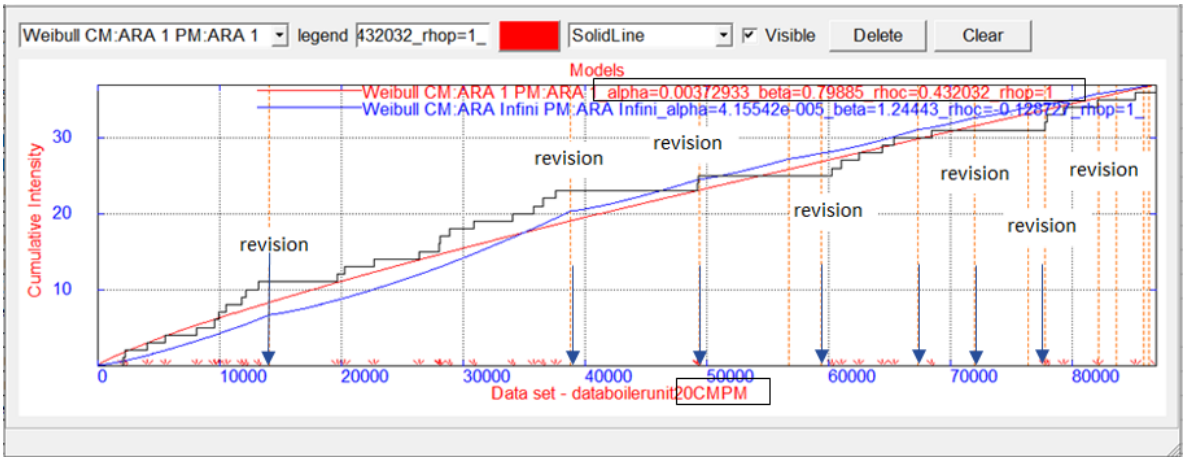
A major effort was to interpret the KISSY data for overhauls as the EMS codes do pinpoint plant overhauls but are insufficient to detail component and sub-system overhauls. Based on the free text, some major damages and conversions were found in which, based on engineering judgement, certainly some boiler inspections / overhauling must have been carried out give the opportunity. Failures were calculated in calendar hrs. starting at the first failure for a particular plant in the databases. Input data such as Figure 11 were copied into separate text files as required by MARS. Some issues to be solved in the new VGB Research project are the use of operating hrs. instead of calendar hrs. and the use of the number of starts and/or combinations (equivalent operating hrs.). Another issue is how to assess identical sister units in which failures may or may not have occurred due to the solutions found from the first failures in the sister units .

A result showing the effect of overhauls for boiler no. 20 is given in Figure 12. Only in the ARA ∞ model ageing seems to be overall present with β = 1.244. In the ARA 1 model β = 0.799 indicating some betterment as a function of time. The figure also shows that not all revisions are equal: the revision at 13000 hrs. seems to halt ageing and clearly shifts the bath tub curve starting at a low failure intensity again. Revisions 2 and 3 at 38000 and 49000 hrs. seem to be almost perfect while revision 4 at 59000 hrs. seems to result in teething troubles after the revision as cumulative # of failures shows a downward curve. Please note that Monte Carlo analysis shows that this pattern might be due to chance only and should be checked further.

Figure 11. Adding PM and CM interpretations to KISSY data

	A	B	C	E	F	G
1	Unit Name	Begin[Date]	Age minus first faildata	PMCM	Duration> 8 hr	Comment
2	1	1/28/2002	0	CM	101.57	Rohrschaden im Eco auf 30 m 2. Zug
3	1	4/4/2002	1608	CM	56.50	Rohrschaden
4	1	8/9/2002	4646	PM	1403.45	Revision
5	1	9/3/2003	14012	CM	76.80	Außerbetriebnahme: Rohrschaden am ZÜ 1
6	1	10/6/2003	14807	CM	36.43	Außerbetriebnahme: Rohrschaden Verdampfer"
7	1	4/9/2004	19260	CM	50.78	Außerbetriebnahme: Rohrschaden Verdampfer
8	1	5/5/2004	19882	CM	38.60	Ausfall wegen Kesselschaden"
9	1	5/14/2004	20104	PM	367.97	Revision"
10	1	5/30/2004	20472	PM	249.33	TÜV-Druckprüfungen
11	1	4/9/2005	28021	CM	91.73	Rohrschaden"
12	1	4/30/2005	28527	PM	481.57	Revision
13	1	11/16/2005	33333	CM	54.25	Ausfall: Rohrschaden
14	1	1/10/2006	34651	CM	54.88	Ausfall
15	1	1/18/2006	34847	CM	31.67	Rohrschaden"

Figure 12. Example of application of MARS to KISSY data showing the influence of revision(s)



The analysis showed that boiler β-values are typically in the range of 0.5 – 1.2 with ρ's in the range of 0.61 – 0.99. The ARA models did not always converge into reasonable ρ's with log likelihood optimization. All MARS results with converging ρ's (0< ρ <1) were sorted, resulting in Figure 13 - Figure 15.

In Figure 13 the relation between β and α is given. This figure is clearly different from that using the overall ABAO Crow model. This figure shows that 50 % of the boilers have values < 1 (teething troubles) and 50 % has a value > 1 (ageing). Evidently there is a relation between the ageing coefficient β and the frequency coefficient λ (α), depicted as red and blue in Figure 13. Yet, this relation is clearly different from that in the conventional ABAO Crow model depicted as grey, see also Figure 9.

Figure 13. β and λ (α) values for boilers

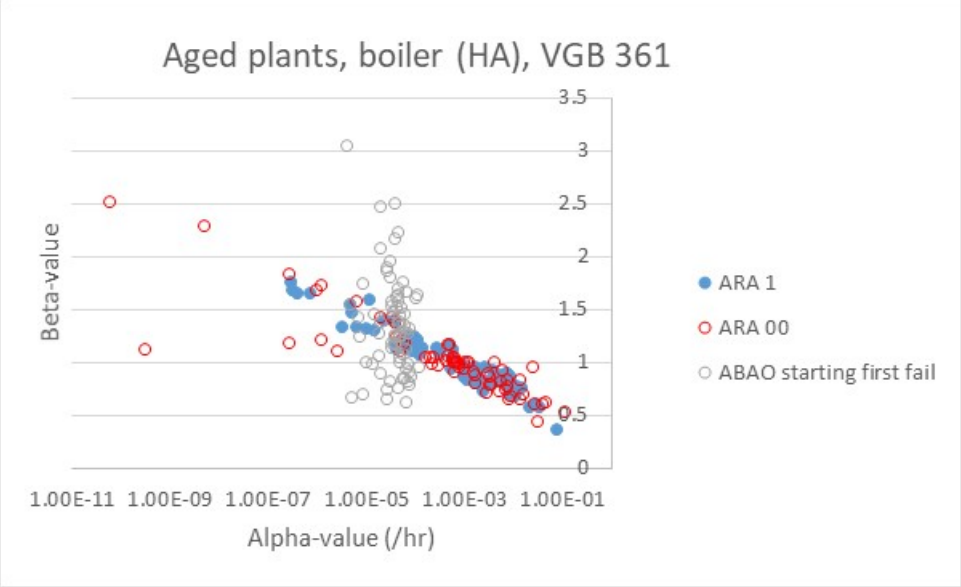


Figure 14. Distribution of β-values for boilers

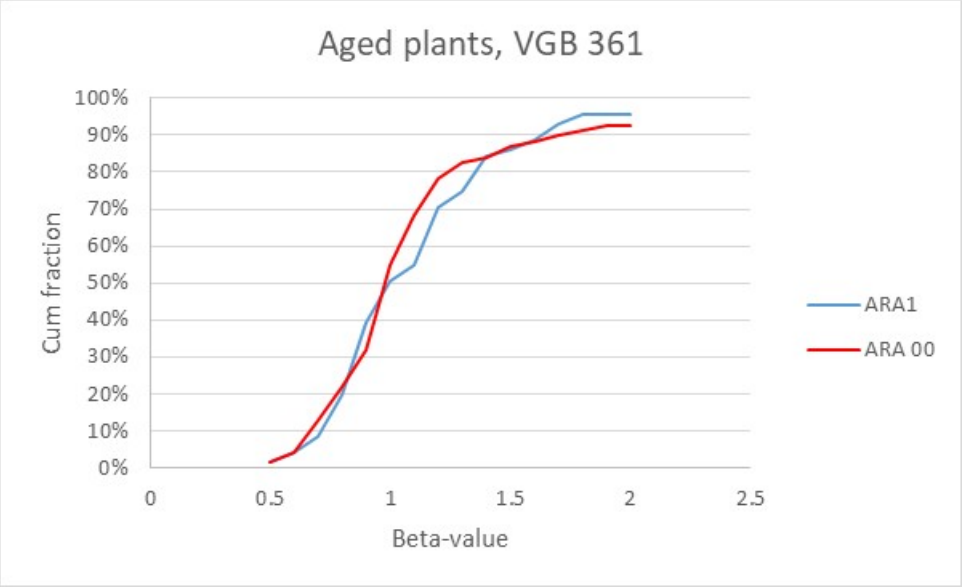
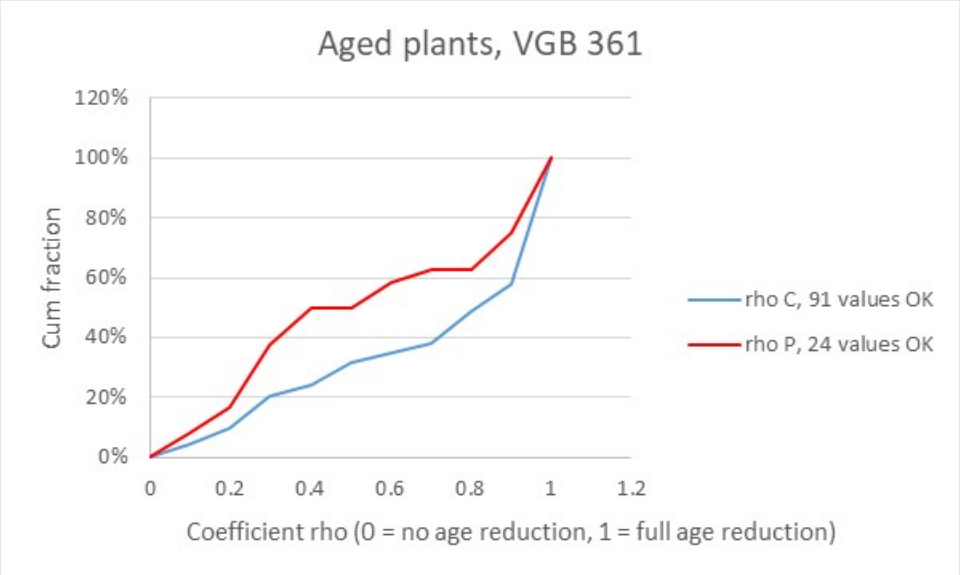


Figure 15. Distribution of maintenance efficiencies for boilers



The distribution of maintenance efficiencies in Figure 15 shows that in general ρ PM is smaller than ρ CM, which is not to be expected. Half of the ρ PM values is less than 0.5, only 40 % is larger than about 0.8. PM for HA = pressure part in boilers therefore does not seem to be very effective. Half of the ρ CM values appear to be less than 0.9, half larger than 0.9. To improve low ρ CM values it is recommended to carry out good failure investigations and, when budget allows, improve the component under consideration. The ρ values appear to be independent on β-values (not shown).

5.3 Effect of overhaul frequency on number of failures for boilers

It is certainly not the case that power plants have a true yearly, 2-yearly, etc. overhaul frequency. Asset managers will postpone or have an overhaul carried out somewhat earlier if company portfolio planning makes this optimum. Some plants according to the VGB KISSY data appear to be experimenting between short quarterly stops and longer fixed intervals.

From analysis there is also no clear relationship between β and the overhaul interval. Yet, with (short) yearly intervals there appears to be some teething troubles after overhaul while at apparently irregular intervals at some plants the β values are > 1. One cannot say that at larger intervals such as 3 years, β is consistently > 1 suggesting such intervals are (too) large. There is also little relationship with the failure rate as one cannot say that with longer intervals the failure rate is per definition high. High being defined as over 50 % larger than average, low as 50 % lower than average.

Tentatively it is concluded that overhaul frequencies are, as they should be, dependent on plant component characteristics. That should allow larger than yearly intervals without much ageing between overhauls. Also high or low failure rates appear to be dependent on component characteristics yet plants that do not operate much consistently have low failure rates7. Therefore failure rates are depending on operating regime.

5.4 Results for steam turbines using KISSY data

VGB in VGB-R 115M [9] has given recommendations for the overhaul of steam turbines. Essentially the interval should take account of starts using 20-30 operating hours per start. Small to medium overhauls, the content depending on need, are recommended per 24000 equivalent hours (2.5 – 3 yrs.) with a large overhaul every 100000 equivalent hours (10-11 years). The 3 yr. interval does show up in the KISSY data yet smaller intervals are also visible. Since in the VGB 361 data each plant is present for at most 10 years, 10 year intervals are not likely to show up at individual plants. The typical duration for a large overhaul including inspection of inner HP, IP and LP turbine parts as per [9] would be 50 days. This duration does show up in the KISSY data.

In a similar way as carried out for boilers, KISSY data were extracted for analysis using the VGB 361 project data. Standard reports were made showing the overall ageing characteristics for MA = steam turbine, with manual exclusion of MAG = condenser as this subsystem is totally different from other steam turbine subsystems. Steam turbine failure rates are typically lower than those for boilers (yet repair times can be high). Again, there is substantial spread between power plants.

All 81 steam turbines were analysed with in total 1830 events. Some events were removed or corrected due to substandard KKS-coding and some events were taken together as 1 (for instance overhaul and overhaul extension). MARS analysis was started using a simple ABAO model (generally green in the plots) followed by ARA1 (red) and ARA ∞ (blue). Some results are:

- A substantial number of turbines appear to show teething troubles after overhaul and after a failure as indicated by $\beta < 1$.
- It appears that some overhauls have been more effective than others. Evidently more details on the content of these overhauls is necessary which is not yet present in KISSY but should be available at utilities.
- Some turbines appear to show that overhauling does not decrease ageing and in that sense the overhauls were less successful as they should have prevented both failures and ageing.

Please note that apparent effects may be stochastic effects simply caused by chance if occurring only for a few turbines such as shown in a Monte Carlo MC analysis. Yet the distribution of β as per Figure 17 seems to point at a systematic effect as the majority of β values is < 1.

[7] In the new VGB Research project the effect of starts is to be taken into account also.

Figure 16. ABAO and ARA models for a steam turbine showing teething problems

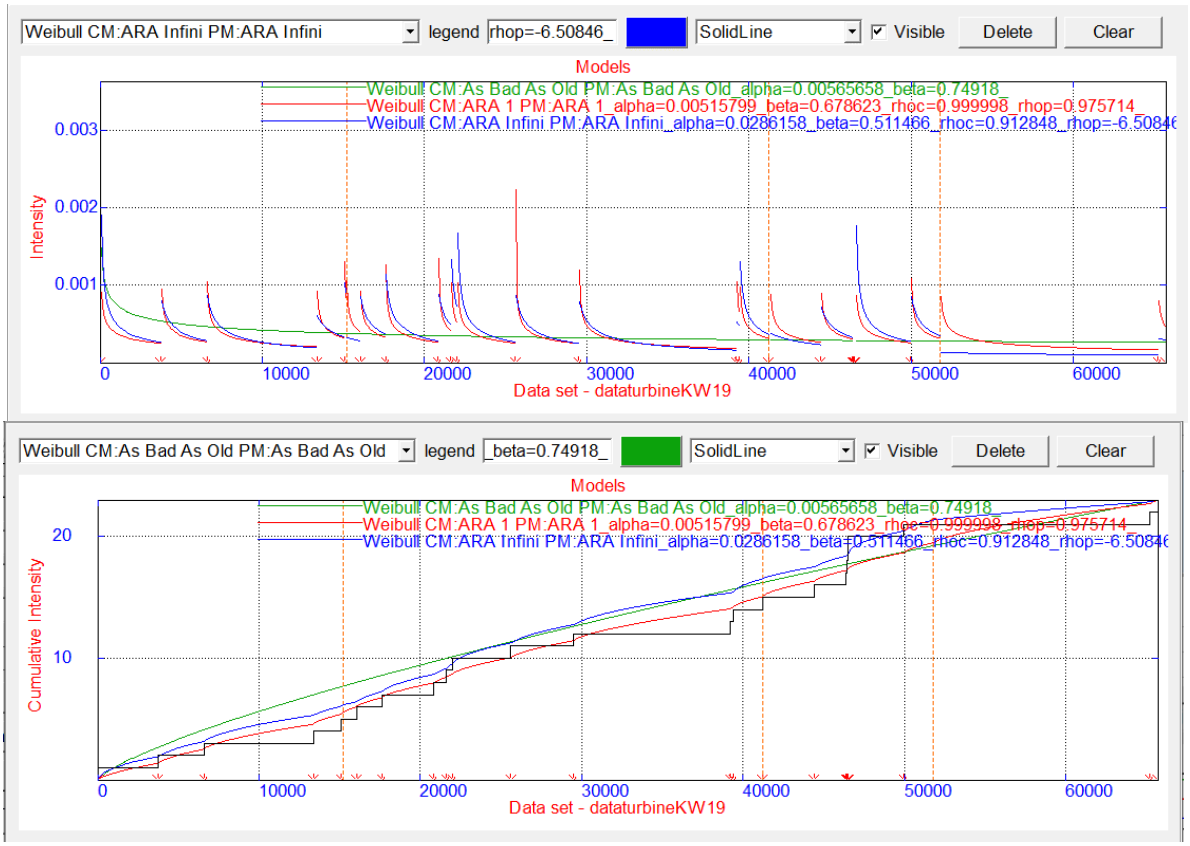
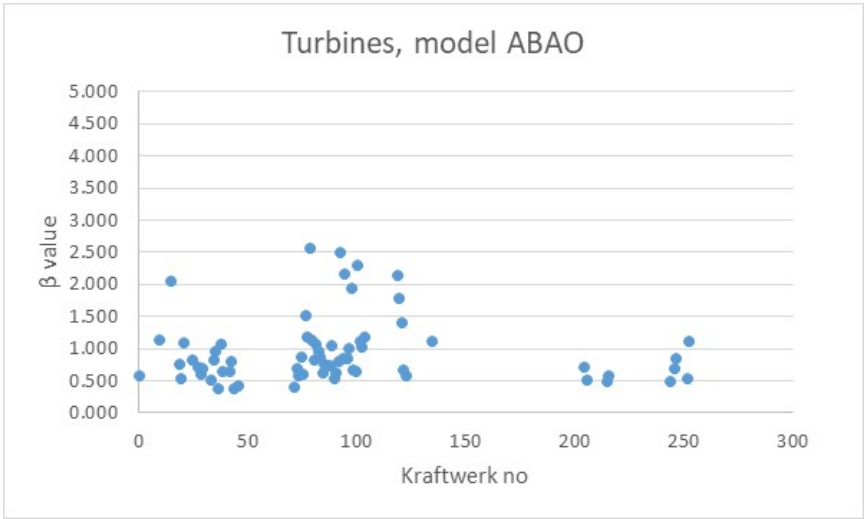


Figure 17. β-values for turbines (not from start of operation), max vertical axis set to 5



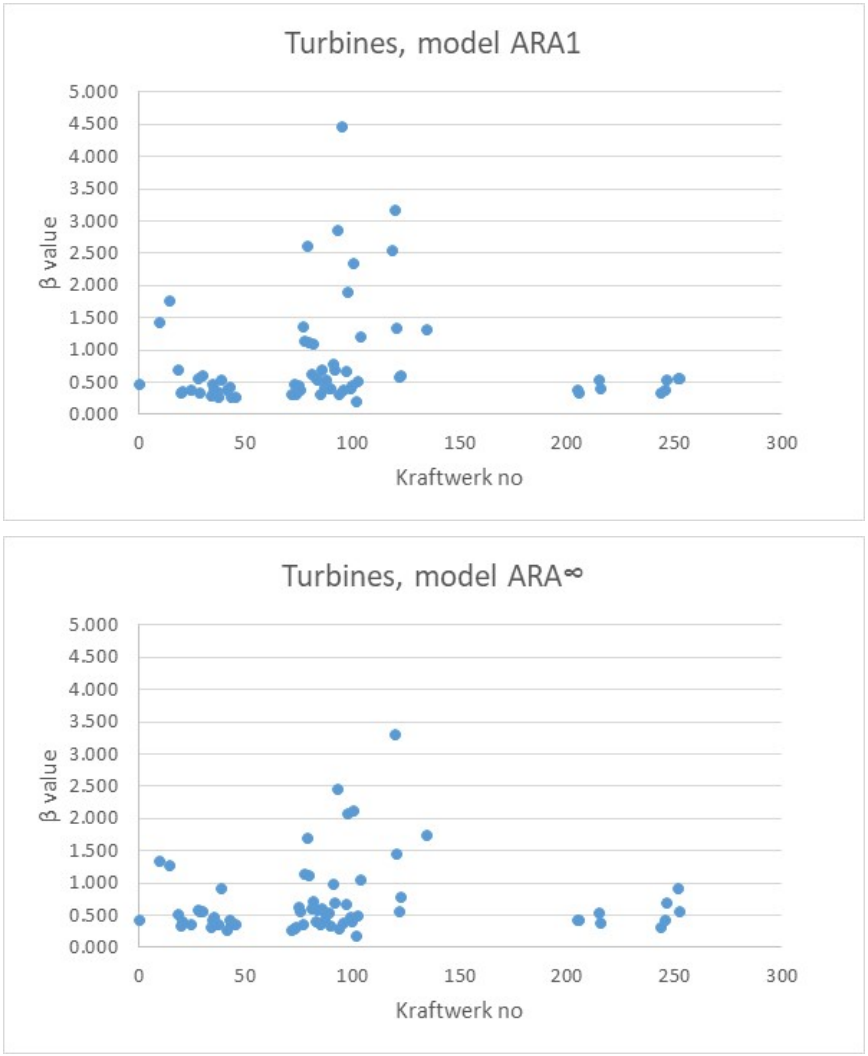
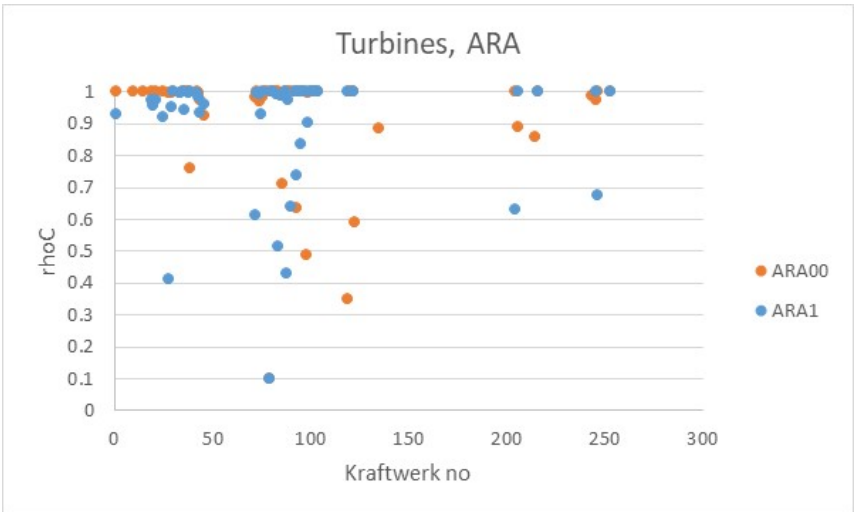


Figure 18. Calculated corrective maintenance efficiencies



In Figure 18 the calculated corrective maintenance efficiencies are given. In general the ρ coefficients are close to 1 with some low values in the range of 0.3 to 0.6. As many coefficients are identical to 1, being close to 1 is thought to be more due to the calculation procedure than the result of reality. In the VGB Research project the issue of a low ρ versus ρ equal 1 is to be investigated further including the use of ARA versus ARA∞ along the lines of [13], a Mixed Kijima Model using Weibull-based Generalized Renewal Processes.

6 A Monte Carlo (MC) simulation model versus an analytical model for maintenance efficiency

An analytical calculation for the average (expected) number of failures with equidistant time steps for the Crow ABAO model is simple. However, this is not the case for an ARA type of model as the life reduction governed by the maintenance efficiency coefficient ρ takes place only at failure times and after overhauls. A MC model simulating failure times and taking overhauls into account after which life is reduced makes sense and it also shows the uncertainty in outcomes. A MC model is however often slow and an analytical model is therefore preferred. It is however the habit of the first author to set up both a MC model and an analytical model for quality checking as the average MC value should be similar to the analytical value. Both the MC and the analytical model are to be used in the new VGB Research project.

The preliminary MC model realized in Excel essentially draws from a list of 100 random failures using an ageing model (AGAN, ABAO, ARA1) as well as random failures (no ageing)). It checks in an equidistant time series if a failure from the list is present at a certain time. Repair processes are not modelled in this spreadsheet.

Six random MC realizations are shown in Figure 19 with coefficients λ and β as per turbine no. 19. Overhauls are assumed each year (8760 hrs.). The realizations show that one must be careful to draw conclusions about ageing based on a single time series as for instance time series e) seems to indicate ageing. This cannot be true given the underlying model with β = 0.68. The distributions for the number of failures in 3 years' time is shown in Figure 20. This figure also shows the uncertainty in 1000 simulations with averaging over 100 each.

At first it seems strange that with increasing maintenance efficiency in the ARA model the average number of failures increases. This is explained by the form of the bathtub curve when teething problems are present. A high maintenance efficiency in terms of shifting the curve to the origin again after either failures or PM, results in a higher failure intensity directly after CM or PM maintenance and consequently a higher number of failures.

There appears to be no closed analytical form for ARA models. Yet, a practical approach is present in Yevkin and Krivtsov [10]. Essentially, for ρ CM or ρ PM is 0, the system is As Bad As Old (ABAO). For ρ CM or ρ PM is 1, the system is As Good AS New (AGAN). Otherwise it is in between with the appropriate amount calculated using the empirical coefficients from [10].
The ABAO equation is easily derived from a Crow-AMSAA model [11] fitted to the failure data or by using MARS for ABAO. For a general AGAN system with underlying Weibull distribution for times between failures, again there is no closed analytical form except for asymptotic expansions or other approximations for small values of time. However, in Tijms [12] on page 36 & 442 it is explained that the renewal function M(t) which is equal to the expected number of failures E[N(t)] is the sum of the cumulative probabilities F(t) in a γ distribution (Tijms [12] eq. 2.1.4) as defined by shape parameters n * α and scale parameter λ. The F(t)'s given α and λ can easily be calculated in Excel using the incomplete γ function. Therefore, by conversion of the Weibull AGAN distribution for times between failures into a γ distribution, the AGAN average, expected, number of failures E(N(t) can be calculated. This was programmed in Excel and is to be further investigated in the VGB Research project.

Figure 19. Realisations in a Monte Carlo ARA1 model

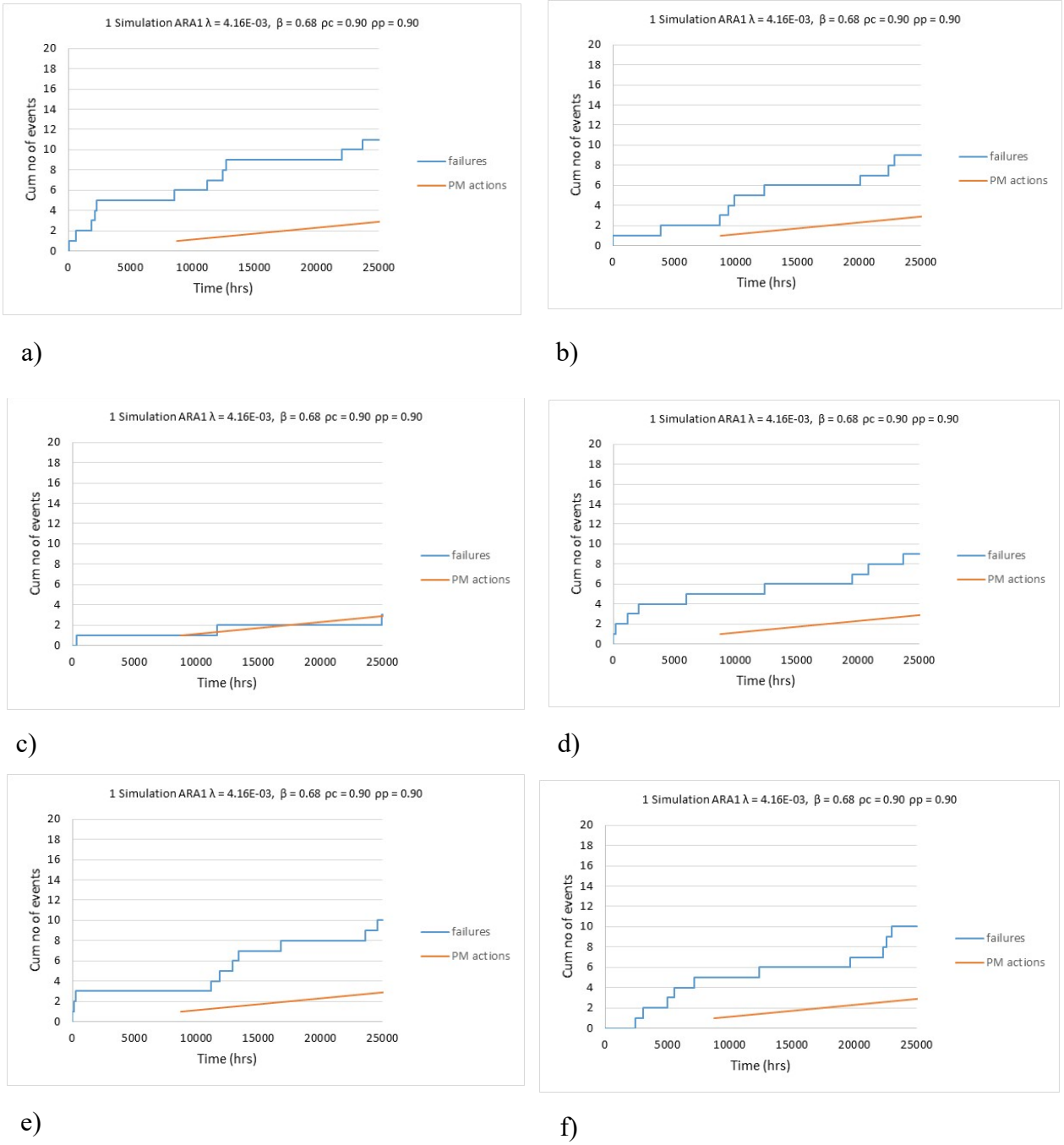
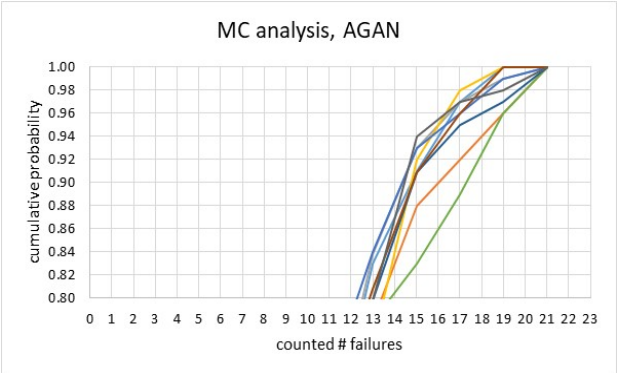
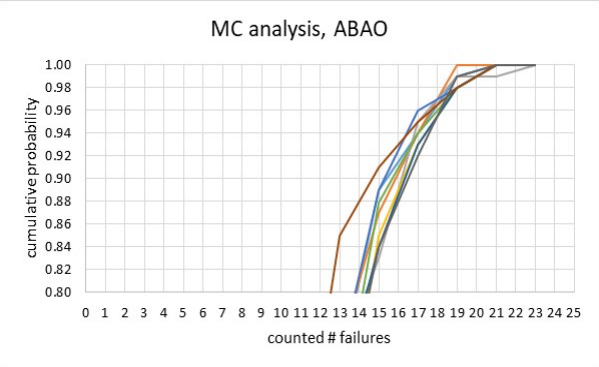


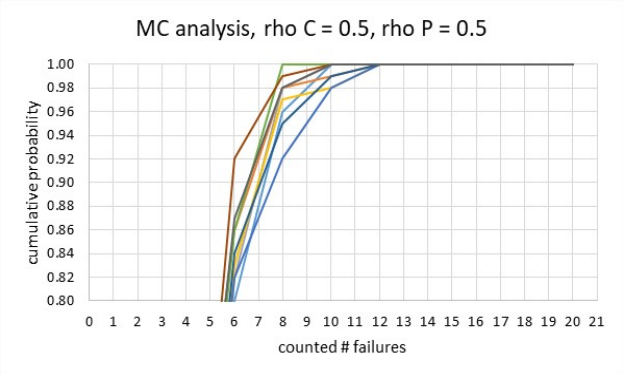
Figure 20. Uncertainty in MC analysis



Average: 8.82 failures



Average: 3.88 failures



Average: 4.78 failures

7 Conclusion

At present, databases for failure data very seldom give clues on the optimum PM interval let alone what would happen with only corrective maintenance (CM) applied. Yet this is important knowledge for optimizing the operation of conventional power plants when they will be increasingly operated as backup for renewables. We do not want brownouts or even blackouts due to insufficient capacity available.

Using the OREDA Handbooks, maintenance efficiency over the years for several components was calculated from degraded and critical failures. However, the tables in the Handbooks do not show shock failures, nor the method of detection or the maintenance interval applied. Maintenance efficiencies should therefore be derived using the raw data in the OREDA database.

Raw KISSY data such as those from the VGB 361 Research Project up to 2011, can be used to derive failure frequencies, ageing patterns and maintenance efficiencies for subsystems and components in power plants in combination with added information on preventive maintenance. The software used is the public version of the MARS software from EDF and Grenoble University. This was carried out for about 4500 failure events on 82 boilers as well as 1830 events on 81 steam turbines in preparation for a new VGB R&D project.

The proposed VGB R&D project is expected to start in 2021 and uses raw OREDA data, plant specific data from the utilities partnering in the project together generic data from VGB's KISSY database in combination with a simple Excel Causal Model along the lines of Pearl & Mackenzie [14]. The project will give the average (expected) number of failures per hr. as a function of PM maintenance interval, the average if no PM maintenance on specific components would be carried out as well as coefficients for PM maintenance efficiency in relation to actual work carried out at partner utility plants.

Acknowledgements

Acknowledgement is given to DNV to present the paper and to VGB for having had the VGB 361 R&D project carried out by DNV KEMA. R&D project 361 resulted, as per the report *"Reliability Indicators with KISSY - VGB Research Project 361"* (only PDF-download), ISBN: 978-3-86875-751-4, 2014, in a wealth of aggregate failure information for conventional power plants. Acknowledgement is given to OREDA and VGB to support the newly proposed R&D project.

References

1. Christer AH and Waller WM,/ 1984, *Reducing production downtime using delay-time analysis*, Journal of the Operational Research Society 35(6): p 499-512.
2. OREDA, Offshore and Onshore Reliability data, Handbooks 2015, 2009, 2002, etc.
3. Procaccia H., Ferton, E. and Procaccia M. *Fiability et maintenance des materiels industriels reparables et non-reparables*. ISBN 978-2-7430-1362-2, Lavoisier 2011
4. H.C. Wels, *Failures and Forced Unavailability of Power Plants*, VGB-B 035, May 2019, ISBN 978-3-96284-165-2 (Print), *-166-9 (eBook)
5. Haugen e.a., *The analysis of failure data in the presence of critical and degraded failures,* Reliability Engineering ad System Safety, 97-107
6. Haugen e.a., *Analysis of OREDA Data for Maintenance Optimisation*, SINTEF Industrial Management
7. *MARS : a software tool for Maintenance Assessment of Repairable Systems*, Franck Corset, Stephane Despréaux, Laurent Doyen and Olivier Gaudoin, Laboratoire Jean Kuntzmann, Grenoble University
8. *Reliability Indicators with KISSY* – VGB Research Project 361 ISBN 978-3-86875-751-4, February 2014
9. VGB-R 115M *Empfehlungen fur die Revision von Dampfturbinen*, second edition 1993, superseded by ISBN: 978-3-86875-890-0 VGB-S-115-00-2015-12-DE, 2016
10. *An approximate Solution to the G-Renewable Equation with Underlying Weibull Distribution*, Yevkin & Krivtsov, IEEE Transactions on Reliability, March 2012
11. Larry H. Crow, *Reliability analysis for complex, repairable systems*, AMSAA Technical Report no. 138, 1975
12. Tijms, *A First Course in Stochastic Models*, 2003, ISBN 471-49881-5
13. R.J. Ferreira e.a., *A Mixed Kijima Model using the Weibull-based Generalized Renewal Processes*, 2015, PLOS ONE.
14. Judea Pearl & Dana Mackenzie, *The Book of Why*, Penguin Books 2018, ISBN 978-0-141-98241-0.

Increasing risk knowledge via different types of transparency for creating an adequate safety culture

Genserik Reniers

Delft University of Technology, The Netherlands, G.L.L.M.E.Reniers@tudelft.nl

Abstract

This talk will discuss the importance of knowledge about risk and safety in terms of different types of transparency, that is, company-company transparency, company-citizen transparency and company-authorities transparency. How transparency and trust relate to each other and how they are key elements for what can be seen as 'true safety' and what are the links with the different types of transparency with the different domains of an organisational safety culture, is thoroughly explained. New ways for truly enhancing and advancing safety with knowledge through transparency are suggested. To this end, the TEAM safety culture model and its three measurable domains are discussed and linked to the different types of transparency: company-authorities transparency relates to the observable domain of safety culture and leads to possible improvement of audited safety; company-citizen transparency links with the (non-observable) perceived domain of safety and leads to the possible enhancement of perceived safety; and company-company transparency will be essential for the (non-observable) motivational domain of safety and results in bettering what can be called 'real safety'. Together, audited safety, perceived safety and real safety, form 'true safety', and will certainly increase safety results in any organisational context if applied with the right knowledge and transparency insights and measures. Very concrete measures will be suggested and expounded for knowledge management and company memory, as well as for further elaborating the needs on the different types of transparency.

See slide presentation in Appendix 1.

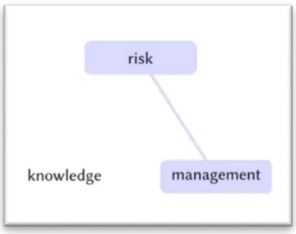
Forum discussion on obstacles to the use of knowledge to manage risks

The forum entitled *Obstacles to the use of knowledge to manage risks* involved a panel discussion, an online poll and a general discussion. The forum aimed to provide an opportunity for transverse discussion on topics related to the seminar, as an input for future work of the project group on Risk, Knowledge and Management.

The forum was chaired by Eric Marsden who also gave a brief introductory speech into the topic, and the panelists were Yves Dien, Sever Paul, Tuuli Tulonen and Sanda Pleslic. A brief summary of the points raised by the panelists and during the forum discussions is given below.

Eric Marsden pointed to a number of questions at the intersection of risk, knowledge and management. In the *link between knowledge and management*, difficulties in sustaining communities of practice and expertise, the effects of fragmentation of organizations (for example due to outsourcing), the perception of safety as a cost centre leading to its positioning at business unit levels, rather than at the corporate level, and the difficulties in decontextualizing safety-relevant information.

In the *link between risk and management*, the difficulties in getting knowledge to decision-makers, then to decision-making, questions of agenda-setting (for example the position of safety experts in the organizational chart which affords insufficient access to decision-makers), and competency issues at the management level, for example inability of board members to understand safety concerns.



In the *link between risk and knowledge*, obstacles include the lack of investment in safety expertise, the poor career paths available to safety experts, lack of a learning culture within organizations, and the difficulties in cultivating a questioning attitude that encourages people to challenge situations and decisions that they feel require further investigation.

Yves Dien identified two obstacles to the use of knowledge for effective risk management:

1. The difference that may exist between management declarations and their decisions concerning priorities and resource allocation. Companies often proclaim that safety is the most important priority, but when compromises between continuing production and reducing risks appear, companies prioritize production. This leads little opportunity use knowledge to improve safety management.
2. The difficulty in challenging outdated scientific knowledge, in particular in identifying risks. Knowledge tends over time to be organizationally absorbed in the form of cultural beliefs, making it difficult to detect and label events that do not fit these embedded beliefs, but which could represent emerging threats to safety.

Sever Paul pointed out that accident investigations often reveal that the direct causes of accidents have not been identified as risks in the organisations' risk assessments. This may be due to lack of risk imagination: people are very good in responding to risks that have realized before, but less clever in imagining threats they have not yet experienced.

Another obstacle to using knowledge to manage risks is not understanding the information we have. Risk assessment is an ongoing project, where information should flow from top

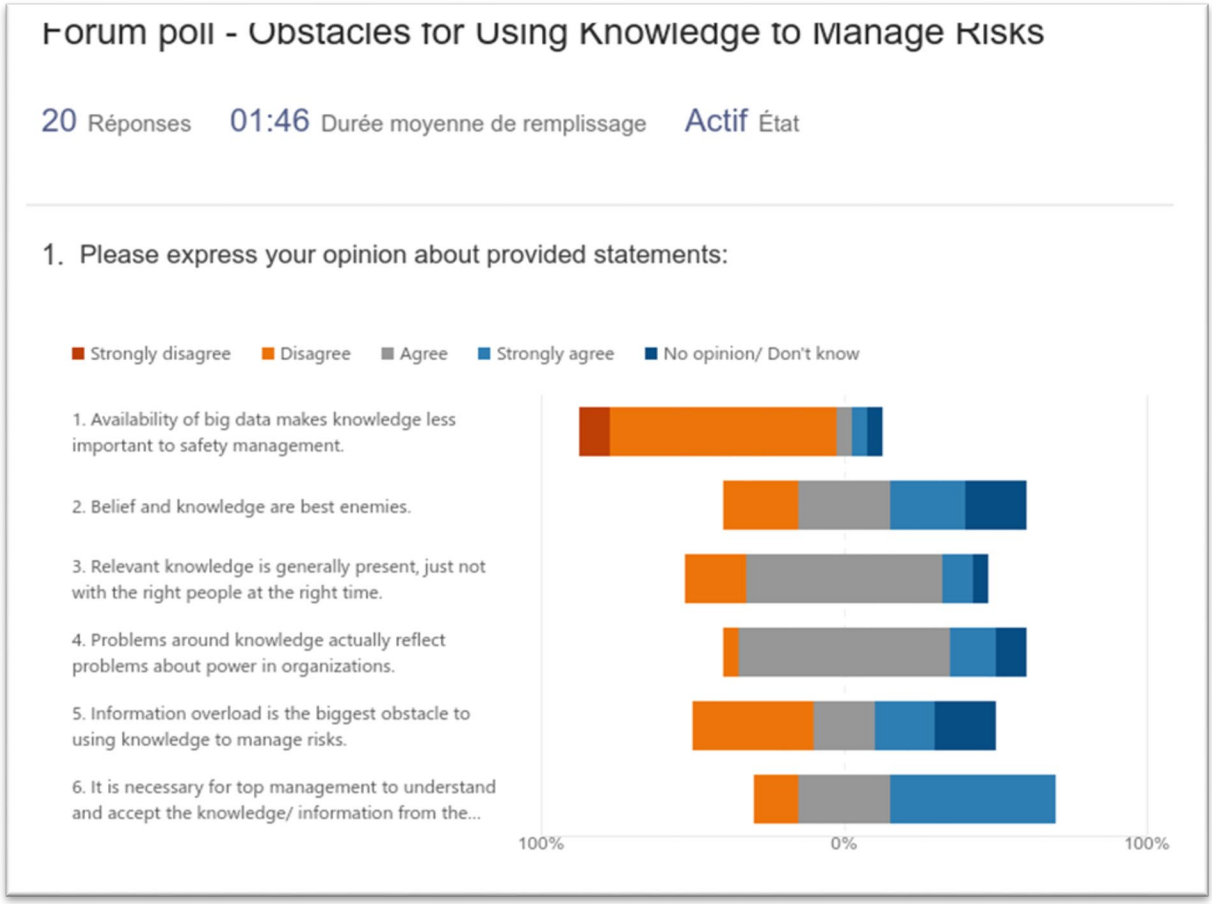
to bottom and from bottom to the top of the organisation. The problem in utilizing the information may be due to the fact that the information is unclear, too tangled, or hard to understand. This is also identified in accident investigation reports. For example, a basic concept such as risk suffers from multiple definitions.

Tuuli Tulonen illustrated the obstacles faced by a safety authority in collecting information and generating knowledge regarding accidents by highlighting the gap between the number of occupational accidents related to electricity reported to the Finnish safety authority, and those reported to insurance companies. The underreporting of these accidents to the safety authority is caused by the voluntary nature of the reporting of the accidents, by lack of awareness of a legal obligation to report, by fear of the authority, and by concerns regarding the extra effort to report versus lack of direct benefits from reporting. The safety authority has little ability to reduce this knowledge gap and its decisions may be affected by biases in the data it collects.

Sanda Pleslic discussed obstacles to the use of knowledge from the viewpoints of organizational culture versus individual behaviour:

- Two very important factors to build organizational culture are *people* and *leadership*. So the *environment and atmosphere* in the company should support the collaboration of people, and leadership should lead the people to find solutions to identified problems. People have to follow *standards and policies*, activities such as knowledge sharing should be *compensated*, and the organizational culture should be based on good *organization and infrastructure*.
- On the other side, individuals are unique and have their own *values, knowledge, experience, expertise and skill*s. Therefore, *teamwork and knowledge sharing* are important, people should be *motivated* to change their behaviour, to follow ideas to manage risks, and to use organizational knowledge as the basis for these activities.

After the panelists' speeches, the seminar participants participated in an online poll, aiming to categorise their opinions on six statements related to the obstacles to effective use of knowledge for risk management. The results of the poll are illustrated below.



As a summary of the poll, one interesting result is related to the second statement on beliefs and knowledge, and whether they are friends or enemies. Here, many of the participants chose "don't know"; the issue can be regarded as quite complex. Another interesting result is that most seminar participants are against the conventional wisdom, believing that big data (and artificial intelligence?) is not the solution to all problems: it does not make knowledge less important. As a third point raised from the results, the seminar participants believe that: top management must understand and accept the knowledge/information from the "front line" to take the necessary safety measures and manage the risk. And vice versa.

The seminar participants raised the following viewpoints during the general discussion period of the forum:

Suggested good practice: a "black book" is a book where you document design problems. There are several incidents that repeat themselves, and a black book will help to prevent the repetition of similar design-related incidents. Major accident reports already have this type of summary of incident causes. A black book can also be maintained as an internal tool for an organisation.

ISO 45001...3 standards tackle occupational health and safety. Is it worthwhile for firms to try to obtain this certification, and what is the role of standards in improving safety? Experience suggests that standardization is useful for small companies to guide their organisational structure and ways of working according to good practice. On the other hand, too much standardization may reduce critical thought about the meaning of what is important and why certain activities are done. In software certification, if you design and manufacture the software according to the specifications, it is a way to check the quality of the design. It should also be noted that the standard may be about safety but from only

a certain viewpoint, e.g. 45001 concentrates on occupational safety but mainly ignores process safety issues, though this limited scope is not always appreciated. Continuous performance improvement is important but it is about people and organizations, and standards are just one tool, and not comprehensive on their own. One-sided usage of a standard may even contribute to accidents.

In addition, the panelist Tuuli Tulonen was asked why, according to her slide, the number of electrical accidents is clearly increasing. Tuuli Tulonen responded that the reason is unknown. This has been discussed, and the only apparent explanation seems to be an increase in the awareness and/or activeness to report. This is supported by the fact that the number of severe accidents has stayed the same, and the increase concerns almost solely those accidents that are reported to have non-severe (0-3 days away from work) consequences.

As a conclusion and summary of the forum as a whole, keywords and phrases that came up during the forum included individual behaviour and organizational culture, environmental conditions that induce collaboration, how to manage risks if you do not understand the information you receive, decision making versus beliefs, risk imagination, knowledge gap, the role of standardization and certification.

List of authors

Appendices

Appendix 1: Slides presentation "Increasing risk knowledge via different types of transparency for creating an adequate safety culture"

Presentation outline

1. Who am I?
2. Types of Safety and types of Risk
3. Understanding the transparency question/problem
4. The transparency problem in a context
5. Ways to deal with the transparency problem
6. Conclusions

Who am I?

- Full Professor TUDelft (+ UA + KULeuven)
- Safety and Security Scientist
- Focus on industries using chemical substances
- Engineering & Technology
- Management & Economics
- Published 30+ books (author + editor)
- Published 250+ articles

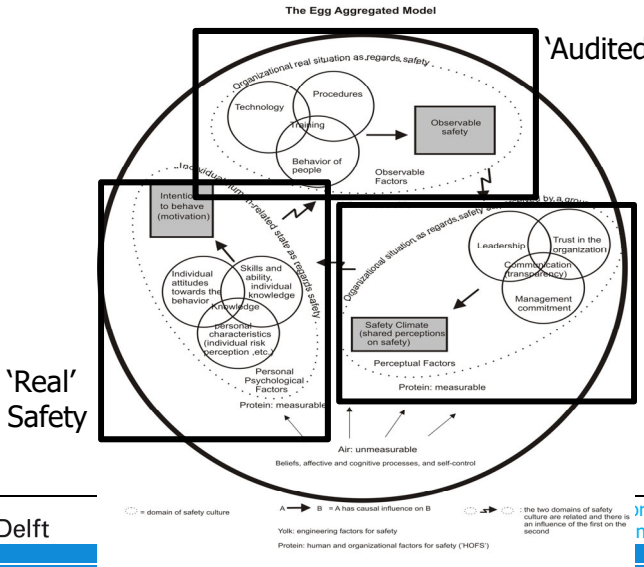
Three types of safety

- 'Real' safety
- 'Audited' safety
- 'Perceived' safety

All three need to be looked at and need to be excellent for **TRUE** SAFETY!!

Focussing on only one or two of the three leads to a sub-optimal situation!

Three types of safety and the TEAM safety culture model, leading to **TRUE safety**



Two types of risks

- Type I : (ordinary) occupational risks – happen a lot, have minor consequences, much info available about these risks, they are independent of the industrial sector
- Type II: (rare) disaster risks – happen rather seldom, (may) have very important consequences, not so much info available about these risks, they are different from industrial sector to sector

Understanding the transparency question/problem ("What?" - Question)

Transparency = communication approach

Different types of transparency/communication:

- Company – authorities transparency
- Company – company transparency
- Company – employee/citizen transparency

Different types of risk communication:

- Pro-active and not linked to specific risk: Communication about risks
- Pro-active and linked to specific risk: Risk communication
- Re-active: Crisis communication

The transparency problem in a context (i)

- **Transparency = means for trust**

(= "(communication) approach for creating trust")

- Trust = goal of transparency;
- **Trust = means for 'Supported safety culture';**

- Safety culture = goal of trust;
- **Supported safety culture = means for 'License to operate';**

- License to operate = goal of '*any organisation*';
- **License to operate = basis for 'Doing business and the ability to make profits';**

- **Doing business and the ability to make profits = the basis for the ability to become and to stay a successful organisation.**

The transparency problem in a context (ii)

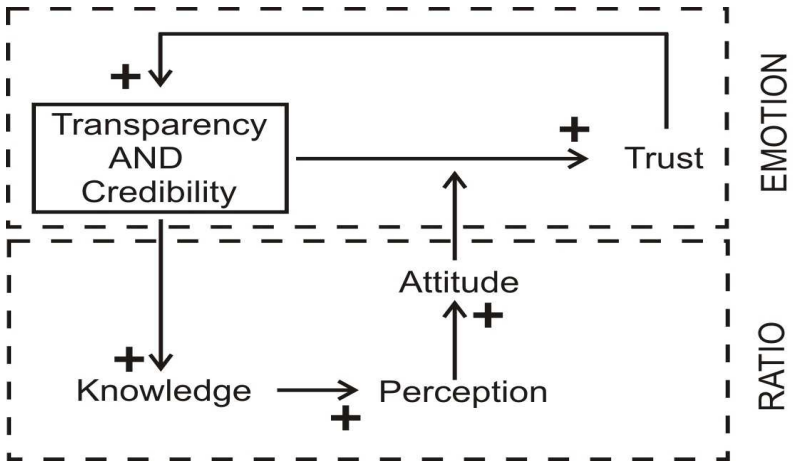
- How does transparency work?

Does a 1-1 causal relationship exist between transparency and trust? No, probably not. Why? Consider the following example:

Aviation: Transparancy: H; Trust: H
Nuclear: Transparency: H; Trust: M to L
Chemicals sector: Transparency: M to H; Trust: L to M

Therefore: **Transparency, but also other factors seem to be important to create trust (complex problem)**

The transparency problem in a context (iii) – Systemic thinking



Ways to deal with the transparency problem ("How?" – question)

- Link between the three types of transparency and the three types of Safety:

- **Company-employee/citizen transparency → 'PERCEIVED safety' improvement**
- **Company-company transparency → 'REAL safety' improvement**
- **Company-authorities transparency → 'AUDITED safety' improvement**

→**'How-question' is about these three types of transparency, and they should be seen as one integrated problem (if you only focus on one or two types, not much will change, it will be a sub-optimization at best)**

Some ways to deal with the **company-employee/citizen transparency** problem

- Enhance trust between companies and employees/citizens by:
- Install a **Counter** for obtaining all kind of safety information for citizens
- Transparency is the **responsibility of industrial parks**, not of individual companies
- Industrial parks take the **initiative to provide risk information** to all their neighboring communities regularly, via meetings as well as via social media and neighbor consultations
- Citizens are informed about the scenarios used for risk assessments within companies belonging to the ind. park, and if they have **comments, suggestions** etc. they are **taken seriously and it is investigated by an independent part of the industrial park**
- Citizens from the surrounding communities are asked to participate in **safety think tanks** for improving safety within the industrial park
- Etc.

→ **'PERCEIVED safety' improvement**

Some ways to deal with the **company-company transparency** problem

- Enhance trust between companies in industrial parks via the stimulation of collaboration, hence:
- **Establish a multi-plant council or a industrial park council**, with part composed of company representatives, and an **independent part**
- Establish pro-active strategic cooperation and improvement by setting up a '**multi-plant safety and security funding**' **budget**
- Establish a dynamic **ind. park database for risk information** of all kind
- Establish an ind. park **database for near-misses**, incidents etc. based on cluster-harmonized accident investigation documents, and dissem. system
- Use company-mixed '**flying risk assessment**' teams and '**flying internal audit**' teams to be deployed in cluster-related plants
- Establish an **ind. park safety management system upgrade** approach
- Establish a '**ind. park safety culture**' and a Joint-learning community
- Etc.

→ **'REAL safety' improvement**

Some ways to deal with the **company-authorities transparency** problem

- Enhance trust between companies and authorities by:
- **Authorities using the cluster council as point of contact** to (more) efficiently plan inspections; e.g. provide access of cluster incident database to inspection services
- **Providing the ind. park council with inspection information** of all companies, so that it may act upon this information (transparency of inspections)
- Make **ind. park audit teams where inspectors are involved** besides company auditors, and change inspectors between ind. parks
- Agreeing upon **what is 'bonafide' and what is 'malafide' behavior** and if needed, **change legislation to avoid any blame culture** in a bonafide setting
- Making sure that **mayors, and by extension politicians, are well informed** about the risks involved in the industrial park activities
- Etc.

→ '**AUDITED safety' improvement**

Conclusions

- '**Trust through transparency' is a complex phenomenon**

- Trust is not given, **trust is earned (credibility is also essential!)**, and that is via transparency as a mediator (this holds for companies, authorities and employees/citizens)
- The different **types of transparency cannot be seen separately**, the solution should be an integrated one **if you *really* want to improve safety in industrial parks**
- Transparency should be accommodated by the accompaying **right/useful legislation, aimed at a just culture**
- **Transparency** doesn't work 'one-way'; it **should come from all sides** (companies, inspection, authorities, employees/citizens)

- **Transparency is intrinsically linked with an excellent safety culture, and also with a longlasting license to operate!**

Wrap-up:

Strategic thinkers fear transparency.

Strategic intellectuals use it to their advantage.

Thank you very much for your attention!

G.L.L.M.E.RENIERS@TUDELFT.NL

Appendix 2: Author biographies

Invited speakers

Tea Bilić Zabric, IAEA, Austria

Ms Bilic leads the Methodology and Services Team, within the Nuclear Knowledge Management Section at the IAEA. 30+ years in nuclear sector. Nuclear industry experience in Nuclear Fuel, Operating Experience, Engineering and Technical fields, Training, Safety Culture and Human Factor across the PWR fleets. Work with governments, regulators, operators, supply chain and R&D organisations across more than 20 countries supporting them in safety and risk assessment, licensing process, independent evaluation, capacity building. Since 2016 working for IAEA on Peer reviews of operating plants and new builds, Managing IAEA/NEA International Reporting System for Operating Experience and Knowledge Management Support to Member States.

Wolfgang Kröger, ETH Zurich, Switzerland

Wolfgang Kröger studied mechanical engineering at the RWTH Aachen and completed his doctorate in 1974. He became full professor of Safety Technology at the ETH Zurich, Department of Mechanical and Process Engineering, by 1990. Before being elected Founding Rector of the International Risk Governance Council (IRGC) in 2003 he headed the nuclear energy and safety research directorate the Swiss Paul Scherer Institute (PSI). After his retirement early 2011 he served as the executive director of the newly established ETH Risk Centre until end of 2014. He has been awarded "Distinguished Affiliate Professor" by the TU Munich and is member of the Swiss Academy of Engineering Sciences (SATW) and heads its topical platform "Autonomous Mobility".

Geert Boosten, Amsterdam University of Applied Sciences, the Netherlands

Geert Boosten has over 32 years of experience in the airport business. Geert is an all-round airport expert with special interest in airport strategy and development, positioning of the airport in the local community (optimizing the added value of the airport), and master planning. Geert has worked for Schiphol Airport and as a consultant for many airports abroad. Nowadays, he is professor Aviation Management at Amsterdam University of Applied Sciences. The Aviation Management research unit focuses on applied research on aviation capacity optimization. Furthermore, he is a board member of DEAC (Dutch Electric Aviation Centre) and a board member of Sustainable Aviation in the Netherlands.

Jan Hayes, Royal Melbourne Institute of Technology (RMIT), Australia

Professor Hayes has 30 years' experience in safety and risk management. Her current activities cover academia, consulting and regulation. She is Program Leader for the social science safety research activities of the Future Fuels CRC and a Board Safety Assurance Advisor for Airservices Australia. Prof Hayes is a former member of the Advisory Board of the National Offshore Petroleum Safety and Environmental Management Authority. Her research interests all connect to organisational accident prevention and include professionalism, expertise, decision making and use of standards.

Professor Hayes holds a Bachelor of Engineering (Adelaide) a Master of Business (Swinburne) and a PhD in Sociology from the Australian National University.

Genserik Reiners, Delft University of Technology, the Netherlands

Genserik Reniers, a Master of Science in chemical engineering and PhD in Applied Economic Sciences, is Full Professor at the Safety and Security Science Group of the Delft University of Technology, in the Netherlands, where he teaches courses related to Risk Analysis and Risk Management. At the University of Antwerp as well as at the KULeuven, both in Belgium, he is also professor lecturing amongst others in Advanced Engineering Risk Management. His main research interests concern the collaboration surrounding safety and security topics and socio-economic optimization within the chemical industry. Amongst many other academic achievements and output, he has published 200+ scientific papers in high-quality academic journals, and has (co-)authored and (co-)edited more than 35 books. He serves as an Editor of the Journal of Loss Prevention in the Process Industries and as an Associate Editor of the Journal 'Safety Science'.

Presenters

Hrabrin Bachev, Institute of Agricultural Economics, Sofia, Bulgaria

Hrabrin Bachev is a Professor at the Institute of Agricultural Economics in Sofia, Bulgaria.

Since 2013 Dr. Bachev has been doing research on Multiple Impacts of Fukushima nuclear disaster on Japanese agriculture, food Industry and agri-food consumption in collaboration with leading experts from Tohoku University, Fukushima University and Tsukuba University.

Nicolas Dechy, IRSN, France

Nicolas Dechy is a specialist in human and organizational factors (HOF) of nuclear safety at IRSN (French National Institute for nuclear safety and radiation protection), since 2010. Graduated as a generalist engineer in 1999, he worked as an expert and researcher at INERIS for ten years. His expertise experiences and research areas are on investigating and learning from accidents from technical aspects to HOF (e.g. Fukushima, Toulouse), emergency response and crisis management (staffing, stress, unexpected), risk analysis, safety and subcontracting management in maintenance in nuclear and petrochemical industrial sectors.

Yves Dien, CHAOS, France

Yves Dien is member of the think tank CHAOS which gathers researchers and practitioners involved in / interested by process safety. His academic background is Social Sciences. He is retired from Électricité de France (EDF) where he had been working for more than 3 decades as a researcher and also as a nuclear advisor for Central and Eastern Europe countries. His main activities at EDF Research & Development Centre were involvement in design and evaluation of the computerized control room for the new nuclear power plant (NPP) series N4 and also of emergency operating procedures for NPPs. He finished his professional career as leader of a project dealing with “Organizational Factors” of industrial accidents, incidents and crises.

Milos Ferjencik, University of Pardubice, Czech

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 2004, he started to work as a teacher of safety engineering at the University of Pardubice. In his research work, he focuses on risk analysis and accident investigations.

Coen van Gulijk, TNO Healty Living, the Netherlands

Coen van Gulijk is senior researcher digital security innovation at TNO Healty Living, professor on the same subject at the University of Huddersfield in England and guest researcher at the Safety and Security Science section of TU Delft. He works on the modernization and digitization of safety (management) systems, on working safely with robots and the safety implications of AI. In this occasion he will discuss the systematic development of a risk control solution for human-machine interaction in the workplace of the future.

Maria Cristina Galassi, EC JRC, Italy

M. Cristina Galassi is a Scientific Project Officer of the Sustainable Transport Unit at the European Commission Joint Research Centre (JRC). She is leading JRC research activities on the safety assessment of Connected and Automated Vehicles, supporting the development of the new EU regulatory framework for the approval of automated driving systems. She studied Aerospace Engineering and received her PhD in Nuclear and Industrial Safety from the University of Pisa.

Eelco Kruizinga, DNV, the Netherlands

Eelco Kruizinga is a senior principal consultant at DNV. He has a background in artificial intelligence and is part of DNV's knowledge management practice. He uses knowledge management tools to help accelerate the energy transition, build communities and provide matchmaking opportunities for project developers and investors. Eelco has delivered knowledge strategy and knowledge risk projects for a variety of industries and types of organisations.

Eric Marsden, FonCSI, France

Eric Marsden is a programme manager at the Foundation for an Industrial Safety Culture (FonCSI), a public-interest research foundation based in France. He holds a PhD in dependable computing. His work at FonCSI concerns the organizational aspects of safety management in high-hazard industry sectors.

Sanda Pleslic, University of Zagreb, Faculty of Electrical Engineering and Computing, Croatia

Sanda Pleslić, PhD, Assist. Prof., University of Zagreb, Faculty of Electrical Engineering and Computing, Dept. of Applied Physics. Mentor at the International School of NKM, Abdus Salam ICTP, Trieste, Italy. Member of: IAEA's international curriculum team for the Nuclear Knowledge Management course; scientific editorial board of the International Journal of NKM. Three IAEA projects in the field of NKM & HRD. Published over 30 papers in journals and conferences in the field of KM.

Chris Rijsdijk, the Netherlands Defence Academy

Chris Rijsdijk is associate professor at the Netherlands Defence Academy. His PhD was on data driven decision support. He continued to work in this field while focusing on maintenance and reliability engineering cases.
To introduce the paper:
As assets increasingly generate data, the potential of data driven decision support is

growing. Still, the causality that a decision maker needs does not necessarily follow from data. This paper will also describe some very simple cases where expert knowledge appeared to be indispensable.

John Stoop, Kindunos, the Netherlands

John Stoop graduated as ana erospace engineer at Delft University of Technology in 1976. He did his PhD on Safety and the Design Process in 1990 and became a professor in Forensic Engineering and Safety Investigation at Lund University in Sweden in 2007. After his retirement in 2016, he was also appointed as a guest professor at Delft University of Technology. His academic work focuses on safety investigation methodology and the role of safety in strategic decision making in the design and development of major infrastructural projects and technological innovation. In parallel with his academic career, he is the owner of Kindunos Safety Consultancy and co-founder of the Partnership Triple ZERO. In this applied context, his focus is on innovation in aviation and the sea going fishing industry and the development of a Good Airmanship 2.0 concept. In the ESReDA working goup, his focus is on ventilation issues regarding the Covid virus and the safety consequences of distinguishing between derivative and disruptive designconcepts.

Zdenko Šimić, EC JRC, the Netherlands

Zdenko Šimić is a senior researcher at the EC Joint Research Centre. He is an adjunct professor at the University of Zagreb and J.J. Strossmayer in Croatia. Focus of his research and expertise is in nuclear power safety assessment and renewable energy source's characterization and utilization. His recent work is about nuclear knowledge management and safety operating experience feedback.

Henk Wels, DNV retiree, the Netherlands

Henk Wels is a senior consultant with over 30 years' experience in assessing the reliability, availability, maintainability and safety of mechanical and electrical systems. His fields of play included power plants, marine engineering, railways and waterways. He is retired now but still loves machines and power plants in special. His relation with power plants started in 1988 when a KEMA (now DNV) project was initiated to gather failure data of Dutch power plants in order to 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. Quantification of the RAM of power plants using failure data allows one to model plants and carry out benchmarking, what-if-studies, predictions for newbuilding configurations, etc. He has had the pleasure after being in newbuilding teams to check realisation against prediction. Key interest is now, besides sailing vessels on model and full scale, the quantification of the relation maintenance – reliability together with DNV.

Zsuzsanna Gyenes, PhD, IChemE Safety Centre, UK

Deputy to the Director of the IChemE Safety Centre with extensive experience in training CEO's of high hazard industrial sites on Process Safety Leadership and Culture, implementing tools and overseeing Process Safety Management systems for industrial sites, reviewing safety reports, advising on risk reduction

and performing on-site inspections. Proven track record of developing guidance documents on Lead Process Safety Metrics, speaking at international conferences and running technical symposiums worldwide. Extensive knowledge of global process safety standards and practices gained working with the world's leading chemical and oil and gas companies across the UK, US, Europe, the Middle East and Australia. Prepares and delivers technical online training materials and webinars on Process Safety Management, Change Management and learnings from major incidents, hazard identification techniques, runaway reactions and facilitated the ISC interactive case studies with extensive worldwide participation.

Hennamari Valkeinen, The Finnish Safety and Chemicals Agency (Tukes), Finland

Hennamari is an electrical engineer with her background strongly in the electrical distribution industry. She works as a Senior Inspector in the Finnish Safety and Chemicals Agency. Her work is to supervise that the Electrical Safety Act, law-based rules and regulations are complied with in the field (both electrical contracting and electrical installations and their maintenance).

Maria Luisa Villani, ENEA Casaccia (Rome), Italy

Maria Luisa is a research scientist at ENEA, the Italian national agency for new technologies, energy and sustainable economic development. She is also adjunct professor at Unimarconi university (Rome) for the course Embedded software engineering. At ENEA, she is member of the Laboratory for the Analysis and Protection of Critical Infrastructures. Her current research interests include ontologies and formal methods for knowledge-based systems in domains such as emergency management/risk assessment. She is currently participating in a Safera research project concerned with collection and formal representation of knowledge for resilience analysis of complex socio-technical systems and a Nato project concerning sensor-based systems for urban security.

Ludwig Benner, Jr., Chemical Engineer, ISAS Fellow, System Safety Society Fellow, PE (Safety, retired)

Benner's career includes industrial, government, academic and consulting experience, primarily in transportation. His industrial responsibilities included design, regulatory approval and operation of chemical transport equipment, and management of truck, rail and aviation fleet operations. His governmental responsibilities included investigations of transportation accidents involving hazardous material in all modes for the National Transportation Safety Board, preparation of special studies, and Chief of its Hazardous Materials Division. His academic experiences include development and presentation of accident investigation, risk management, (MORT) and hazmat emergency response courses. He served on the editorial board for the Journal of Safety Research, INPO's Advisory Council, Chairman of ISASI's Board of Fellows, an elected officer of professional organizations and a Corresponding Member of an ESReDA Project team, among others.
He has been a pioneer in the accident investigation field for more than 45 years. Benner's observations, research and analysis of investigations have yielded more than 100 publications, including the widely referenced Accident Investigation: Multi-Linear Events Sequencing. Mr. Benner developed the investigation concepts and methodology presented in Investigating Accidents with STEP (1987). A library of his publications can be found at www.ludwigbenner.org. and at his pro bono web site, www.iprr.org. His continuing research includes the study of disparate

foundational thinking driving the diversity of accident investigation methods, the study of investigation functions and required competencies, and investigation input data documentation and integration.
Called the "father of hazardous materials emergency response," his hazmat investigations and analyses produced models of how hazmat emergencies progress (GEBMO), emergency responders' decision-making (DECIDE) and Time/Loss Analysis in the 1970s that changed the hazardous materials emergency response paradigm from attack and extinguish to hazmat emergency behavioral and decision models still in use today. When used, responder casualties were essentially eliminated.

Appendix 3: Seminar programme

DAY 1	15	June, Tuesday, 9:00 ÷ 14:50 (Connection link 1)
Opening	**9:00**	Luis Ferreira, former president of ESReDA
	9:05	Franck Wastin, JRC
	9:10	Zdenko Simic, PCC
Invited i	**9:15**	**Tea Bilić Zabric, IAEA Knowledge Management Programmes to Support Organisational Capacity Building; Chair: Tuuli Tulonen**
Break	**9:40**	Short 5 minutes pause.
Session 1	**9:45**	***1st Session: Knowledge for safety I; Chairs: Kaisa Simola, Hrabrin Bachev***
8	9:45	*Agri-food Implications of Fukushima Nuclear Accident - Lesson Learned for Risk Management, Hrabrin Bachev*
10	10:00	*Knowledge management for nuclear energy research and policy - JRC activities in foresight, Z. Šimić, K. Simola, J. Tanarro Colodrón and A. Liessens*
33	10:15	*A method to manage critical knowledge and associated risk, Eeleco Kruizinga, J. Alberts and R. Van Der Spek*
7	10:30	*New Demands on Knowledge Loss Risk Assessment, Sanda Pleslic*
Break	**10:45**	Longer 15 minutes pause.
Invited ii	**11:00**	**Wolfgang Kröeger, Assessing and Managing Reliability and Risk Issues of Autonomous Vehicles: Emerging Practices and Challenges; Chair: Maria Cristina Galassi**
Break	**11:25**	Short 5 minutes pause.
Session 2	**11:30**	***2nd Session: Knowledge for safety II; Chairs: John Stoop, Hrabrin Bachev***
17	11:30	*Non-financial reporting as an instrument for safety risk management, Eric Marsden*
24	11:45	*New approaches for Autonomous Vehicles certification: learning best practices from Nuclear Reactor Safety, M. C. Galassi, B. Ciuffo, M. Sangiorgi, , L. Di Cesare, C. Sollima*
38	12:00	*Getting a GRIP on robot safety with collaborating data-systems, C. Gulijk, W. Steijn, J. van Oosterhout, J. Willemsen, M. Wilms and D. van der Beek*
34	12:15	*Model-based alarms, an approach to reduce the risk of incorrect asset integrity assessments, C. Rijsdijk, W. Sluis and T. Tinga*
Break	**12:30**	Lunch 45 minutes pause.
Invited iii	**13:15**	**Geert Boosten, Transition towards sustainable aviation: do we need new tools to gain insight?; Chair: Eric Marsden**
Break	**13:40**	Short 5 minutes pause.
Session 3	**13:45**	***3rd Session: Knowledge gaps and risk; Chairs: Tuuli Tulonen, Kaisa Simola***
2	13:45	*Disruptive or derivative, that's the question, John Stoop*
18	14:00	*Existing Knowledge in Risk Based Electrical Safety Surveillance, Hennamari Valkeinen and Ville Huurinainen*
15	14:15	*A creative factory of knowledge to support city resilience management, Antonio De Nicola and Maria Luisa Villani*
22	*	*Maximising New Safety knowledge from safety investigations, Ludwig Benner (*paper submitted without presentation)*
	14:30	*Close of the Day 1, PCC Zdenko Simic*
	14:35	*End of the day 1.*
ESReDA	**15:35**	***ESReDA General Assembly meeting***
GA	**16:45**	

DAY 2	**16**	**June, Wednesday, 9:00 ÷ 14:15** (Connection link 2)
Invited iv	**9:00**	**Jan Hayes, Safety knowledge: the challenge of action; Chair: Nicolas Dechy**
Break	**9:25**	Short 5 minutes pause.
Forum	**9:30**	***Obstacles for using Knowledge to manage risk; Chairs: E. Marsden, Y. Dien, T. Tulonen, S. Paul, S. Pleslic***
Break	**10:20**	Short 5 minutes pause.
Session 4	**10:30**	***4th Session: Knowledge and risk management; Chairs: Yves Dien, Zdenko Simic***
3	10:30	*Learning from creeping changes, Zsuzsanna Gyenes*
14	10:45	*Old School or New School, myths or questions?, John Stoop and Sverre Roed-Larssen*
4	11:00	*How Knowledge is Knowledge Enough for Managing Risks?, Yves Dien and Sever Paul*
13	11:15	*Safety-I outdates learning and knowledge from failures and accidents: is it relevant?, N. Dechy, Y. Dien, M. Llory, A. Largier and J.-M. Rousseau*
Break	**11:30**	Longer 10 minutes pause.
Session 5	**11:45**	***5th Session: Knowledge and risk management in industry; Chairs: Zsuzsanna Gyenes, Dan Serbanescu***
5	11:45	*Accident Analysis Benchmarking, Lee Allford and Maureen Wood*
19	12:00	*Practices and Challenges of Risk Management in Small or Medium Enterprises, Miloš Ferjencik*
9	12:15	*On risk management for some complex and highly innovative artefact systems, Dan Serbanescu*
32	12:30	*Application of models for the effectiveness of maintenance on practice failure data from power plants, Hank Wels and Patrick Wolbers*
Break	**12:45**	Lunch 45 minutes pause.
Invited v	**13:30**	**Genserik Reniers, Increasing risk knowledge via different types of transparency for creating an adequate safety culture; Chair: Eric Marsden**
Break	**13:55**	Short 5 minutes pause.
Closing	**14:00**	Zdenko Simic PCC
	14:05	Kaisa Simola, JRC
	14:10	The announcement of the 59th ESReDA seminar
	14:15	Luis Ferreira, former president of ESReDA

Programme Committee and Organisation

Organisations and Chairpersons

Mohamed Eid, ESReDA (European Safety, Reliability & Data Association), www.esreda.org/

Kaisa Simola, **EC JRC** (European Commission Joint Research Centre), ec.europa.eu/jrc/

Program Committee Members

Zdenko Šimić*, EC JRC, NL
Ludi Benner, Starline, USA
Nicolas Dechy, IRSN, FR
Yves Dien, CHAOS, FR
Antonio Felicio, ESReDA, PT
Milos Ferjencik, University of Pardubicze, CZ
John Kingston, NRI Foundation, NL
Paulo Maia, EDP, PT
Eric Marsden, FonCSI, FR
Sever Paul, AGIFER, RO
Sverre Røed-Larsen, SRL HSE, NO
Kaisa Simola, EC JRC, NL
John Stoop, Kindunos, NL
Miodrag Stručić, EC ENER, LX
Tuuli Tulonen, Tukes, FID
Frank Verschueren, Ministry of Labor, BE
Ana Lisa Vetere Arellano, EC JRC, IT
**Technical Programme Committee Chairperson*

Organisation Committee, EC JRC, NL

Zdenko Šimić

Kaisa Simola

Ariane Liessens

Thomas Panagopoulos

About the Seminar

Scope of the seminar

High-risk industries, critical infrastructures, and urban settlements benefit from many decades of experience from risk management and regulation in different domains. Best practices have been formalised, research and development programs have been completed, and workers have been trained to acquire the available knowledge and transfer know-how. Risk analysis helped actors to better know and foresee the systemic risks, while the analysis of events, accidents and crisis have generated hindsight knowledge that remains useful to face the emerging risks and unexpected events.

Both risk management and knowledge management are still developing and maturing theoretically and in practice. While it is easy to see connection between knowledge and risk, they seem to be studied and practiced almost independently by different communities. This seminar is also about exploring existing and potential relations and complementarity between knowledge and risk management.

Exponentially developing knowledge is helping to better face with emerging risks from continuous innovation and increasing complexity. However, even for old systems, the question is "how difficult is it to apply existing knowledge to manage and regulate related risks". Knowledge is mostly applied by people and a large proportion resides in them rather than disembodied sources; individual and collective skills and practices to produce and use knowledge are seldom highlighted. Knowledge remains a broad term that covers many distributed phenomena with various sources (from data and information to expertise), forms (from tacit to explicit), types (from generalized principles to specific cases), dimensions (from individual to social) and is addressed by various scientific disciplines (engineering, ergonomics, management, sociology,…). This likely raises numerous important questions, among them, e.g.:

- What knowledge is required to manage and regulate risks for old and new technologies?
- How to combine knowledge and imagination for foresight in risk assessment and management?
- How to manage knowledge needs in engineering design and optimization for both derivative and disruptive technologies?
- How to best use past knowledge? Could it become obsolete for present and future situations?
- What kind of knowledge is useful to identify and interpret early warning signs?
- How to integrate reported accident/incident investigation data into the knowledge base required to manage and regulate risks for old and new technologies?
- How to use big data and machine learning to complement experts and improve existing knowledge?
- What about real practices at work? -How is knowledge different from knowing? How is knowledge best embedded in actual professional practice?
- Is using knowledge automatic? What artefacts and boundary objects help to establish the links between knowledge, risk and safety and practices?
- Are the characteristics of skills and know-how acquisition and transmission really integrated in the engineering processes and knowledge management processes? How do they integrate memorization issues?
- What is the role of case based learning and how does this vary from the teaching of general principles and theories for risk management and regulation?

- How is knowledge influenced or disturbed by different pressures (production, political, economic, and managerial)? Is there a pressure for knowledge when we speak about risk rationale? How can these pressures be managed?

The 58th ESReDA seminar will be a forum for exploring these and other related questions. We aim to discuss theories, concepts, and experiences of enhancing the use of knowledge for better risk management and governance. Authors are invited to present their research and operational proposals and raise challenges, but also to discuss as well successes and failures in enhancing risk management through better use of risk knowledge. We want to encourage new ideas, scientific papers, conceptual papers, case studies and cross-sectoral and inter-disciplinary research on the theme of challenges and practices for using knowledge in risk management and governance. This seminar will bring together researchers, practitioners, specialists and decision-makers to discuss strategies and practical experiences.

Target groups and domains of application

Papers for the seminar are invited from various stakeholders, from practitioners to researchers (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, renewables) power plants and networks.
- Process industry: oil and gas, chemical and petrochemical facilities, industry 4.0.
- Transport (rail, road, air and maritime): supply and distribution network, operations, emerging such as driverless cars.
- Aerospace industry.
- Critical infrastructure: electricity, water, telecommunications, information systems.
- Public sector and government
- Urban planning and management.

This seminar is aimed at addressing issues, risks (industrial, natural, na-tech…) and threats (malicious, cyber-security, terrorism) met by different industries, critical infrastructures and urban settlements.

Other topics may be included if they fit well within the theme of the seminar and are related to using knowledge to manage risks and threats, such as product safety, food safety, biotechnology, sanitary crisis.

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

- at the following standard number: +32 22999696, or

- by electronic mail via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications
You can download or order free and priced EU publications from EU Bookshop at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

KJ-06-21-130-EN-N

The European Commission's science and knowledge service

Joint Research Centre

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

EU Science, Research and Innovation

EU Science Hub

Publications Office of the European Union

doi:10.2760/443612

ISBN 978-92-76-42383-6