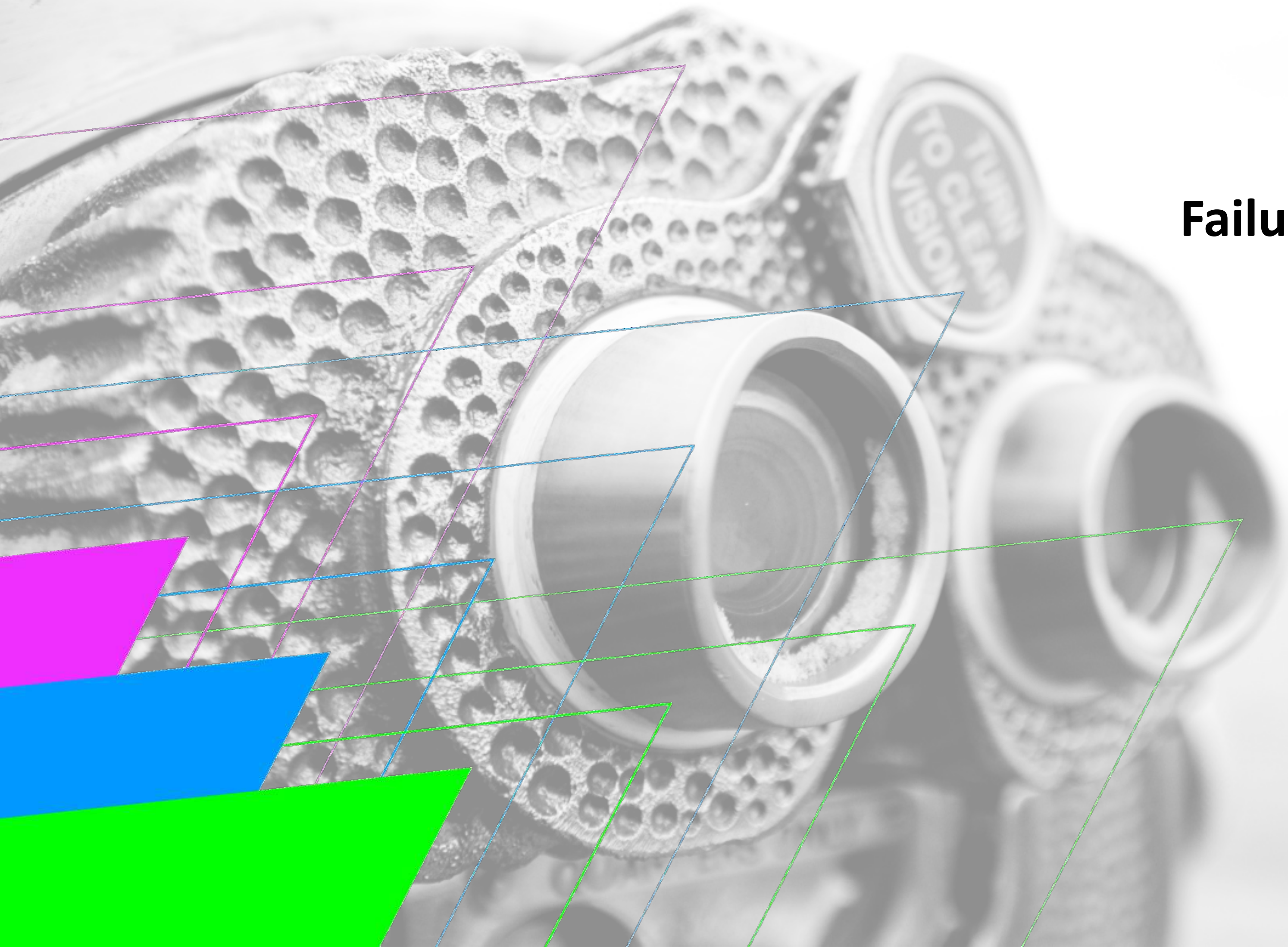
Enhancing Safety: The Challenge of Foresight

ESReDA Project Group *Foresight in Safety*

Chapter 3

Failures of Foresight in Safety: Fantasy Risk Analysis and Blindness



Nicolas Dechy
Yves Dien
Jan Hayes
Nicola Paltrinieri

ESReDA
European Safety, Reliability & Data Association

Table of contents

3 Failures of Foresight in Safety: Fantasy Risk Analysis and Blindness

Nicolas Dechy, Institut de radioprotection et de sûreté nucléaire (IRSN), France,
Yves Dien, Collectif heuristique pour l'analyse organisationnelle de sécurité (CHAOS), France,
Jan Hayes, RMIT University, Australia,
Nicola Paltrinieri, Norges teknisk naturvitenskapelige universitet (NTNU), Norway.

3.1 Executive summary

In order to foster the continuing debate about the best strategies to enhance foresight in safety, the aim of this chapter is to characterise some of the failures to foresee negative outcomes from a safety point of view. The approach followed is to review the lessons that should be learned from negative event, especially the accidents, across industrial sectors. It will enable some typical patterns to be identified that explain why companies and their regulators have recurring difficulties to anticipate risk related scenarios and accidents.

One such recurring theme is the inability to make the right assumptions when risk analyses are performed. It shows that some fantasy planning may occur especially when addressing major risk assessments. Seeking to identify a worst-case scenario is a useful concept, working in principle but not always in practice. Another recurring difficulty is mainly in recognising an accident waiting to happen. Indeed, early warning signs are usually available before an accident, but they may be too weak to trigger a learning loop or a risk analysis process. Some signals are strong, but they are not treated accordingly. The pathologies are some form of blindness (failure to see warning signs) and deafness (failure of those in charge to act on concerns raised). Those patterns of difficulties show some features of the foresight pitfalls thus giving directions for implementing measures for better anticipation.

3.2 Key messages

Failures of foresight in safety recall how difficult the challenge of risk anticipation is, especially for low probability and high consequence events including black swans. All actors in high-risk industries should remain humble.

Many provisions for foresight in safety have been implemented, but accidents highlight some of the flaws of the processes to anticipate risks. The exhaustiveness and efficiency achieved with traditional risk analysis systematic approaches remains a myth.

The implications are to remain sceptical and critical, to permanently update models and to challenge assumptions. Others are to seek out early warning signs, to prioritize risks in order to focus the available resources on critical risks.

Risk identification is a social construct. It is performed by analysts, designers, operators, and it involves decision-makers within resource (time, budget, expertise) constraints and should remain under scrutiny to avoid fantasy planning.

Analysis of risks, events and early warning signs can be assisted by tools. However, those tools integrate the designer's worldviews and purposes and may not be relevant to address some sociotechnical dimensions. Analysts use artefacts (tools, documents) to formalise their analysis, which may excessively constrain their questioning and attention, leaving them blind in important areas. To better capture risks, more open risk analysis approaches including different worldviews, opinions, transparent and flexible approaches to anticipate the unthinkable are required.

Most accidents are not inevitable but are preventable. Disasters are hard to obtain and not created overnight. They develop during an incubation period and during this time actors have an opportunity to identify latent flaws or early warning signs. Such signs and alerts provide opportunities to challenge safety beliefs and act but they are not always seized upon. It can lead to actions that are too little, too late.

One challenge is to develop high quality intelligence which requires fragmented data and disjointed information to be connected, in order to identify patterns like in a puzzle. This requires data and information structures, and processes but also people to make the expert link to the risk. Interpretation relies on worldviews, lenses and paradigms that should be debated. Assumptions and old patterns should be challenged, while new interpretations should be welcome.

Organisations are defined by what they chose to ignore and forget. Many deviations are normalised for too long. Memories of lessons from accidents are not kept and revived. Foresight in safety shifts organisations from fantasy risk planning, blindness, deafness, denial, apathy and inaction to the need to sustain proactive action on safety and thereby robust and resilient performance.

3.3 Introduction: defining challenges in foresight in safety

In order to foster the continuing debate about the best strategies to enhance foresight in safety, the aim of this chapter is to characterise some failures to foresee adverse events (serious incidents, accidents and disasters). By taking this approach, we aim to complement some of the literature in foresight in safety regarding conditions that favour failures of foresight. We have chosen case studies that we estimate are important to share and help to highlight some key vulnerabilities, rather than attempting a broad review of disaster cases.

3.3.1 Foresight and management

In everyday life, it seems that our abilities to foresee adverse outcomes from our daily activities are challenged by the limits of our planning. We tend to rely on overly optimistic assumptions that fail to integrate the surprises and unexpected events we seldom face. The same is true of organisations.

A century ago, formalisation of management as a new discipline recognised foresight as a key capability especially for engineers, managers and leaders (Stark, 1961): "*'Managing means looking ahead', gives some idea of the importance attached to planning in the business world, and it is true that if foresight is not the whole of management, it is an essential part of it. To foresee, in this context, means both to assess the future and make provision for it* (Fayol, 1916)". In summary (Kingston and Dien, 2017), foresight is about imagining the future possibilities based on knowledge of the past and present.

Stark (1961) considers the future in terms of extensions of the present which are potentialities or temporal possibilities. He defines foresight as a "*productive thinking with the elementary rules of logic its only constraint*"'. Part of foresight is 'reproductive' based on past experiences while another part is more 'creative'. He considers that prediction can be conducted after foresight: prediction is rather a judgmental thinking with the establishment of subjective probabilities to a relatively narrower set of scenarios or period of time. Prediction is measured at a given time and verified after the event while foresight can be continuously assessed.

Ansoff (1975) already remarked that anticipating "*strategic surprises*" in a military perspective and business perspective has historically been a key issue. Many companies were surprised by the petroleum crisis in the seventies, although advance forecast about potential actions of OPEC[8] were publicly available and on the desks of some surprised managers. Ansoff points out that the assumption that those organisations were unaware because they lacked a forecasting and planning system was falsified as many had such a capability. Corporations and industries who had those planning processes were also surprised by other discontinuities. Discontinuities and surprises differ significantly from extrapolation of experience. Depending on levels of information and uncertainty and associated states of knowledge and ignorance, Ansoff (1975) opposed strategic planning which is adequate for strong signals, prepared periodically and organisation-focused; while strategic issue analysis is promoted to respond to weak signals and discontinuities, and requires a continuous, problem focused process.

With this distinction in mind, Ansoff (1975) identified "*an apparent paradox: if the firms wait until information is adequate for strategic planning, it will be increasingly surprised by crises; if it accepts vague information, the content will not be specific enough for thorough strategic planning*". Ansoff invites development of a *"gradual response through amplification and response to weak signals"* […] *"which permits gradual commitment on the part of the management*".

3.3.2 Challenges in foresight in safety

Within a reliability and safety perspective, Lannoy (2015) recalled that foresight requires a forecast to be made in an uncertain, ambiguous, controversial context or to construct a likely future by using information from the past, present and some expected future trends.

Turner (1976, 1978[9]) considers that administrative organizations may be thought of as cultural mechanisms developed to set collective goals and make

[8] ***O**rganization of **P**etroleum **E**xporting **C**ountries (which decided a significant reduction in production and an embargo against the United States and the Netherlands after the Yom Kippur War)*

[9] *We have to note that the pioneering book by Barry Turner ('Man-made disasters') was published with the working subtitle 'The failure of foresight'.*

arrangements to deploy available resources and attain those goals. To manage safety in high-risk industries, risk anticipation activities received a lot of attention and resources for several decades in order to engineer safer systems and to demonstrate control to the regulators. In other words, risk anticipation or foresight in safety is socially constructed (Short, 1984) by different actors and through different processes, provisions and procedures.

In our experience with high-risk industries, the work of 'risk anticipation' or 'foresight in safety' currently relies on four main strategies:

- planning especially through risk assessment when addressing safety threats;
- monitoring the system (e.g. indicators), detecting and treating the early warning signs, weak or strong, indicating a threat to safety;
- setting up an operational feedback process for learning the lessons from past, internal and external events, in order to improve the system;
- preparing for the unexpected and crisis management which implies development of adaptive capabilities such as resilience.

In this chapter, we will not address the fourth strategy, though some research in these directions also provides some concepts and case studies related to weak signals of a crisis waiting to happen (e.g. Lagadec, 1994; Roux-Dufort, 2003) and also some indicators of brittleness (Woods, 2009).

In a conference organised by the French Institut pour la Maîtrise des Risques in 2015 titled "Exploring the unpredictable: how and how far?", in the aftermath of several unexpected disasters (Fukushima, German Wings, Deepwater Horizon, Eyjafjöl,…), several terms were employed by the authors in relation to foresight in safety and its failures (in table 1), with some synonymous, and some addressing different categories (Dechy et al., 2016*)*.

With no surprise, the time dimension is essential to distinguish categories of foresight. However, the terms of the first line (atypical, unimaginable, inconceivable, unthinkable) underline the capabilities required to identify and recognise some scenarios with some difficulties to establish causal links between fragmented elements and limits of knowledge to model the phenomenon. Terms in the second line highlight the temporal difficulties to anticipate, either ultimately (unforeseeable) or about the occurrence time (unpredictable). Terms in the third line refer to their occurrence frequency or likelihood on a given period of time. The fourth category integrates the time dimension but refers to its prevention.

Table 1: Categories of phenomenon linked to event foresight and its failures

		Events	
		Expected, foreseen, without surprise	***Unexpected, unforeseen, surprising***
Category of foresight phenomenon	*Scenario imagination without time*	Identified because typical, imaginable, conceivable, thinkable	Unidentified because atypical, unimaginable, inconceivable, unthinkable
	Temporal prediction	Foreseeable, predictable	Unforeseeable, unpredictable
	Probability estimate in a time period	Probable, likely	Unlikely, improbable, 'black swan'
	Prevention until the period end	Avoidable, preventable	Unavoidable, inevitable

Risk assessment is about imagining and foreseeing what could go wrong and estimating how bad it could be in order that controls can be put in place. Poor risk assessment can lead to ineffective risk controls – controls that are ineffective or inadequate in several ways. In this way, risk assessment is a form of planning. As Clarke said, organizations that 'don't plan are seen as ineffective, poorly managed, irresponsible or sometimes just plain dumb' (Clarke, 1999, p 1). In this way, high risk industries mobilize engineers to identify process and system risks and related accidents scenarios, to model their causation, likelihood and severity. To conduct their work, they use several tools and procedures which may involve workers/experts at all levels of sociotechnical systems.

When uncertainty is high, planning is no longer simply "*a straightforward instrumental activity (a means to an end)*"(Hayes and Hopkins, 2014, p 83) rather, it can become a symbolic undertaking. When planning takes on a primarily symbolic role, the purpose of the plan becomes "*asserting to others that the uncontrolled can be controlled*" (Clarke, 1999, p 16). In this situation, symbolic plans represent a **"*fantasy*"** (Clarke, 1999) – in the sense of a promise that will never be fulfilled – and are often couched in a special vocabulary which then shapes discussion. The danger is that the plan itself takes on a life of its own and organizational effort is focused on managing the plan, rather than taking care of the physical system itself.

On top of the strategy to anticipate risks and related critical scenarios, a complementary strategy to prevent an accident is to foresee an 'accident waiting to happen' by relying on the feedback of system performance, especially its deficiencies such as safety related events, weak signals, precursors, near-misses incidents but also trends and drifts in key and safety performance indicators (KPIs, SPIs). Within this ESReDA FiS project group, we choose to label them 'Early Warning Signs' (EWS) as it enables to cover several concepts recalled hereafter.

Ansoff (1975) provided some elements of a definition of weak signals related to strategic management of companies and strategic surprise as "*early in the life of a threat, when the information is vague and its future course unclear*". A later definition was provided (Ansoff and Mc Donnell, 1990, p. 490) "*[a] development about which only partial information is available at the moment when response must be launched, if it is to be completed before the development impacts on the firm*."

Some EWS of potential hazards of a system can be captured while it is designed and operated. Indeed, in-depth investigations of some accidents showed that some weak signals, precursors of accidents, near-misses (Vaughan, 1996; Llory, 1996; Carroll, 2004; Dechy et al., 2011; Jouniaux et al., 2014; Dien et al., 2012, 2014) have been recognized, at least by some actors, during an 'incubation period' (Turner, 1978) but they were disregarded. Notice that Vaughan (1996) introduces the distinction between weak signals (that are ambiguous to their link to a risk), mixed signals (signs of potential danger that are followed by signs that all was well) and routine signals that frequently recur and even if they are serious, perception of them is altered as they recur without damage.

For some of accidents, the missed opportunities to recognize the threats relates to issues of **blindness** and deafness. However, this is not an easy task and one should remain humble, vigilant and proactive. Indeed, several researchers warn investigators regularly that some signals of danger become clear only with the benefit of hindsight (Reason, 1990; Vaughan, 1996, Woods, 2009). It may lead to the following limit (Woods, 2005) "the past seems incredible, the future implausible". Though retrospective bias is a risk of event analyst, empirical analysis of several accidents showed that some signals are recognised by several actors and processes (auditing, learning) prior to a major accident (Dechy et al., 2011) showing that identification is possible without the benefit of hindsight.

Therefore, Turner (1976, 1978) considers that the challenge in normal operations is to develop "*high-quality intelligence*" (in a military context) to connect "*disjunct information*" distributed in complex systems so as to recognize an "ill-structured problem" (Simon 1973, Turner 1976). We would add to that point that the information is rooted in the history of the system and other systems (e.g. lessons from incidents in other countries, from similar systems and on generic aspects such as organisational failures). This organizational capability goes beyond effective communication as it requires an organization, processes, people to connect different fragment of information, to interpret them, to establish a link between them, referring to the "*puzzle*" metaphor (Lesca, 2001), to resolve ambiguities and to establish a well-structured problem (Turner, 1976).

In a French research project of Institut pour la Maîtrise des Risques (Jouniaux et al., 2014), the weak signal recognition process was defined in three phases:

- link data and fragments of information by experts or by data analytics pre-treatment;
- link this information to a risk or scenario; this relationship' relevance has to be qualified by experts;
- the signal is amplified when risk is redefined by management; strong signals can be minimized.

The two first steps can be aided by data analytics pre-treatment (e.g. big data, natural language processing), but any suspected link, or correlation, or surprise has to be qualified by an expert (Jouniaux et al., 2014). For more development on this issue, see chapter 10 by Marsden et al. (2020).

Near-misses and surprises are therefore opportunities to re-assess assumptions and effectiveness of risk prevention measures but also to imagine what could happen in other circumstances (applying the 'what if' motto).

This is not new, as Weick (1991) (quoted by Reason, 1997) was approaching the issue with a few proposals: *"we know that single causes are rare, but we do not know how small events can become chained together so that they result in a disastrous outcome. In the absence of this understanding, people must wait until some crisis actually occurs before they can diagnose a problem, rather than be in a position to detect a potential problem before it emerges. To anticipate and forestall disasters is to understand regularities in the way small events can combine to have disproportionately large effects"*.

3.3.3 Failures of foresight in safety literature

Accidents continue to happen despite risk anticipation, foresight in safety and the implementation of risk control measures. Moreover, accidents recur that demonstrate failures to learn. Several opportunities to identify the risk or the accident waiting to happen were missed. All the prevention and protection measures, including foresight, come under scrutiny after a serious event during the investigation process.

Woods (2009) recalls that:

- *"establishing foresight encompasses extremely difficult forms of cognitive work and is an unstable process, given pressures on or from an organization's management;*
- *the difficulties arise from basic dynamic and cyclic patterns in how adaptive systems behave;*
- *emerging measures of how and where a system is brittle or resilient provide a critical resource for developing and sustaining foresight when organizations need to achieve high performance (faster, better, cheaper) and high safety (Hollnagel et al., 2005*)".

Turner (1976, 1978) considers a disaster as a "*cultural collapse"*, because of the inaccuracy or inadequacy in the accepted norms and beliefs. The end of an accident is defined not in technical terms but refers to the "*full cultural readjustmen*t" that occurs when risk representation and risk management measures are changed. These deep changes do not occur for every near-miss.

Derived from an empirical analysis of several accidents, Turner (1976) identifies a sequence that leads to failure of foresight (table 2).

Table 2: Sequence of events of a failure of foresight (Turner, 1976, p381)

The sequence of events associated with a failure of foresight	
Stage I	Notionally normal starting point: (a) Initial culturally accepted beliefs about the world and its hazards (b) Associated precautionary norms set out in laws, codes of practice, mores, and folkways.
Stage II	Incubation period: the accumulation of an unnoticed set of events which are at odds with the accepted beliefs about hazards and the norms for their avoidance.
Stage III	Precipitating event: forces itself to the attention and transforms general perceptions of Stage II
Stage IV	Onset: the immediate consequences of the collapse of cultural precautions become apparent.
Stage V	Rescue and salvage -first stage adjustment: the immediate post collapse situation is recognized in ad hoc adjustments which permit the work of rescue and salvage to be started.
Stage VI	Full cultural readjustment: an inquiry or assessment is carried out, and beliefs and precautionary norms are adjusted to fit the newly gained understanding of the world.

The key stage regarding the failure of foresight process occurs with missed opportunities during the "*incubation period*"' when events accumulates, either not known to anyone or not fully understood by all concerned as it will be the case after the disaster, either it did not lead to changes in the risk controls.

Turner further invites us to identify conditions that make it possible for unnoticed, misperceived and misunderstood events to accumulate in a manner that leads eventually to cultural disruption. Turner (1976) identified several of those conditions that occur in stage II of 'incubation period':

- "*failure to comply with existing regulations"*: they failed to realize that regulations apply or to implement them (this belongs to stage I and II about inadequate initial beliefs and norms);
- "*Rigidities in perception and belief in organizational settings"*: accurate perception of the possibility of disaster was inhibited by cultural and institutional factors; 'collective blindness';
- "*The decoy problem"*: attention is focused on "well -structured problems" and is distracted from "ill structured problems" in the background;
- "*Organizational exclusivity*": disregard of non-members' point of view, outsider's information or alerts are dismissed, considering the better knowledge of insiders, which can lead to forms of arrogance;
- "*Information difficulties"*: associated with ill-structured, vague and complex problems; on top of communication difficulties (necessary but not sufficient condition); disjointed information is common in large organizations and the organizational risk is that they are not intelligently treated which leads to unresolved ambiguities of warning signs, orders and procedures, and responsibilities and controls;

- "*Involvement of strangers*": some people involved in the system are uninformed and untrained, which creates difficulties on top of oversimplified stereotypes about their likely behaviour;
- "*Minimizing emergent danger*": failure to see or appreciate the magnitude that remains under-estimated; under-valuation of evidence by the more complacent group and fearing the worst outcome; when impossible to ignore, (surprisingly) strengthening the response is not systematic; it may even lead to shift the blame or to believe in the use of quasi-magical means.

When reviewing Turner's added value, Weick (1998) warns that all organizations appear more vulnerable than they admit, because all develop culturally accepted beliefs and associated norms, and then accumulate unnoticed events that contradict with these world views. "*'Assumptions* […] *carry an organization's learning as well as its blind-spots'*. […] *'Assumptions conceal warning signals, deflect attention to safe issues, leave signals unnoticed because they are undefined and set the stage for surprises that necessitate revision in administrative practices'*".

Westrum (1992) distinguished three organizational cultures[10] according to the way they deal with safety-related information:

Table 3: How different organizational cultures handle safety information (Westrum, 1992)

Pathological culture	Bureaucratic culture	Generative culture
Don't want to know. Messengers (whistle-blowers) are shot. Responsibility is shirked. Failure is punished or concealed. New ideas are actively discouraged.	May not find out. Messengers are listened to if they arrive. Responsibility is compartmentalized. Failures lead to local repairs. New ideas often present problems.	Actively seek it. Messengers are trained and rewarded. Responsibility is shared. Failures lead to far-reaching reforms. New ideas are welcome.

Beside the processual, organizational and cultural views of foresight in safety, Perrow (1982, 1984) insisted on the inherent cognitive limits of operators and engineers to anticipate all interactions and cascading effects in complex systems. To some extent, many accidents are 'impossible accidents' at least from the perspective of those involved (Perrow, 1984). 'Accidents appear to be the result of highly complex coincidences which could rarely be foreseen by the people involved. The unpredictability is caused by the large number of causes and by the spread of information over the participants… Accidents do not occur because people gamble or lose, they occur because people do not believe that the accident that is about to occur is at all possible (Wagenaar and Groeneweg, 1987). In Perrow's view, foresight is always limited and some technologies should not be used because accidents are inherent, indeed can be said to be 'normal'.

3.3.4 Approach, structure and content of this chapter

First, in the next section (§3.4), we draw on past major disasters across a range of sectors (chemical, oil and gas, space) to identify patterns of failures of foresight. This empirical approach, that relies on case studies of accidents to highlight patterns of accident causation and especially organizational patterns of failure of foresight, has been implemented by several researchers on accidents and safety (e.g. Turner, 1976, 1978; Perrow, 1984; Llory, 1996, 1999; Reason, 1997; Dien et al., 2004; Llory and Montmayeul, 2010, 2018).

Indeed, from a practical point of view, those accidents and disasters investigation reports are often public and have been produced by large expert teams in relation to presidential or parliamentary commissions or independent safety boards (ESReDA, 2005). Their reports of several hundred pages may provide "*thick descriptions*" (Geertz, 1998), meaning very detailed accounts about daily activities of people, interactions and organizational and institutional processes. Those reports are of various qualities. Some can be considered as school cases that every safety specialist should read and know [e.g. Ladbroke Grove trains collision in United Kingdom in 1999 (Cullen, 2000); loss of space shuttle Columbia in 2003 (CAIB, 2003), Texas City refinery explosion in 2005 (CSB, 2007)]. In other cases, some reports are criticised publicly and associated with controversies in relation or not with the judicial investigation. No reports should be considered as perfect: the investigation may have grey zones or uncovered scopes and so can be complemented by other published material.

[10] *Other cultures may be categorized (e.g. Hudson (2001) added reactive, calculative, and proactive (replacing bureaucratic, between pathological and generative) within a safety culture maturity model). Notice that several sub-cultures or maturities co-exist within the same organisation, department which questions their overlapping, integration and interactions.*

More fundamentally, this approach aims at identifying organizational "vulnerabilities". Indeed, accidents offer the 'gift of failure' (Wilpert according to Carroll and Fahlbruch, 2011) - an opportunity to learn about safe and unsafe operations. Accidents are the "*royal road*" (Llory, 1996) to access to real (mal) functioning of organizations[11], as some hidden phenomena in the "*dark side*" of organizations (Vaughan, 1999) may become more visible in accidents. This strategy is opposite to the study of normal operations and banality of organizational life (Vaughan, 1996) that is often conducted to identify "best ways" to cope with variability, to enhance reliability and to adapt and recover from adverse events ('High Reliability Organizations' (Roberts, 1990, Laporte and Consolini 1991), 'Resilience engineering' (Hollnagel et al., 2006), and 'Safety II' (Hollnagel, 2014)).

Second, analytical developments start in section §3.5 by discussing how risk analysis can fail and continue in section §3.6 with blindness patterns. This analysis also relies on our investigator and risk analyst's practical experiences in the field, either within high-risk industries, expert's institutes that support the safety regulation and consultancy firms, or also as researches in risk assessment and management. We provide a few conclusions and perspectives in section §3.7.

3.4 Accidents that highlighted some failures of foresight

3.4.1 Toulouse disaster in 2001 in France

On 21st September 2001, a powerful explosion occurred at the AZF fertilizer and chemical plant in Toulouse suburbs which lead to significant damage and effects[12]. The direct causes are still under debate and controversy between prosecution, lawyers for Total and other stakeholders even after the third trial in 2017 (Dechy et al., 2018). In summary, the explosion of off-specification ammonium nitrate was not prevented and turned into disaster due to several failures in risk assessment, management, governance, control and regulation (Dechy et al., 2004).

This accident belongs to the category of '*atypical*' accidents (Paltrinieri et al., 2012). It means that this low probability-high consequence accident was not among the worst-case scenarios captured by traditional risk analysis and formalised within the safety case submitted under Seveso I and II directives by the licensee to the regulator, nor one of the scenarios used in the eighties and nineties to establish land use planning and emergency planning. This striking lesson revealed flaws not only in the risk analysis process used to identify the relevant scenarios but also in the negotiations upon the scenario's basis on which to define safety measures.

An underlying reason is that the residual scientific uncertainty on ammonium nitrate chemical sensitivity were underestimated. There were ambiguities in the behaviour of ammonium nitrate that belong to the category of "*occasional explosives*" (Médard, 1979). In some conditions (e.g. contamination by chemical impurities, fuel, air pressure…), inherent and residual explosion risk could increase. In addition, lessons from accidents in the last century were assumed to be learned, and also gave decision-makers confidence to exclude the occurrence of those conditions and initiators if industries operate normally. The conservative approach was therefore limited. There were also deficiencies in knowledge management about accidents lessons and chemical properties. Also, the fertilizer industry lobby pushed to consider that the "worst-case scenario" for ammonium nitrate storage were fires with toxic fumes, because such consequences are more likely, rather than a massive explosion. Imagination was therefore limited though the explosion risk remained inherent, especially if conditions were gathered. In addition, the "envelope approach" of safety case studies lead the licensee and regulator to focus on other scenarios of the plant and of the neighbouring plants which were more severe (several toxic cloud release) than a potential ammonium nitrate explosion.

Once approved in 1989, the land use planning (LUP) process and plan enabled local authorities to freeze further nearby urban development, but it was too late as buildings and houses were already close by, and the plan had no retroactive force to expropriate people (Dechy et al., 2005). In addition, the effects' distance was under-estimated because scenarios were rather incidents than worst cases. This occurred as an outcome of negotiation between the regulator and operator after Seveso I regulation. A reason was that regulator and operators wanted to find an incentive such as a way to value the financial investment in prevention measures with an impact on a reduced safety distance that impacts the land-use.

[11] *In reference to Sigmund Freud's metaphor: "Dreams are the royal road to the unconscious. "*

[12] *31 fatalities, estimates of French national health institute (InVS) are about 10 000 injured, 14 000 post-traumatic acute stress, 27 000 houses/flats damaged, 1,5 to 2,5 billion euros of damages; Dechy et al., 2004a).*

3.4.2 Buncefield accident in 2005 in United Kingdom

The Buncefield oil depot fire and explosion the 11th of December 2005 destroyed a large part of the site and the surrounding area. The immediate trigger for the catastrophe was a large petrol storage tank that overflowed whilst being filled from a pipeline. About 300 tons of petrol escaped from the tank, 10% of which turned to a flammable vapour cloud. Once ignited, the magnitude of the resultant vapour cloud explosion (VCE) was much greater than anyone knew was possible. The effects were fortunately more limited (43 injuries) as it occurred at 6 am of a Sunday morning (MIIB, 2008; COMAH Competent Authority, 2011).

The Buncefield oil depot was subject to the so-called ''Seveso-II'' Directive, but the scenario that occurred was not taken into account in the mandatory safety report, as in the case of Toulouse accident (Paltrinieri et al., 2012). Formation of a vapour cloud due to tank overfilling and consequent VCE were not deemed possible, neither by the company nor by the competent authorities. The design of the tank itself may have contributed to the vapour/mist formation in a manner that was not foreseen by designers. The tank was fitted with a deflector plate that led to a cascade of petrol droplets through the air. Moreover, most of the remaining fuel running down the wall hit a structural stiffening ring and detached from the tank wall, creating a second cascade of droplets. These conditions promoted the evaporation of the lighter components of petrol, (e.g. butane), which were allowed in higher concentration in the winter season. The unexpected strength of the subsequent VCE was caused by presence of equipment and trees increasing the turbulence of the flow and/or providing a certain level of confinement and a substantial energy of the ignition source (MIIB, 2008).

The worst credible scenario included in the site safety report was a major liquid fuel pool fire (COMAH Competent Authority, 2011). Although, risk analyses of oil depot in France in the early 2000's considered potential leaks that could form an explosive cloud especially for volatile hydrocarbons, the risk considered was the one of *unconfined* vapour cloud explosion, implying that it did not lead to overpressures over 200 mbar. Therefore, pool fires were often the worst case for safety cases reports with envelope effects out of the plant site. For this reason, the actual accident scenario can be defined as "atypical" (Paltrinieri et al., 2012).

Hazard identification has important aims: it may highlight possible malfunctions of the systems, outline related losses of containment and describe potential consequences. An atypical accident may occur when hazard identification does not produce a complete overview of hazards due to a lack of specific knowledge and a low awareness of associated risks, because it deviates from normal expectations of unwanted events or worst-case reference scenarios (Paltrinieri et al., 2013). This qualitative pre-assessment is the foundation of risk management. For instance, Seveso safety reports are supposed to conservatively evaluate worst-case scenarios and safety measures that are used for the operation licensing, calculation of effects' distance used in emergency response planning and in the design of safety area in land use planning (LUP).

Further accident databases analysis and research (Paltrinieri et al. 2012) demonstrates that VCEs in oil depots were not unknown before. In fact, since the middle of 1960s, there is record of VCE accidents occurring approximately every five years in oil depots around the world. Effective knowledge management searching for and considering such historical lessons and strong warnings was missing in Buncefield. It can be speculated that this was due to the inaccuracy of the analysis process (availability of resources to seek for accident data?) while assessing related risks, whose results were (only apparently) validated because it was consistent with similar process safety studies (addressing similar plants or the former plant documents) and within the basic experience. In other words, the risk analysis process was affected by social conventions and by an implicit code of practice that failed to integrate some knowledge about accidents.

3.4.3 Texas City refinery accident in 2005 in USA

On March 23, 2005, an explosion and fire at the BP refinery in Texas City lead to 15 deaths and 180 injuries. The CSB (2007) noted that: "*The Texas City disaster was caused by organizational and safety deficiencies at all levels of the BP Corporation*". The board member and CEO of the US Chemical Safety Board (CSB), Carolyn Merritt (2007) underlined: "*cost cutting, production pressures, and a failure to invest left the BP Texas City refinery vulnerable to a catastrophe*."

Failures in major risk assessment have been noticed. The risk of the blowdown drum releasing a potential explosion cloud was identified as it was known as an "*antiquity of the fifties*" by the operator and the industry standard had changed to require a flare for new designs. It was known by the regulator (OSHA) who requested the removal of antique flare, but the operator (Amoco in the nineties) relied on ‘grandfathering’ [13]to avoid the need for modification and replacement by a safer equipment. Internal audits of the BP group in early 2000’s already blamed the BP refinery ‘*check book mentality*’ for maintenance of equipment, for safety policy and more generally for selection of risk controls.

The failures to learn (Hopkins, 2008) and the blindness to process safety deterioration and alerts (e.g. loss of containment incidents were increasing) have been eased by the confusion with worker safety metrics that were improving (further explanations in section §3.6.3). CSB (2007, p18) investigation found that “*warning signs of a possible disaster were present for several years, but company officials did not intervene effectively to prevent it*.” Merritt added (2007) that “*adhering to and enforcing federal regulations already on the books would likely have prevented this accident and its tragic consequences*.”

Indeed, the CSB investigation showed that some BP members had identified the rise of major risks already in 2002. The new director of BP’s South Houston Integrated Site observed in 2002 that the Texas City refinery infrastructure and equipment were “*in complete decline*”. (CSB, 2007). An internal follow-up analysis concluded that “*the current integrity and reliability issues at TCR* [Texas City Refinery] *are clearly linked to the reduction in maintenance spending over the last decade*” (CSB, 2007, p153). Several other internal studies, surveys, audits and also serious incidents alerted and signalled the severity of deficiencies but the response of BP managers was “*too little and too late*” (Merritt, 2007). For example, there was a poor (only 30% of corrective actions were implemented) and declining implementation of corrective actions. Furthermore, a safety culture assessment conducted by an external company (Telos Group) alerted the managers in January 2005 about the critical and degraded state of the refinery. The Telos report identified the organisational and process safety problems that were found by the CSB in retrospect.

3.4.4 San Bruno pipeline failure in 2010 in USA

In September 9, 2010, eight members of the public were killed when a gas transmission pipeline ruptured at San Bruno, California (NTSB, 2011). The rupture occurred when a longitudinal seam weld failed. The weld had been poorly made during construction of the pipeline in 1956. The line had not been inspected or tested since that time. Failure of pressure control at the upstream terminal led to a pressure rise in the line to close to the maximum allowable operating pressure (MAOP). Control room operators chose to troubleshoot the pressure problems but not to isolate the downstream pipelines. After exposure to higher than normal pressure for approximately one hour, the line failed.

Integrity management of ageing buried pipeline networks is an exercise in managing risk. In this case, the involved operating company PG&E (Pacific Gas and Electric) had put significant effort into developing a risk model of the system but the primary focus of the system was not on fault identification and repair. Indeed, the database contained inaccurate data, inappropriate risk algorithms and lacked any real-world connection. In summary, shortcomings in the GIS (geographic information system) and associated procedures include (Hayes and Hopkins, 2015):

- The database used as the basis for risk ranking included physical data that was optimistic and / or incorrect and there was no system of data checking in place.
- Algorithms for establishing inspection priorities averaged risk scores for a given pipeline segment across all threats to pipeline integrity thereby hiding problems, rather than highlighting them.
- Regardless of the identified threat, higher risk segments were mostly subjected to external corrosion direct assessment, a type of inspection which finds pipeline integrity problems for external corrosion threats only.
- There was no system in place to review the performance of the integrity management system overall i.e. to compare high risk segments identified with inspections done and with actual leaks seen to determine if the system was effective and/or how it might be improved.
- The system produced only a prioritised list of pipeline segments based on threats to integrity. Whilst such a system could, in theory at least, be used to determine where funds should be spent to improve integrity, it makes no attempt to comment on overall risk acceptability and the total budget required.

[13] *‘Grandfathering’ is a legal process that gives the benefits of anteriority to existing processes over new legal requirements which have no retroactive force.*

Another significant factor in this accident was the MAOP for the pipeline segment that ruptured. It had been determined based on the highest operating pressure seen in the system in the previous five years, rather than by testing. This was specifically allowed for pipelines of this age under the relevant regulations. Newer pipelines are required to be hydrotested but pressure testing requirements of the relevant standard had been grandfathered in this case, in a similar way to the old design of the Texas City refinery blowdown system. Given the flawed weld, it is unlikely that the pipeline would have passed a hydrotest and yet such a test was not required by the regulator, nor seen as necessary by the operating company.

3.4.5 NASA space shuttle losses in 1986 and 2003

On the 28th of January 1986, after an unusually cold night for Florida (minus seven degrees Celsius) which required a launch delay due to ice on the shuttle launch pad, the space shuttle Challenger exploded 73 seconds after its launch with all seven astronauts killed. The technical explanation of the accident centred on the failure of the joint between two segments on the right Solid Rocket Booster (SRB). The O-rings that were intended to seal this joint from hot gases leaking through the joint failed to perform properly, due to the extremely low temperatures for the intended launch environment. This leak allowed a flame to emerge from the SRB and to impinge upon the external fuel tank (Rogers et al., 1986).

On 1st of February 2003 the space shuttle Columbia disintegrated during its re-entry phase into the Earth's atmosphere after a 16-day mission on orbit around the Earth. The seven astronauts died in the accident. The Columbia mission was the 113th space shuttle flight. The technical cause for the loss of Columbia is clearly identified. During the shuttle's ascent phase, a piece of insulating foam separated from the left bipod ramp located on the external fuel tank. It struck the leading edge of the orbiter's left wing at a relative speed of about 800 km/h. The impact caused a hole in the shuttle thermal protection system, a particularly vulnerable area during re-entry in the dense layer of Earth’s atmosphere (CAIB, 2003).

Beyond direct technical causes of the accidents, there is a similarity in the organizational patterns of the two accidents, with “*echoes*” of Challenger’s causes in Columbia’s (CAIB, 2003). Both disasters can be seen as symptoms of foresight blindness. Indeed, for the Challenger case, organizations (the NASA and its contractor Morton Thiokol Inc.) were unable to fully acknowledge the design flaw of the rocket joint: they fail to recognize it as a problem to be fixed and they perceive it as an acceptable flight risk. According to the Presidential Commission it was “*an accident rooted in history*”. There were warnings from several lower-level engineers from the subcontractor and concerns within some NASA engineers, that the joints were poorly designed, including one report that said they could cause a catastrophe. Unfortunately, it had no significant impact on decision makers. Warnings were unheeded by top managers.

In addition, NASA did not retain memory of the lessons learned. As Diane Vaughan noted (1996, p. 422): “*Few of the people in the top NASA administrative positions exposed to the lessons of the Challenger tragedy are still here. The new leaders stress safety but they are fighting for dollars and making budget cuts. History repeats, as economy and production are again priorities*”. One effect of this policy is the feeling that as long as no serious problem occurs, the situation is seen to be under control (“so far, so good!!”): “*success-engendered safety optimism*” (CAIB, 2003, p. 114) and “*it could lead to a tendency to accept risk solely because of prior success.*” (CAIB,2003, p. 114). Risk is measured by past successes: “*The acceptance and success of these [past Challenger] flights is taken as evidence of safety*” (Feynman, 1986). Example of the Columbia accident is typical of inability to take account of small failures “forgotten” during the risk analysis carried out during the design phase. The fatal flight was the 113th mission of a space shuttle. The various shuttle orbiters had been hit by debris for each of the previous 112 missions[14]. It was the 7th detachment from the left bipod, knowing that a detachment from the right bipod was never seen. Those events were identified as safety issues by designer that defined specifications to prevent them. The consequence of these multiple failures was not a risk (re)assessment but a progressive shift in evaluation of the severity of incidents, gradually, mission after mission:

- From “safety of flight issue” to a “turnaround issue” (simple maintenance);
- From "Out-of-Family" problem (operation or performance outside the expected performance range for a given parameter or which has not previously been experienced) to "In-Family" problem (a reportable problem that was previously experienced, analysed, and understood);
- In other words, from jeopardizing safety to acceptable risk.

[14] *Knowing that no data were available on the fatal Challenger mission.*

3.5 Failures of foresight due to inadequate risk assessment

Risk prevention through anticipation relies especially on the ability to identify safety threats and to model risk levels adequately in order to ensure proportionate risk control measures. It is mainly depending on what is imagined and considered in input, at the modelling phase of risk analysis and finally about what is done with the output to prevent accidents. These processes are collective and socially constructed and relate to engineering standards and regulation.

When addressing low frequency-high consequences events that are for some beyond experience, this becomes more challenging. Many accidents have taken companies apparently by surprise as a result of poor engineering risk assessments. Among the mechanisms highlighted by accidents, the next paragraphs discuss some of the failures, especially on complexity modelling, imagination, quantification, and point to some recurring flaws and biases that downgrade these activities.

3.5.1 Limits in capturing the complexity of reality

Engineers have developed several formal methods in safety and reliability to identify (e.g. What if? Systematic questioning) and assess risk (e.g. failure mode and defects analysis, preliminary risk analysis, HAZOP, fault trees, bow-ties…) and more complex tools (e.g. 2D, 3D) to model physical and chemical phenomenon (fire, explosion…). A first limit stands in the inability to capture the complexity of reality into risk assessment approaches and risk modelling. The use of scenarios is fairly common, providing benefits and showing limits as well (see chapter 5, Ferjencik et al., 2020).

A striking lesson of both the Toulouse disaster and the Buncefield accident was that their scenarios were not identified as the worst-cases scenarios that were integrated in the safety case studies reports, emergency and land use planning area. We therefore called them "*atypical*" (Paltrinieri et al., 2012) as they are not enough typical to serve for those purposes. This recurring finding hampers the legitimacy of such engineering plans to anticipate risk and prepare emergency procedures (with the risk of becoming a "*fantasy*" (Clarke, 1999)).

Everyone knows that models are a simplification of reality. Similarly, some researchers (Perrow, 1984) have criticized system designers' abilities to address the complexity of sociotechnical systems and even to prevent and protect from inevitability of accidents in such settings. Though this 'normal accident' theory has been challenged for different reasons (Hopkins, 2001; Dechy et al., 2011; Dien et al., 2013) mainly because in most accidents, warning signs (weak or strong) are available before the major accident, but often not treated accordingly, the warning from Perrow should lead to vigilance attitude when establishing such scenarios.

The more we study risk assessment practices and failures of foresight, the more we become cautious about the interpretation of results provided by the application of formal approaches of risk analysis (e.g. hazard identification techniques) as they oversimplify reality [e.g. Buncefield with bow-tie, HAZOP, Paltrinieri et al., 2012; with FMEA, Thellier, 2017, 2018]. Several incidents, events, near-misses reveal some unexpected scenarios with unanticipated interactions and combinations of systems, sub-system, and component failures that were not captured in the risk analysis format. Then the question can become to wonder if they are used as opportunities to learn about those missed scenarios applying the 'what-if' motto as a driver for risk imagination.

Finally, it is widely acknowledged that engineering approaches poorly address and even divert from addressing human and organisational factors and the sociotechnical interactions and complexity (Rasmussen, 1997, Wilpert and Fahlbruch, 1998; Thellier, 2017; Vautier et al., 2018, Llory et al., 2018). This remains a major blindness and favours the "*cultural collapse*" mentioned by Turner.

3.5.2 Failures of imagination in defining the worst case

Preventing accidents through foresight requires safety threats to be identified. Efficiency criteria are the 'imagination', 'exhaustiveness' and the 'filtering' or defining a "hierarchy of risks". For decades, deterministic approaches have been widely used in several industrial sectors in order to specify appropriate measures and barriers to deal with major risks and protect workers and neighbours of industrial plants. This approach requires conventional scenarios to be defined and studied by postulating some "worst-case scenarios" that can lead to the complete degradation of a storage and pipe in order to study "envelope effects" (Hourtoulou, 2002, Libmann, 1996). Notice that the nuclear reactor meltdown was not formally postulated in conventional scenarios (Libmann, 1996) before Three Mile Island accident in 1979, though it had been imagined by some nuclear engineers, even before the WASH1400 probabilistic risk assessment report (Rasmussen, 1975). Though this report brought some advances, it was also largely reviewed and criticized.

For some researchers (e.g. Clarke, 1999, 2006), the "worst-case approaches" become an exercise in "*fantasy planning*" when they convince their users and fool them. It can lead to fantasy land use planning around pipelines (Hayes and Hopkins, 2015) or petrochemical plants if we look at Toulouse and Buncefield accidents. Indeed, in our experience (Dien and Dechy, 2016), the imagination is often limited by a dose of realism.

First, some initiators are excluded: e.g. at Toulouse disaster in 2001, some explosion triggering factors were excluded such as the confinement or the contamination factors, considering that those conditions would not occur in "normal operations" thus preventing any explosion. The industry lobby focused on the more likely event of a fire as the worst-case scenario, (Dechy et al., 2004, 2005). In the nuclear sector, some phenomena were not taken into account until recently (e.g. tornado in France) and the severity of natural hazards was under-estimated in Japan as shown by Fukushima accident (Diet, 2012) and worldwide. Meteorites are excluded by all industries.

Then, major risk modelling is supposed to espouse the so-called 'conservative approach' but in practice there are limits. "Worst case-scenario" are supposed to display "envelope effects" but are not always the maximum physically possible. All the parameters that influence them are not integrated in the model with all at the highest intensity. In France, in the early 2000s, for oil storage tanks in an open environment, it was considered that the highest overpressures of *unconfined* vapour cloud explosion were below 200 mbar. During the Buncefield accident (2005), overpressures were over one bar in some locations, due to differences in the initiating energy, the oil mist, the nature of hydrocarbons and turbulence factors. The impact of those parameters was more or less known by some experts and researchers but often not modelled by practitioners. But, in addition specific adverse conditions occurred. Indeed, trees acted to increase turbulence and played a role of flame accelerator (MIIB, 2008; COMAH Competent Authority, 2011; Paltrinieri et al., 2012). The oil mist explosion was very energetic because a deflector increases droplets when the liquid was leaking along the tank; there was a higher concentration of relatively more volatile components in the gasoline (in winter it is allowed by law).

At Fukushima, a tsunami wave with a height level of 14 meters was imagined before the accident but excluded for probabilistic reasons. Therefore, the chairman of the independent commission concluded *"It was a profoundly manmade disaster – that could and should have been foreseen and prevented. And its effects could have been mitigated by a more effective human response"* (Diet, 2012, p9).

In the end, the exhaustiveness and efficiency achieved through the use of these systematic approaches remained a myth for some time. These beliefs (Turner, 1978) are better challenged today as some stakeholders of these analysis would maintain some doubts that the residual risks have been achieved (e.g. for French nuclear safety after Fukushima, Couturier et al.; 2016).

To better capture risks, our main lesson to share is to support more open risk analysis approaches including different worldviews, opinions, transparent and flexible approaches to anticipate the unthinkable.

3.5.3 Traps of quantification

Several benefits but also several traps from quantification can be identified (Lannoy, 2016). Probabilities and frequencies of accidents are commonly underestimated in several industries by more than an order of magnitude, before accidents occur and for several reasons. We could insist here only on a few limits that appear to us as noteworthy.

A first limit that appears to us as quite important is expert dependence or sensitivity to the expert approach. A European research project, ASSURANCE (Hourtoulou, 2002) showed that for the same chemical plant, with seven different experts from Europe who selected their scenarios, their modelling tools and data, the results could differ by a factor of 6 in effects distances modelled for worst-case scenarios and by three orders of magnitude for probability estimates.

A second limit, relies on the beliefs in quantification that can lead to perverse effects that can be detrimental to safety. Before the Challenger launch decision, engineers were asked to "*quantify their doubts*" about the robustness of the O-rings, as the engineer perceptions were treated as "subjective", "uncertain", "qualitative", "affective", "emotional" and could not comply with a technical culture that required quantitative data (Vaughan, 1996). Of course, the engineers would have been equally stumped if they had been told to demonstrate numerically that the system was safe, showing that it is not quantification itself that is necessarily a problem but the way in which it is brought to bear in decision making.

Problems with pipeline integrity management at PG&E are similar in that the data used for quantification was significantly incorrect. Some critical information had been entered into the system as 'dummy' values when a new database was introduced some years before the accident. This "garbage in" resulted in graphical output showing that risk was declining whereas, in fact, pipeline integrity management was grounded in 'garbage out' results.

Third, there can be some inappropriate use of statistical laws which are often used in reliability of equipment due to great number laws. For example, Gaussian distribution towards the average that are applied inadequately to low probability events and high consequences, infrequent extreme events, some of them could be considered as black swans hidden in the "fat tail" of statistical distribution (Taleb, 2007). We see this in the San Bruno case specifically where the entire pipeline network was divided up into several hundred segments with a risk score produced for each possible threat to integrity (external corrosion, ground movement, design and materials, third party interference) and each segment. The problem, however was that all threats for a given segment were averaged, thus effectively hiding high scores. In some cases, the use of multi-criteria decision analysis procedures may prevent some of the quantification traps (Linkov and Moberg, 2017; Merad and Trump, 2020).

3.5.4 Cognitive biases and social conventions

In addition, one should remember that the map is not the territory; therefore analysts and managers should be very cautious about the limits of the approaches, especially the dependency on experts with regards to the limits in their background knowledge, their procedures to treat limited data, their tools (e.g. Dien et al., 2012, Maguire and Hardy, 2013; Power, 2016; Merad and Trump, 2020). There are several cognitive biases especially with perception of low probability-high consequences events (work of Tversky and Kahneman, 1974; Taleb, 2007; Merad et al., 2016). A famous example is also related to the NASA space shuttle Challenger explosion, with under-estimates by NASA managers of the likelihood of a failure of a launch (Feynman, 1986).

The constraints in which risk assessments are performed should be addressed, as risk assessment are projects conducted under constraints (Merad, 2010). The resources, the methods or level of guidance and aiding, the level of openness and flexible mindset, should be questioned.

Several "worst-case scenarios" are conventions that are a social construct (e.g. a vapour cloud explosion could not occur on an oil depot because of lack of confinement). They may inherently integrate residual risk (Couturier et al., 2016) that is not treated accordingly (e.g. occasional explosives such as ammonium nitrate fertilizer that are not inherently safe (Dechy et al., 2004; Marlair and Kordek, 2005)). These conventions are changed especially after disasters and are in retrospect better acknowledged to be some fantasy planning (Clarke, 1999, 2006) that fooled their users for a while.

3.6 Failures of foresight due to blindness

First, we should notice that "blindness" may refer to several phenomena. It is obvious that it puts an emphasis on the inability to see and recognise from a cognitive and cultural point of view the early warning signs. But it can also be related to some failures to learn the lessons from strong signals such as lessons from accidents, by lack of memorisation or poor knowledge management. And it could also be understood as the inability to react to weak signals and change the course of actions as planned. Those contradictory signs may offer opportunities to reassess assumptions, models, controls and barriers, but are they seized? At some point, from a pathology such as blindness, it can shift to the inability to listen to and ear the alerts (deafness) or even some denial, apathy and inaction.

3.6.1 Engineering failures to reassess models against warning signs

The previous sections describes possible pitfalls in model development. The focus here is on issues with models in use. As the map is not the territory, in principle, a key preoccupation for risk analysts is to benchmark their predictions against real observations and collect new information that could challenge or help them to update and increase the reliability of their models. However, evidence from accidents shows that this is not always performed adequately either by the analysts in charge or by the professional community. This first argument hereafter relates to quality assurance in risk modelling; while the second addresses the opportunities to revise assumptions based on EWS treatment.

The strength of the explosion of Buncefield accident was unexpectedly severe. However, history shows (see next table n°3) that it was not the first accident with important effects for unconfined vapour explosion. Moreover, several modelling approaches were available to take into account various parameters that influence explosion strength (e.g. multi-energy methods by TNO[15] since the eighties aimed at better taking into account turbulence and confinement parameters). The explosion in Saint-Herblain in 1991 in France was also surprisingly severe and did help to some extent to reveal to some experts (e.g. in France at INERIS, Lechaudel and Mouilleau, 1995) some under-estimates in unconfined vapour explosion modelling. However, common practices of risk analysts for such modelling were not so aware of this kind of phenomenon.

Beyond a quality assurance approach to benchmark the quality and the reliability of risk modelling, a complementary strategy is to be reactive to EWS. Those EWS should be proactively seized as opportunities to check safety assumptions, risk modelling, and therefore relevance of designs, rules and decisions. EWS should be both captured and treated within an engineering loop (redesign a design flaw) or operational loop (monitor or change the organisation).

To some extent, this issue deals about the treatment of risk under uncertainty. Several accidents (e.g. Therac-25, (Leveson and Turner, 1993), DC-10 crash in Ermenonville, (Llory, 1996)) have revealed these difficulties to be reactive and proactive to different magnitude of EWS.

As described above, PG&E operated a risk-based model for pipeline integrity management to determine inspection priorities. The major problems with the data and algorithms on which the model was based might have been identified before the San Bruno failure if only a link had been made between field experience and model predictions. Two kinds of field data were available (inspection results and pipeline leaks) and neither of these were used to verify that the risk model was operating as intended.

NASA engineers observed that O-rings of space shuttle boosters were damaged. Specifications of designers required no damage. The engineers discussed redesigning the system but this would take two years and could introduce new risks. Engineering preferred to choose evils that were known rather than unknown (Vaughan, 1996). This position was supported by the success of ongoing launches with anomalies but no major failures, which was taken as proof of safety, despite the fact that it was rather a confusion with reliability (Dien and Llory, 2006).

The Challenger accident provided another lesson on this issue on the eve of the launch, when low temperatures in Florida generated concerns for some engineers from the subcontractor and manufacturer of the booster. Engineers lacked data to challenge prevailing assumptions about O-rings behaviour for low temperatures and were asked to quantify their doubts in order to convince NASA managers to set-up a new safety criterion for the decision to launch space shuttle.

For this reason, an extended strategy of dynamic risk management is suggested by Paltrinieri et al. (2015) to define an appropriate decision-making process based on comprehensive monitoring activity. It should also integrate a dynamic learning as a follow-up from events (ESReDA, 2015) as described hereafter.

3.6.2 Failures to learn, to memorize and to manage knowledge

After an event, investigations seek to identify lessons to avoid a similar accident in the future, here and elsewhere. Failures to learn were numerous in BP's Texas City refinery before their major accident (CSB, 2007; Hopkins, 2008) and are a common root cause of accidents, potentially an "ultimate root cause" (Dechy et al., 2009, 2011, 2018; Dien et al., 2012; ESReDA, 2015).

Dynamic learning should avoid blindness, forgetting and continuous improvement should be observed. Accidents, however, recur (Kletz, 1993) with similar organisational root causes, as for NASA space shuttles and BP accidents. Losses of memory of lessons from accidents do occur (Kletz, 1993; Ferjencik and Dechy, 2016, Dechy et al., 2016), with both individuals and organisations forgetting (see chapter 4 by Ferjencik and Dechy, 2020). One should humbly acknowledge that learning to prevent the next accident, remains a high challenge.

Some accidents show that lessons from accidents are missed which highlights a lack of awareness and poor knowledge management. Problems with the modelling of unconfined vapour cloud explosions at Buncefield have already been described. Surprisingly, the trend to underestimating the overpressure that could be achieved continued after the event, highlighting the difficulty to learn and change systems.

[15] *https://www.tno.nl/en/*

Table 4: VCE events in oil depots caused by gasoline LOC before and after the Buncefield accident (Paltrinieri et al., 2012)

	Location	Date	Loss of containment
Before Buncefield	Houston, Texas, USA	April 1962	Leak from a gasoline tank
	Baytown, Texas, USA	27 January 1977	Overfilling of a ship with gasoline
	Newark, New Jersey, USA	7 January 1983	Overfilling of an unleaded gasoline tank
	Naples, Italy	21 December 1985	Overfilling of an unleaded gasoline tank
	St Herblain, France	7 October 1991	Leak of gasoline from a transfer line
	Jacksonville, Florida, USA	2 January 1993	Overfilling of an unleaded gasoline tank
	Laem Chabang, Thailand	2 December 1999	Overfilling of a gasoline tank
After B.	San Juan Bay, Puerto Rico	23 October 2009	Overfilling of a gasoline tank
	Jaipur, India	29 October 2009	Valve left open

The ammonium nitrate accidents in 1947 at Texas City (United States) and Brest (France) ports, occurred in specific configurations with fuel and confinement in cargo of ships. Those accidents were used as a proof of the need for the two necessary conditions to have explosions. It led the fertilizer industry to consider that these two conditions could not happen in open ground storage in normal operation therefore explosion risk could be excluded. Scientific knowledge management and information sharing about physical properties is sometimes considered as insufficient and not addressed by systematic risk analysis procedures. Even in the study of better known physical and chemical phenomenon, surprises can happen. The case of "occasional explosives" (Médard, 1979) is typical; specifically, for ammonium nitrate where some residual risks were not intrinsically excluded thus forgotten (Dechy et al., 2004, Gyenes and Dechy, 2016) as dramatically recalled by the 2020 Beyrouth disaster. Several properties at the limits are not discovered through quality tests but could be more likely if safety and research tests were conducted more often. In the nuclear industry, some phenomenon are still research subjects, fifty years after the first nuclear power plants started.

An explanation of the severity of the consequences of the Texas City refinery explosion in 2005 (15 fatalities) comes from the location of temporary buildings for maintenance workers that were too close to the hazardous processes highlighting an inadequate siting procedure. It showed a lack of vulnerability analysis and worst case approach, but also a failure to remember the logic of targets removal learned from explosions in refineries (e.g. after La Mède (France) accident in 1991, control rooms became "blast proof"') or in silos (e.g. with the Blaye (France) explosion in 1997 where the administrative quarters were below the silo causing the death of workers not directly necessary to the process.

It can be seen in these cases that lessons from past incidents were not always explored with the aim "what if", rather past accidents were reinterpreted as proof of reliability or resilience instead of warnings of danger. The December 1999 storm that devastated western Europe and created an emergency situation at the French nuclear power plant of Blaye due to loss of power after a flooding of equipment, was fortunately properly managed. The side-effect is that it did not trigger an international strong learning process as Fukushima did. It is considered in retrospect as one of the precursors of Fukushima – an EWS that was lost.

3.6.3 Failures in monitoring and in listening EWS, failures to change

Early warning signs are often missed but there are opportunities during the incubation period to recognise them, to listen to alerts from people, especially during windows of opportunity (Edmondson, 2005) to implement changes. Here again, the challenge is not easy especially in highly complex systems with many EWS, a lot of noise, some difficulties to filter issues and determine the priorities. This is additionally more difficult for major risk prevention with low frequency and probability events.

In the Buncefield accident, the Automatic Tank Gauging (ATG) system preventing tank overfilling had been stuck 14 times in the months before the accident. Sometimes this was logged as a fault by the supervisors and other times it was not. Moreover, the contractor company that installed the ATG system never considered that the gauge should be investigated, even if they had been frequently called to rectify the matter (COMAH Competent Authority, 2011). The problem with measurement of the critical parameter of tank level was therefore known by many people and yet it was not fixed.

The Texas City refinery explosion in 2005 (CSB, 2007) highlighted a few design flaws with latency effects, such as the “antique” flare (build in the fifties) which was abandoned in petroleum standards available since the eighties. The opportunity to remove it was investigated by a former owner of the refinery in the nineties especially under regulatory pressure, but the cost was used as a factor to postpone the corrective actions, as well as the ‘grandfathering’ argument. These missed opportunities to comply to a new regulation in order to improve safety (Ferjencik and Dechy, 2016) were normalised by control authorities.

But one of the most striking lesson from this accident remains the inability to learn (Hopkins, 2008) implying a difficulty to change which was “too little, too late” (Merritt, 2007). The numerous latent flaws (Reason, 1990, 1997) caused by the lack of maintenance were severe "*cost cutting, production pressures, and a failure to invest left the BP Texas City refinery vulnerable to a catastrophe*" (Merritt, 2007). Their severity was visible before the accident by many actors at the refinery (managers, operators "closest to the valves", health and safety engineers, investigators, auditors) (Dechy et al., 2011). A 2003 internal BP audit warned that the reasons for “such a poor state” of the infrastructure “in complete decline” were known to be “culture and money”. The check book mentality was under-fire but was not turned around. The hindsight bias excuse does not apply here (and not only here, see chapter 11 about whistle-blowers, Dien et al., 2020)! It was not a failure of detection of weak signals, nor a myopia or blindness, but rather some deafness and denial to strong signals and inaction. CSB (2007) found: “warning signs of a possible disaster were present for several years, but company officials did not intervene effectively to prevent it.”

In addition, BP managers failed to manage major risks and process safety, as they over relied on the wrong metrics related to worker safety (CSB, 2007; Baker et al., 2007). Notice that BP is not the only company that made this error, it remains a preoccupation in health and safety management. This tragic confusion contributed to their own blindness and deafness. Indeed, process safety and major risks are recognised to be hard to measure in safety literature and practice. However, several efforts have been made by industries to define key performance indicators to benchmark, leading and lagging risk indicators, safety performance indicators. In process safety, a famous indicator is the "loss of containment" (LoC) that is a precursor of an accident (fire, explosion, toxic cloud), which defines the separation between prevention and protection. At Texas City, this indicator was measured and was degrading over time: "*the number of loss of containment incidents at the Texas City refinery increased each year from 2002 to 2004*" (Baker et al., 2007, p187)” "*with an increase of “52 percent from 399 to 607 per year*” (CSB, 2007, p168). These indicators were not in the main picture of SPI’s monitored by BP management. They relied too much on worker safety performance indicators and were measuring an improvement in the lost time injuries statistical indicator. This indicator was among the key performance indicators of the management especially for attributing bonuses to managers (Hopkins and Maslen, 2015) and communicating to control authorities.

The temptation to use a measurable indicator is a common issue as recalled by (Kingston and Dien, 2017) which can lead to the 'McNamara Fallacy' which is attributed to Daniel Yankelovich (Smith, 1972) and is described in four steps:

- “The first step is to measure whatever can be easily measured. This is okay as far as it goes”.
- “The second step is to disregard that which can't be measured or give it an arbitrary quantitative value. This is artificial or misleading”.
- “The third step is to presume that what can't be measured easily really isn't very important. This is blindness”.
- “The fourth step is to say that what can't be easily measured really doesn't exist. This is suicide”.

More generally, the blindness process is more subtle. It can for instance come from over reliance of management tools and processes that put under the light some phenomenon leaving in the shadow some others, reinforcing “organisational blinkers” (Largier, 2008). They can produce "*an effect of blindness by producing an artefact of rationality. They participate to the setting on frontstage of a unique definition of the organisational situation, though other definitions are always present, but stay in the backstage*" (Boussard, 2003). Often "*the most used indicators give more consistency and resistance to some organisational representations*" (Boussard, 2001).

Listening to divergent opinions (as promoted by Navy Submarine in CAIB, 2003) and to ‘bad news’ (e.g. at Texas City, "*bad news was not welcome*", CSB, 2007) is not always easy especially for managers under pressure to achieve high performance without adequate resources. Divergent opinions on the new NASA policy "*Faster, Better, Cheaper"* associated with cost-cutting, by new administrator Dan Goldin were dismissed: "*When critics would raise the possibility that such cuts were going to affect safety the CAIB notes "Goldin described himself as "sharp-edged" and could often be blunt. He rejected the criticism that he was sacrificing safety in the name of efficiency. In 1994 he told an audience at the Jet Propulsion Laboratory, "When I ask for the budget to be cut, I'm told it's going to impact safety on the Space Shuttle ... I think that's a bunch of crap.*" (CAIB, 2003). EWS come from alerts from staff, analysts and auditors who may provide another interpretation. While managers value coherence and coordination in action, for fostering foresight in safety they should value more the diversity of analysis. Indeed, in Cybernetics theories, researchers valued the diversity of views with Ashby's principle of requisite variety that implies a greater diversity of the controlling system to be able the control a complex system (Ashby, 1956; Vautier et al., 2018).

3.7 Discussion and conclusions

High-risk industries invest many resources every day in risk anticipation and many measures have already been in place for many years. However, the failures of foresight recalled here, highlight how industries, their experts and their regulators can fail. Every contributor to risk anticipation and foresight in safety should remain humble, cautious and sceptical and voice their doubts towards the challenge of accident prevention as it remains very difficult in practice. Anticipating and preventing accidents is a continuous struggle or never-ending war, bringing new changes, new risks and new threats, and also new safety degradation to discover before it is too late.

"Disasters '*are not created overnight*"' (Turner, 1976, 1978); accidents are therefore "*hard to obtain*" (Perrow, 1984); and require a "*rare conjunction of a set of holes in successive defences*"' (Reason, 1997). Accidents are not the result of one error but a combination of multiples causes, conditions and influence factors (Dien, 2006, ESReDA, 2009). Accidents develop (Guillaume, 2011) during an "*incubation period*' (Turner, 1976, 1978), which sometimes lasts for years (with "*latent defect*"(Reason,1997); in the example of San Bruno for more than 50 years). "*Latent conditions*"' and "*resident pathogens*" within the workplace and organizations are "*time-bombs*" that can be identified and removed before the event (Reason, 1997) but sometimes they are not. In contrast to Perrow's view (1984), the majority of accidents are not inevitable (Dechy et al., 2012, Dien et al., 2013), because of the frequent occurrence of EWS prior to serious events, with some of them recognised by some actors. This empirical accident modelling makes clear the possibility of accident prevention. But will the opportunities to recognize an accident waiting to happen, be seized in the time window available? Indeed, some windows of opportunity and recovery (Edmondson et al., 2005) are recognised by some actors and require responses which are not always implemented in due time showing a form of apathy.

While high-risk industries devote time, money and analysts to identify hazards, assess risks, learn from early warning signs, near-misses and from others' hard lessons and best practices through benchmarking, many flaws in risk prevention are found in accident reports and sometimes in internal audits and event reports prior to the accident or in external regulatory inspections. These flaws are among the root causes of accidents. The few accident cases (Toulouse, Buncefield, Texas City, San Bruno, Challenger and Columbia) used as references for this analysis have highlighted some of the flaws in risk anticipation and prevention.

There are many techniques, tools and procedures to identify risk and assess related scenarios. Some of the methods have limits, domains of validity, and conditions for being adequately applied and used, but these are sometimes forgotten. For instance, are they adapted to address extreme events or black swans (Taleb, 2007)? Also, we find it necessary to fight the recent growing trend that defines high consequence/low probability as black swans, against which little or nothing can be done. Risk assessment may be incapable of thoroughly quantifying them, but this should not be taken as an excuse. Accidents are made up of a chain of events and focusing on what we already know and understand may help to break such chain and lower both the probability and severity of disasters.

Beyond the methods, implementation is dependent on the judgement of risk analysts. So, who are the analysts (Dien et al., 2012), what are their competencies, what are their collective resources to perform the job of conducting 'risk work' (Power, 2016) or risk expertise (Merad and Trump, 2020)?

Stark (1951) already claimed that foresight is partly reproductive and partly creative. Therefore, foresight in safety requires 'out-of-the-box' thinking and there are some processes to foster imagination better than with traditional risk analysis methods. In other words, although the use of techniques can bring a systematic approach useful to demonstration of safety management to a regulator, identification of risks requires imagination and creativity. Identification of risks requires diversity in the ways of thinking when questioning 'what-if'. Diverse views can be shared in brainstorming including in debates over work practices, in 'speak-up' (Edmondson, 1999), listening to divergent opinions, listening to 'bad news' or to those who disagree even outside the industrial system with citizens, residents, consumers, NGOs (Dechy et al., 2016). In a systemic perspective, this diversity of views is a way to obtain requisite variety to control the system.

As risk is a social construct (Short, 1984) so is foresight in safety. Failures of foresight can be approached as a 'cultural collapse' because of the inadequacy of accepted norms and beliefs (Turner, 1976). A key implication is to remain critical on the processes of risk identification, risk assessment, performance monitoring to detect EWS. As identified by Clarke (1999), 'fantasy planning' may occur sometimes at the expense of actors' consciousness when stakeholders put too much confidence in their collective choices which rely on inadequate assumptions and are impacted by a multitude of biases and constraints. This can lead to the "*decoy problem*", focusing on well-defined problems rather than ill-defined problems which can lead to collective blindness (Turner, 1976).

"*Organizations are defined by what they ignore – ignorance that is embodied in assumptions – and by the extent to which people in them neglect the same kinds of consideration*" (Weick, 1998; p74). Engineering underlying assumptions are not often challenged during these processes. Expected scientific procedures are sometimes inadequate and may lead to inadequate beliefs from stakeholders. Risk management by companies and regulatory science are subject to criticism. Different values and goals may lead to controversies between regulators and high-risk industries but negotiations do also occur. Worst case scenarios are reduced to realistic scenarios and only reasonable changes after near-misses are made. Norms and standards which have been approved by expert groups, institutions are "normalised" (Vaughan, 1996) within the organizational culture and it becomes harder for those in the system to question and challenge. "Fresh eyes" or *Candide*, external auditors and investigators can help and this is known for decades. But, the challenge is for actors of the system to challenge themselves, their competencies, their tools, their assumptions which require some mindset shift, to become more than a sceptic (questioning or doubt attitude in safety culture concepts).

As remarked by Weick (1998, p72) about Turner's input on cultural failures of foresight, the issue is not only about world-views, lenses and paradigms. The *"mastery of pattern generation with sufficient requisite variety to match and register the patterned variety in the complex events* […] *is best captured by the imagery of kaleidoscope': 'just as the image of switching lenses can represent the changing of patterns in the realist schema, the changing of turning a kaleidoscope can represent the changing of patterns in the subjectivist schema, since the patterns of kaleidoscope may be internally generated with minimal dependence on information from outside. Turning a kaleidoscope can: (1) dislodge old patterns, (2) generate new patterns and (3) foster awareness that numerous configurations are possible"* attributed by Weick to Nord and Connell (1993, p117).

This remark invites organisations to create spaces and times where diversity of views and thinking fosters 'requisite imagination' (Westrum, 1992), that can help to recognize patterns, share explicitly doubts and uncertainties about systems behaviour, to identify well-defined and ill-defined problems. The goal is also to understand the assumptions, the artefacts, the tools used, the constraints met by operators, engineers, experts, managers, regulators in conducting their 'riskwork' (Power, 2016) and even to put under questions and scrutiny the expert work and regulatory science (Vaughan, 1996; Llory 1996; Maguire and Hardy, 2013; Boudia and Demortain, 2014; Merad and Trump, 2020). Every study of risk can be considered as a project (Merad, 2010) that has inherent constraints in the resources. The goal or 'preoccupation with failure' (in HRO, Weick and Sutcliffe, 2007) is to wonder if 'safety imagination' highlights or hides risks (Pidgeon and O'Leary, 2000). Spaces may be self-organized informally by groups of engineers such as observed with the 'Debris assessment team' at NASA to characterise the foam strike consequences or institutionalized such as 'tiger teams' after Apollo 13 crisis. During the Columbia mission in space, the informal team was not given the status of a tiger team, and its conclusions were dismissed by mission' managers.

The challenge of foresight in safety is to identify all risks and recognize all EWS. But this is impossible in practice in general and at a given time. A reduced scope is to focus on major risks which implies the critical scenarios, those which escalate and damage system, assets and stakeholders. Some filtering of important signals is necessary otherwise channels are flooded with more and more data to treat. Making sense, prioritising are key processes to develop the relevant focus of resources with issues at risk, and proportionate the risk controls and implement them in due time. Decisions and trade-offs must be made, aided and revised. Safety margins and the burden of proof should be challenged. Especially, time is providing new opportunities to capture new signs and new knowledge to revise assumptions and judgments. Dynamic learning and risk management approaches should be developed and promoted (ESReDA, 2015; Paltrinieri, 2015).

Often, people within the system recognised early warning signs before the accident (Turner, 1976, 1978). These recurring empirical findings reject the hindsight bias excuse (Reason, 1990; Vaughan, 1996; Woods, 2009). This does not mean to reject the risk of the hindsight bias. In Texas City accident, several actors and several processes (auditing, learning) recognised EWS of safety degradation (Dechy et al., 2011). It is clear that some signals are blurred, contradictory or are “mixed signals” (Vaughan, 1996). But organisations are not monolithic (Dien, 2014), and some workers, engineers and managers may know that safety is deteriorating. Many employees, whistle-blowers and citizens have warned before disasters (in chapter 11, Dien et al., 2020). In some case, beyond blindness and myopia pathologies, deafness, denial and apathy are major obstacles to change. The problem is not anymore, a problem of foresight but rather becomes managerial and political related to a lack of adequate reactions.

Echoing Weick’s suggestion (1988) to define organisation by what they choose to ignore, organizations should also be defined by what they choose to remember and forget. Barriers and failures to learn are numerous. Accident and event reports often fail to address root causes (CAIB, 2003; Dien et al., 2012) and can themselves be considered as ‘fantasy’ documents (Birkland, 2009). There are losses of memory and similar accidents recur even in the same organizations (e.g. NASA, BP). Organizational patterns that lead to a failure of foresight are similar (Turner, 1976, 1978). In-depth analysis of accidents already provided the "hard lessons" to be learned especially from other industries (Dien et al., 2004). These lessons are part of an international history of industrial accidents, from which can be derived some "knowledge of accidents" (Dechy et al., 2010, 2016). It can provide useful frameworks to interpret EWS and organizational weaknesses in normal operations (Dechy et al., 2016, 2018) and can develop some specific attitudes, such as vigilance, doubt and prudence as components of safety culture, and ‘preoccupation with failure’ (Weick and Sutcliffe, 2007). The alternative (Reason, 1997) is that managers forget to be afraid and allow drift to occur. In summary, foresight in safety relies on exploitation of existing knowledge and resources and exploration mechanisms (related to innovation, changes) (March, 1991).

After all, practically speaking, what can be done? In addition to previous remarks and suggestions, one key factor to mention here is temporality. Foresight is fundamentally about time which highlights the dynamic nature of managing risk that is either improving or eroding. Time is potentially an enemy with pressures on decision and action but is also a resource as an opportunity to investigate and collect more information about an ill-structured problem, to help make a more objective judgment, to recalibrate a risk model with new data from the real world. Engineers have to make assumptions and decisions, but they have to remain sensitive to warning signs that would confirm or otherwise the safety envelope and margins. Managers are under business and time pressure to make decisions sometimes with insufficient information to understand all implications and side-effects (Ansoff, 1975). Decisions with their rationale and information should be formatted and recorded in order to be monitored with regard to new signals and effects of actions, changes or inactions. In high-risk industries with many risk management provisions, degradation of safety can be insidious, but is announced to some extent by EWS that may be recognised by some actors and may provide windows of opportunity to take a reactive action if only those in control are listening. Will these opportunities be seized or will the reaction be ‘too little or too late’?

3.8 Acknowledgements

To our reviewers: Franck Anner, Sarah Fourgeaud, Alexandre Largier, Bernard Chaumont (IRSN).

3.9 References

Ansoff, I. (1975), Managing Strategic Surprise by Response to Weak Signals, California Management Review, Vol.18 (2), pp.21-33.

Ansoff, I., Mc Donnell, E. (1990), Implanting Strategic Management, Second edition, Prentice Hall International, United Kingdom.

Ashby, W. R. (1956) An Introduction to Cybernetics, Chapman & Hall, London, 1956.

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://sunnyday.mit.edu/Baker-panel-report.pdf.

Boudia, S., Demortain D. (2014), La production d'un instrument générique de gouvernement. Le "livre rouge" de l'analyse des risques, Gouvernement & Action Publique 3(3): 33–53, 2014.

Boussard, V. (2001), Quand les règles s'incarnent. L'exemple des indicateurs prégnants, Sociologie du Travail, 43 533-551.

Boussard, V. (2003), Dispositifs de gestion et simulacres de contrôle, In : V. Boussard, , S. Maugeri, (Eds), Du politique dans les organisations. Sociologies des dispositifs de gestion, l'Harmattan, Paris, pp. 173-191

Birkland, T. A., (2009), Disasters, Lessons Learned, and Fantasy Documents, Journal of Contingencies and Crisis Management, vol 17, N°3.

Carroll, J. S. (2004), Knowledge Management in High-Hazard Industries, Accident Precursors as Practice, in J. R Phimister., V. M Bier., H. C. (Kunreuther Eds), Precursor Analysis and Management, Reducing Technological Risk Through Diligence, National Academy of Engineering of the National Academies

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.

Clarke, L., (1999), Mission Improbable, Using Fantasy Documents to Tame Disasters, University of Chicago Press.

Clarke L., (2006), Worst Cases – Terror and Catastrophe in the Popular Imagination, University of Chicago Press.

Columbia Accident Investigation Board (2003), Report Volume 1, National Aeronautics and Space Administration, https://www.nasa.gov/columbia/home/CAIB_Vol1.html.

COMAH Competent Authority (2011), Competent Authority for the Control of Major Hazards, Health and Safety executive, Buncefield: Why did it happen? The underlying causes of the explosion and fire at the Buncefield oil storage depot, Hemel Hempstead, Hertfordshire on 11 December 2005, Edited by HSE, https://www.hse.gov.uk/comah/buncefield/buncefield-report.pdf

Couturier J., Bruna G., Tarallo F., Chanton O., Dechy N., Chojnacki E. (2016), Quelques considérations sur le risque résiduel dans l'industrie nucléaire, in M., Merad N., Dechy L. Dehouck, M. Lassagne , Risques majeurs, incertitudes et décision : approches pluridisciplinaire et multisectorielle, Editions ESKA,.

CSB (2007). Investigation Report, Refinery Explosion and Fire, BP – Texas City, Texas, March 23, 2005, Report N°2005-04-I-TX. 2007, https://www.csb.gov/bp-america-refinery-explosion/.

Cullen, W. D. [Lord] (2000), The Ladbroke Grove Rail Inquiry, Part 1 & Part 2 Reports, HSE Books, Her Majesty's Stationery Office, Norwich, 2000. [Part 2: 2001], https://www.jesip.org.uk/uploads/media/incident_reports_and_inquiries/Ladbroke%20Grove%20Rail%20Inquiry%20Report%20Part%201.pdf, https://www.railwaysarchive.co.uk/documents/HSE_Lad_Cullen002.pdf.

Dechy N., Bourdeaux T., Ayrault N., Kordek M.-A., Le Coze J.-C. (2004), First lessons of the Toulouse ammonium nitrate disaster, 21st September 2001, AZF Plant, France, Journal of Hazardous Materials 111 pp. 131-138

Dechy, N., Descourrière, S., Salvi O. (2005), The 21st september 2001 disaster in Toulouse : An historical overview of the Land Use Planning, 28th ESReDA Seminar on the Geographical component in risk management, Karlstad University, June 2005

Dechy, N., Rousseau, J.-M., Llory, M. (2011), Are organizational audits of safety that different from organizational investigation of accidents?, Proceedings of ESREL Conference, Troyes, , 18-22 September.

Dechy N., Rousseau J.-M., Jeffroy F. (2011), Learning lessons from accidents with a human and organisational factors perspective: deficiencies and failures of operating experience feedback systems, Proceedings of the EUROSAFE 2011 conference, Paris.

Dechy N., Mortureux, Y., Planchette, G., Blatter, C., Raffoux, J.-F. (2016) ; Explorer « l'imprévisible » : comment et jusqu'où ? actes de la conférence λμ20, Saint-Malo, France

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 IAEA Conference 30 Years of Safety Culture

Dechy, N., Gyenes, Z., Merad, M. (2018), A Review on Toulouse Accident Trials: Can We Learn the Lessons Despite Uncertainty on Direct Causes?Proceedings of the Hazards 28th conference, Edinburgh, U.K., Icheme.

Dechy N., Dien Y., Marsden E., Rousseau J.-M. (2018), Learning Failures As the Ultimate Root Causes of Accidents: Managing Errors in Organizations in 'How could this happen ? Managing error in organizations', Edited by Hagen J., Palgrave Macmillan

Dechy, N., Rousseau, J.-M., Largier, A., Tillement, S., Hayes, J., Journé B., (2018), Using the 'Knowledge of Accidents' in Normal Operation: a Case Study on the Framing of Organisational Diagnosis of Safety Management, Proceedings of the 55th ESReDA seminar on - Accident Investigation and Learning to Improve Safety Management in Complex Systems: Remaining Challenges, Romania, 9 – 10 October, AGIFER

Dien, Y., "Les signaux faibles à l'aune des lanceurs d'alerte" Congrès λμ19 de l'IMdR, Dijon, 21-23 octobre 2014.

Dien, Y. & Llory, M. (2004). Effects of the Columbia Space Shuttle Accident on High Risk Industries or: Can We Learn Lessons from Other Industries? Conference Hazards XVIII, November 23-25, Manchester, UK.

Dien, Y., Llory, M., Montmayeul, R. (2004). Organisational Accidents Investigation Methodology and Lessons Learned, Journal of Hazardous Materials, 111 (1-3), pp 147-153.

Dien, Y., Dechy N., Guillaume, E., (2012) Accident Investigation: from Searching Direct Causes to Finding In-Depth Causes. Problem of Analysis or / and of Analyst? Safety Science, 50 (6), , pp 1398-1407.

Dien Y., Dechy N., Llory M., (2013), Is the Complexity of Hazardous Socio-Technical Systems "Directly" Connected to Major Event Occurrence?, Proceedings of the American Nuclear Society National Meeting, November 2013, Washington, D. C. USA.

Dien Y., Dechy N., (2016), L'impensé est-il impensable ? Ce que nous apprennent les accidents industriels, in Merad M., Dechy N., Dechouck L., Lassagne M., Risques majeurs, incertitudes et décisions, Editions MA- ESKA – ISBN 978-2-8224-0430-3

Dien, Y., Maia, P., Paul S., Røed-Larsen, S., Stoop, J., Marsden, E., (2020), The Whistle-Blowers: Active Actors in Foresight for Safety, chapter 11 in "Enhancing Safety: The Challenge of Foresight", ESReDA.

Diet, (2012), "The National Diet of Japan - The official report of The Fukushima Nuclear Accident Independent Investigation Commission - Executive summary" http://warp.da.ndl.go.jp/info:ndljp/pid/3856371/naiic.go.jp/wp-content/uploads/2012/09/NAIIC_report_lo_res10.pdf, 2012.

Edmondson, A. C. (1999), Psychological Safety and Learning Behavior in Work Teams, Administrative Science Quarterly June 1999 vol. 44 no. 2 350-383

Edmondson, A., C., Roberto, M. A., Bohmer, R., M., J., Ferlins, E., M., Feldman, L., (2005), The Recovery Window: Organizational Learning Following Ambiguous Threats, in W., H. Starbuck, , and M. Farjoun, , Organization at the limit, Blackwell publishing.

ESReDA (2005), editors Roed-Larsen S. R., Stoop J., Funnemark E, Shaping public safety investigation of accidents in Europe, DNV publishing, ISBN 82 5150304 3

ESReDA (2009), Guideline for Safety Investigation of Accidents, ESReDA Working Group on Accident Investigation, (2009), disponible sur le site www.esreda.org

ESReDA (2015) Case study analysis on dynamic learning from accidents - The ESReDA Cube, a method and metaphor for exploring a learning space for safety, edited by Van der Vorm and the ESReDA Project Group on Dynamic Learning Available from www.esreda.org

ESReDA (2015), Barriers to learn, edited by Marsden E. and the ESReDA Project Group on Dynamic Learning. Available from http://www.esreda.org.

Fayol, H. (1916) General and Industrial Management. Institute of Electrical and Electronics Engineering, Paris.

Ferjencik, M. and Dechy, N. (2016). Three accidents in European dynamite production plants: An attempt to improve the external lessons learning. Journal of Loss Prevention in the Process Industries 44, 12-23.

Ferjencik, M., Dechy N. (2020), Loss of Memory as a Cause of Failure of Foresight in Safety, chapter 4 in "Enhancing Safety: the Challenge of Foresight", ESReDA

Ferjencik M., Strucic M., Tulonen T., Marsden E., Stoop J. (2020), Use of Scenarios as a support of foresight in safety, chapter 5 in "Enhancing Safety: the Challenge of Foresight", ESReDA

Feynman, R. (1986), Personal Observations on Reliability of Shuttle, Report of the PRESIDENTIAL COMMISSION on the Space Shuttle Challenger Accident, Volume 2: Appendix F.

Geertz, C (1998), La description dense, in: La description, revue enquêtes, n°6, Ed. Marseilles, pp73-105

Guillaume E. (2011) Identifying and Responding to Weak Signals to Improve Learning from Experiences in High-Risk Industry, PhD doctoral dissertation

Gyenes, Z. and Dechy, N. (2016), Risk and safety management of ammonium nitrate fertilizers: keeping the memory of disasters alive, Loss Prevention Bulletin n°251, October 2016, pp32-36, Edited by Icheme.

Hayes J., Hopkins A., (2014) Nightmare Pipeline Failures: Fantasy Planning, Black Swans and Integrity Management, Edited by Wolters Kluwer, CCH,

Hollnagel, E., Woods, D. D. & Leveson, N. C. (Eds.) (2006). Resilience Engineering: Concepts and Precepts. Aldershot, UK: Ashgate

Hollnagel E. (2014), Safety-I and Safety-II, The Past and Future of Safety Management, Ashgate.

Hopkins, A., (2001) 'Was Three Mile Island a Normal Accident?', Journal of Contingencies and Crisis Management, vol. 9, no. 2, pp. 65-72.

Hopkins, A. (2010). Failure to learn: the BP Texas City Refinery Disaster, CCH Australia Ltd. Wolters Kluvers.

Hopkins, A., Maslen, S., (2015), Risky Rewards: How Company Bonuses Affect Safety, Edited by CRC Press, Taylor and Francis.

Hourtoulou, D. (2002), Projet ASSURANCE – Assessment of Uncertainties in Risk Analysis of Chemical Establishments, E. C. project ENV4-CT97-0627. rapport final d'opération a – DRA-07 – INERIS – Dho-2002-26824, 2002.

Hudson P. (2001), Safety Culture - Theory and Practice, RTO HEM Workshop on "The Human Factor in System Reliability - Is Human Performance Predictable? ", Siena, Italy, 1-2 December 1999, published in RIO MP-032.

Jouniaux P., Hadida D., Dechy N., Marle L., Billy F., Pierlot S., Parrennes F., Rouvière G., Husson D., (2014), "Détection, pertinence et amplification des signaux faibles dans le traitement du retour d'expérience", Congrès λµ19 de l'IMdR, Dijon, 21-23 octobre.

Kingston J., Dien Y. (2017). The McNamara Fallacy Blocks Foresight for Safety, Proceedings of the 53rd ESReDA Seminar "Enhancing Safety: the Challenge of Foresight" Edited A. L. Vetere Arellano, Z. Šimić, N. Dechy, 14-15 November 2017, Ispra, Italy

Kletz, T. (1993). Lessons from Disasters: How Organizations Have No Memory and Accidents Recur. Gulf Publishing Company, Houston. ISBN: 0-88415-154-9, 183 pages.

Lagadec P. (1994). Apprendre à gérer les crises. Les éditions d'organisation. Paris.

Lannoy A., (2016) Limites, insuffisances et apports des approaches probabilistes actuelles, quelles leçons tirer?. in M.Merad, N. Dechy, L.Dechouck, M Lassagne., Risques majeurs, incertitudes et décisions, Editions MA- ESKA – ISBN 978-2-8224-0430-3

Laporte, T.R. and Consolini, P.M. (1991), Working in Practice But Not in Theory: Theoretical Challenges of "High-Reliability Organizations" , Journal of Public Administration Research and Theory, vol.1, n°1, p 19-47

Largier, A. (2008). Dispositif de gestion des compétences et logique métier. Socio-logos n°3. https://journals.openedition.org/socio-logos/1323

Lesca, H. (2001), Veille stratégique : passage de la notion de signal faible à la notion de signe d'alerte précoce, Proceedings of the VSST Conference, Barcelona, Spain.

Lechaudel, J.F., Mouilleau, Y. (1991), Assessment of an accidental vapour cloud explosion - A case study: Saint Herblain, October 7 1991, France", Proceedings of the 8th International Loss Prevention Symposium, pp 333-348, Antwerp, Belgium, 1995.

Leveson N. G., Turner C. S. (1993), An investigation of the Therac-25 Accidents, Computer, 26, 7, pp18-41

Libmann, J. (1996), Éléments de sûreté nucléaire, Édité par l'Institut de Protection et de Sûreté Nucléaire. 1996.

Linkov I., Moberg E. (2017), Multi-Criteria Decision Analysis - Environmental Applications and Case Studies, CRC Press, Taylor and Francis,

Llory, M. (1996) Accidents industriels : le coût du silence, Opérateurs privés de parole et cadres introuvables, Éditions L'Harmattan,.

Llory, M. (1999),L'accident de la centrale nucléaire de Three Mile Island", Éditions L'Harmattan, .

Llory, M. Dien, Y. (2006) Les systèmes sociotechniques à risques : Une nécessaire distinction entre fiabilité et sécurité, Performances n°30 pp 20-26, n°31 pp 9-13, n°32 pp. 20-26,.

Llory, M., Montmayeul, R. (2010) L'accident et l'organisation, Éditions Préventique,.

Llory, M. & Montmayeul, R. (2018). Comprendre l'accident, la pratique de l'analyse organisationnelle de sécurité, Editions L'Harmattan.

Maguire, S., & Hardy, C. (2013), Organizing Processes and the Construction of Risk: A Discursive Approach. Academy of Management Journal, 56 (1), 231-255.

March, J. (1991) Exploration and Exploitation in Organizational Learning, Organization Science, Vol. 2, No. 1, pp. 71-87

Marlair, G. and Kordek M-A. (2005) Safety and security issues relating to low capacity storage of AN-based fertilizers, Journal of Hazardous Materials Volume 31;123(1-3), pp 13-28.

Marsden, E., Dechy, N., Vetere Arellano, A., (2020) Big data analytics and early warning signs, chapter 10 in "Enhancing Safety: the Challenge of Foresight", ESReDA.

Médard, L. (1979) Les explosifs occasionnels, deuxième édition ; Technique et Documentation, Éditions Lavoisier, Volume 2.

Merad M. (2010) Aide à la décision et expertise en gestion des risques, Editions Lavoisier

Merad, M., Dechy N., Dehouck L., Lassagne, M. (2016) Les décisions face aux risques majeurs, retours d'expérience et pistes d'améliorations, in M Merad., N Dechy., L. Dehouck, M. Lassagne, Risques majeurs, incertitudes et décisions, Editions MA- ESKA – ISBN 978-2-8224-0430-3

Merad M. and Trump B. D., (2020) Expertise Under Scrutiny 21st Century Decision Making for Environmental Health and Safety, Springer.

Merritt, C. (2007) Testimony of Carolyn W. Merritt Chairman and Chief Executive Officer U.S. Chemical Safety Board Before the U.S. House of Representatives Committee on Energy and Commerce Subcommittee on Investigations and Oversight, May 16, 2007.

MIIB (2008) The Buncefield Incident 11 December 2005, The final report of the Major Incident Investigation Board, Volumes 1 & 2. Buncefield Major Incident Investigation Board, Richmond, Surrey.

NTSB. (2011). Pipeline Accident Report: Pacific Gas and Electric Company Natural Gas Transmission Pipeline Rupture and Fire, San Bruno, CA, September 9, 2010.

Paltrinieri, N., Dechy, N., Salzano, E., Wardman, M., & Cozzani, V. (2012) Lessons Learned from Toulouse and Buncefield Disasters: From Risk Analysis Failures to the Identification of Atypical Scenarios Through a Better Knowledge Management, Journal of Risk Analysis, 32(8). pp 1404-1419.

Paltrinieri N., Dechy N., Salzano E., Wardman M., Cozzani V. (2013) Towards a new approach for the identification of atypical accident scenarios, Journal of Risk Research, 16:3-4, 337-354.

Paltrinieri, N., Khan, F., Cozzani, V., (2015) Coupling of advanced techniques for dynamic risk management, Journal of Risk Research, 18:7, 910-930,

Perrow, C. (1982) The President's Commission and the Normal Accident, , in D. L. Sills, C.P. Wolf, & V. B Shelanski, (Eds), Accident at Three Mile Island: The Human Dimensions, Westview Press, Boulder, Colorado (1982). 2. p. 173-184

Perrow, C., (1984) Normal Accidents – Living with High Risk Technologies, Princeton University Press,.

Pidgeon N., O'Leary (2000) Man-made disasters: why technology and organizations (sometimes) fail, Safety Science 34, pp 15-30

Power, M. (2016) Riskwork: Essays on the Organizational Life of Risk Management. Introduction." In: M. Power (ed.): Riskwork: Essays on the Organizational Life of Risk Management. Oxford, UK: Oxford University Press, 1–25.

Rasmussen, N. C. et al. (1975) "Reactor safety study. An assessment of Accident risks in U. S. commercial nuclear power plants. Executive Summary". WASH-1400 (NUREG-75/014). Rockville, MD, USA: Federal Government of the United States, U.S. Nuclear Regulatory Commission.

Rasmussen, J. (1997) Risk management in a dynamic society: a modelling problem, Safety Science, 27 (2-3), pp 183-213.

Reason, J. (1990) Human Error, Cambridge University Press.

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

Rogers, W. P. et al., (1986), Presidential Commission on the Space Shuttle Challenger Accident (1986), Report to the President by the Presidential Commission on the Space Shuttle Challenger Accident, Government Printing Office, Washington DC.

Roux-Dufort C. (2003) Gérer et décider en situation de crise : Outils de diagnostic, de prévention et de décision. Dunod. Paris

Simon, H. A. (1973) The Structure of Ill Structured Problems, Artificial Intelligence, 4 (3), 1973, p 181-201.

Short, J., F., (1984), The Social Fabric at Risk: Toward the Social Transformation of Risk Analysis, American Sociological Review, Vol. 49, No. 6 , pp. 711-725

Stark, S., (1961) Executive Foresight: Definitions, Illustrations, Importance, The Journal of Business, Vol. 34, No. 1, (Jan., 1961), pp. 31-44, Published by: The University of Chicago Press

Taleb, N. (2007) The Black Swan: The Impact of the Highly Improbable, Random House,

Thellier, S. (2017) Approche ergonomique de l'analyse des risques en radiothérapie : de l'analyse des modes de défaillances à la mise en discussion des modes de réussite. Thèse de doctorat en ergonomie. Conservatoire National des Arts et Métiers, Paris, soutenue le 12 décembre 2017, 294 p.

Thellier S., Jeffroy F., Cuvelier, L., & Falzon, P. (2018) L'analyse des risques en radiothérapie : quelle alternative à l'AMDEC ? Congrès λμ21, 16 – 18 octobre 2018, Reims, France.

Turner B. (1976), The Organizational and Interorganizational Development of Disasters, Administrative Science Quarterly, Vol. 21, No. 3 , pp. 378-397

Turner, B., & Pidgeon, N. (1997), Man-Made Disasters, Second edition, Butterworth Heinemann [1rst edition: Turner, B. (1978), Wykeham Publications].

Tversky, A., Kahneman D. (1974), Judgment under Uncertainty: Heuristics and Biases, Science, Vol. 185, Issue 4157, pp.1124-1131

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

Vaughan, D. (1999) The Dark Side of Organizations: Mistake, Misconduct, and Disasterr. Annual Review of Sociology, n°25, pp 271-305

Vautier, J.-F., Dechy N., Coye de Brunélis, T., Hernandez, G., Launay, R., Moreno Alarcon, D., P. (2018) Benefits of systems thinking for a human and organizational factors approach to safety management, Journal of Environment System and Decision, 38:353-366

Wagenaar W., A. and Groeneweg, J. (1987) Accidents at Sea: Multiple Causes and Impossible Consequences, International Journal of Man-Machine Studies, 27, pp587-598

Weick, K., E., (1991) The vulnerable system: an analysis of the Tenerife air disaster, in P. J. Frost, et al., eds, Reframing organizational culture, London, Sage Publications.

Weick K. E. (1998) Foresights of Failure: An Appreciation of Barry Turner, Journal of contingencies and crisis management, volume 6, number 2

Weick, K. and Sutcliffe, K. M. (2007) Managing the Unexpected: Resilient Performance in an Age of Uncertaintyy, Second Edition, Jossey Bass.

Westrum, R., (1992) Cultures with Requisite Imagination, in J.Wise, , D. Hopkin,, P. Stager, (eds), Verification and Validation of Complex Systems: Human Factors Issues: Human Factors Issues, Berlin, Springer Verlag, pp 401-16

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.

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

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

"Enhancing Safety: The Challenge of Foresight"

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

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.

ESReDA
European Safety, Reliability & Data Association