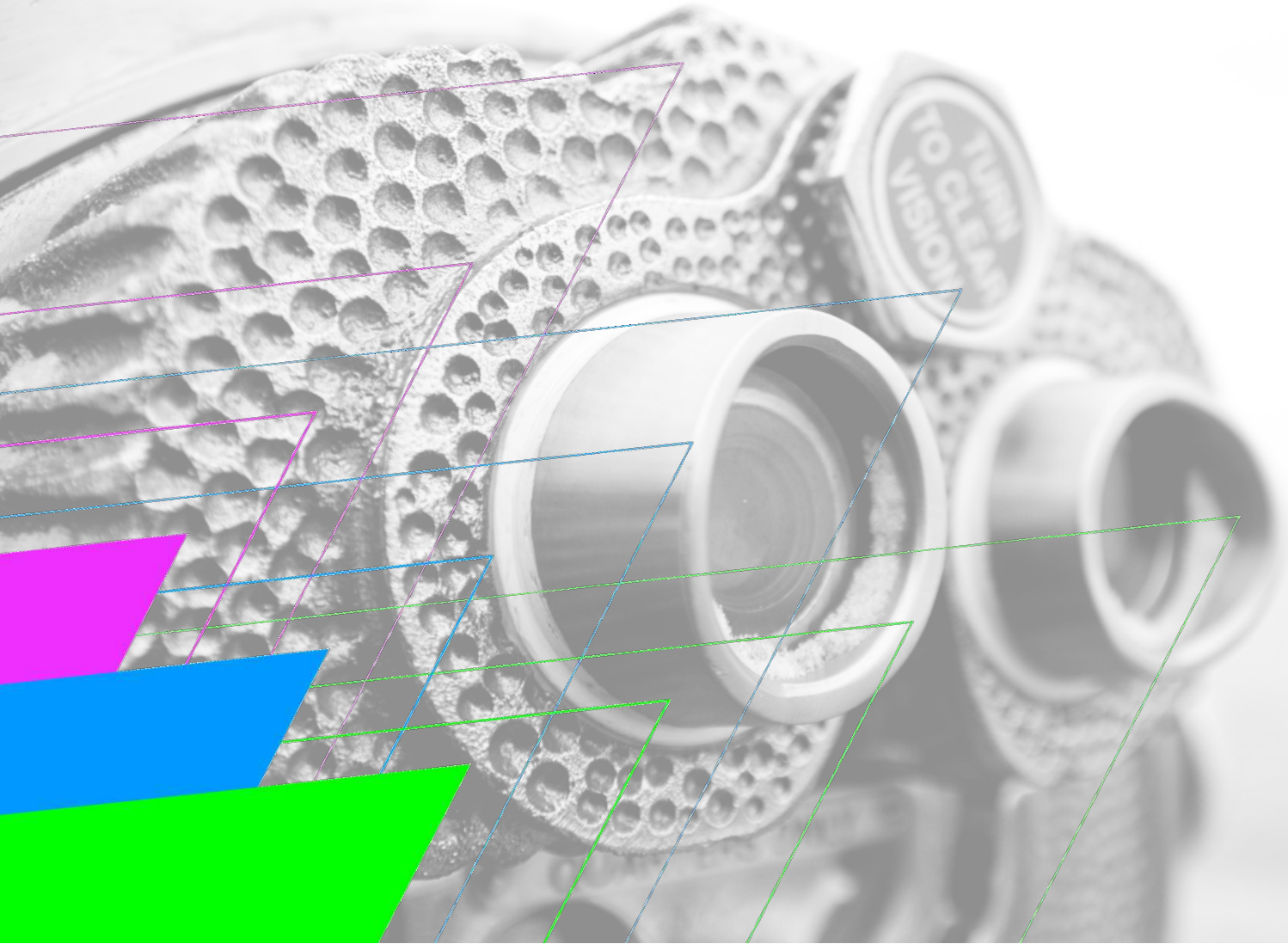
Enhancing Safety: The Challenge of Foresight

ESReDA Project Group *Foresight in Safety*



Chapter 2

Foresight between whistle blowers and resilience

John Stoop

ESReDA
European Safety, Reliability & Data Association

Table of contents

2 Foresight between whistle blowers and resilience

John Stoop, Kindunos, The Netherlands

2.1 Executive summary

In the safety debate emphasis is laid on the need for a paradigm shift:

- From reactive to proactive
- From prescriptive to responsive

and:

- coping with the unanticipated.

In short: the relation between safety and foresight has become a focus of attention in both theory and practice.

Several successive schools of thought can be identified in the socio-organisational and -psychological scientific domain. The role of operational feedback in each of these schools -in particular from the hot seat- is quite different. After a period of exclusion of operator feedback and compulsory compliance with a single actor -managerial- control, a re-integration of operational feedback and multi-actor involvement is emerging. A recognition of 'weak signals' in their systemic context is emerging as a means to cope with system complexity and dynamic interactions. Such recognition acknowledges the value of human variability in task performance, irrespective of blaming, shaming or framing. Such recognition should facilitate foresight on acceptable safe operator performance.

Due to the very nature of socio-technical systems however, foresight historically has been assessed in a wider context than operations variability to reduce uncertainty on unanticipated and unacceptable future performance. New technologies, disruptive designs and innovative concepts demand foresight on a safe performance without the benefits of future operational experience and feedback. From our analysis it is concluded that the old school of Reason and Rasmussen is deficient while the new school of resilience is not yet fully capable of coping with foresight in legacy systems such as aviation.

Economic theories, disruptive designs and innovative technologies, professional airmanship and subject matter expertise are identified as prime change drivers in socio-technical systems of a legacy nature. Such drivers determine the acceptance of schools of thought beyond their own internal rationales or scientific paradigm. Reflecting on the role of foresight it is concluded that new approaches such as resilience engineering have potential but can only applied successfully if they take into account the inherent properties of the legacy of the systems in which they are applied. In resilience engineering, the outsiders role of whistle blowers becomes obsolete as subject matter expertise is acknowledged as input from within the system. Such input is not restricted to individual operational experts, but is also covering independent and qualified safety investigations and inspections during both design and operations on the organisational and institutional levels.

2.2 Introduction

This paper explores the role of resilience engineering contributing to foresight in general. It focuses on feedback from reality and dealing with complexity with respect to reducing uncertainty and predicting future behaviour. It delves into several rationales that have come up in the debate about foresight and resilience engineering and puts these rationales in the context of managing risk and safety. This chapter discusses the role of whistleblowing and resilience in assessing weak signals as indicators for mishaps in matured and established socio-technical domains, referred to as legacy systems. Several competing schools of thought in the socio-psychological domain about human behaviour are explored, contrasting the 'old' school of Reason and Rasmussen with the 'new' school of resilience engineering. Questions are asked about the validity of assumptions and the role of operational feedback in such concepts, in particular regarding whistle blowers.

Moreover, these socio-psychological schools are confronted with technological thinking about foresight, in particular in the aviation domain. Aviation as a legacy sector is based on technological flexibility through the variation-selection process and knowledge management as a driver for innovation. How aviation as a unique socio-technical system has been dealing with uncertainty and foresight is explored in view of acceptance of resilience as a new notion in legacy systems. A revision of resilience engineering, with additional essentials 'initiative' and 'reciprocity' opens up opportunities to accept resilience as an engineering approach in aviation. Such acceptance complies with Good Airmanship principles in this legacy system integrating foresight in system feedback processes on both the individual, organisational and governance level.

2.3 Foresight in context

Over the past few years, a crisis in safety science and risk assessment is proclaimed (Safety Science 2014; Stoop, De Kroes and Hale 2017). In exploring new perspectives, a literature analysis indicated a reconsideration of fundamentals of safety management, risk analysis and risk management (Aven 2016, Pasman and Reniers 2016, Lannoy 2016) and a generic applicability of independent safety investigations (Vuorio et.al. 2017). Simultaneously, changes in a socio-economic context from New Economy to Circular Economy, raise questions about the validity of existing safety notions and paradigms. There is an increasing interest in resilience engineering, recovery from non-normal situations and feedback of operational experience from practitioners. Such interest is aiming to bridge the gap between Work as Done and Work as Imagined (Hollnagel 2011). Evidence Based Interventions in the medical sector are discussed as a prospective approach in processing empirical data, based on best available evidence to justify a remedy, given the state of the art in the disciplines involved. In high tech transport sectors such as aviation, railways and the maritime, forensic engineering is acknowledged as a powerful approach in providing an evidence-based intervention (Strauch 2002, Stoop 2015). Field operators and engineers are concerned with 'weak signals' as indicators for immanent failure. 'Weak signals' are considered a symptom of degradation of a system in its operational phase, exposing their assumptions, simplifications, linearizations and knowledge limitations (Dekker 2011, Dekker and Pruchnicki 2013). Safety theories and notions as developed in the 1960's and 1970's are criticized, based on experience and expertise of practitioners in various domains. Rather than hindsight, foresight should be favoured to predict, analyse and control imminent danger (Roed-Larsen and Stoop 2017).

In essence, the safety foresight debate is about uncertainty and predictability. Foresight is required because disasters are unpredictable and unacceptable, in particular in complex socio-technical systems. Foresight is concerned with questions such as: where to find data, how to interpret the information and how to adapt and change? In this quest, a specific role for whistleblowers is proclaimed. Whistleblowers fulfil a role of interpreters of scarce and uncertain information, based on their professional, domain specific knowledge and experience. How such a role can be conducted however, seems to be dependent on the specific reporting culture and type of feedback in their sector. In the nuclear sector, operational experience feedback is advocated, in the transport sector, independent safety investigations are institutionalized, in the medical sector, resilience engineering is preferred. Although not fully similar to whistle blowing in a strict sense, in the ICT sector hacking and sabotage are predominant as failure coping mechanisms, requiring a specific form of ethical engineering (Van den Hoven 2013).

The debate on feedback from operations has been dealt with from two perspectives:

- Feedback during recovery from major disruptions after an event
- Feedback during normal operations exploring the gap between theory and practice.

In dealing with uncertainty, flexibility, variety, divergence and adaptive potential, allocation of these systemic, dynamic properties can result in two equivalent, primary system configuration options:

- Keep organisations and institutions constant and vary technology. This system configuration is referred to in the Cynefin model of Snowden (2007) as 'complicated'
- Keep technology constant and vary organisational and institutional arrangements. Such a system configuration is referred to in the Cynefin model as 'complex'.

Keeping both technology and organisations constant creates closed, rigid systems without the ability to respond and adapt, while keeping both technology and organisations variable will create chaotic systems lacking effective control options on disruptive technologies.

These options require reflection on two main issues in such a configuration allocation to either man or machine:

- Human performance and the debates between the 'old school' of human factor thinking and the new 'Resilience school' of organisational thinking
- Engineering design in high tech systems and sectors with respect to variability and selecting either derivative or disruptive designs, discriminating adaptation from innovation.

These perspectives, options and configuration allocations will be dealt with in the next paragraphs by analyzing the aviation sector as a case study.

2.4 Unravelling complexity

2.4.1 Competing paradigms

In establishing a new way of thinking in safety, an artificial contrast is frequently created between an 'old' and 'new' view. Over the past decades, debates in safety have been initiated in distinguishing between occupational versus process safety, internal versus external safety, deterministic versus probabilistic thinking, technological versus social safety, safety versus security and Safety I versus Safety II. Such dialectic controversies have not been fruitful due to a seemingly endless variation on the same theme of contrasting and mutually exclusive notions and competition between scientific disciplines and industrial domains.

In their battle for recognition of humanities as a scientific discipline in safety issues, a disdain for technology and engineering design as a scientific activity has been expressed. Over 40 years, phrases were launched such as: 'Safety, too an important matter to be left to engineers' (Booth 1979) or expressed by Edwards in his presentation to the British Airline Pilots Association Technical Symposium advocating a dominant role for human factors in aviation safety (Edwards 1972). This plea coincided with the roll out of the first of a new generation of wide body aircraft, the Boeing 747, representing a leap in technical reliability and safety. Putting safety first as an objective in the Vison Zero philosophy is criticized as a 'shining example of altruism' from the perspective of trading- off safety against other system goals. Claiming zero accidents as a goal should be 'equivalent to the cries of fundamental religious groups on the right path to salvation or paradise' (Hale 2006). In 2017 however, this 'hard and shining ideal' of zero fatal accidents was actually achieved (sic!) by the international community of commercial aviation (CASV 2017). More recently, the right to exist of safety science as an academic discipline as superfluous to psychology and organisational theory was brought up in a Special Issue of Safety Science of August 2014 (Safety Science 2014).

Without achieving consensus and a synthesis that is both theoretically consistent and generically applicable in a new socio-economic and technological context, such debates frustrate progress. Rather than dialectically designing a new variation of safety notions within the same scientific paradigm from a theoretical supply perspective, a demand driven approach could be favoured with a general, basic understanding of complex socio-technical systems and the context in which they operate. Woods suggests to overcome this dialectic stall in the safety debate by defining a new unit of analysis: the man-machine-interface unit, replacing the either man or machine perspective (Woods 2016).

In the academic safety debate two competing paradigms exist: a technological systems engineering perspective and a resilience engineering perspective (Stoop 2015):

- A systems engineering approach provides a new perspective by shifting from a disciplinary to a problem solving oriented approach (Stoop 1990, Stoop 2017/1)
- A resilience engineering approach provides a new paradigm by shifting from a technical, causal approach to a socio-organisational approach with a focus on consequences and recovery from mishap and disaster (Hollnagel et.al. 2011).

As postulated by resilience engineering professionals, the latter approach conflicts with some of the fundamental assumptions which define human factors, ergonomics and socio-organisational theories as applied in industry (Zimmermann et.al. 2011).

They state that Resilience is 'the antithesis of the traditional and still prevailing, human factors and safety paradigm', referred to by Hollnagel as the 'Traditional Safety Perspective' (Zimmerman et.al. 2011). Adhering to this traditional perspective should not meet the needs of ultra-safe, complex modern industries such as aviation and may prevent further progress. Traditional ideas seem to 'remain entrenched in the perspectives and approaches of industry practitioners'. According to Amalberti, matured systems such as commercial aviation may no longer have the flexibility for dramatic or profound change (Amalberti 2001). Adaptations are supposed to remain restricted to the same underlying scientific paradigm. Their adaptation in safety thinking applies an epidemiological model as an extension of the usual sequential models. Although commercial aviation is highly standardised and regulated at an international level, there should be room for interpretation and variation of how people perform, understand and manage their work (Zimmermann et.al. 2011). Zimmermann et al. claim that it was their aim to advocate Resilience Engineering attitudes by the rejection/acceptance of the Traditional Safety perspective. They pose the question whether aviation is ready to make the paradigm shift to Resilience in view of -to their opinion- an apparent much-needed paradigm shift. They intend to 'dispel the myth that aviation is a purely technical domain in which standardisation has eliminated all

variations in how people do their work'. To their opinion, 'flying, controlling and maintaining aircraft involves more than just checklists, radio frequencies and torque settings' (Zimmermann et.al. 2011). Cultural differences between world regions should justify striking a balance between rule following and creativity, in particular in a context of diminishing resources and skills. Coping with adverse situations and conditions should not only advocate resilience on the micro level, because the macro level has stretched assets and resources too far. The system as a whole should favour resilience as a property. Although not yet formulated in terms of resilience, this is exactly what the aviation sector has achieved since the foundation of the International Civil Aviation Organisation (ICAO). Aviation has adopted a system life cycle perspective with continuous adapting, multiple feedback loops across life phases, actors and system levels (Stoop and Kahan 2005).

Zimmermann et al. (2011) notice a paradox in the relationship between Resilience and Safety: 'an unsafe system may be more flexible, more cautious, and may inadvertently foster resilience at the micro level. Similarly, a stable, safe system would have difficulty maintaining flexibility'. They observe a 'natural' tendency to increase production levels when things go right. Increasing production could increase the inherent –volume driven- risks, reduce flexibility and tighten coupling. They state: 'As aviation keeps evolving towards higher levels of standardisation, automation, procedures and stability, we must recognise that this comes at the expense of Resilience' (Holling 1973). Such a strive for operational excellence in order to increase production is driven by New Economy arguments of optimizing production algorithms (Winters 2017).

In proclaiming the myth that aviation is a 'purely technical domain in which standardization has eliminated all variation in how people do their work', social scientists are ignoring the technological and design assumptions and restrictions that are inherent to high tech safety critical systems in which open, global network configurations dominate. Since its conception, ICAO has dedicated its attention and efforts to all aspects of the aviation system performance regarding fees and fares, tariffs and trades (Freer 1986). ICAO has created an encompassing and coherent framework of Annexes to the ICAO Convention since 1951. Eventually, the civil aviation community has achieved a Non-Plus Ultra-Safe state (Amalberti 2001). In aviation, a distributed and delegated responsibility was allocated to the operators under the notion of Good Airmanship to avoid rigidity in their task performance and to enable them to deal with unanticipated situations. To avoid a chaotic system with too many degrees of freedom and disruptions, ICAO chose a strategy with technology as the flywheel for progress, keeping organisational and institutional standardization and harmonization as the prerequisite for access to a high level playing field (Freer 1986).

The desire of Zimmermann et.al. to introduce Resilience in aviation as a paradigm shift raises fundamental questions (Zimmermann 2011):

- Is there a need to make a paradigm shift in safety thinking in aviation?
- Does aviation need resilience to make such a shift?
- How did aviation become so safe in the first place as a Non-Plus Ultra-Safe system?
- What have been the safety achievements in this legacy system?
- Can we identify 'natural' tendencies as change agents for adaptation?
- How can aviation deal with foresight in view of major changes in its socio-economic, geo-political and technological context?
- Which scientific paradigms, theories and notions obstruct a transition to a Next Generation aviation industrial concept and system architecture?

In answering these questions, we elaborate on:

- Feedback loops such as whistle blowers and establishing institutional arrangements
- Change drivers such as economic business models
- Forensic engineering as a knowledge development and diagnostic potential
- System architecture regarding choices about stability, uncertainty, flexibility and trade-offs
- Creative destruction of obsolete constructs such as human error, drift into failure and complexity by replacing them with new constructs such as resilience engineering.

Developments towards resilience as a new concept for safety enhancement have their origin in criticisms on the human performance and organisational management as developed by Reason and Rasmussen. These concepts have allocated a specific role for whistle blowers and their foresight capabilities.

2.4.2 Reason: the traditional approach revisited

In his early work, Reason (2015) focused on the systemic factors underlying what he defined as 'organizational accidents'. Such accidents should differ in sharp

contrast from 'individual accidents' where damaging consequences have limited impact, restricted to their direct environment. In addition, they are supposed to have 'quite different causal pathways' compared to organisational accidents, resulting merely in loss-time injuries. Individual accidents should not have potential for predicting the likelihood of organisational accidents. In his revisited perspective on organisational accidents, Reason shifts the focus of intervention and control potential from management to those who are in the first line of defence: the operators on the spot. They are supposed to have an improved error wisdom and the power to halt the accident trajectory before harm or damage can be done. In his approach, awareness is a pivotal notion. A system safety approach should require the integration of systemic factors –labelled as collective mindfulness- and individual skills – labelled as personal mindfulness-. Political and commercial pressure are considered underlying factors for senior management to underplay in hindsight emergent, obvious threats. Because incompatible goals and organisational shortcomings may lead to disregarding clear warning signals, there should be no unambiguous responsibility for responding to weak signals by senior management. Reason advocates a shared responsibility with line management, and newly defined Safety Duty Holders, as the subject matter experts in assessing risks. All employees should be made aware of their individual safety responsibilities, supported by standards, procedures and job descriptions. A state of chronic unease should be maintained in the safety war (Reason 2015).

Reason allocates a specific responsibility to designers in their "frequent lack of awareness of the capabilities and limitations of the end user" (Reason 2015). According to Reason, many design-induced errors arise because "designers underestimate the extent to which necessary knowledge should be allocated in reality rather than in theory". In his opinion, organisational accidents are assumed to be the result of a mismatch between theory and practice. Training the mental skills of operators on underlying risk awareness are considered hallmarks for High Reliability Organisations. In order to make front-line workers more vigilant, organisational support from management is required. Individual mindfulness of danger needs to be informed, sustained and supported by a collective mindfulness of the operational risks (Reason 2015). This should enhance system resilience, converted to a lasting mental skill of foresight and maintaining situational awareness. By applying mindfulness, as Reason states, it is possible to foresee and recover from an accident. Predefined knowledge, theories and models, generated by safety scientists may even displace or marginalize existing local or system-specific safety knowledge embedded in operational practices. Hiring external safety professionals and experts with well-intended efforts, might even have a detrimental effect (Almklov, Rosness and Storkersen 2014) because their subject matter expertise might dominate managerial expertise. Reason emphasises an indispensable role of error for front-line workers: 'an incident story without mention of error or individual wrong actions is a story without a beginning. Accidents and incidents are inevitable in complex and tightly coupled systems and –hence- they are normal'. Due to hindsight biases and distorting influences in dealing with unexpected events, a narrowing of focus on the systemic factors may induce a 'premature closure on the actions of those at the sharp end', disregarding the balance between individual and collective mindfulness. Local factors distinguish systems that suffer from accidents from those that do not, because local circumstances are necessary and sufficient. Organisational factors are only conditions, not causes and insufficient to bring about the disaster (Reason 2015).

Towards a shared responsibility

Changes in the initial conditions of –complex- systems of systems create difficulties in understanding their behaviour and adaptation to the changes. These changes may incrementally decline a system into disaster by environmental pressure, social processes and unruly technology that normalize increasing risk (Harvey and Stanton 2014). Adapting to such changes throughout the lifetime of systems of systems, may be too short to enable the development of sufficient knowledge and experience to cope with the consequences. While responsibilities for systemic risks remain at an organisational level, regulations are to be developed to shift the official ownership of risk from organisation to the individual. Placing responsibilities at an individual level, is based on the assumption that each individual will do everything within their power to mitigate the risk. This assumption ensures a more rigorous safety management than the old approach of assigning risk at an organisational level, where accountability was more difficult to ascribe (Harvey and Stanton 2014). These insights in assessing risk should explicitly take into account recent incidents, changes to policies, predicted changes in government, predicted lifespan of technical components and national/international economic climates. Assessing a 'Risk-to-Life' comes down to trust in the skills and experiences of the subject matter expert involved in the risk assessment. Such a moral and ethical burden puts high demands on foresight capabilities and their potential role as 'early warning' signalling expert. Such an individual responsibility institutionalizes a role as potential whistle blower for a

subject matter expert and Safety Duty Holder. They are faced with the responsibility to communicate with stakeholders across disciplinary and paradigmatic borders of a technical, social and organisational nature.

2.4.3 Rasmussen's' role on systems modelling

In the domain of human behavior a shift of focus occurred from inferred and uncertain states of mind towards characteristics of human factors that can be framed in generic performance models. Rasmussen takes this shift one step further by proclaiming a distinction between stable conditions of the past, versus a present dynamic society (Rasmussen 1997). The present society is allegedly different by a very fast change of technology, a steadily increasing scale of industrial installations, a rapid development of information and communication technology and an aggressive and competitive environment which influence the incentives of decision makers to use short term financial and survival criteria.

Rasmussen states that modeling can be done by generalizing across systems and their particular hazard sources. Risk management should be modeled by cross-disciplinary studies, considering risk management to be a control problem and serving to represent the control structure involving all levels of society for each particular hazard category. This, he argues, requires a system-oriented approach based on 'functional abstraction rather than structural decomposition'. Therefore, task analysis focused on action sequences and occasional deviation in terms of human errors, should be replaced by a model of behavior shaping mechanisms in terms of work system constraints, boundaries of acceptable performance and subjective criteria guiding adaptation to change (Italics added). System models should be built not by a bottom-up aggregation of models derived from research in the individual disciplines, but top-down, by a systems oriented approach based on control theoretic concepts.

According to Rasmussen, rather than striving to control behavior by fighting deviations, the focus should be on making the boundaries explicit and known. Risk management should provide opportunities to develop coping skills at boundaries. For a particular hazard source, the control structure must be identified, including controllers, their objectives and performance criteria control capability. Information should be available about the actual state of the system. Control over the pace of technology at a societal level created a specific role for the regulator in protecting workers. By stating safety performance objectives, safety becomes just another criterion in multi-criteria decision making and becomes an integrated part of normal operational decision making in a corporate setting. In this way, the safety organization is merged with the line organization. This requires an explicit formulation of value criteria and effective means of communication of values down through society and organizations. The impact of decisions on the objectives and values of all relevant stakeholders are to be adequately and formally considered by a newly introduced notion of 'ethical accounting' (Reason 2015).

A full scale accident then involves simultaneous violations of all the designed defenses. The assumption is that the probability of failure of the defenses individually can and will be verified empirically during operations even if the probability of a stochastic coincidence is extremely low. Monitoring the performance of the staff during work is derived from the system design assumptions, not from empirical evidence from past performance. It therefore should be useful to develop more focused analytical risk management strategies and a classification of hazard sources in order to select a proper management policy and information system. When the anatomy is well bounded by the functional structure of a stable system, then the protection against major accidents can be based on termination of the flow of events after release of the hazard. When particular circumstances are at stake, the basis for protection should be on elimination of the causes of release of the hazard. Design of barriers is only accepted on the basis of a predictive risk analysis demonstrating an acceptable overall risk to society. When the predicted risk has been accepted, the process model, the preconditions, and assumptions of the prediction then become specifications of the parameters of risk management. Preconditions and assumptions must be explicitly stated in a Probabilistic Risk Assessment. In this view, fortunately, Rasmussen states, it is not necessary for this purpose to predict performance of operators and management. Data on human performance in operation, maintenance, and management can be collected during operations and used for a 'live' risk analysis. Thus, predictive risk analysis for operational management should be much simpler than the analysis for a priori acceptance of the design. This also should require far less subject matter expertise. Such performance data should be collected through other sources than accident investigations; incident analysis and expert opinion extraction may compensate for the lack of abundant accident data. According to Rasmussen, the models required to plan effective risk management strategies cannot be developed by integrating the results of horizontally oriented research into different features of hazard sources and systems configurations. Instead, vertical studies of the control

structure are required for well bounded categories of hazard sources, although uniform control strategies would suffice (Rasmussen and Svedung 2000).

In conclusion, in their advocacy for managerial control, Reason and Rasmussen initially have positioned the feedback from design and operators in an outsiders role of whistleblowing. This has only partly been compensated in their revision by introducing a Safety Duty holder and ethical accounting for shop floor workers. The assumptions, limitations and simplifications of Reasons' and Rasmussens' concepts have initiated a debate among sociopsychological and -sociological researchers on a successive concept for operational control and managerial oversight in safety critical systems: the resilience engineering concept.

2.4.4 The fallacy of lack of foresight and management control

Claiming a role for resilience engineering

In his theory, James Reason shifts stability of systems from the individual operator level to the organisational level. Such a stability is shifting from individual control to organisational and hence, managerial control. As stated by Hollnagel (2011), individuals have a natural and uncontrollable variance in behaviour, restricting the ability of higher management order to control individual behaviour as compliant to their desired/imagined pattern.

Resilience is discriminating between organisational control and predetermination of planned tasks and procedures. While organisational control deals with variety in performance (As Done), predetermination is controlled by the specifics of task and mission characteristics (As Imagined). The nature and imagined behaviour of the systems is determined by both complexity/coupling and legacy/change rate of its technology.

Discrepancies and anomalies between performance and the potential role as 'early warning' signalling expert as Imagined and as Done are either intentional deviations -stigmatized as 'violations' from rules and regulations- or unintentional -triggered by internal patterns of slips, lashes or mistakes-. Reason developed a generic and normative categorization of human error, based on individual characteristics (Generic Error Modelling System, GEMS).

In aviation, anomaly management occurs on an organisational level: compliance with predefined performance is organised by compliance to drafting a flight plan, pre-flight preparation and in-flight responses based on scenarios and Standard Operating Procedures. Various modes of operations are foreseen, based on the specifics of flight phases, as the ability to switch between operational modes and balancing stability and manoeuvrability, while maintaining flexibility and adaptivity to variety in cultural and conditional aspects. Operational excellence can be achieved by organisational robustness and managerial control (Winters 2017).

Table 1 Organisational and technological control

	Low technological control	**High technological control**
High organisational control	Fire fighting Medicine	Aviation Nuclear power plants Process industry
Low organisational control	Fishing industry	ICT

There is an increasing role for resilience moving from high organisational control and high predetermination to low organisational control and predetermination, with a shift from proactive to reactive interventions.

Such characterizing of systems by their legacy, high tech nature, change rate and complex/coupled properties identify strategic choices that have to be made in controlling modes of operations of systems: do we select organisational resilience instead of technological resilience (Zimmermann et.al. 2011)? Can we rely on collecting precursor data of what went right as 'proactive' -and consequently superior-instead of investigating what went wrong as a 'reactive' reduction of uncertainty. Or do we need both to comply with the full information paradigm (Klir 1987, 1994)?

Resilience engineering revisited

With the distinction between organisational control and technological control, Zimmermann et.al. (2011) suggest a dilemma in choosing either one of them as the exclusive approach. Such a dilemma however, does not comply with the evolution of a socio-technical nature, such as aviation. Reluctance to accept resilience engineering as the new way forward did pose the question: is the aviation industry ready for resilience (Zimmermann et.al. 2011)? The other question: is resilience engineering ready for the aviation industry as a legacy systems of a Non-Plus Ultra-Safe nature, is as appropriate.

Woods identified several initial fundamentals for resilience engineering from a sociological perspective (Woods 1996). In his inquiry to make progress in resilience engineering thinking, he identifies two additional fundamentals: initiative and reciprocity (Woods 2016, 2019).

In overcoming brittleness in complex systems, he heavily leans on engineering design principles that are basic knowledge in aerospace engineering, in particular the principles of operating envelope and graceful degradation. He coins the fundamentals of a new notion of 'graceful extensibility' to cope with inherent variability and surprise events in a continuous changing world (Woods 2019). In coping with immanent failure, he turns to exploring the design of governance mechanisms and system architecture in order to control long term performance of complex systems, facing multiple cycles of change. In his exploration of initiative and reciprocity, a specific role for communication and interaction across system life phases and system states emerges. Feedback from operational experience to planning and design could be re-integrated in such systems design. This could provide a timely interference with actual system performance, based on foresight and proactiveness. Implicitly, Woods introduces the principle of Good Airmanship for all industrial sectors. Explicitly he acknowledges the value of complementarity across engineering, biological, social and cognitive sciences. This creates opportunities for new thinking of systems design and operations, combining socio-psychological notions with engineering design methodologies. Optimization and control strategies could be developed from an integral systems perspective. In such a perspective, there is ample room for disruptive and innovative thinking, necessitated by changes in environment, economy and risk perception.

2.5 Selecting strategic options

Creating a disruptive change should comply with both economic and technical developments in complex systems as the new context for developing intellectual constructs on dynamic systems behaviour, mobilizing new domains and disciplines. Selecting either organisational or technological change is dictated by the sector and its inherent technology to avoid a drift into chaotic systems.

2.5.1 Economic developments

It is doubtful whether there is a 'natural' tendency to increase production when things are going right. Trade-offs between efficiency and thoroughness in a traditional economy are frequently conducted at the expense of safety. Such trade-offs are realised by increasing flexibility and organisational resilience. Eventually, new opportunities are being created in a New Economy market model for aviation. Subject matter expert(ise) frequently plays the role of whistleblowing in such situations. They are labelled also frequently as 'resistance to change' or 'unconscious cognitive stubbornness' in objecting such change (De Boer 2012). Resistance to change and unconscious cognitive stubbornness may have a positive or negative effect on performance. On one hand they may block sharing of mental models in a team, hindering a shared understanding of the situation. They may create a cognitive lockup in supervisory control tasks, change blindness, cognitive mismatch, fixation and eventually may create accidents in dealing with contradicting signals. On the other hand, they may stimulate vigilance, danger avoidance, stimuli detection and rapid reflection on immanent situations. They may induce less automatic, intuitive behaviour and enhance analytic competences. These notions are considered instrumental attributes of Good Airmanship and Good Seamanship.

New Economy models focus on lean efficient production, eliminating superfluous costs and waste. They do not take into account the consequences of reductions in training costs and subsequent, decay of proficiency and basic flying skills of pilots, as demonstrated by the AF447 disaster.

With respect to economic developments and models, Minsky identified four different phases of driving forces for business models at a macroscopic level of economy (Minsky 1986). :

- Optimizing expectations on a short term with operational trade-offs at a corporate level
- Speculative extrapolations of these expectations in a seemingly stable situation
- Profit expectations on a long term despite stalling investments and erosion of precautionary measures
- Innovative powers of disruptive solutions and creative destruction of old concepts, disclosure of new markets, substantiated by research and development investments to achieve value preservation.

Such disruptive innovations are supported by disclosure of unchartered scientific domains and a new interdisciplinary cooperation (Woods et.al. 2016, Woods 2019, Stoop 2017/3).

In particular in the domain of human decision making, the work of Slovic (2004) on emotions and empathy, Kahneman (2013) on cognition, intuition and perception and Taleb (2008) on rare events and after the fact explanations have drawn attention in the safety science community.

Over the past decade, circular economy principles have been developed. In the environment, zero emission, recycling and closing circular chains are advocated. Sustainability requirements lead to disruptive technologies, new business models and entrepreneurial competences (Berkhout 2000). Systems should be intrinsically safe, while safety is considered a strategic asset in the value chain. Such changes in the socio-economic environment also require disruptive changes in safety thinking and scientific interests. Traditional scientific constructs may run short in explanatory potential (Stoop 2017/2).

According to Troadec, the chairman of the French safety investigation authority BEA, based on the experiences of the Air France AF447 accident, only flight recorder retrieval clarified operating circumstances. Combination of ergonomics of warning designs, training conditions and recurrent training processes DID NOT generate expected behaviour, showing limits of current safety models of human behaviour (Troadec 2013). The AF447 case triggered new and unchartered scientific interests in the man-machine interaction domain, focusing on non-normal situations, intuition, habituation and exploration of the 'startle' effect (Mohrmann et.al. 2015).

2.5.2 Technological developments

With respect to developments in aviation in 1949 at the foundation of ICAO, technology was chosen as the flywheel for progress (Freer 1986). Technological flexibility, variability and technical adaptation were chosen as the prime system change agents (Vincenti 1990) under conditions of tight coupling to an international institutional framework of ICAO standards and operational practices. This choice was evident: during the negotiations at Yalta in 1945 between Roosevelt, Stalin and Churchill on the progress of aviation after the ending of the Second World War, none of the participants was willing to grant primacy to another economic system than their own, being either a Capitalist, Communist or Commonwealth model. The only alternative was to agree on a technological harmonisation and standardization for reasons of interoperability and accessibility of the international aviation network (Freer 1986). Such a flywheel function was readily available for technology after the world war due to the huge R&D and production potential in the aviation industry in the USA, UK and Soviet Union.

This selection of technology as the flywheel for progress demands a very high organisational continuity and stability at the corporate level to introduce a high level performance (safety) playing field. Harmonization was achieved by introducing certification and supranational standardization such as at the sectoral level ICAO Annexes structure for all primary systems functionalities. The role of the State as the prime mover for change was selected as the natural entity for imposing legislation and enforcement on their State owned carriers.

Simultaneously, a very high technological flexibility to adapt to new developments and operational conditions, constraints and specificity was required, introducing a rapid technological development in the context of private corporations, stimulating competition and innovative exploration.

As a consequence, a combination of high technological flexibility –nowadays indicated as 'unruly technology' and low organisational or individual flexibility – nowadays labelled as 'resistance to change' and 'cognitive stubbornness' – are two complementary notions that in conjunction enable both flexibility and reduction of uncertainty in acceptance of technological innovations. The fading role of the State as the leading entity in this development process and the merging of a multitude of aircraft manufacturers into a limited number of leading global companies has called for reflection on the future of aviation. Tensions have arisen with respect to the pace and rate of innovation and organisational adaptation in adapting to new global economic, market and environmental developments. Programmes like Horizon 2050 have been created, facilitating innovative research and development programmes on a sectoral level.

Advocating resilience engineering has not been embraced by the aviation community (Zimmermann 2011). Resistance to organisational change, cognitive stubbornness and underspecification of technological development have been noticed as obstacles for such an acceptance. These phenomena however are functional and complementary in making progress under conditions of minimizing uncertainty. Unruliness is a precondition for technological adaptation and innovation. This property of technology has been recognized already in 1949 with the foundation of ICAO. It has been described by Vincenti as a basic property of aerospace engineering design (Vincenti 1990). To reduce uncertainties in this technological developments and to guarantee a safe operational performance, an

elaborated system has been developed, linking the various phases of the system life cycle. Exchange of knowledge and experience is established by an international agreed system of certification and licensing by modelling, simulation, testing, training and investigations. In due course, the scope expanded from aircraft airworthiness criteria to flight envelope and system viability criteria (Stoop 2017.2).

2.6 Vincenti: the variation selection model

Specifications and regulations are considered properties of control mechanisms at a sectoral high performance level that enable progress. Simultaneously, they create resistance to organisational change and facilitate underspecification of technological development to enable deviation and adaptation. At a sectoral level, harmonization and standardization and sharing design and operational experiences and knowledge are prerequisites to implement this philosophy of technological progress. Foresight on operational behaviour of innovative and disruptive solutions is established by a sophisticated framework of Annexes to the ICAO Agreement by certification, testing and training.

In his analytical study on aerospace engineering methodology, Vincenti indicates the transition from craftsman thinking in experimental progression towards knowledge based design of artefacts and evidence based learning (Vincenti 1990). In the 1930's the empirical and experimental design of aerofoils was gradually replaced by analytical and mathematical understanding of the mechanisms that ruled aerofoil design. Such transition from scientific theory and aerodynamic models as developed by Bernouilli, Navier Stokes, Mach, Schlichting and others towards a knowledge-based design was supported by wind tunnel testing of scale models and flight tests. Scientific research focused on the role of viscosity, transition between laminar and turbulent flow, laminar flow aerofoils and elliptic lift distribution. This application of scientific research in order to reduce uncertainty in the attempts to achieve increased performance created a growth in knowledge. This knowledge was applied directly in the design of new combat aircraft. The British Supermarine Spitfire was designed based on elliptical lift distribution on its wings. The US North American Mustang was designed based on the laminar flow characteristic of its aerofoils. Both aircraft represent a leap in aerodynamic performance. The German Messerschmitt Me 262 marked the transition from piston engine powered to the fighter jet age.

Many technological innovations became available for civil aviation applications in the desire to expand civil aviation to a global network after the war and beyond. In the fourth generation of fighters, the application of IT controlled thrust vectoring enabled the Russian Sukhoi SU-35 to perform the Puchachev Cobra manoeuvre.

2.6.1 Presumptive anomalies

Increased knowledge in turn acts as a driving force to further increase knowledge. As defined by Constant (quote by Vincenti 1990) the phenomenon of 'presumptive anomaly' may stimulate better understanding of the behaviour of an artefact:

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

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

Challenging design assumptions, model simplifications and operational restrictions in examining the validity of this knowledge store have contributed to the growth of design knowledge. Through safety investigations, systemic and knowledge deficiencies were identified, leading to novel safety principles in engineering design. Eventually, this has led to Knowledge Based Engineering and Multidisciplinary Design Optimization as a specific school of aeronautical design thinking (Landman 2010, Torenbeek 2013, Van Tooren 2003).

The search for performance optimization and reduction of uncertainties has created a continuous exploration of design variations and selection of better performing design solutions. This has created generations of commercial and military aircraft designs with similar morphology, configurations and properties. Such solutions can either have a derivative or disruptive nature. Vincenti elaborates on the role of this variation-selection process in the innovation of aerospace design (Vincenti 1990). Developing 'anomalies' should be considered in a historical context of design requirements, gradual changes in the operating context and consequences of design trade-offs.

Although ‘anomalies’ may temporarily deviate from prevailing engineering judgement, specific concerns may force to deviate from this mainstream in exploring innovations.

Foresight on performance has been both tested at the component and subsystem level prospectively by modelling and simulation and retrospectively by flight testing and operational feedback. Such ‘unforesightedness’ comes with balancing gains as well as costs. The outcomes of such a balancing may favour specific design trade-offs, but should be considered in their historical context and operational demands. As speed increased, drag became dominant in the design trade-offs in designing retractable gears. The generalized knowledge that retractable gears were favourable, was the product of an unforesighted variation-selection process and was valid for a specific class of aircraft designs (Vincenti 1990). Similar trade-offs in context can be observed in the design of modern commercial aircraft in balancing weight and fuel consumption versus structural integrity and dynamic stability (Torenbeek 2013).

Flight envelope protection was introduced to refrain the pilot from entering the margins of the operational envelope (De Kroes and Stoop 2012). The application of automation in cockpits has a proven track record of substantial gains in safety, efficiency and accuracy, but comes at a cost of loss of pilot situation awareness in critical situations, increased cognitive task loads and loss of basic flying skills. In aviation, the notion of ‘unforesightedness’ due to trade-offs has been acknowledged on both the component and the systems level.

Warnings against costs in trade-offs in design and operations requires subject matter expertise: an understanding of the relations between technological and socio-organisational aspects is indispensable. Otherwise, an undefined and compiled notion of ‘complexity’ is generated to disguise the ignorance of understanding ‘emergent’ properties –as defined by Rasmussen- and dynamics of ‘complex systems with tight couplings’ –as defined by Perrow-, which might -according to Turner- ‘drift into failure’ due to ‘human error’ –as defined by Reason-. In such a combination of undefined notions, the ability of ‘foresight’ is easily lost, in particular when analysing design trade-offs and feedback from reality by safety investigations have been dismissed from the diagnostic toolkit. Losing specific and context dependent knowledge in safety critical situations resulted in loss of understanding why in a specific case an accident could occur. By losing oversight over the nature of a triggering event, remedial control options are lost as well.

All this occurs in Non-Plus Ultra-Safe systems where Vision Zero has been achieved for the first time ever in large commercial aviation due to the fact that in 2017 no fatalities occurred. Such an achievement has crossed the – according to Amalberti- ‘mythical barrier‘ of the 10-7 , falsifying the assumed asymptotic nature of safety performance and all their derivative assumptions in such systems (Amalberti 2001). It also questions the ambitions of human behavioural sciences to serve as a promising and needed ‘antithesis’ for a ‘conventional’ technological perspective. According to Troadec and Arslanian of the French BEA on the AF 447 case, factual evidence in air safety investigation experiences have demonstrated limitations of present human performance scientific thinking.

Rather than challenging the interpretation of various scientific schools of thinking, a descriptive diagnosis of the nature and dynamics of complex systems should provide insight in their architecture and developments towards a next safety integrity level. Unravelling rather than accepting their complexity becomes of prime importance for achieving Vision Zero and First Time Right principles in a safety for design approach (Stoop 1990).

2.6.2 Complexity, a social construct

In order to control the complexity of this development process, a distinction is necessary between structural complexity (single functional structures) for the benefit of flexibility and functional complexity (multifunctional structures) to enable adaptation. Since combining both types of complexity creates uncontrollable uncertainty in performance variations, limiting any trustworthy foresight of intended behaviour, such a combination of complexities can only be combined in one design at a high cost of increased uncertainty and reduced controllability. A choice should be made for either structural complexity or functional complexity. Additional design properties such as robustness, redundancy, reliability and resilience of technical artefacts to reduce the uncertainty in the design, should be guaranteed throughout the design process and operational life. To the purpose of foresight in aviation safety, various safety design principles were derived from theoretical notions, experimental design evaluations and safety investigations: fail safe, safe life, damage tolerance, crash worthiness, graceful degradation, self-relianceness, situation and mode awareness. In this process, the role of accident investigations and forensic engineering to disclose failure cannot be underestimated (Petroski 1992, Noon 1992, Carper 2001, Barnett 2001, Arslanian 2011).

This design philosophy of preferring technology as the flywheel for progress has been specific for the aviation industry. In the process industry the choices have been different: technology was chosen as a constant, while organisational variety and change was selected as the engine for change for multinational companies without State interference. The context of multinational corporations in a different socio-economic competitive and political climate with the state of technology and its inherent maturity level, differs from the aviation industry. In aviation international cooperation, interoperability, accessibility of global networks and a harmonized and standardized high performance level playing field prevail. This sector has seen the development of several generations of aircraft of similar configuration, performance and operating envelopes.

In the process industry technological development has been different across multinational companies, each with their specific organisational constitution and structures (De Rademaeker et.al. 2014, Pasman and Reniers 2014, Lannoy 2016). Safety is embedded in the organisation rather than in its technology, differentiating between line or staff responsibilities, creating tensions between subject matter expertise resources, foresight capabilities and operational feedback responsibilities. Such differences raise questions about the role of technology, its variability, unruliness and physical boundaries of its production principles and operational processes. But above all, such a choice for organisational change raises questions about the control over organisational change and technological change and vice versa, by either subject matter experts, corporate management, national public governance or supranational institutions. This dilemma between technological and organisational has created a specific role for whistle blowers in an organisation and a choice between top-down or bottom-up initiation of change, including the power relations in an organisation. In the engineering design community, the role of designers and technical experts is quite different, where the role of change agent is fulfilled by inventions and disruptive changes according to the theory of Vincenti's on presumptive anomalies and the variation-selection model. In aviation, the role of pilots as the delegated and distributed responsible expert operators is established by the notion of Good Airmanship, providing feedback from reality while safety investigations provide feedback form anomalies, deficiencies and failure.

2.7 Foresight and whistle blowers, an analysis

2.7.1 Some observations

In describing the development of safety in the aviation sector, technology has been chosen as the flywheel for progress, keeping organisational and institutional arrangements constant. The way technological design alternatives were developed and selected has gone through a process of variation-selection, testing 'anomalies' on their trade-offs by feedback from reality. In such a validation process, a distinct role has been allocated to safety investigations to provide evidence of the system's functioning under normal and non-normal conditions. Reducing uncertainty and variance in operator behaviour has been covered by the notion of Good Airmanship, covering delegated and distributed responsibilities between corporate and individual performance in the global network. The role of design in reducing uncertainty has evolved towards Knowledge Based Design and Value Engineering paradigms.

In order to decide on the consequences, feasibility and acceptability regarding the safety properties of derivative or disruptive solutions, new safety notions have to be developed.

Resilience engineering has presented itself as a serious prospect candidate.

However, 'old school' safety notions, such as human error, drift into failure and normal accidents have dominated the debate over the past decades, accompanied by mathematical and quantitative assessment of risk. Such old school notions have been challenged by sociological theories about 'complexity' and 'unforesightedness', popularized by notions such as 'unknown unknowns' and 'unpredictability'. Such a reductionist approach from a socio-organisational perspective does not pay credit to technological and systemic analytic potential that is practically available in the engineering design community. The link between technology and organisation as two primary and mutually independent characteristics is yet to be reinstalled by adhering to a socio-technical systems approach, acknowledging both hierarchical and network characteristics (Woods 2016, Boosten 2017). In such an approach, both operational performance, organisational arrangements and institutional conditions have to be taken into account for the sake of innovation (Berkhout 2000).

2.7.2 Analysis of assumptions

In proclaiming fundamental shifts in dealing with human behavior, Rasmussen disconnects design from operations, eliminating the feedback and feed forward relations between these two life cycle phases of systems. He replaces a design orientation with an operational orientation, controlled exclusively by corporate management. Systems performance is only to be discovered by deviations from normal and intended performance during operations through 'emergent' behavior. The role of the State is reduced to providing performance standards, criteria and limits. In his construct, there is no room for accident investigations. Minor accidents are considered statistical aberrations from normal, while major accidents are unique events, beyond control and learning. Eliminating safety investigations -providing operational transparency and knowledge on a system's life time behavior- reduces a control perspective from dealing with cause to only dealing with consequences after the release of a hazard. As stated by Perrow (1999), consequences are consequently assumed to be 'normal' to any complex system behavior. By taking this perspective, Rasmussen reduces safety from a sectoral strategic value to a corporate operational constraint. Rasmussen also applies a different definition of 'systems'. In this construct, systems are considered open horizontally organized networks, while in the engineering perspective, a hierarchical dimension prevails at the sectoral control mechanism with a distributed allocation of responsibilities and control mechanisms. Such an engineering perspective does not notice a paradox in almost perfectly safe systems as proclaimed by Amalberti (Amalberti 2001). The reductionist perspective of Rasmussen on systems as horizontal networks and his restriction to a corporate level opens up debates on discrepancies between Work As Imagined (by management) and Work as Done (by operators). This perspective leaves out the assumptions as formulated during the design and the development of the system itself.

The shift in perspective as proclaimed by Reason and Rasmussen also rejected the tools and techniques that were readily available in the engineering domain. Rasmussen suggests to replace the engineering toolkit by tools and techniques from the mathematical domain –QRA in particular-. In validating the applicability of QRA to this managerial construct, frequent criticisms on their assumptions and limitations have been formulated by the QRA and resilience engineering community (Aven 2016). Over time, Reason's and Rasmussen's assumptions proved to be inadequate: later versions of human behavior reinstalled an interest in operational feedback from incidents, Just Culture and High Reliability Organization behavior. A shared responsibility between management and operators is proclaimed, introducing the notion of 'mindfulness' with allocation of a prime responsibility to the shop floor level of performance. The 'ethical accounting' as defined by Rasmussen introduces the phenomenon of Whistleblower. Any impact of decisions on the objectives and values is inevitably normative: they are either undesirable and non-compliant with established ethics in an organization –defining a negative connotation for a whistleblower- or are the ethical responsibility of a corporate employee, -defining individual mindfulness- and contribution to a 'Risk-of Life' assessment of risk.

Accepting any of the newly proposed paradigms as successor of 'old school' –including their obsolete- notions should be accompanied by an assessment of residual risks and side effects.

Such acceptance should not be restricted to the individual level of 'whistle blower' functionality. At the institutional level, safety investigations by independent agencies have seen a global development in the aviation sector. It is a part of the legacy of aviation, supported by forensic engineering and governance as distinct scientific disciplines (Stoop and Dekker 2010).

In its efforts to enhance safety in aviation further, ICAO has drawn up a set of management processes based on the theories of Reason and Rasmussen, that could be adopted by corporate management (SMS) and state safety programs (SSP). This initiative was not to suggest to exclude, discount or downplay other preventive activities. An empirical analysis of Farrier (2017) showed an unintended outcome of the role of safety investigations in aviation. It has become clear that ICAO's various moves to consolidate guidance on SSPs has been to downplay the role of accident investigations in the SMS environment, or even to disconnect them entirely from other preventive processes.

The trend seem to be to discount investigations as a part of the larger preventive process. He concludes that for a variety of reasons, investigations -including their recommendations that result from them- are not always a good fit with each other. Farrier notices inherent tensions between the two philosophies: a focus on what might happen versus what has happened: a desire to consider hazards in the abstract instead of focusing on concrete experiences of actual loss. A focus on Hazards as Imagined versus Hazards as Experienced shift the attention from perceived issues to 'precursors', expecting a higher added value of the latter. A

downplaying of 'reactive' investigations takes place against support for 'proactive' management efforts. In practice, the underlying philosophy of Reason and Rasmussen supports the notion that 'safety culture' has preventive value and costs a lot less than investigations and design based safety impact assessments. Farrier concludes: accident investigations and their recommendations need to be properly baked into the fabric of current and future safety management systems. 'Proactive' outcomes need not be pursued exclusively through 'proactive' sources of data. Safety investigations should form the basis for follow-up inquiries and analysis, while their recommendations should be scrupulously tracked and managed. This is in accordance with the principle of the Full Information Paradigm (Klir 1987) that feedback and feed forward should be combined to achieve full information on systems behaviour.

Farrier states (2017): Introducing new concepts such as Safety Management Systems and State Safety Programs puts two principles of safety management and safety investigations in opposition instead of leveraging their respective advantages. Such opposition pits the active against the passive, the hard work of investigation and analysis against the easy tasks of collecting and recording. Both have their place in the aviation safety professionals' toolkit, and neither should be disregarded or discounted (Farrier 2017). In discarding safety investigations from the analytical toolkit, such investigations are expelled from foresight from within a system and forced into a role of adversary whistle blowers (Vuorio et.al. 2017, Wilson and Straker 2018).

Such an exorcizing also has consequences on the investigative functionality of the capability to change systems. This introduces two problems (Karanikas, Roelen and Piric 2018).

First, the interpretation of investigative findings is submitted to differences in perspectives between investigators and safety managers. Investigation reports are consensus documents on the investigative reconstruction of an event. A transition from what happened to how to deal with the consequences has to take place by analytic interpretation and adaptive intervention on those investigative findings. Such a transition depends on the capabilities, responsibilities, resources, response capabilities and intervention strategies of each of the stakeholders in the safety enhancement process.

Second, such an intervention strategy lacks procedures for transforming drafting investigative recommendations into incorporating these findings in a safety management system in a specific corporate, stakeholders and governance context.

2.8 Discussion

In making an inventory and analysis of the role of whistle blowers in foresight various scientific opinions about uncertainty, variety, flexibility and controllability emerge. There are different perspective with respect to how to maintain control over complexity of socio-technical systems.

2.8.1 Old school of thinking

'Old school' human factor thinking has become deficient: it contains a normative opinion about human performance due to 'human error', has little predictive potential due to an unnoticed 'drift into failure' and has no control over consequences due to 'normal accidents'. There is a wilful decline of cause in favour of consequences. The rejection of accident investigations as a source of information deprives the concept from operational feedback. Foresight should be provided by incidents, early warnings and whistle blowers. While a first version claims managerial control responsibility over the system performance, a revisited version shifts responsibilities back to front line operators and designers, demanding a permanent awareness and mindfulness to predict, to cope and to anticipate disaster. Managerial responsibilities are reduced to only 'conditional' factors, replacing safety as a sectoral, strategic value.

Warnings against costs in trade-offs in design and operations requires subject matter expertise: an understanding of the relations between technological and socio-organisational aspects is indispensable. Otherwise, an undefined and compiled notion of 'complexity' is generated to disguise the ignorance of understanding 'emergent' properties –as defined by Rasmussen- and dynamics of 'complex systems with tight couplings' –as defined by Perrow-, which might -according to Turner- 'drift into failure' due to 'human error' –as defined by Reason-. On the instrumental level, safety oversight was replaced by a Safety Case approach as the coping mechanism for management over emerging risks.

In their claim for exclusive control over organisational safety performance, oversight was replaced by a shared but undefined responsibility to evade liability and accountability (Koivisto et.al. 2009)

In such a combination of undefined notions, the ability of 'foresight' is easily lost, in particular when analysing design trade-offs and feedback from reality by safety investigations have been dismissed from the diagnostic toolkit. Such reframing of the theoretical concept of foresight and uncertainty in socio-organisational terms fitted in quite well with the New Economy principles that were favoured in the 1990's by the UK government (Martin 201, Stoop 2017.2). Consequently, operational safety feedback warning systems -such as Good Airmanship and Seamanship in aviation and maritime- could not be reconciled with such exclusive corporate management responsibilities. For subject matter experts, an antagonistic role emerged as a Whistle Blower for early warnings of immanent systemic mishaps.

Losing specific and context dependent knowledge in safety critical situations on the operational level resulted in loss of understanding why in a specific case an accident could occur. By losing oversight over the nature of a triggering event, remedial control options are lost as well.

2.8.2 New school of thinking

The 'new school' thinking in human factors claims a necessary paradigm shift but still focuses primarily on consequences instead of causes, on operations instead of design and prefers to analyse the positive rather than the negative. They apply a multi-actor approach and take a non-normative perspective in an operational environment. The emphasis is on organisational flexibility, irresponsive of technology, legacy and socio-economic context of the systems under scrutiny. This school does not (yet) reinstall a highly necessary relation with technology, engineering design and system theory as fundamental characteristics of socio-technical systems.

Consequently, their plea for adhering to resilience may favour recognition of their discipline and perspective, but may not fulfil the needs of highly elaborated and matured industrial legacy sectors such as aviation.

The needs of such sectors and systems are dictated by their specifics and operational context. Rules of a higher hierarchical order, economic market mechanisms and control strategies at the level of system architecture and configuration, public governance, economic and business models and social culture prevail.

Advocating resilience without taking into account such a context and hierarchy may even jeopardize the goals of such legacy systems in disregarding strategic decisions and choices made in the past. These strategic decisions have been successfully applied in aviation by avoiding slipping complex systems into chaotic states, achieving an unprecedented non-plus ultra-safe performance level. In aviation, a high organisational and institutional stability combined with technological change has accommodated permanent economic growth, adaptation to new business requirements and societal constraints. Institutional arrangements were made at the sectoral level such as establishing ICAO. Selecting technology as the flywheel of progress and independent investigations at a State level proved feedback from reality, combined with delegated responsibilities to the cockpit crew by Good Airmanship principles (McCall 2017). Such Good Airmanship principles are derived from the maritime history, where a very open operating environment forced to comply with Good Seamanship and standardized operating procedures to survive unexpected situations. The very high rate of diversity and open operating environment did not allow room for variation and interpretation, but adaptation to the margins of a physical operating envelope in non-normal situations.

2.9 Conclusion

The debate about applicability of resilience has brought about the need to have foresight on future performance and stability in a dynamic operational environment, relative to the 'old school' of safety thinking (Zimmermann et.al. 2011). For aviation however, there is no need per se for proselytizing to a new belief of Resilience. A more pragmatic approach of incorporating useful notions in the needs of the sector prevail. Taking both technological and organisational variety on board may jeopardize the overall stability of the sector and threaten the present non-plus ultra-safety performance of the sector. Creative destruction of old paradigms is a necessary step towards innovation but is a serious risk to the sector in a phase of expanding capacity and growth combined with developing into a next generation of aircraft, airports and traffic management systems. There is no 'natural tendency' towards increased productivity, but as Minsky has shown, socio-economical market mechanisms and societal developments of a higher order dictate change. A chaotic system may emerge from such uncontrolled series of changes if technological and organisational configurations are made flexible

simultaneously. Such a transition from complex to chaotic also changes the role of subject matter experts as professional safety assessors into whistle blowers and restricts the ability to incorporate their foresight during such changes. Although Reason and Rasmussen have revised their concepts, fundamental deficiencies have not been addressed (Reason 2015). Advocating new concepts as such to accommodate the enhancement of safety during changes is a valuable and necessary plea. There are some valid hesitations in the aviation community to embrace resilience engineering. Aviation may 'drift into failure' by disrupting the architecture of the sector too much, not only on the safety aspects. Releasing organisational variety may cause stagnation of technological innovation by emphasizing legal liability and accountability to failure as unforeseen consequences. Recent British legislation on Corporate Manslaughter and Corporate Homicide has aggravated the legal liability situation after the Concorde crash in July 2000 by introducing massive repercussions for manufacturers after failure of their products. There is an unexplored relation between Resilience and Safety. In such a context, the role and position of whistle blowers is undefined.

Foresight is about reducing uncertainty and predicting future performance. New approaches, theories and notions are still open and their desirability, feasibility and applicability is still undetermined. The future role of the State, increase in automation, security, sustainability and circular economy principles are not yet fully explored, let alone validated regarding their consequences. There are no Golden Bullets in enhancing safety in such developments.

Revising resilience engineering by adding two fundamentals -initiative and reciprocity- may create a basis for cross-disciplinary participation, communication and commitment. This could make the outsiders role of whistle blowers obsolete and could reinstall their role as subject matter experts from within the system. Such a transition poses challenges on creating a shared repository of expertise, experiences and knowledge management, combining feedback and feed forward loops to design and operations of complex systems. As such, it may benefit foresight in safety by identifying early warnings of system degradation.

2.10 References

Almklov P., Rosness R. and Storkersen K., 2014. When safety science meets the practitioners: Does safety science contribute to marginalization of practical knowledge? Safety Science 67 (2014) 25-36

Amalberti R., 2001. The paradoxes of almost totally safe transportation systems. Safety Science 37, p 109-126

Arslanian P.L., 2011. Acknowledgement speech ISASI's Jerome Lederer Award 2011. ISASI Forum, October-December 2011 p 12-13

Aven T., 2016. Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational research 253 (2016) 1-13

Barnett P., 2001. Ethics in Forensic Science. Professional Standards for the Practice of Criminalistics. Protocols in Forensic Science Series. CRC Press

Berkhout G., 2000. The Dynamic Role of Knowledge in Innovation. The Netherlands Research School for Transport, Infrastructure and Logistics TRAIL. June 2000

Boosten G., 2017. The (Congested) City in the Sky. The capacity game: finding ways to unlock aviation capacity. Inaugural Lecture October 2017. Amsterdam University of Applied Sciences. Aviation Academy.

Booth R., 1979. Safety: too important a matter to be left to the engineers? Inaugural lecture Aston University, 22 February 1979.

Çarper K., 2001. Forensic Engineering. Second Edition. CRC Press LLC

CASV, 2017. Civil Aviation Safety Review 2017.

De Boer R.J., 2012. Seneca's error: An Affective Model of Cognitive Resistance. Doctoral Thesis, Delft University of Technology, 7th May 2012.

De Kroes J. and Stoop J., 2012. Stall shield devices, an innovative approach to stall prevention? Air Transport and Operations Symposium 18-20 June 2012, Delft University of Technology

De Rademaeker E., Pasman H. and Fabiano B., 2014. A review from the past, present and future of the European Loss Prevention and Safety Promotion in the Process Industry. Process Safety and Environmental protection, July 2014

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

Dekker S. and Pruchnicki S., 2013. Drifting into failure: theorizing the dynamics of disaster incubation. Theoretical Issues in Ergonomic Sciences, 2013. http;//dx.doi.org/10.1080/1463922X.2013.856495

Edwards E., 1972. Man and Machine: Systems for Safety. Proc. British Airline Pilots Association Technical Symposium, British Airline Pilot Association, London, 21-36

Farrier T.A., 2017. Investigations, recommendations and safety management systems. MO3763 Senior Safety Analyst JMA Solutions, LLC, ISASI Forum June 29, 2017

Freer D., 1986. Chicago Conference 1944. Special Series ICAO Bulletin 41. http://www.icao. Int/publications/Pages/ICAO-Journal aspx

Hale A., 2006. Method in your madness: System in your safety. Valedictory lecture Andrew Hale, Delft University of technology 15 September 2006.

Harvey C. and Stanton N., 2014. Safety in System-of Systems: ten key challenges. Safety Science 70 (2014) 358-366

Holling C., 1973. Resilience and stability of ecological systems. Annual Review of Ecology and Systematics. Vol 4 (1973) p 1-23

Hollnagel E., 2011. Resilience Engineering in Practice. A Guidebook, edited by Erik Hollnagel, Jean Paries, David Woods and John Wreathall. Ashgate Studies in resilience Engineering

Kahneman D., 2013. Thinking, Fast and Slow. Farrar, Straus & Giroux Inc

Karanikas N., Roelen A. and Piric S., 2018. Design, scope and focus of safety recommendations: results from aviation safety investigations. Policy and Practice in Health and Safety. ISSN 1477-3996 (Print) 1477-4003 http://www.tandfonline.com/loi/tphs20

Klir G., 1987. The role of methodological paradigms in system design. Dept. of Science. Thomas J. Watson School of Engineering. State University of New York at Binghamton. New York

Klir G., 1994. On the Alleged Superiority of Probabilistic Representation of Uncertainty. IEEE transactions of fuzzy systems. Vol 2, no 1 Febr. 1994

Koivisto R., Wesberg N., Eerola A., Ahlqvist T., Kivisaari S., Myllyoja J. and Halonen M., 2009. Integrating future-oriented technology analysis and risk assessment methodologies. Tchnological Forecasting & Social Change 76 (2009) 1163-1176

Landman Q., 2010. Risk assessment in preliminary Aircraft Design Using Bayesian Networks and Knowledge Based Engineering. Literature report. Delft University of Technology

Lannoy A., 2016. Risk Management, safety and dependability: looking back from 1990 to 2015, which future? 51st ESReDA Seminar on Maintenance and Life Cycle Assessment of Structures and Industrial Systems. October 20-21, 2016, Clermont-Ferrand, France

Martin B. 2010. The origins of the concept of 'foresight' in science and technology: An insider's perspective. Technological Forecasting & Social Change 77 (2010) 1438-1447

McCall J., 2017. Modern day heroes: a multiple case study of how successful flight crew and air traffic control coordination helped prevent disaster. International Journal of Current Research Vol 9, Issue 11, pp. 61268-61275, November 2017

Minsky H., 1986. Stabilizing an Unstable Economy. McGraw-Hill Companies

Mohrmann F., Lemmers A. and Stoop J., 2015. Investigating Flight crew Recovery capabilities from System Failures in Highly Automated Fourth Generation Aircraft. Journal for Aviation Psychology and Applied Human factors.

Noon R., 1992. Introduction to Forensic Engineering. The forensic library. CRC Press inc.

Pasman H. and Reniers G., 2014. Past, present and future of Quantitative Risk Assessment (QRA) and the incentive it obtained from Land-Use Planning (LUP). Journal of Loss prevention in the Process Industry 28 (2014) 209.

Perrow C., 1999. Normal Accidents. Living with High Risk Technologies. Princeton University Press.

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

Rasmussen J., 1997. Risk management in a dynamic society: a modelling problem Safety science Vol 27, No2/3, pp 183-213, 1997

Reason J., 2015. Organizational Accidents Revisited. CRC Press Book

Roed-Larsen S. and Stoop J., 2017. Uncertain future. Unsafe future? 53th ESReDA Seminar. Enhancing Safety: the Challenge of Foresight. November 14 - 15, European Joint Research Centre, Ispra Italy

Safety Science, 2014. Special Issue on the foundations of safety science. Vol 67, August 2014, pp 1-70

Slovic P., Finucane M., Peters E. and MacGregor D., 2004. Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk and rationality. Risk Analysis, Vol 24, no 2, 2004

Snowden D., 2007. The origins of Cynefin. Cognitive Edge Pte Ltd. www.cognitive-edge.com

Stoop J., 1990. Safety and the Design Process. Doctoral Thesis Delft University of Technology, April 1990

Stoop J. and Kahan J.P., 2005. Flying is the safest way to travel: How aviation was a pioneer in independent accident investigation. European Journal of Transport and Infrastructure Research, 5, no. 2 (2005), pp. 115-128

Stoop J., 2015. Challenges to the Investigation of occurrences. Concepts and Confusion, Metaphors, Models and Methods. Side Document of the ESReDA Project group Dynamic Learning from Accident Investigation. January 2015

Stoop J., De Kroes J. and Hale R., 2017. Safety Science, a founding fathers' retrospection. Safety Science 94 (2017) 103-115

Stoop J., 2017/1. Resilience for Engineers. 7th Resilience Engineering Association Symposium, Poised to adapt. Enacting resilience potential through design, governance and organisations. 26-29 June Liege, Belgium

Stoop J., 2017/2. Drift into failure, an obsolete construct. Second International Cross-industry Safety Conference. Work as Imagined – Work as Done, Balancing Rule and Reality. 1-3 November 2017, University of Applied Science, Aviation Academy Amsterdam

Stoop J., 2017/3. How did aviation become so safe, and beyond? 53th ESRedA and EU/JRC Seminar. Enhancing Safety, the Challenge of Foresight. 14-15 November 2017, Ispra Italy

Strauch B., 2002. Investigating Human Error. Incidents, Accidents and Complex Systems. Ashgate

Taleb N., 2008. The Black Swan. The Impact of the Highly Improbable. Penquin Books Ltd

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

Van den Hoven J., 2013. Value Sensitive Design and Responsible Innovation. Wiley Online Library. https://doi.org/10.1002/9781118551424.ch4

Van Tooren M., 2003, Sustainable Knowledge Growth. Inaugural Lecture Delft University of Technology March 5th 2003, the Netherlands

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

Vuorio A., Stoop J. and Johnson C., 2017. The need to Establish Consistent International Safety Investigation Guidelines for the Chemical Industries. Safety Science 95, pp. 62-74. (doi:10.1016/j.ssci.2017.02.003)

Wilson K. and Straker D., 2018. Fiction versus reality: The Impact of Hollywood on Accident Investigation. ISASI Forum, Oct-Dec 2018. P 24-26

Winters B., 2017. How to manage safety based on operational excellence principles? A case study at KLM Royal Dutch Airlines. MSc Thesis Delft University of Technology

Woods D., Patterson E., Corban J. and Watts J., 1996. Bridging the gap between user-centered intentions and actual design practice. Human Factors and Ergonomics Society Conference 40th Annual Meeting 1996.

Woods D., 2019. Essentials of resilience, 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

This chapter is extracted from the final technical report of the ESReDA Project Group *Foresight in Safety*. The full report is freely downloadable from the ESReDA web site and from the EU Joint Research Centre publications repository.

Bibliographic identifiers for the full report are indicated below.

PDF	ISBN 978-92-76-25189-7	ISSN 1831-9424	doi: 10.2760/814452	KJ-NA-30441-EN-N
Print	ISBN 978-92-76-25188-0	ISSN 1018-5593	doi: 10.2760/382517	KJ-NA-30441-EN-C

How to **cite this report**: ESReDA Project Group Foresight in Safety, *Enhancing Safety: The Challenge of Foresight*, EUR 30441 EN, Publications Office of the European Union, Luxembourg, 2020. ISBN 978-92-76-25189-7, doi: 10.2760/814452, JRC122252.

"Enhancing Safety: The Challenge of Foresight"

Edited by the ESReDA Project Group *Foresight in Safety*.

ESReDA
European Safety, Reliability & Data Association