



Thinking the unthinkable: A perspective on Natech risks and Black Swans

Elisabeth Krausmann^{*}, Amos Necci

European Commission Joint Research Centre (JRC), Ispra (VA), Italy

ARTICLE INFO

Keywords:

Natech
Black Swan
Technological risk
HILP
Resilience engineering
Foresight

ABSTRACT

Technological accidents are a threat to the population, the environment and the economy. Occasionally, the notion of “Black Swan” event is applied to such accidents as an explanation for why they could not be prevented. By their very nature, Black Swans are considered extreme outliers which are impossible to anticipate or manage. However, technological accidents are generally foreseeable and therefore preventable when the associated risk is managed responsibly and when warning signs are not ignored. Consequently, such accidents cannot be considered Black Swans. We contend that the same holds for technological accidents triggered by natural hazards (so-called Natech accidents) which usually result from a lack of corporate oversight and insufficient application of state-of-the-art knowledge in managing the associated risk. We argue that the successful reduction of Natech risk requires a corporate mindfulness of the risk and the need to address it using updated approaches, the recognition that organizational behavior influences the risk significantly, and risk ownership that departs from the “Act-of-God” mindset which much of the discussion around natural hazards is fraught with. The study also highlights the importance of scientific research and knowledge management to reduce risks.

1. Introduction

On 29 May 2020, the collapse of a diesel tank in the Siberian Arctic spilled 21,000 tons of fuel into a river and a lake. Cleanup is estimated to cost over 1.4 billion USD and it will require at least 5–10 years for the local environment to recover. The accident was reportedly caused by foundation failure possibly due to permafrost thawing, contributed to by corrosion (Sukhankin, 2020). This event was the latest in a long line of major technological accidents with significant human consequences, catastrophic environmental impacts or important economic losses. In March 2019, a major explosion at a chemical facility in Xiangshui industrial park in China killed 78 people and injured a further 716 (You et al., 2020). The Deepwater Horizon accident in the Gulf of Mexico in 2010 caused one of the largest marine oil spills in history, resulting in extensive damage to marine and wildlife habitats, and heavily affecting the drilling, fishing and tourism industries (Snow, 2010). In total, BP paid over 65 billion USD related to the spill in response, cleanup, restoration and settlement costs (Vaughan, 2018).

Major technological accidents seemingly coming out of the blue are sometimes labeled “Black Swan” events to explain why they could not be prevented (e.g. the accident in Bhopal in 1984 (Murphy and Conner, 2012) or the Deepwater Horizon oil spill (Lodge, 2010)). Black Swans are extreme outliers impossible to foresee (Taleb, 2010), and as such can

provide an excuse for risk owners and managers for why no or insufficient risk management measures were taken prior to an accident (Paté-Cornell, 2012). For instance, after the Deepwater Horizon accident the CEO of Exxon reportedly accused BP of doing a great disservice to international oil companies by suggesting that the disaster was not a Black-Swan event but that it instead had implications for the whole industry (Crooks, 2011).

For the chemical process industry, several studies firmly reject the notion of Black Swans but rather point to failures in corporate risk management as accident causes. Baybutt (2016) reviewed 68 incidents and found that all involved some type of (sometimes multiple) deficiency or omission in adhering to established process safety practices. He concludes that “All of the incidents were predictable and preventable.” Similarly, Bridges (2016) indicates that not a single out of 50 analyzed process safety events over a 25-year period was a Black Swan although some in industry referred to them as such. He also highlights deficiencies in corporate risk management as underlying accident causes. This is echoed by Amyotte et al. (2014) who go as far as saying that “There is no such thing as a Black Swan process incident.”, and Thomson (2015) contends that accident analysis almost always shows that warning signs were present before an event but were ignored, and that the “Inability to imagine the consequences of your actions (or inactions) is no excuse.”

^{*} Corresponding author at: Via E. Fermi 2749, 21027 Ispra (VA), Italy.

E-mail address: elisabeth.krausmann@ec.europa.eu (E. Krausmann).

Another technological accident that generated global attention due to its catastrophic consequences is the Fukushima Daiichi nuclear power plant meltdown during the Great East Japan Earthquake and Tsunami (GJET) in 2011. An event of this magnitude was considered beyond the realm of regular expectations and hence a Black Swan by Tokyo Electric Power Company (TEPCO), which operated the plant, and some nuclear power experts (TEPCO, 2012; Song and Kim, 2014; Tosa, 2015; Ogawa, 2016). Fukushima is the poster child of a sub-category of technological accidents which are triggered by natural hazards. These so-called *Natech* accidents are multi-hazard cascading events which have occurred in the aftermath of many natural disasters (Krausmann et al., 2017). The term *Natech* is derived from “natural-hazard triggered technological” accident and was coined by Showalter and Myers (1994) (Fig. 1).

More often than not, *Natech* accidents were considered “unexpected” or “unforeseeable”, forcing them into the Black-Swan class of events. Even more so than for accidents caused by human error or technical failure, the natural-hazard trigger in *Natech* accidents invites complacency in accepting responsibility for an event. After all, natural hazards are often considered inevitable “Acts of God” and no responsibility for their consequences has to be taken (Fraley, 2010). This is also reflected in the Polluter-Pays-Principle, which assigns the costs of preventive or remedial action to the actual polluter but exempts the risk owner from liability if the pollution is caused by “a serious natural disaster that the operator cannot reasonably have foreseen” (OECD, 1992, 1989). The Black-Swan notion – even if not applicable – only reinforces this message to the detriment of effective *Natech* risk management.

This study examines *Natech* risk in relation to the Black-Swan narrative to understand if *Natech* accidents are truly unpredictable and hence unpreventable. Using historical case studies it identifies the reasons for why prevention has so often failed and analyzes why there is a tendency to underestimate these risks. It then discusses approaches for more effective *Natech* risk management vis-à-vis Black Swan and HILP risks.

2. The nature of Black Swans

Black Swans are characterized by three attributes which must all apply for an event to qualify (Taleb, 2010, p. xxii). Firstly, an event must be an outlier with respect to normal expectations, making it unpredictable. Secondly, it has to have a major impact, and thirdly, it can be explained in hindsight, making it appear predictable. Epistemic uncertainty is central to the Black-Swan concept, as such events express the ultimate lack of fundamental knowledge, representing “unknown unknowns” (Paté-Cornell, 2012). Aven and Krohn (2014) distinguish the following three interpretations or types of Black Swans:

1. Events completely unknown to science (“unknown unknowns”, e.g. due to novel chemistry or technology);
2. Events unknown according to a person’s present knowledge (“unknown knowns”, e.g. safety practices known in one company but unknown in another);
3. Events that are known but judged to have negligible probability (e.g. scenarios removed from risk analysis below a specific cut-off value).

The event types above relate to either an objective or subjective lack of knowledge (event types 1 and 2), or represent the acceptance of a certain level of risk (event type 3). Aven (2015) therefore suggests that whether an event is a Black Swan or not lies in the eyes of the beholder. Also Taleb (2010, p. 339) defines a Black Swan as a subjective phenomenon that is unexpected for a particular observer only, but not necessarily for others.

So which of the three Black-Swan types proposed above makes sense for incidents involving highly hazardous activities? From an industrial and process-safety perspective, Black-Swan type 2 and 3 definitions can be ambiguous as they may enable a fatalistic view of accident causation and incorrectly convey the impression that such accidents are inevitable. Event type 2 could, for instance, have manifested due to the failure to learn lessons of the past, leaving knowledge unavailable, or because there was a lack of safety-management oversight in industry, discouraging communication and knowledge transfer. Neither of these causes would be unpredictable or unthinkable but rather a consequence of bad risk management.

Type 3 events, on the other hand, would be subject to the flaws inherent in probability-based approaches to treat risk and uncertainty. Such approaches depend on underlying assumptions that could provide a misleading description of the possible occurrence of future events (Aven, 2013). Also, probability expresses the likelihood or degree of belief that an event will occur given specific background knowledge. This knowledge can be strong or weak, and the associated uncertainties small or large, which affects the resulting probability used for decision making (Norwegian Oil and Gas Association, 2017). Thus, Aven and Krohn (2014) emphasize that decisions on the acceptability of risk on the basis of probabilities alone should be avoided. Needless to say, the strength of background knowledge is also relevant for decision making based on qualitative risk analyses. Taleb (2010, p. 355) takes it a step further and cautions that there is no reliable way to calculate the small probabilities that characterize rare events. It would therefore be irresponsible to rely on such theoretically derived probabilities when taking potentially far-reaching decisions about high-risk activities.

For the purpose of this study we adopt the definition of event type 1 (“unknown unknown”) to denote a Black Swan. For such events, science has not established prediction models and they can truly not be foreseen



Fig. 1. Left: Collapsed structure at a fertilizer producer due to the 2008 Wenchuan earthquake in China (Photo © E. Krausmann); Right: Burning oil from a breached pipeline caused by flooding of the San Jacinto River in Houston, TX, in 1994 (Photo © U.S. Geological Survey).

(Aven, 2013). Event types 2 and 3 do not fall into this category and calling them Black Swans diverts attention away from the fact that more efforts in risk management could have prevented an accident or that a conscious decision was taken to accept a specific risk. Neither of these cases qualifies as a Black Swan in our opinion. Type 2 poses the additional problem that it would require the establishment of an objective threshold for which knowledge can be considered universally available and which cannot. This renders the concept completely subjective, creating loopholes in safety management and difficulties for litigation in case of accidents.

3. The nature of Natech accidents

Natech accidents are a class of cascading events that manifest when the natural and technological worlds collide. The associated risk is therefore not restricted to any particular country or region but is present wherever hazardous industry is located in areas prone to natural hazards. Natech events are a recurring feature in many natural-disaster situations and have often had significant impacts on public health, the natural and built environment, and the local, national or even global economy (Krausmann et al., 2017). However, contrary to common belief, Natech events can also be triggered by “minor” natural hazards, highlighting a discrepancy in the perception of actual versus perceived accident triggers. For instance, in a study reviewing Natech risk management in the European Union (EU), Krausmann and Baranzini (2012) found that lightning and low temperatures were significantly underestimated as accident triggers while the perceived importance of high winds and earthquakes as triggers was greatly overestimated. Climate change and human development, stimulating urbanization and industrial growth, will amplify future Natech risk.

Past experience shows that generally Natech accidents could have been prevented if awareness and recognition of the risk had existed. When prevention fails, because the risk was neglected or beyond-design-basis events occur, adequate preparedness can limit the damage significantly. Natech accidents usually create a complex response environment as they feature a number of characteristics that require targeted planning to guarantee effective crisis response (Steinberg et al., 2008). For example, some natural hazards, e.g. earthquakes, floods or storms, can affect large areas and hence many industrial facilities at the same time. Consequently, they can trigger multiple Natech accidents simultaneously. This can easily overwhelm response capacities as emergency responders are usually not prepared to handle multiple release events at the same time (Necci et al., 2018). This might also lead to situations in which resources are unavailable for some crisis-management actions as efforts to respond to the multiple hazardous-materials releases and the natural-disaster effects on the population compete for the same resources.

Similar to how natural events damage or destroy industrial buildings or equipment, they can also affect engineered protection barriers (e.g. containment dikes, deluge systems) and down lifelines (e.g. power, water, communication) needed for accident prevention or consequence mitigation. Coupled with potentially numerous hazardous-materials releases that need mitigation, the risk of cascading events is high under these circumstances (Krausmann et al., 2017, p. 4). Natech accidents also deserve special attention because standard civil-protection measures ordinarily implemented in case of chemical-release events, such as shelter-in place or evacuation of residents, might not be feasible. The conditions created by a natural disaster might render roads impassable, e.g. due to flooding or debris flows, thereby blocking access of emergency responders to the release site and slowing down response, or impeding evacuation altogether (Steinberg et al., 2008). Similarly, protection from chemical releases by staying indoors (“shelter-in-place”) is only practicable when the structural integrity of a building is intact and has not been weakened by, e.g., a preceding earthquake. After-shocks might then lead to complete building collapse, trapping people inside who seek shelter from the Natech accident.

4. Landmark Natech accidents and why they were not Black Swans

The investigation into the Fukushima nuclear power plant accident – one of the most consequential technological accidents of this century and for some a prime example of a Black Swan – conclusively showed that the Black-Swan notion did not stick. Rather, the accident was the result of insufficient design assumptions, faulty decision-making and complacency, arising from oblivion to the dangers of siting hazardous facilities on a tsunami-prone coast, and failure to consider natural-hazard records from the past (NAIIC, 2012; INPO, 2011). The official investigation report of the National Diet of Japan concluded that Fukushima was a man-made disaster, caused by “collusion between the government, the regulators and TEPCO, and the lack of governance by said parties” (NAIIC, 2012).

Many other important Natech accidents have been associated with an element of surprise, using adjectives like “unexpected”, “unforeseen” or “surprising” to describe the accidents’ causes and dynamics. In doing so, these events are shifted into the realm of Black-Swan events as the surprise factor suggests that they could not have been foreseen and hence prevented. In the following, we present examples of Natech accidents considered unexpected and we contend that all of them could likely have been prevented with mindful risk management and consideration of all information available.

4.1. Tailings dam break, snowmelt and rain, Romania, 2000

In January 2000 a tailings dam at a gold-mining operation in Baia Mare breached and released about 100,000 m³ of tailings waste containing cyanide, copper and other heavy metals. About 50–100 tonnes of cyanide entered several rivers (including the Tisza and Danube) before reaching the Black Sea, affecting some 2000 km of the Danube’s catchment area in Romania, Hungary and former Yugoslavia (UNEP/OCHA, 2000). The toxic load in the rivers resulted in major kills of fish and other species and was considered the worst environmental disaster since the Chernobyl nuclear power plant accident in 1986 (BBC, 2000). In the Tisza River alone some 1200 tonnes of dead fish were reported.

At the time of the accident snow had accumulated on the pond surface and it was raining, melting part of the snow cover and increasing the water burden in the reservoir which overflowed and failed. No provisions existed for the emergency discharge of the tailings to conserve dam integrity in case of uncontrollable water input into the system (UNEP/OCHA, 2000). The operator of the mining operation blamed the accident on excessive snowfall and downplayed the reports of damage as grossly exaggerated (BBC, 2000). The investigation into the accident concluded that the spill was caused by design deficiencies and challenges related to the operation of the pond, and was contributed to by unusual, though not unprecedented, weather. The circumstances under which the relatively new pond system failed could in principle have been foreseen (UNEP/OCHA, 2000). This *trans*-boundary accident was one of the events that led to increased awareness of Natech risks in the EU and recognition of the need for better governance of the risk.

4.2. Chlorine release from a chemical facility, flood, Czech Republic, 2002

In August 2002 the river Elbe burst its banks due to heavy rains in Central Europe. On 15 August the flood inundated a chemical facility in the Czech Republic, where it triggered the release of over 80 tonnes of toxic chlorine (Fig. 2). When the water flooded a storehouse containing pressurized chlorine tanks, some of them were lifted by buoyancy, tearing off the safety valves of a full tank in the process (Hudec and Lucš, 2004). Most of the chlorine was released into the floodwaters, and there were no fatalities as the site had already been evacuated. However, the environment and agricultural land near the chemical facility were severely affected.



Fig. 2. Flood-triggered chlorine release (in yellow) into the air and floodwaters in the Czech Republic in 2002 (Photo © Václav Vašků). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

The flood height at the site exceeded the water level expected during a 100-year flood, for which the facility was prepared, by 1.3 m, rendering the implemented anti-flooding measures ineffective (eNATECH, 2018). Hudec and Lucš (2004) indicate that the flood arrived from an unexpected direction and that the speed of inundation was unlike that of any flood observed over the past 100 years. In contrast, historical records show that similar floods had already happened in the area (P. Danihelka, personal communication, 2020). Consideration of the available historical data could have raised awareness of the risk of extreme floods at the site and possibly have led to more adequate protection measures.

4.3. Chemical facility fires, flood, USA, 2017

In August 2017 Hurricane Harvey hit Texas as a Category 4 hurricane, delivering the most rain of any hurricane in recorded history over the Houston area. A chemical facility located in a floodplain was inundated and suffered fires when organic peroxides, reactive substances that require refrigeration, decomposed violently (CSB, 2018). Cooling capabilities were lost when primary power and back-up generators failed due to the flood. Upon realizing the magnitude of the situation, company personnel moved the substances into refrigerated trailers in an attempt to evacuate them to higher ground. However, it was too late to pull the trailers out of the flooded area, and they were left when the operator evacuated the site. Eventually, the temperature inside the trailers rose until the substance started to self-combust. 200 residents in a 1.5-mile radius around the facility had to be evacuated and 21 people were hospitalized (Lozano, 2020).

The facility operator is currently being prosecuted for releasing a toxic substance by not properly preparing for a hurricane. Although located inside a designated flood zone and having been warned by its insurance company that it was at risk, the company did not consider the flooding of safety systems (power, cooling) a credible risk (Lozano, 2020, CSB, 2018). In contrast, the operator sustains that the fire was caused by an Act of God and it does therefore not bear criminal liability for the accident (DiStefano, 2020). The outcome of the court proceedings will be an interesting precedent for determining a company's liability in the face of storms driven by climate change. But regardless of the verdict, this accident might have been avoidable had all available

information, e.g. on worse flooding in 1994 and 2015 (DiStefano, 2020), been considered.

4.4. Marine oil spill, underwater landslide, USA, 2004

In September 2004, Hurricane Ivan caused a submarine landslide in the Gulf of Mexico (GoM) that toppled an offshore rig and severed 25 connected sub-sea wells which were buried under a massive amount of mud. The combined efforts of the operator and government to plug the wells have not been successful. There has been an ongoing and little publicized oil release from the site ever since, making it the longest oil spill in U.S. history. If left unchecked, it is estimated that the release could continue for the next 100 years or more (BSEE, 2020, Casey, 2019). The most recent federal assessment found that since 2004 the accident has been spewing as much as 4500 gallons of oil per day into the Gulf. This is about a thousand times more than the volume indicated by the operator (Mason et al., 2019).

The risk of underwater mudslides caused by storms or earthquakes is not new and the GoM shows signs of past underwater mudslides (Casey, 2019). The region is also frequently battered by strong hurricanes, and the risks of building infrastructure in unstable areas prone to mudslides is known. Nevertheless, the rig operator contends that the spill was an Act of God under the legal definition and that there was no evidence to prove that any of the wells were leaking. 200 million USD in cleanup efforts later and having fixed only a third of the leaking wells, the operator has sued the U.S government, claiming the return of about 450 million USD left in trust to cover the cleanup and recovery costs (Fears, 2018). Offshore infrastructure in the GoM continues to be vulnerable to mudslides.

5. Why do we underestimate Natech risk and are surprised when something happens?

Natech accidents are a frequent byproduct of natural events, suggesting that by now the root causes of these accidents are well known, lessons have been learned and that the risk is more effectively managed. However, contrary to expectations, Natech accidents keep occurring, indicating persisting gaps and deficiencies in corporate Natech risk-management systems and government oversight. Like for other types

of risk, and in particular those related to multi-hazard situations, different factors drive Natech risk. This renders risk reduction more complicated, albeit not unmanageable. These factors are anchored in the characteristics of Natech risk, risk-governance challenges, human biases, and socio-economic context which increase overall vulnerability and risk, and may reward risk-taking behavior (Krausmann et al., 2019).

5.1. Risk-management traditions and the Act of God doctrine

Natech risk management is a multi-disciplinary topic which cuts across traditional professional boundaries, involving different scientific domains and stakeholder communities that usually do not interact much with each other. At international level, the difficulties of placing the reduction of natural and technological risks under the same umbrella are plain to see with the implementation of the Sendai Framework for Disaster Risk Reduction (UNDRR, 2015) which aims to be all-inclusive in terms of hazards and stakeholder involvement. While this is in principle a step forward, the change in mindset needed to accompany such a move, including the creation of an equal footing between natural and non-natural hazards as well as recognition of the differences in risk-management approaches, has not happened. The natural-risk community focuses on the social drivers of vulnerability and on crisis response while failing to appreciate that for technological risks prevention is key (and to a limited extent preparedness). At the same time, the technological-risk community ignores socio-economic aspects of vulnerability or links to the surrounding territory because its prime objective is to identify accident triggers and pathways at site level.

Much of this discrepancy is due to historically grown approaches for coping with unwanted events. Natural events are often considered an Act of God – also from a legal perspective (“force majeure”). This means that they are assumed to be beyond human control and influence, in principle absolving humans of any liability for losses (Fraley, 2010). Accordingly, the main focus for managing natural risks has been on the response side and hence on disaster management, rather than on prevention and risk management. In contrast, a technological hazard can be reduced or even eliminated to ensure that the crisis will not materialize at all. Also, technological risks always have a risk owner responsible (both legally and operationally) for managing the risk-reduction process. Consequently, the technological-risk community has always focused on risk- rather than disaster management.

Natech risk is sandwiched between these two worlds, and neither community feels very much at ease with taking ownership of the risk. This has already resulted in cases where it was hard for authorities to establish if a company was the victim of a disaster or responsible for it (e.g. Arkema fires in Texas in 2017 (Hersher, 2020)). With Natechs being technological accidents, the risk is clearly within the purview of the operator of a hazardous installation and hence with the technological-risk community. These are also the only actors who have the knowledge and tools to manage the risk effectively. However, industry and experts alike sometimes hold the mistaken view that Natechs belong to the natural-risk community, as the trigger of the accident is natural and not man-made (Krausmann and Baranzini, 2012). This has led to situations where natural hazards were neglected or insufficiently considered in the design and operation of facilities, and where operators then expressed consternation about Natech accidents they had not foreseen or protected against (see examples in Sections 1 and 4). EU law, for instance, has clarified the responsibilities conclusively, and operators of high-risk chemical establishments in the European Union subject to the Seveso Directive are obliged to explicitly consider natural hazards in their safety documents (European Union, 2012). In other parts of the world the situation may be less clear, and undefined obligations of industry owners or the fragmentation of responsibilities between different ministries and government agencies may have detrimental effects on Natech risk-management oversight.

5.2. The intricacies of Natech risk

Owing to its multi-hazard nature, Natech risk is a risk class that needs special treatment due to the complications generated by the natural-hazard trigger. As discussed in Section 3, the possibility of multiple and simultaneous accidents over large areas, the increased likelihood of cascading events, and the accompanying challenges in managing the emergency, might overwhelm on- and offsite response capacities alike. Preparedness is fundamental for ensuring readiness when a natural event hits an industrial facility, provided that emergency plans are based on realistic assumptions which often they are not.

For instance, although safety measures and systems in place to prevent accidents or mitigate their consequences are usually not designed to resist natural-hazard loading, there is the misconception that they will also protect against Natech accidents. Hence, these protection barriers are believed to remain intact and functional during a natural event, despite strong evidence from past Natech accidents that suggests otherwise. Accident analyses showed that in addition to damaging process and storage equipment, earthquakes can rupture retention bunds around tanks, or floods can cause containment dikes to overflow. In these cases, any prior spills from the natural event would not remain contained (e.g. Girgin, 2011; Krausmann et al., 2010; Steinberg et al., 2008). Also, the main goal of natural-hazard resilient design for buildings and other structures in industry (e.g. Eurocodes, 2021; ASCE, 2015) is the prevention of structural collapse and hence the preservation of life safety but not necessarily the avoidance of loss of containment.

Similarly, natural-event damage to on- and offsite water storage and distribution infrastructure has repercussions on process cooling or fire-fighting, while power blackouts may disrupt active safety systems (e.g. cut-off valves). Also, there is often a blind reliance of operators on the continuous availability of offsite utilities and response resources, should onsite systems fail. This may be a valid approach in case of accidents caused by conventional triggers, but natural events can affect on- and offsite systems alike. This is a painful insight from, e.g., the Fukushima accident, which many industry operators in natural-hazard areas have not fully embraced yet. Since assumptions can only be tested during an accident, a cavalier attitude towards preparedness may result in potentially significant losses that could easily be avoided.

5.3. Natech risk assessment and the drawback of scenario cut-off

Directly linked with the intrinsic features of Natech risk is the complexity of Natech risk analysis. Extensions to traditional risk-analysis methodologies are needed to capture the multi-hazard nature of the risk and the multitude of possible simultaneous scenarios, regardless of the analysis approach chosen (Krausmann, 2017). Also, as Gowland (2013) and Murphy and Conner (2012) note, common hazard-identification tools and techniques, such as HAZOP or “what if” analysis, may be limited and shy away from building multiple failure events. If the risk analysis is deficient and neglects Natech scenarios, the resulting preparedness levels will be poor as past accidents showed.

Studies aiming to compare risk levels at a representative industrial facility subjected to earthquakes and floods, clearly demonstrated the importance of Natech scenario contributions to the total individual and societal risk (Antonioni et al., 2015, 2007). These risk increments can in extremis lead to an exceedance of risk acceptability thresholds with possible repercussions on operating licenses. This might explain at least in part the reluctance of some operators to systematically analyze Natech risks at their facilities to avoid compulsory retrofitting and other costly updates to their safety-management systems (personal communication, 2010).

Also, in spite of the increasing availability of methodologies and tools for capturing Natech risk, their uptake has been slow. With Natech being a multi-hazard risk, data from different disciplines (natural and technological sciences) is needed for the risk analysis. Natural-hazard information is a particular problem because operators of hazardous

installations might not have easy access to it or not know how to use it in the assessment process. For some natural hazards, e.g. hydro-meteorological events, the data is not static but can be affected by climate change, requiring periodic reviews of the natural-hazard assumptions that went into the risk analysis. With the exception of the European Commission's RAPID-N system (Girgin and Krausmann, 2013), no tool unites the necessary natural-hazard and technological-risk analysis models, which makes the analysis more cumbersome and might intimidate the user into abandoning the analysis altogether. Additionally, even in the European Union there is no guidance or minimum criteria for operators on how and at which level of detail natural hazards should be considered in the design and operation of hazardous facilities, leaving them considerable freedom in how to conduct the risk analysis.

Failing to consider Natech scenarios can also lead to a severe underestimation of risk levels used for scenario ranking and cut-off. Scenario cut-off is a common practice in industrial safety where a limit probability is defined according to some acceptability criteria below which scenarios are deemed so unlikely as to be negligible. The residual risk is then accepted. Sometimes, scenarios that can be imagined but for which there is no evidence are also dismissed as not credible (Murphy and Conner, 2012; Nafday, 2009). Since it is too expensive to design for all (extreme) events, this approach helps to save resources by screening out scenarios considered less important. However, the assumptions underlying the definition of acceptable risk and negligible probability can be highly uncertain or flawed, and absence of evidence of a risk is not evidence of its absence (Aven, 2015; Taleb, 2010, p. 55).

Clearly, scenario cut-off can only work when risk-analysis assumptions are sound and subject to low uncertainty, and all significant risk contributors have been captured. This is not the case for risks due to natural hazards where the possible scenarios are highly variable and uncertainties quite large. Also, the weakness of such an approach is immediately obvious as the artificial cut-off means that low-probability scenarios with potentially high consequences (so-called High-Impact Low-Probability events or HILPs) could be lost from the risk-management process, leaving significant gaps in prevention and preparedness (and response).

In our experience, Natech accidents are quite frequent and hence there is no "absence of evidence". Some major Natech events were unquestionably HILPs, while not a single Natech we encountered would have qualified as a Black Swan. In a proper risk analysis the associated scenarios and their likelihood would have become evident and risk-reduction measures could have been implemented. Unfortunately, scenarios that feature a combination of conditions and events which are each plausible on their own, are often disregarded as extremely unlikely or even impossible when taken together (Aven and Krohn, 2014). Lack of a systematic analysis of Natech risk, including disregard of the reliability and robustness of data and models used, might result in errors in probabilities and the discarding of potentially important risk contributors.

5.4. Natech risk governance

Risk governance describes the structures and processes for collective decision making related to identifying, assessing, managing and communicating a specific risk. The governance process is based on the interplay between governmental institutions, economic forces and civil-society actors and needs to consider institutional arrangements and political culture, including different perceptions of risk (Renn, 2008, pp. 8-9). Renn and Walker (2008) argue that with the emergence of new types of risk and increasing complexity, risk governance is becoming exceedingly important. They caution, however, that governance mechanisms might lag behind the processes that drive change, with potentially deleterious effects on the handling of risk.

Due to its multi-hazard and multi-stakeholder nature the governance of Natech risk is challenging. Also, since natural hazards can impact

large areas simultaneously, effective Natech risk governance would require a territorial approach to address the protection of individual industrial installations and their possible safety-relevant interactions with neighboring industry, lifelines and communities (Suarez-Paba et al., 2020). In some countries, the potential for cascading (or domino) effects is analyzed from a general industrial-risk perspective, and land-use planning around high-risk industry aims to ensure the protection of the surrounding communities from industrial accidents (e.g. in the EU in the context of Seveso Directive implementation (European Union, 2012)). However, none of these actions focuses on Natech risk, and critical dependencies on external resources, including lifelines, or natural-hazard and Natech impacts on emergency-response procedures or first responders are seldom – if ever – assessed.

Risk governance (including at corporate level) should ensure that risks are understood, managed and communicated (OECD, 2014). This characterization assumes that risks can be managed to reduce them to an acceptable residual level. However, not everybody shares this point of view. Perrow (2011), for instance, argues that accidents are inevitable in complex and tightly-coupled systems which cannot be made safe despite our best efforts. Therefore, in his view some high-risk technology may be too dangerous to even exist. This contrasts with the benefits society gleans from a myriad of industry products, and a tradeoff is usually sought between what is deemed acceptable considering the "greater good" and what is not. This is where risk management comes into play.

5.5. Natech risk management

Risk management deals with the identification, analysis and control of a risk. For Natech (and all other technological) risks, the risk owner (a person or entity) has the authority to manage the risk and the accountability for doing so (ISO 31000, 2018). For risk management to be effective, a risk – once identified – has to be acknowledged by the risk owner. A multitude of possibly conflicting and often intangible issues are usually on a manager's radar, making it challenging to balance interests and keep focus on the essential business risks. Indeed, there is overwhelming evidence that risk-management failures were triggers of or key contributors to many technological (including Natech) accidents, big and small. Baybutt (2016), in his analysis of almost 70 accidents in the chemical process industry, identified notable similarities in deficiencies and omissions across events, including: deficient design, failures to identify non-routine operations, lack of or poor safety reviews after process changes, inadequate process safeguards, or non-compliance with industry or company standards and practices. In her review of accident investigations by the US Chemical Safety and Hazard Investigation Board (CSB), Blair (2004) found that in every investigation, failures of the management system in place to prevent accidents were causative factors. Wood et al. (2017) identified 12 underlying causes of chemical accidents, including failures of risk assessment, corporate disconnect from risk management, and failure to manage risk across organizational and geographic boundaries. Murphy and Conner (2014) contend that the root causes of all major process-safety incidents were management-system deficiencies.

Along the same lines, a study of major corporate crises across different types of production sectors highlighted root causes indicative of "organizational risk blindness" and a flawed attitude towards performing proper risk management (AIRMIC, 2011). Akkerman and van Wassenhove (2018) note that management is often too slow in picking up problems that are building up, and they identified inadequate managerial sense-making, willful denial and flawed decision making as root causes of many incidents in the production environment.

Another common thread that emerges from these and many other studies is the near ubiquitous failure of organizations to use information from the past to prevent incidents in the future. For instance, the Fukushima accident could likely have been prevented if information on large historical tsunamis on that coastline (Synolakis and Kanoğlu, 2015) had been heeded and had the power plant been constructed

elsewhere or on higher ground. Taylor et al. (2015) note that organizations' failure to learn from past events was a recurring issue in many major accidents. Kletz (1993) highlights the difficulties with retaining information from previous incidents and deplors poor knowledge sharing, failure to use available knowledge, and corporate memory loss due to changes in staff and management, frequent ownership changes, and instability in business continuity. Additionally, the valuable learning opportunity afforded by the study of near misses is largely overlooked in industry (Murphy and Conner, 2014).

Major crises are always preceded by multiple warning signals and precursors that should alert companies to impending disaster. These signals can be weak or strong, and unfortunately often go unheeded. Weak signals are frequently perceived only as noise, making it difficult for them to be detected (Leveson, 2015). Even in case of strong signals, when the writing is on the proverbial wall, high-inertia risk management may fail to react fast enough to allow intervention before a loss occurs. Fear of false alerts or downright denial may mean that information is not communicated or that the potential severity of a situation is not believed at the decision-making level (Paté-Cornell, 2012).

Inadequate risk management, fueled by weaknesses in corporate and government oversight, is therefore at the bottom of a great many incidents and crisis situations in the industrial sector. Rasmussen (1997) contends that over time organizations tend to drift to a higher risk state, relaxing safeguards and controls as they try to accommodate conflicting business goals and tradeoffs. Natech risk management is fraught with the same deficiencies, aggravated by the added layer of complexity inherent in Natech risk. So what does this mean for the Black-Swan debate? It would seem highly disputable that incidents triggered by poor risk management are explainable and predictable only after they happened. For instance, accidents facilitated by knowledge gaps resulting from failure to learn (and remember) would in principle fall under the type 2 Black-Swan category of Section 2 where the absence of subjective knowledge determines if an event qualifies as a Black Swan or not. Clearly, one would be hard pressed to consider such accidents as unforeseeable or surprising. Similarly, the failure to observe and react to warning signals deprives an organization of the chance to address incidents while they are still minor anomalies (Mascone, 2013). The issue is therefore not a fundamental inability to foresee or anticipate an incident (and hence not the notorious Black Swan) but rather bad management caused by risk blindness at corporate (and government) level. Paté-Cornell (2012) suggests that government and industry are using the term Black Swan too liberally in the wake of disaster as an excuse for poor planning. Interestingly, the cost of risk-management failures is frequently underestimated (OECD, 2014), providing further evidence that its role as principal causative factor of catastrophes and losses is not fully appreciated.

5.6. Socio-economic context

The emergence of a risk and the subsequent failure to manage it often stem from a concurrence of factors, such as group interests and power (which determine exposure and vulnerability), economic pressure, or public and media indifference. Leaving lack of political will and corruption aside as reasons for failed risk management, economic considerations are a powerful driver in decision making which can – intentionally or unintentionally – lead to bad safety decisions. Productivity gains, short-term optimization of costs and operational efficiency, or increasing a company's shareholder value often come at the expense of safety (Wood et al., 2017). Also Dekker (2004) discusses the tension created by trying to reconcile the fundamentally irreconcilable goals of operating safely and staying in business while Woods (2006) highlights the series of mishaps that befell NASA after its adoption of the “faster, better, cheaper” policy. Besides, inappropriate incentives sometimes reward risk-taking behavior by prioritizing performance over safety (Hopkins and Maslen, 2015). After the BP Texas City refinery fire in 2005, an analysis showed that under BP's system of executive

incentives, 70% of executive bonus accounted for financial performance while a mere 15% were attributed to attained safety targets. This might have inadvertently distorted the company's risk-management objectives (Airmic, 2011).

These effects may be magnified in countries suffering from economic instability and for activities with poor profit margins (Wood et al., 2017). Where resources are stretched, the risks perceived to be the most critical and not too infrequent are prioritized (which ultimately translates into dismissing all HILP risks). Natech risk is mostly (and often wrongly) perceived to be non-critical for the reasons discussed in the previous sections (improper or no risk assessment, Act of God mindset). Also, industry is generally reluctant to make investments not considered self-financing when major (Natech) events are presumed to be extremely unlikely and to possibly never materialize at all. Economic constraints may also mean that physical industrial infrastructures deteriorate due to age or neglect (Quarantelli, 1997), making them particularly vulnerable to natural-hazard forces and thereby adding to the risk of major Natech accidents. Wood et al. (2017) note that causes are not mutually exclusive, as the presence of one underlying risk factor can make an industrial site susceptible to other dangerous conditions and mindsets that can eventually lead to disaster.

There is a recognized pattern that governments rarely engage proactively in managing chemical (and Natech) accident risks until one or more major accidents have occurred (Wood et al., 2017). The sudden media visibility and public interest in the wake of a major event usually mean that the effectiveness and application of existing safety laws, standards and industry practices come under close scrutiny. Where gaps are identified, improvements quickly follow while the specter of the accident is still present in people's minds. After Fukushima, regulators stress-tested nuclear power plants in the EU and updated nuclear emergency-response plans to improve the management of the related risk (European Commission, 2012). This shows how quick government and operator action is possible when media attention is high and public pressure strong. This is also an example of how society's risk perception and risk tolerance can shape decisions (although risk perception alone is not a good guide for making choices due to its subjectivity and the resulting decision bias). The downside is that once media attention abates, also stakeholder interest fades, and a risk might no longer be considered a threat. This is usually accompanied by a redefinition of priorities and a drop in resources made available for mitigating the risk. Taylor et al. (2015) contend that this lack of interest can lead to an erosion of safety standards which often goes unnoticed, threatening decades of progress in risk reduction.

5.7. Human fallacies and cognitive biases

The frequent surprise at major Natech (or other) accidents which makes some stakeholders resort to the Black Swan narrative is also linked to human fallacies and personal biases that can corrupt the experiences we draw on for estimating risks. These biases do not trigger accidents and are not meant to provide an excuse for flawed risk-management practices. However, they offer additional insight into why our handling of risks is often so inadequate. Incidentally, according to Taleb (2010, p. 50) these fallacies and biases are what makes us blind to true Black Swans.

Confirmation bias is the gathering and interpretation of information that bolsters our prior beliefs or supports our existing position, even in the face of contrary evidence (Taleb, 2010, pp. 51ff.). In other words, we look for evidence that confirms our beliefs but ignore facts that would refute them. If we then generalize based on this preselected information, poor decisions can result. During Hurricane Harvey, the ride-out crew at the Arkema plant in Crosby, TX, was convinced that the flood height at the site would be limited as this was what had happened during previous floods. Consequently, they did not adapt their flood defense strategy even when the weather forecasts predicted further rain. When the floodwaters kept rising and the ride-out crew realized that the water

would short-circuit power to the refrigeration systems that kept the organic peroxides on site from combusting, it was too late for moving them offsite (CSB, 2018). That time had come and gone, and plant personnel could only watch while the accident unfolded.

The *narrative fallacy* addresses our tendency to construct simplified stories out of sequential facts to reduce the dimension of an event and make sense of the world (Taleb, 2010, pp. 62ff.). By explaining events in a simplistic way, patterns in random data might appear where there are none, and the illusion of understanding is created which shapes (and distorts) our expectations of the future. This illusion gives us the misplaced confidence to linearly project into the future with potentially wrong conclusions due to our simplified explanation of the past. The Turkey illusion, in which the well-fed and cared-for turkey could not imagine that the good life would come to a sudden and catastrophic end with the arrival of Thanksgiving (Taleb, 2010, p. 40), is a graphic illustration of the fallacious belief in linear model projections from limited data. When in 1994 the San Jacinto River in Texas burst its banks after heavy rainfall in the wake of Hurricane Rosa, several hydrocarbon pipelines crossing the floodplain ruptured, releasing flammable materials into the floodwaters which eventually ignited. The design envelope of most pipelines that suffered damage did not include flood hazards and used only generic design criteria. Believing design assumptions could be stretched to accommodate also flood-related hazards, most pipeline operators in the affected area continued operations without evaluating if their pipelines would eventually be able to resist (NTSB, 1996).

Taleb (2010, pp. 85ff) also contends that *human nature* is designed for linear causality which makes it difficult for us to perceive Black Swans and other rare events with their complex causal relationships. Failing to grasp complexity, we proceed under a business-as-usual scenario, and behave as if Black Swans and HILPs did not exist. These very infrequent events go counter to our appetite for instant “feedback” and our aversion to long periods of waiting in anticipation of an event. Hence, if nothing happens for long stretches of time we might delude ourselves into thinking that nothing will continue to happen in the future, making us complacent and mentally inert. For example, when the Tohoku earthquake hit the Cosmo Oil refinery in Tokyo Bay in 2011, one storage tank in the liquefied petroleum gas (LPG) tank farm was filled with water for inspection. Contrary to good industry practice, the water had already been in the tank for 12 days rather than the recommended 2–3 days (personal communication, 2011). The LPG tanks had undergone proper earthquake design – assuming LPG filling. Since water is almost twice as heavy as LPG, the additional weight exceeded seismic design assumptions and the first earthquake shock cracked the tank’s support braces. The aftershock that followed caused the tank to collapse, tearing connected LPG pipes while falling. The leaking LPG ignited, and the fire continued to be fuelled through an emergency shut-off valve on a pipe which had been manually switched to open. The ensuing blaze and explosions destroyed the whole tank farm while also triggering domino incidents (including a fire) at two neighboring facilities (Krausmann and Cruz, 2013). Neither bad industry practice nor the switching of the valve in violation of safety regulations had raised any concern at the refinery prior to the earthquake, pointing to severe complacency issues which eventually led to disaster.

Another human trait is the disregarding of *silent evidence* which reduces the information used for predicting the future to the evidence that catches the eye rather than searching for and considering what is there (Taleb, 2010, pp. 100ff.). This creates a sampling bias that distorts our perception of reality and how likely events really are. For instance, minor incidents often go unnoticed due to a reporting bias that favors high-consequence accidents. Also near misses are rarely reported while their analysis would be crucial to understand if an accident failed to materialize out of sheer luck or because protection measures were effective. This knowledge would be critical since it affects failure rates used in risk analysis. Natech events tend to be even more underreported than accidents due to technical failures or human error, and the derived event probabilities and risk estimates might be unrealistically low,

leading to a potentially dangerous de-prioritization of the risk. In reality, analyses of major industrial accident databases found that 2–5% of all accidents were indicated as caused by natural hazards (Suarez-Paba et al., 2020). Also, while Natech accidents appear comparatively lower in numbers in the analyzed datasets, their consequences might exceed those of the average technological accident. In an analysis of onshore pipeline accidents in the USA over a 27-year period and different reporting regimes, Girgin and Krausmann (2016) found that about 6% of all events in the dataset were triggered by natural hazards, while accounting for 18% of total economic costs. The study also found that 24% of Natech events had originally been incorrectly categorized as *not* being natural-hazard related, further leading to an underestimation of the actual risk. Only a painstaking analysis of the dataset involving automatic classification followed by expert review revealed this discrepancy.

The *ludic fallacy* is centered on our focus on well-known sources of uncertainty, and our tendency to predict the future with tools and models that cannot capture rare events. Yet we continue to believe the numbers these predictive models yield and base important decisions on them, happily oblivious to their inadequacy (Taleb, 2010, 122ff.). Gigerenzer (2015) is equally critical about the predictive capabilities of mathematical models, adding that the numbers these models produce of an uncertain risk create a false sense of certainty, thereby possibly doing more harm than good. Nafday (2009) summarizes the situation by asserting that “No probabilistic model based on *in-box* thinking can deal with *out-of-box* type events.” From a Natech perspective, we have often encountered cases in which operators had (laudably) considered natural hazards in the design of a hazardous installation but failed to reflect on what would happen if assumptions were inadequate or exceeded, e.g. if flood levels were higher than the design flood, if an earthquake exceeded the design-basis severity, etc. This is the crux of the problem. We generally focus on the ordinary but fail to account for the exceptional which escapes our *in-box* thinking. And where there is no *out-of-the-box* thinking there is no Plan B.

6. Black, Gray or White Swans and how to successfully manage Natech risk

Adverse events come in all sizes, ranging from frequent minor incidents to rare catastrophic shocks. The standard line of attack to prevent or control any such incident is to apply appropriate risk-management strategies in fulfillment of some legal requirement and following industry best practice. Different types of risk (conventional, extreme, unknown) require different management approaches. There is no “one-size-fits-all” solution. Enter White, Gray and Black-Swan risks.

White Swans are characterized by certainty as to their eventual occurrence (Taleb and Spitznagel, 2020). For instance, if a LPG tank lacking any kind of seismic design experiences a strong earthquake, damage to the tank or its destruction is highly certain, including secondary effects, such as LPG releases, fires or explosions. Similarly, if heat-sensitive chemical substances are stored outside in the direct sun in summer, there is great certainty that they will decay and/or ignite at some point. White Swans can be predicted using standard approaches which can be deterministic and based on past experience, as return periods are short and probabilistic extreme-event modeling is not needed. It is straightforward to manage the associated risk, as such events can be captured by (mindful) conventional design and operational practices. Most Natech accidents we have encountered fall into this category. Since these events are entirely foreseeable and therefore preventable, their occurrence is testimony to a certain ineptitude in managing Natech risks. For this reason, we will not focus on White Swans in the following discussions.

In contrast to the certainty of White Swans, *Gray Swans* represent “known unknowns” and are an expression of random (aleatory) uncertainty (Nafday, 2009). They are extreme events which can be captured using probabilistic assessment approaches (Taleb, 2010, p. 272). HILPs are a subset of Gray Swans (Nafday, 2009) which are characterized by

long return periods and high impacts. However, as discussed in Section 5.3, HILP scenarios are often screened out from the risk-analysis process, falling victim to the scenario cut-off that prioritizes higher-probability events in risk management. Since they can be modeled in principle they should not come as a surprise to anybody. Also, while a single rare incident might appear like an unexpected isolated event (a Black Swan), taking a holistic view of the whole industry might reveal that the very same incident has already happened elsewhere, and possibly several times (Akkermans and van Wassenhove, 2018; Aven, 2015). Past experience is therefore available for predicting and managing the risk. Consequently, the occurrence of Gray Swans is a sign of either risk-management flaws or a deliberate acceptance of risks. Prominent Natech examples of Gray Swans are the Fukushima nuclear power plant accident, destruction of the offshore infrastructure in the Gulf of Mexico due to Hurricanes Katrina and Rita (Cruz and Krausmann, 2008), or the rupturing of the Trans-Ecuador oil pipeline by a landslide which caused a cross-border pollution accident for which the government declared force majeure (ENS, 2013).

As we have seen in Section 2, *Black Swans* are an entirely different beast which is characterized by epistemic uncertainty caused by a lack of knowledge. They represent the true “unknown unknown” for which no prediction tools – probabilistic or other – exist. There is no means to compute their likelihood, and risk management is in principle futile, as we do not know *what* we should manage. In our experience, one form or other of organizational failure has always played a role in Natech accident causation, and events could have been prevented using available knowledge and good risk-management practice. Are Natech Black Swans then conceivable, at all? We believe they are, especially considering possible surprises due to climate change (e.g. impacts on infrastructure in thawing permafrost zones), as well as the increasing use of new technologies or processes for which we still lack a satisfactory degree of working experience and which might inadvertently add vulnerabilities (e.g. LNG, remote operation of hazardous sites). The line of inquiry is then to ask if there is some way to make Black-Swan risks more accessible to study and reduce surprises, being aware that we can never know their probabilities. Different methods have been proposed which incidentally also help to better handle HILP (Gray Swan) risks, both Natech and others, as well as address the fallacies and biases discussed in Section 5.7. The main approaches are discussed in the following sections.

6.1. Getting a grip on the unknown

Black-Swan risks are not captured by standard probabilistic assessment models, requiring a broader risk perspective that transcends traditional engineering risk analysis and risk management practice. This is true for all types of unknown rare and extreme risks. Realistically, we will never be able to fully access all Black-Swan risks, but with a change in mindset that fosters out-of-the-box thinking and improved assessment approaches, the surprise effect can be mitigated.

6.1.1. Exit Act-of-God doctrine

For Natech risks it is imperative that the existence of the risk but also the possibility to reduce it are acknowledged by the stakeholders. This requires a departure from the Act-of-God mindset, recognition that effective Natech risk-management options are available, and a conscious acceptance of the responsibility and accountability for the risk. Fraley (2010), in her excellent review of the Act-of-God doctrine, notes that it continues to be used in tort, contract and insurance law while also being enshrined in environmental statutes to create limits on liability. Thus, in the legal application of the doctrine a sharp line is drawn between damages due to natural hazards and those caused by human failure (e.g. as a result of deficient risk management), while ignoring their possible interaction that might lead or contribute to catastrophe in the first place. The Act-of-God doctrine is increasingly problematic and contested (e.g. Stammer, 1993), especially considering the recognized role of

anthropogenic influence on climate change. Also, over the years significant scientific progress has been made in natural-hazard modeling and forecasting, allowing industry in principle to prevent against or prepare for natural-hazard impacts. This renders the doctrine an outdated concept that should be abandoned to avoid creating the impression that industry must be shielded from liability at all costs which may ultimately hurt companies' reputation.

Along the same lines, the Polluter-Pays-Principle adopted 30 years ago (OECD, 1989) should be adjusted to reflect the realities of modern science and industry practice and to check the continued validity of the existing exceptions in liability for natural-hazard induced pollution. Already in 2012 the participants of an OECD Workshop on Natech risk management recommended that the Polluter-Pays-Principle be revised and that resulting liability gaps be addressed (OECD, 2013). It was argued that the natural causes of pollution accidents may well be unforeseeable or unavoidable, but their harmful consequences (e.g. chemical accidents, environmental damage) may not. In other words, even if natural hazards cannot be controlled, the resulting Natech scenarios are largely known *before* they materialize and are not only predictable in retrospect (Taleb's third Black Swan attribute).

Updating legal instruments by discarding the Act-of-God doctrine and making the link between natural and technological hazards more tangible should discourage an attitude of complacency towards Natech risk while leading to a higher acceptance of risk ownership and a better appreciation of the tools available for risk reduction. In turn, this should help to prevent most Natech accidents, including those which might be dismissed as Black Swans after the fact.

6.1.2. Risk-based versus precaution-based strategies

Aven (2015) contends that risk-based approaches for managing risks can only be used in situations where knowledge is strong and uncertainties are small. When the risk is high and uncertainties large, i.e. in case of Black-Swan risks, a precautionary approach is called for which prioritizes resilience, robustness and adaptive capacity. Based on the level of certainty of damage extent and occurrence probability, Klinke and Renn (2002) defined six risk classes and assigned risk-management strategies to each. Of relevance from a Gray and Black-Swan perspective are the risks *Damocles*, *Pythia* and *Pandora*. *Damocles* is characterized by a known large damage potential with low probability (e.g. conventional nuclear or chemical-accident risks) and is representative of a Gray-Swan or HILP risk which can be managed using standard risk-based strategies. For both *Pythia* and *Pandora*, which represent Black-Swan risks, the event probability and level of damage are uncertain although the consequences can be potentially catastrophic. This includes major risks from, e.g. new technologies with established causal relationship between hazard and consequences for which the maximum impact and likelihood can currently not be estimated (*Pythia*), or e.g. ecosystem changes or release of persistent chemicals for which this relationship is unknown at present (*Pandora*). Risk-based management strategies are unsuitable in both situations, and precautionary measures are needed. This includes, inter alia, the development and deployment of alternative processes, containment of the application in space and time, or introduction of strict liability (Klinke and Renn, 2002).

One option to avoid Natech risks altogether is to limit construction of high-risk installations in or in close proximity to known natural-hazard zones to keep them out of harm's way. Sensible land-use-planning strategies must ensure that technological and natural risks will not clash. Nonetheless, some older facilities might suddenly and unintentionally find themselves in natural-hazard areas, e.g. flood plains, if climate change alters the assumptions that went into the siting of the plant. In this case, relocation – where feasible – or retrofitting might be an option, accompanied by monitoring, situational awareness, and preparedness for an impact. Inherent safety is another strategy that reduces the risk when knowledge is limited and uncertainties are large. It favors less dangerous substances and production processes, lowers the quantity of hazardous substances on site, and implements passive safety

systems where practicable. This reduces the risk even if an accident does occur. On the other hand, redundancies might not necessarily be an effective Natech risk-reduction option as they might all fail via common-cause failure when a natural hazard hits.

6.1.3. Disaster incubation theory and warning signals

Disaster theorists generally accept that major accidents do not materialize spontaneously but are preceded by a period of increasing and often unrecognized risk in which a system slowly drifts towards failure (Dekker and Pruchnicki, 2014, Dekker, 2004). Turner (1978) found that multiple precursor events usually accumulate during what he called the disaster “incubation” period, pushing the system closer to the edge of its safety envelope until it fails. In this context, Vaughan (2005, p. 34) formulated the concept of “normalization of deviance” which illustrates how organizations routinely and over long time periods convert (normalize) anomalies and deviations into acceptable risk or simply ignore them until a disaster happens. The event then manifests as, e.g. a sudden technical breakdown or structural collapse, but its root causes are more often than not buried deep in the social processes and organizational, management and communication failures that occurred before the event (Pidgeon, 2012). Also Sornette (2009) contends that extreme events (termed Dragon Kings) in complex systems do not come out of the blue but are the result of the system’s drift towards instability. This is usually accompanied by visible (and measurable) precursors which render Dragon Kings predictable to some degree.

The good news is that if an accident is not sudden but incubates over time, there might be some possibility to control the risk by monitoring for warning signals and accident precursors, and by providing for corrective action before disaster strikes. For instance, Amyotte et al. (2014) stress that in the process industries warning signs are always present prior to an incident and emphasize that all individuals in a company hierarchy must be trained to detect these signs. Paltrinieri et al. (2012) discuss the integration of early warning indicators already in the hazard identification process with the aim to prevent major accidents. Similarly, the US Center for Chemical Process Safety provides guidance on how catastrophic incident warning signs can be recognized (CCPS, 2012). This guidance addresses risk analysis and management of change, procedures, audits, asset integrity, but also lessons learning, leadership and culture, as well as training and competencies. Also de Sousa Cavalcante et al. (2013) in their analysis of Dragon Kings demonstrate that such extreme events can in principle be suppressed by implementing appropriate control strategies.

Even for Black-Swan risks it is reasonable to assume that precursors and warning signs exist that are accessible to observation and intervention, opening a doorway to averting the in-principle unforeseeable catastrophe. This requires an organization to foster a vigilant mindset involving monitoring and evaluation, and to create the conditions for the quick detection of and fast response to warning signs. Goble et al. (2018) argue that two types of vigilance are needed for effective hazard management under uncertainty. They pertain to alertness to predictable changes of hazards and risks (Type 1) or to potential surprises we fail to anticipate (Type 2). For Black-Swan precursors or warning signs to be detected, the questioning attitude and contrarian thinking approach of Type 2 vigilance is required. However, also some HILP risks judged too unlikely to matter will benefit from Type 2 vigilance, especially to catch if the boundary conditions by which they were dismissed may be changing. Probabilities can then be updated using Bayesian analysis.

When warning signals manifest they have to be observed and quickly followed up on to ascertain that the risk can be managed successfully and the accident averted. Clearly, a screening of signals needs to take place as not all possible warning signs can and should be responded to with the same priority, and some might be false alarms. Otherwise, too many resources might get tied up in monitoring, and vigilance might saturate to the detriment of safety. Criteria for prioritization could be the credibility of the signal, the lead-time of a possible event and the potential for severe consequences (Paté-Cornell, 2012).

Warning signals that could indicate a slow drifting towards a Natech accident, thinkable or not, can involve the industrial site itself or its surroundings. The accident record of a site is usually a good indicator of the general safety culture adopted, and it is reasonable to assume that if conventional technological accidents could not be prevented in the past, it is even less likely that complex Natech risks could be controlled. A record of past minor Natech events and near misses should also alert the operator to existing vulnerabilities that could at some point materialize as an accident of possibly major proportions. Likewise, indirect natural-hazard effects on site, such as loss of power or flooded sewers, can trigger or aggravate Natech accidents and their occurrence should be cause for concern. The age of an industrial facility is also an indicator of how well the site will fare under natural-hazard loading. Old facilities that are corroded, affected by fatigue or designed to outdated standards are less likely to survive the impact of a natural hazard. From a natural-hazard perspective, attention should be paid to indications for future shifts in the hydro-meteorological regime at the industrial site, such as changing weather patterns, increased rainfall, stronger winds, or higher storm surge. Where historical data on natural hazards at or in the vicinity of an industrial site exists, even if anecdotal, it should be heeded to be better prepared for large and previously forgotten events.

6.1.4. Mindfulness

The early detection of warning signals in hazardous industry requires a mindset that is attentive, non-superficial, and which expresses a collective “mindfulness” of risks that helps to turn around Vaughan’s normalization of deviance. The concept of mindfulness is based on the seminal work of Weick and Sutcliffe (2006, 2007) and their studies of high-reliability organizations (HROs). HROs operate complex, tightly coupled hazardous technological systems which provide important benefits to society but whose failure can be catastrophic. Also, operators in HROs tend to work near or at the very edge of human capacity, increasing the risk significantly (Roberts and Rousseau, 1989). Examples of such systems are nuclear power plants, air traffic control, spacecraft, etc. They are designed and managed to avoid failure, with reliability being the primary goal, since the magnitude of damage due to an accident might be so immense that it could endanger the very existence of the organization itself. HROs therefore have to juggle the operational goals of managing a complex hazardous technology safely while at the same time maintaining production or service capacity even during peak demand periods (LaPorte and Consolini, 1991). Nonetheless, and perhaps surprisingly, the safety record of HROs suggests that accidents can indeed be avoided by adopting a risk-management approach that aims for reliability via anticipation, early detection of what might go wrong, and a high degree of executive preparedness. Consequently, Weick and Sutcliffe (2006) assert that organizations can discover and manage unexpected events by focusing on the five characteristics of mindfulness:

1. *Preoccupation with failure*: regards near misses as failure rather than as evidence of success, and uses them as warning signs for future learning;
2. *Reluctance to simplify*: encourages going beyond assumptions and simple truths;
3. *Sensitivity to operations*: establishes a situational awareness of ongoing operations, allowing organizations to pick up more easily minute details that could point toward failure;
4. *Commitment to resilience*: locates the pathways to recover from an unforeseen crisis;
5. *Deference to expertise*: identifies the expertise and experience needed to combat failure and migrates decision making to all levels while deprioritizing hierarchical rank.

The concept of mindfulness can and should be applied to the management of all types of hazardous activities for which high reliability is needed due to the potentially catastrophic cost of failure. Aven and

Krohn (2014) propose mindfulness as part of an integrated framework to better understand and manage Black-Swan risks. Recognizing the deficiencies of state-of-the-art knowledge and assessment methods, the framework unites mindfulness with the basic tenets of risk assessment and management, and brings in ideas from quality management to better understand, assess and manage the risk of surprise events.

6.1.5. Resilience engineering

Organizational resilience is a capability that allows an organization to recognize and recover from a loss of control (Dekker, 2004). Resilience is therefore a strategy that protects against adverse events, including those unpredictable and unknown, for instance via the implementation of redundancies, buffer capacities, or through diversification. Hollnagel and Woods (2006) contend that for a system to be resilient, it needs to exhibit the following abilities:

- Anticipation of unexpected events (knowing what to expect);
- Monitoring of events that could undermine resilience, and of the adaptive performance of the system itself (being attentive);
- Response to all types of threats, including unusual ones (knowing what to do);
- Learning from successes and failures (updating of knowledge, competence and resources).

Resilience engineering is a relatively recent safety-management paradigm that aims to investigate and expand an organization's adaptive capacity to emerging risks under production pressure. It acknowledges that for effectively managing safety in complex socio-technical systems, e.g. industrial installations, engineering approaches need to be enriched with insights from the social sciences on human and organizational behavior (Woods, 2006). As such, resilience engineering fully embraces the principles of collective mindfulness. In order to manage the risk proactively, it develops measures and indicators of the factors that contribute to organizational resilience and those which undermine it to capture deficiencies in safety management early and before the system drifts to its failure boundaries. Numerous authors have discussed resilience in high-risk industry to gauge the status of safety management, e.g. Ranasinghe et al. (2020), Shiralilal et al. (2016), Azadeh et al. (2014), or Dinh et al. (2012), to name a few. Indicators that were proposed include flexibility, awareness, preparedness, buffering capacity, tolerance, learning culture, anticipation, etc.

When it comes to Natech resilience in industry, deficits in resilience-engineering research have been highlighted. Suarez-Paba et al. (2020) point out that in the process industries the application of resilience engineering is focused solely on the industrial installation itself without considering existing interconnections with the area outside the facility's fence line. This is problematic for a multi-hazard cascading risk like Natech which is triggered by an external agent that simultaneously affects the surroundings of the industrial plant with potential repercussions on the plant itself. A broader, inclusive and area-wide resilience perspective that reflects the synergistic effects of the overall system is needed. Using ideas from resilience engineering, Suarez-Paba et al. (2020) put forward a novel conceptual framework for building Natech resilience in industry by examining the interaction and interdependencies between infrastructure (plant-internal equipment, buildings, utilities and backup systems), the organization, risk communication, risk governance, and the external environment (external secondary hazards, lifelines, community and environment).

Along the same lines, Krausmann et al. (2019) propose a set of simple indicators and ranking criteria for gauging the performance of Natech risk management in industry and by public authorities. They reflect the recognition that a territorial approach is necessary for effectively tackling Natech risks. The indicators comprise:

- Awareness;
- Existing legislative frameworks;

- Collection of accident and near-miss data;
- Severity of natural hazards and types of industrial activities considered;
- Type of Natech risk assessment and risk maps; and
- Measures for Natech preparedness.

The performance ranking depends on the level of sophistication and inclusiveness achieved in managing the risk. Low scores indicate major oversights that should be critically reviewed and corrective action taken. The indicators are useful for self-assessing Natech risk-management performance over time, or between different organizations or countries at the same point in time. A great many of the Natech accidents that occurred could have been prevented by a more realistic perception of one's risk status.

Similarly, the OECD developed a Natech addendum to its Guiding Principles for Chemical Accident Prevention, Preparedness and Response with detailed guidance for industry, public authorities and communities for governing, managing and communicating Natech risks (OECD, 2015; 2003).

6.1.6. Scenario planning and red teaming

The identification of future risks (or opportunities) under high levels of uncertainty cannot rely on predictions based on past data or Bayesian approaches that requires foresight using "disciplined imagination" that goes beyond what we know from experience (IRGC, 2015). For this purpose, (qualitative) scenarios are developed which do not describe the future to come, because it is variable and unknowable, but a set of possible futures that helps decision makers to orient themselves in the maze of uncertainties they have to tackle. Scenarios question existing beliefs and worldviews, and frequently include elements that cannot be formally captured through models, highlighting the epistemic level of analysis of the approach (Shoemaker, 1995). Masys (2012) argues that the thought process characteristic for scenario planning helps to explore uncertainties while at the same time contesting traditional mental models and assumptions, thereby defying the assumption that the future will look like the past. It provides a structured and disciplined approach that opens minds to previously unconceivable possibilities and which can provide insights into the emergence of Black Swans. Scenario planning also enables the determination of intervention points to which risk-management solutions can be anchored (IRGC, 2015). Depending on the field of application, there is a wide variety of approaches for developing scenarios in the literature. Shoemaker (1995) describes the scenario-construction technique in a 10-step process, emphasizing the strength of the approach in introducing alternative concepts and promoting out-of-the-box thinking. The technique he outlines is applicable to any kind of situation in which a forward-looking perspective is sought for identifying future threats and opportunities.

A method successfully applied in businesses and especially the military for eliciting alternative scenario perspectives and contesting established plans and assumptions is *red teaming* (see e.g. Zenko, 2015, Mateski, 2009). Red teaming serves as devil's advocate that challenges linear thinking to help reveal potential (catastrophic) surprises and unintended consequences of decision-making (Masys, 2012). With its contrarian line of attack, which views near misses as failure as well as an opportunity to learn, it also moderates the sense of achievement and complacency that frequently follows successful outcomes (Defense Science Board, 2003). Red teaming can complement and inform the scenario-planning process, coupled with other non-traditional methods for scenario identification, such as anticipatory failure determination (AFD) and inventive problem solving (TRIZ). AFD and TRIZ differ from conventional scenario-identification methods by investigating how failures can be caused deliberately. Analysts start at the final imagined outcome (e.g. the most catastrophic failure conceivable) and creatively analyze backwards to establish the conditions under which a specific adverse event can occur (Aven, 2015). In Fig. 3 Masys (2012) illustrates the use of red teaming, AFD and TRIZ under a systems-thinking

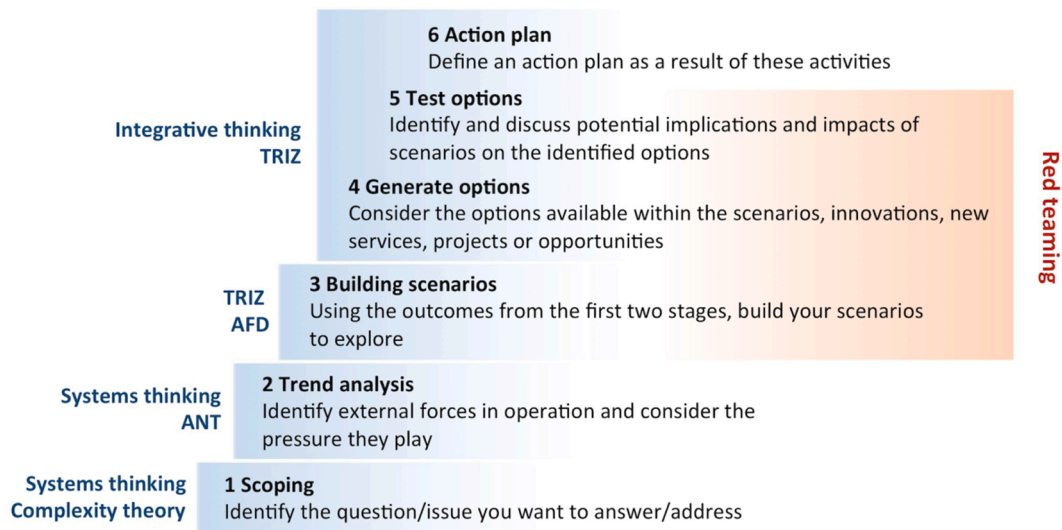


Fig. 3. Scenario-planning steps from JISC (2013) and supporting methodologies according to Masys (2012) (adapted).

perspective for a 6-step scenario-planning situation as outlined by JISC (2013).

Natech scenario development is still in its infancy, and scenarios used in risk analysis are primarily based on accident data from past events. This is due to the complexity of assessing multi-hazard risks and the scarcity of industrial equipment damage models for most types of natural hazards (Krausmann, 2017). For earthquakes, floods and lightning, some equipment fragility data is available from empirical studies (e.g. Salzano et al., 2003) and theoretical modeling (e.g. Necci et al., 2013, Landucci et al., 2014). For other natural hazards, one has to rely on incident data for reconstructing the event dynamics (e.g. using industrial accident databases, such as eNATECH¹). Further research in this direction is needed. Nonetheless, the currently available scenarios, even if coarse, are a good starting point for managing most types of Natech risk, provided they are properly taken into account in the risk analysis. Considering that on- and offsite lifelines are often damaged or destroyed by the natural hazard (see Section 5.2), it is recommended that a worst case is postulated for building Natech scenarios, where plant-internal and -external safety barriers and mitigation systems are assumed to be unavailable (Antonioni et al., 2007). Aiming to explore the impact of natural hazards on safety barriers in more detail, Misuri et al. (2020) recently investigated the performance of active and passive safety barriers in Natech scenarios.

Natech scenarios based on past data are not necessarily a good predictor of the future, in particular for surprise threats, e.g. those that climate change might hold in store (e.g. Cruz and Krausmann, 2013). For instance, for hydro-meteorological hazards, safety factors should be added in predictions of trigger frequency and severity to account for actual and potential changes in the environment and climate. Nevertheless, accident databases can be a valuable tool for scenario building for Natech risks that have already manifested. However, for any risk that is new or unthinkable, creative brain storming efforts and out-of-the-box thinking are needed to go beyond what we know from the past and to make these risks more accessible to study. Scenario planning is a valid method for stimulating this thinking process.

While there is no structured approach for imaginative scenario building for Natechs yet, significant progress has been made in extending industrial risk-analysis methodologies to incorporate Natech-specific features. Antonioni et al. (2007) carried out pioneering work in developing a systematic approach for considering Natech risks in

Quantitative Risk Analysis (QRA) which takes into account scenario combinations typical for Natech accidents. Since QRA requires a large amount of data and is time-consuming, Girgin and Krausmann (2013) proposed a semi-quantitative methodology for analyzing Natech risks with their so-called RAPID-N system² as an alternative for situations in which data is limited and a fast analysis is required. Other researchers propose more or less systematic approaches for Natech risk analysis which differ in scope and level of detail (e.g. Vallée and Duval, 2012; Cruz and Okada, 2008; Ayrault and Bolvin, 2004). In an attempt to include Natech risks in National Risk Assessment, an instrument to identify, analyze, compare and prioritize a wide range of risks of national relevance, Girgin et al. (2019) developed guidance to support the governmental decision-making process.

6.2. Preparing for the consequences

However resourceful and effective we become in anticipating disaster risks via imaginative scenario design, heeding warning signals or building resilience, it is unlikely we will manage to capture all risks that harbor a Black-Swan potential. Consequently, while the prevention of catastrophic accidents must remain the primary goal, we need to be prepared to minimize adverse consequences in case our prevention efforts fail. Since the probability of unknown events cannot be estimated and is therefore not a criterion for decision-making, Taleb (2010, pp. 2010–213) argues that decisions should instead be based on the potential consequences that are easier to guess. Scenario planning aided by red teaming can help to explore worst-case consequences and enhance preparedness to better cope with the unexpected. Also Nafday (2009) recommends a shift from risk management to consequence management to deal with uncertain risks whose impact can be disastrous, including both HILP and Black-Swan risks. Murphy and Conner (2012) take a similar stance. They acknowledge the difficulty of investing in protection against scenarios that have never occurred and whose likelihood is hard to assess or deemed negligible. Nevertheless, they emphasize that for events with potentially major impacts, regardless of the uncertainty surrounding their likelihood, appropriate safeguards are needed unless the hazard can be reduced or eliminated.

Experience from past Natech accidents showed the near impossibility of handling the consequences of a major event, let alone a Black Swan, without adequate preparedness. Without a significant portion of luck,

¹ <https://enatech.jrc.ec.europa.eu>

² <https://rapidn.jrc.ec.europa.eu>

ad-hoc crisis management for such complex events would likely not be very successful. Using past accident information, Necci et al. (2018) studied gaps in Natech emergency management and developed recommendations for industry and local authorities on how to address on- and offsite Natech emergency planning considering the specific challenges discussed in Section 5.2. For instance, they strongly advise that onsite emergency planning should assume that safety barriers, personnel responsible for implementing protective actions (e.g. safe shutdown), and offsite response resources and lifelines are unavailable. They recommend, inter alia, that operators should provide for reliable onsite backup power and ensure that it will not fail under the same conditions as the primary power supply. They also address the protection requirements of first responders and the needed response capacity in view of a simultaneous natural-hazard impact and hazardous-materials release, as well as the preparedness of the medical sector in case of such an event.

OECD guidance on Natech emergency management in the chemical industry reflects these findings and expands on training and education requirements that should allow all personnel to perform their tasks competently at all times (OECD, 2015). It also highlights the need for clear procedures to follow during abnormal conditions, such as those occurring during natural-hazard impacts, which outline roles, responsibilities and lines of communication. Based on experience gathered during hurricanes, the U.S. Chemical Safety and Hazard Investigation Board (CSB, 2005) issued a safety bulletin on how to safely start up oil and chemical facilities that were shut down while riding out hurricanes. Considering that restarting after an emergency shutdown is one of the most dangerous phases and that damage to equipment inflicted by the natural hazard might not be detected prior to restart, precautions and strict adherence to protocols are needed to avoid major accidents. Training is also required on how to prepare and use natural-hazard maps in the industrial context, as industry would usually not collect natural-hazard information themselves or know how to act upon it. Government authorities should collect the data for all relevant natural hazards in a region, develop maps and disseminate them to industry and adjacent communities for use in Natech prevention and preparedness planning (OECD, 2015).

The adoption of performance-based design for safety-critical buildings, equipment and systems in industry, and compliance with performance criteria would help to improve preparedness to Natech events by ensuring that such structures and systems, e.g. control rooms or cooling loops, remain functional during a natural event (Cruz and Okada, 2008). But preparedness for Natech events, in particular for HILPs and potential Black Swans, must also reflect on and anticipate the expected level of damage and loss of containment if design-basis assumptions are exceeded by a natural hazard. When natural-hazard loads are considered in the design and operation of an industrial installation, they are usually based on *credible* worst-case reference scenarios which represent assumptions that may be insufficient in extreme situations. Scenario planning and other tools discussed in Section 6.1.6 can be valuable instruments to support the preparedness planning process.

Preparing for rare or unexpected events can be costly and a balance needs to be struck between the prudence recommended by science and budget constraints. Although priority setting is unavoidable under these conditions, impossible risk trade-off situations can be overcome by building generic and not necessarily threat-specific emergency-management capacities that can be applied to different risk domains. Regardless of whether emergency plans address a particular hazard or are generic, they must be reviewed and tested on a regular basis to ensure that the assumptions that went into their preparation are still valid (e.g. the natural hazard frequency and severity). Emergency exercises and drills raise stakeholder awareness, stress-test procedures, and help to reveal gaps and weaknesses in preparedness planning.

However, the readying and testing of emergency plans and instruments alone is insufficient if we lack the alacrity and courage to implement them once a crisis emerges. The COVID-19 pandemic is an

illustrative example of a rare occurrence for which awareness and preparedness plans in principle existed due to recent precursor events (SARS, MERS, swine flu). It can therefore not be considered a Black Swan. Nevertheless, the contagion managed to quickly spread all over the world. Harford (2020) suggests that the unpredictability of events is often not the problem in such situations, but that even if faced with evident risks we fail to act, collectively and individually. COVID-19 is just another example of our tendency to use the past as a basis for our future expectations, of assuming that if the worst did not happen before, it will also not happen in the future. Also Norman et al. (2020) contend that decision-making and policy action in the face of impending disaster must be swift and unaffected by fears of overacting and appearing paranoid. Conversely, it should also not be impeded by a sense of surrender to the inevitable. For scenario planning this means that however accurate we may be in predicting the future, scenarios are only useful if taken seriously and if there is no hesitation to act upon them once a crisis materializes.

6.3. Systemic risks

In complex and tightly-coupled systems (e.g. many of today's social and technical systems with their interconnections), small initial shocks can propagate through the individual subsystems, interacting in unexpected ways and creating a chain reaction that can ultimately lead to complete system failure (Scheibe and Blackhurst, 2018). In such systems, risk management measures must aim to preserve safety margins (buffer capacity or slack). However, while risk managers prioritize the risks they are interested in, impacts on other parts of the systems are hard to foresee and might actually reduce resilience. In this way, management interventions to mitigate one risk might inadvertently create or aggravate other risks in unforeseeable ways (IRGC, 2010). The Black Swan potential is evident under such conditions. Networks (e.g. power grid, communication networks, supply chain) exhibit systemic risk character and are more vulnerable to Black Swans (Taleb, 2010, p.226).

Goble (2019) suggests that Natech risk is a gateway to the systemic risk landscape. Due to its multi-hazard risk nature, it cuts through conceptual boundaries and drives the interaction of disciplines that would usually be considered in isolation from each other. It also makes visible the linkages of risks which are not always obvious to decision makers and demonstrates the possible knock-on effects of natural-hazard impacts. For instance, the 2011 GJET not only triggered the Fukushima nuclear power plant accident, rendering large swaths of land unusable for living and agriculture, it also damaged a high number of industrial facilities, causing chemical releases, fires and explosions, with subsequent contagion into the global supply chain due to a loss of production capacity (Kajitani et al., 2013). The mindful management of Natech risks will therefore also help to mitigate potential systemic risks by containing the accident before its effects can propagate deeper into the system in unexpected ways.

7. Conclusions

Risks from hazardous industrial activities are widely accepted as they provide society with essential goods and services. Public acceptance is, however, based on trust that risks are managed well and reduced to an acceptable level, and on the expectation that residual risks are taken care of through preparedness. Nevertheless, major technological accidents continue to happen, raising questions as to the effectiveness of corporate oversight and the application of state-of-the-art knowledge in managing risks. The vast majority of these accidents, if not all, could have been foreseen and prevented using available information and knowledge. Consequently, they should not be considered inevitable or Black Swans.

The same applies to Natech accidents, including HILPs. Specific Natech risk-management tools and instruments are in principle available and effective but often not implemented, as Natechs are considered

a long-shot risk and the Act-of-God mindset persists. There is a case for Natech Black Swans due to climate change whose effect on scenario assumptions cannot be clearly anticipated (e.g. risks due to thawing permafrost), or because of technological advancements (e.g. increasing automation and artificial intelligence) whose impact is difficult to predict. This highlights the importance of scientific research and knowledge management to expand our knowledge horizon. But also in these cases, mindfulness and organizational resilience will help to reduce the risk of surprises significantly and to not leave things to luck. Nevertheless, as the COVID pandemic has shown, the best preparedness planning will be unsuccessful if its implementation falters once a disaster looms at the horizon.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

We thank our former colleague Dr. Serkan Girgin, now at the University of Twente, for useful conceptual discussions during the early stages of the study preparation, and Dr. Zsuzsanna Gyenes of the IChemE Safety Centre for her insightful suggestions.

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

- Airmic, 2011. Roads to ruin, A study of major risk events: their origins, impact and implications. Airmic, UK. <https://www.airmic.com/technical/library/roads-ruin-analysis>.
- Akkermans, H.A., van Wassenhove, L.N., 2018. A dynamic model of managerial response to grey swan events in supply networks. *Int. J. Prod. Res.* 56 (1–2), 10–21.
- Amyotte, P., Margeson, A., Chiasson, A., Khan, F., 2014. There is no such thing as a Black Swan process incident. In: Proc.: HAZARDS 24, Edinburgh, 7–9 May 2014, Symposium Series 159, Institution of Chemical Engineers.
- Antonioni, G., Landucci, G., Necci, A., Gheorghiu, D., Cozzani, V., 2015. Quantitative assessment of risk due to NaTech scenarios caused by floods. *Reliab. Eng. Syst. Saf.* 142, 334–345.
- Antonioni, G., Spadoni, G., Cozzani, V., 2007. A methodology for the quantitative risk assessment of major accidents triggered by seismic events. *J. Hazard. Mater.* 147 (1–2), 48–59.
- ASCE, 2015. Flood resistant design and construction, ASCE/SEI 24-14. American Society of Civil Engineers.
- Aven, T., 2015. Implications of Black Swans to the foundations and practice of risk assessment and management. *Reliab. Eng. Syst. Saf.* 134, 83–91.
- Aven, T., Krohn, B.S., 2014. A new perspective on how to understand, assess and manage risk and the unforeseen. *Reliab. Eng. Syst. Saf.* 121, 1–10.
- Aven, T., 2013. On the meaning of a Black Swan in a risk context. *Saf. Sci.* 57, 44–51.
- Ayrault, N., Bolvin, C., 2004. Analyse des risques et prévention des accidents majeurs – Rapport partiel d’opération f: Guide pour la prise en compte du risque inondation, INERIS Report DRA-2004-Ava-P46054 (in French).
- Azadeh, A., Salehi, V., Arvan, M., Dolatkhah, H., 2014. Assessment of resilience engineering factors in high-risk environments by fuzzy cognitive maps: a petrochemical plant. *Saf. Sci.* 68, 99–107.
- Baybutt, P., 2016. Insights into process safety incidents from an analysis of CSB investigations. *J. Loss Prev. Process Ind.* 43, 537–548.
- BBC, 2000. Death of a river, BBC News, 15 February. <http://news.bbc.co.uk/2/hi/europe/642880.stm>.
- Blair, A.S., 2004. Management system failures identified in incidents investigated by the U.S. Chemical Safety and Hazard Investigation Board. *Process Saf. Prog.* 23 (4), 232–236.
- Bridges W.G., 2016. Black Swans or Wild Geese? Process Improvement Institute, 4 May. <http://www.process-improvement-institute.com/black-swans-wild-geese/>.
- BSEE, 2020. Incident archive – Taylor Energy oil discharge at MC-20 site and ongoing response efforts, U.S. Bureau of Safety and Environmental Enforcement. <https://www.bsee.gov/newsroom/library/incident-archive/taylor-energy-mississippi-ca-ngo/ongoing-response-efforts>.
- Casey, J.P., 2019. Danger from the deep: underwater mudslides in the Gulf of Mexico, Offshore Technology, 10 June. <https://www.offshore-technology.com/features/danger-from-the-deep-underwater-mudslides-in-the-gulf-of-mexico/>.
- CCPS, 2012. Guidance on how to recognize warning signs: Recognizing catastrophic incident warning signs in the process industries. Center for Chemical Process Safety.
- Crooks, E., 2011. Exxon’s Tillerson rejects BP take on spill, Financial Times, 9 March. <https://www.ft.com/content/a3d637b2-4a88-11e0-82ab-00144feb49a>.
- Cruz, A.M., Krausmann, E., 2013. Vulnerability of the oil and gas sector to climate change and extreme weather events. *Clim. Change* 121, 41–53.
- Cruz, A.M., Okada, N., 2008. Methodology for preliminary assessment of Natech risk in urban areas. *Nat. Hazards* 46 (2), 199–220.
- Cruz, A.M., Krausmann, E., 2008. Damage to offshore oil and gas facilities following hurricanes Katrina and Rita: an overview. *J. Loss Prev. Process Ind.* 21, 620–626.
- CSB, 2018. Organic peroxide decomposition, release, and fire at Arkema Crosby following Hurricane Harvey flooding, No. 2017-08-I-TX, U.S. Chemical Safety and Hazard Investigation Board, Washington, D.C.
- CSB, 2005. Safety Bulletin After Katrina: Precautions Needed During Oil and Chemical Facility Startup, No. 2005-01-S, U.S. Chemical Safety and Hazard Investigation Board, Washington, D.C.
- Defense Science Board, 2003. Defense Science Board Task Force on The Role and Status of DoD Red Teaming Activities. US Department of Defense, Washington.
- Dekker, S., Pruchnicki, S., 2014. Drifting into failure: theorizing the dynamics of disaster incubation. *Theor. Issues Ergon. Sci.* 15 (6), 534–544.
- Dekker, S.W.A., 2004. Why we need new accident models. *Human Factors Aerospace Saf.* 4 (1), 1–18.
- de Sousa Cavalcante, H.L.D., Oriá, M., Sornette, D., Ott, E., Gauthier, D.J., 2013. Predictability and suppression of extreme events in a chaotic system. *Phys. Rev. Lett.* 111, 198701.
- Dinh, L.T.T., Pasman, H.J., Gao, X., Mannan, M.S., 2012. Resilience engineering of industrial processes: Principles and contributing factors. *J. Loss Prev. Process Ind.* 25 (2), 233–241.
- DiStefano, J.N., 2020. ‘Act of God’ or ‘felony assault’? These Pa. chemical execs face prison for a Texas plant fire, 9 February 2020. <https://www.inquirer.com/busines/chemical-criminal-arkema-prosecutors-texas-prussia-20200209.html>.
- eNATECH, 2018. Natech information. <https://enatech.jrc.ec.europa.eu/Natech/6>.
- ENS, 2013. Oil Spilled Into Ecuador’s Rivers Reaches Peru, Environment News Service. <http://ens-newswire.com/2013/06/11/oil-spilled-into-ecuadors-rivers-reaches-peru/>.
- Eurocodes, 2021. Eurocodes – Building the future. <https://eurocodes.jrc.ec.europa.eu/publications.php>.
- European Commission, 2012. Commission Staff Working Document – Technical Summary on the Implementation of Comprehensive Risk and Safety Assessment of Nuclear Power Plants in the European Union, SWD(2012) 287 final/2, 22 August.
- European Union, 2012. Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC. *Off. J. Eur. Union*, L197, 1–37.
- Fears, D., 2018. A 14-year long oil spill in the Gulf of Mexico verges on becoming one of the worst in U.S. history, The Washington Post, 22 October. <https://tinyurl.com/yyc6nr7w>.
- Fraleigh, J., 2010. Re-examining acts of god. *Pace Environ. Law Rev.* 27, 669–690.
- Gigerenzer, G., 2015. Risk savvy - How to make good decisions. Penguin Books, New York.
- Girgin, S., Necci, A., Krausmann, E., 2019. Dealing with cascading multi-hazard risks in national risk assessment: the case of Natech accidents. *Int. J. Disaster Risk Reduct.* 35, 101072.
- Girgin, S., Krausmann, E., 2016. Historical analysis of U.S. onshore hazardous liquid pipeline accidents triggered by natural hazards. *J. Loss Prev. Process Ind.* 40, 578–590.
- Girgin, S., Krausmann, E., 2013. RAPID-N: rapid Natech risk assessment and framework. *J. Loss Prev. Process Ind.* 26 (6), 949–960.
- Girgin, S., 2011. The natech events during the 17 August 1999 Kocaeli earthquake: aftermath and lessons learned. *Nat. Hazards Earth Syst. Sci.* 11, 1129–1140.
- Goble, R., 2019. The human side of systemic risks. In: Presentation at: “Risk management and governance in the Anthropocene: Workshop on Natural Hazards Triggered Technological Risks (NATECH)”, Nanjing, China, 19 March.
- Goble, R., Bier, V., Renn, O., 2018. Two types of vigilance are essential to effective hazard management: maintaining both together is difficult. *Risk Anal.* 38 (9), 1795–1801.
- Gowland, R., 2013. Atypical scenarios and dependent failures, Loss Prevention Bulletin 230, IChemE.
- Harford, T., 2020. Catastrophes such as coronavirus are all too predictable. What makes us do nothing in the face of danger?, Financial Times Magazine. <https://www.ft.com/content/74e5f04a-7df1-11ea-82f6-150830b3b99a>.
- Hershner, R., 2020. Texas criminal trial highlights climate liability for factories in floodplains, NPR, 2 March. <https://www.npr.org/2020/03/02/723217659/texas-criminal-trial-highlights-climate-liability-for-factories-in-floodplains>.
- Hollnagel, E., Woods, D.D., 2006. Epilogue: resilience engineering precepts. In: Hollnagel, E., Woods, D.D., Leveson, N. (Eds.), Resilience engineering – Concepts and precepts. CRC Press, Boca Raton.
- Hopkins, A., Maslen, S., 2015. Risky Rewards: How Company Bonuses Affect Safety, first ed. CRC Press, Boca Raton.
- Hudec, P., Lucš, O., 2004. Flood at SPOLANA a.s. in August 2002. *Loss Prevent. Bull.* 180, 36–39.
- INPO, 2011. Special report on the nuclear accident at the Fukushima Daiichi nuclear power station, INPO 11–005. Institute of Nuclear Power Operations, Atlanta, GA.
- IRGC, 2015. Guidelines for emerging risk governance, International Risk Governance Council (IRGC), Lausanne, Available from www.irgc.org.
- IRGC, 2010. The emergence of risks: contributing factors, International Risk Governance Council (IRGC), Lausanne, Available from www.irgc.org.
- ISO 31000, 2018. Risk management – guidelines, International Organization for Standardization, Geneva.

- JISC, 2013. Scenario planning - A guide to using this strategic planning tool for making flexible long-term plans. <https://www.jisc.ac.uk/guides/scenario-planning>.
- Kajitani, Y., Chang, S.E., Tatano, H., 2013. Economic impacts of the 2011 Tohoku-Oki earthquake and tsunami. *Earthquake Spectra* 29 (S1), S457–S478.
- Kletz, T.A., 1993. Lessons from Disaster: How Organisations Have No Memory and Accidents Recur. Institute of Chemical Engineers, Rugby, UK.
- Klinke, A., Renn, O., 2002. A new approach to risk evaluation and management: risk-based, precaution-based, and discourse-based strategies. *Risk Anal.* 22 (6), 1071–1094.
- Krausmann, E., 2017. Natech risk and its assessment. In: Krausmann, E., Cruz, A.M., Salzano, E. (Eds.), *Natech risk assessment and management – Reducing the risk of natural-hazard impact on hazardous installations*. Elsevier, Amsterdam.
- Krausmann, E., Girgin, S., Necci, A., 2019. Natural hazard impacts on industry and critical infrastructure: Natech risk drivers and risk management performance indicators. *Int. J. Disaster Risk Reduct.* 40 <https://doi.org/10.1016/j.ijdrr.2019.101163>.
- Krausmann, E., Cruz, A.M., Salzano, E., 2017. *Natech Risk Assessment and Management – Reducing the Risk of Natural-Hazard Impact on Hazardous Installations*. Elsevier, Amsterdam.
- Krausmann, E., Cruz, A.M., 2013. Impact of the 11 March 2011, Great East Japan earthquake and tsunami on the chemical industry. *Nat. Hazards* 67, 811–828.
- Krausmann, E., Baranzini, D., 2012. Natech risk reduction in the European Union. *J. Risk Res.* 15 (8), 1027–1047.
- Krausmann, E., Cruz, A.M., Affeltranger, B., 2010. The impact of the 12 May 2008 Wenchuan earthquake on industrial facilities. *J. Loss Prev. Process Ind.* 23, 242–248.
- Landucci, G., Necci, A., Antonioni, G., Tugnoli, A., Cozzani, V., 2014. Release of hazardous substances in flood events: damage model for horizontal cylindrical vessels. *Reliab. Eng. Syst. Saf.* 132, 125–145.
- LaPorte, T.R., Consolini, P.M., 1991. Working in practice but not in theory: theoretical challenges of “high-reliability organizations”. *J. Public Admin. Res. Theory* 1 (1), 19–47.
- Leveson, N., 2015. A systems approach to risk management through leading safety indicators. *Reliab. Eng. Syst. Saf.* 136, 17–34.
- Lodge, M., 2010. Gulf spill is ‘Black Swan’ event: Industry insider, CNBC, 9 June. <http://www.cnbc.com/id/37593961>.
- Lozano, J.A., 2020. Trial over Arkema chemical plant fire during Harvey set to begin, *Insurance Journal*, 18 February. <https://www.insurancejournal.com/news/south-central/2020/02/18/558682.htm>.
- Mascone, C., 2013. Editorial – Moving beyond the Black Swan excuse. *Chem. Eng. Prog. February*.
- Mason, A.L., Taylor, J.C., MacDonald, I.R., 2019. An integrated assessment of oil and gas release into the marine environment at the former Taylor Energy MC20 site, NOAA Technical Memorandum NOS NCCOS 260, Silver Spring, MD.
- Masys, A.J., 2012. Black Swans to grey swans: revealing the uncertainty. *Disaster Prevent. Manage.* 21 (3), 320–335.
- Mateski, M., 2009. Red Teaming – A short introduction (1.0). Red Team J..
- Misuri, A., Landucci, G., Cozzani, V., 2020. Assessment of safety barrier performance in Natech scenarios. *Reliab. Eng. Syst. Saf.* 193, 106597.
- Murphy, J.F., Conner, J., 2014. Black Swans, White Swans, and 50 shades of grey: remembering the lessons learned from catastrophic process safety incidents. *Process Saf. Prog.* 33 (2), 110–114.
- Murphy, J.F., Conner, J., 2012. Beware of the Black Swan: the limitations of risk analysis for predicting the extreme impacts of rare process safety incidents. *Process Saf. Prog.* 31 (4), 330–333.
- Nafday, A.M., 2009. Strategies for managing the consequences of Black Swan events. *Leadersh. Manage. Eng.* 9 (4), 191–197.
- NAIIC, 2012. The official report of the Fukushima Nuclear Accident Independent Investigation Commission, The National Diet of Japan. https://www.nirs.org/wp-content/uploads/fukushima/naic_report.pdf.
- Necci, A., Krausmann, E., Girgin, S., 2018. Emergency planning and response for Natech accidents. In: *Towards an all-hazards approach to emergency preparedness and response – Lessons learnt from Non-Nuclear Events*, NEA No. 7308, Nuclear Energy Agency, Organization for Economic Co-operation and Development, Paris.
- Necci, A., Antonioni, G., Cozzani, V., Krausmann, E., Borghetti, A., Nucci, C.A., 2013. A model for process equipment damage probability assessment due to lightning. *Reliab. Eng. Syst. Saf.* 115, 91–99.
- Norman, J., Bar-Yam, Y., Taleb, N.N., 2020. Systemic risk of pandemic via novel pathogens – Coronavirus: A note, *New England Complex Systems Institute* (January 26). <https://necsi.edu/systemic-risk-of-pandemic-via-novel-pathogens-coronavirus-a-note>.
- Norwegian Oil and Gas Association, 2017. *Black Swans – an enhanced perspective on understanding, assessing and managing risk*, Nork olje&gass.
- NTSB, 1996. Evaluation of pipeline failures during flooding and of spill response actions, San Jacinto River near Houston, Texas, October 1994, Pipeline Special Investigation Report, NTSB/SIR-96/04. National Transportation Safety Board, Washington, D.C.
- OECD, 2015. Addendum Number 2 to the OECD Guiding Principles for Chemical Accident Prevention, Preparedness and Response (2nd ed.) to address natural hazards triggering technological accidents (Natechs), Organization for Economic Co-operation and Development, Paris.
- OECD, 2014. Risk Management and Corporate Governance, Corporate Governance, OECD Publishing. <https://doi.org/10.1787/9789264208636-en>.
- OECD, 2013. Report of the workshop on Natech risk management, 23–25 May 2012, Dresden, Germany, ENV/JM/MONO(2013)4, Series on Chemical Accidents No. 25, Organisation for Economic Co-operation and Development, Paris.
- OECD, 2003. Guiding Principles for Chemical Accident Prevention, Preparedness and Response (2nd ed.), Series on Chemical Accidents No. 10, Organization for Economic Co-operation and Development, Paris.
- OECD, 1992. The Polluter-Pays-Principle – OECD analyses and recommendations, OCDE/GD(92)81, Organization for Economic Co-operation and Development, Paris.
- OECD, 1989. Recommendation of the Council concerning the Application of the Polluter-Pays Principle to Accidental Pollution, C(89)88, Organization for Economic Co-operation and Development, Paris.
- Ogawa, A., 2016. Before and after Fukushima: The politics of nuclear power in time and space, *Global Urban Studies* No.9, Rikkyo University, Tokyo.
- Paltrinieri, N., Öien, K., Cozzani, V., 2012. Assessment and comparison of two early warning indicator methods in the perspective of prevention of atypical accident scenarios. *Reliab. Eng. Syst. Saf.* 108, 21–31.
- Paté-Cornell, E., 2012. On “Black Swans” and “perfect storms”: risk analysis and management when statistics are not enough. *Risk Anal.* 32 (11), 1823–1833.
- Perrow, C., 2011. Fukushima and the inevitability of accidents. *Bull. Atomic Sci.* 67 (6), 44–52.
- Pidgeon, N., 2012. Complex organizational failures – Culture, high reliability, and lessons from Fukushima, *The Bridge*, 42(3), National Academy of Engineering, USA.
- Quarantelli, E.L., 1997. Future disaster trends: implications for programs and policies, Preliminary Paper 256. University of Delaware, USA.
- Ranasinghe, U., Jefferies, J., Davis, P., Pillay, M., 2020. Resilience engineering indicators and safety management: a systematic review. *Saf. Health Work* 11 (2), 127–135.
- Rasmussen, J., 1997. Risk management in a dynamic society: a modelling problem. *Saf. Sci.* 27 (203), 183–213.
- Renn, O., 2008. *Risk Governance – Coping With Uncertainty in a Complex World*. Earthscan, London.
- Renn, O., Walker, K.D. (Eds.), 2008. *Global risk governance – Concept and practice using the IRGC framework*. Springer, Netherlands.
- Roberts, K.H., Rousseau, D.M., 1989. Research in nearly failure-free, high-reliability organizations: having the bubble. *IEEE Trans. Eng. Manage.* 36 (2), 132–139.
- Salzano, E., Iervolino, I., Fabbrocino, G., 2003. Seismic risk of atmospheric storage tanks in the framework of quantitative risk analysis. *J. Loss Prev. Process Ind.* 16, 403–409.
- Scheibe, K.P., Blackhurst, J., 2018. Supply chain disruption propagation: a systemic risk and normal accident theory perspective. *Int. J. Prod. Res.* 56 (1–2), 43–49.
- Shirali, G.A., Motamedzade, M., Mohammadfiam, I., Ebrahimipour, V., Moghimbeigi, A., 2016. Assessment of resilience engineering factors based on system properties in a process industry. *Cogn. Technol. Work* 18, 19–31.
- Shoemaker, J., 1995. Scenario planning: a tool for strategic thinking. *MIT Sloan Manage. Rev.* 36 (2), 25–40.
- Showler, P.S., Myers, M.F., 1994. Natural disasters in the United States as release agents of oil, chemicals, or radiological materials between 1980–1989: analysis and recommendations. *Risk Anal.* 14 (2), 169–181.
- Snow, N., 2010. Deepwater drilling moratorium may temporarily cost 8000–12000 jobs, Senate panel told. *Oil Gas J.* 108 (36), 17–18.
- Song, J.H., Kim, T.W., 2014. Severe accident issues raised by the Fukushima accident and improvements suggested. *Nucl. Eng. Technol.* 46 (2), 207–216.
- Sornette, D., 2009. *Dragon Kings, Black Swans and the prediction of crises*, Swiss Finance Institute Research Paper No. 09-36. <https://ssrn.com/abstract=1470006>.
- Stammer, B.J., 1993. Nothing we could do: the defense of Act of God in environmental prosecutions. *J. Environ. Law Pract.* 4 (1), 93–118.
- Steinberg, L.J., Sengul, H., Cruz, A.M., 2008. Natech risk and management: an assessment of the state of the art. *Nat. Hazards* 46 (2), 143–152.
- Suarez-Paba, M.C., Tzioutzios, D., Cruz, A.M., Krausmann, E., 2020. Toward Natech resilient societies. In: Yokomatsu, M., Scawthorn, C., Hochrainer-Stigler, S. (Eds.), *Disaster risk reduction and resilience*. Springer, Singapore.
- Sukhankin, S., 2020. Could the ‘Norilsk disaster’ be the harbinger of a looming catastrophe in the Russian Arctic? (Part one), *Eurasia Daily Monitor*, 17(93). <https://jamestown.org/program/could-the-norilsk-disaster-be-the-harbinger-of-a-looming-catastrophe-in-the-russian-arctic-part-one/>.
- Synolakis, C., Känäğlu, U., 2015. The Fukushima accident was preventable. *Philos. Trans. Roy. Soc. A*. <https://doi.org/10.1098/rsta-2014.0379>.
- Taleb, N.N., Spitznagel, M., 2020. Corporate socialism: the government is bailing out investors and managers not you, 26 March. <https://medium.com/incerto/corporate-socialism-the-government-is-bailing-out-investors-managers-not-you-3b31a67b44>.
- Taleb, N.N., 2010. *The Black Swan – The impact of the highly improbable*, second ed. Penguin, London.
- Taylor, R.H., van Wijk, L.G.A., May, J.H.M., Carhart, N.J., 2015. A study of the precursors leading to ‘organisational’ accidents in complex industrial settings. *Process Saf. Environ. Prot.* 93, 50–67.
- TEPCO, 2012. Fukushima Genshiyoku Jiko Cyosa Houkokusyo (Fukushima Nuclear Accident Investigation Report). Tokyo Electric Power Company, Tokyo.
- Thomson, J.R., 2015. High Integrity Systems and Safety Management in Hazardous Industries. Elsevier, Amsterdam.
- Tosa, H., 2015. The failed nuclear risk governance: Reflections on the boundary between misfortune and injustice in the case of the Fukushima Daiichi nuclear disaster. *Protosociology* 32, 125–149.
- Turner, B., 1978. *Man-made disasters*, first ed. Wykeham Publications.
- UNDRR, 2015. Sendai Framework for Disaster Risk Reduction 2015–2030. UN Office for Disaster Risk Reduction, Geneva.
- UNEP/OCHA, 2000. Cyanide spill at Baia Mare Romania, UNEP/OCHA Assessment Mission, UN Environment Programme, Geneva.
- Vallée, A., Duval, C., 2012. Flooding of industrial facilities - Vulnerability reduction in practice. *Chem. Eng. Trans.* 26, 111–116.

- Vaughan, A., 2018. BP's Deepwater Horizon bill tops \$65bn, *The Guardian*, 16/01/2018. <https://www.theguardian.com/business/2018/jan/16/bps-deepwater-horizon-bill-tops-65bn>.
- Vaughan, D., 2005. Organizational rituals of risk and error. In: Hutter, B., Power, M. (Eds.), *Organizational encounters with risk*. Cambridge University Press, New York.
- Weick, K.E., Sutcliffe, K.M., 2007. *Managing the Unexpected: Resilient Performance in an Age of Uncertainty*. Jossey-Bass, San Francisco.
- Weick, K.E., Sutcliffe, K.M., 2006. Mindfulness and the quality of organizational attention. *Organ. Sci.* 17 (4), 514–524.
- Wood, M., Allford, L., Gyenes, Z., Hailwood, M., 2017. Technological risks: chemical releases. In: Poljansek, K., Marín Ferrer, M., De Groeve, T., Clark, I. (Eds.), *Science for disaster risk management: knowing better and losing less*, EUR 28034 EN. Publications Office of the European Union, Luxembourg.
- Woods, D.D., 2006. Essential characteristics of resilience. In: Hollnagel, E., Woods, D.D., Leveson, N. (Eds.), *Resilience engineering – Concepts and precepts*. Ashgate Publishing Ltd., UK.
- You, Z., Yu, J., Liu, Y., Zhang, Y., Zhang, B., 2020. A summary of the investigation report on the Tianjiayi explosion incident (21 March 2019). *Process Saf. Prog.* 39 (1), e12132.
- Zenko, M., 2015. *Red Team: How to Succeed by Thinking Like the Enemy*. Basic Books, New York.

All links accessed on 26 January 2021