the Energy to Lead

FINAL REPORT

DOT CONTRACT DTPH5615T00001L, PROJECT NUMBER 638
GTI PROJECT NUMBER 21878

Approaches for Preventing Catastrophic Events

Reporting Period
October 1, 2015 to June 15, 2016

Report Issued
June 15, 2016

Prepared for
Robert Smith
U.S. Department of Transportation Pipeline and Hazardous Materials Safety Administration
919-238-4759
robert.w.smith@dot.gov

GTI Project Manager
Andrew Hammerschmidt
Program Director, Energy Delivery and Utilization
847-768-0686
Andrew.Hammerschmidt@gastechnology.org

GTI Technical Contact
Ernest Lever
R&D Director, Infrastructure
847-544-3415
Ernest.Lever@gastechnology.org

GTI Team Members
Ernest Lever and Daniel Ersoy

Gas Technology Institute
1700 S. Mount Prospect Rd.
Des Plaines, Illinois 60018
www.gastechnology.org

*File Name: DTPH5615T00001_Prj_*638_Final.Docx

Signature Page

Print or typed First M. Last	Signature	Date
AUTHOR: Ernest Lever	SS//Ernest Lever	June 15, 2016
	Title: R&D Director	
AUTHOR: Daniel Ersoy	SS//Daniel Ersoy	June 15, 2016
	Title: Exec. R&D Director	
REVIEWED/APPROVED: Andrew Hammerschmidt	SS//Andrew Hammerschmidt	June 15, 2016
	Title: Program Director	

Legal Notice

This information was prepared by Gas Technology Institute ("GTI") for the U.S. Department of Transportation Pipeline and Hazardous Materials Safety Administration.

Neither GTI, the members of GTI, the Sponsor(s), nor any person acting on behalf of any of them:

a. Makes any warranty or representation, express or implied with respect to the accuracy, completeness, or usefulness of the information contained in this report, or that the use of any information, apparatus, method, or process disclosed in this report may not infringe privately-owned rights. Inasmuch as this project is experimental in nature, the technical information, results, or conclusions cannot be predicted. Conclusions and analysis of results by GTI represent GTI's opinion based on inferences from measurements and empirical relationships, which inferences and assumptions are not infallible, and with respect to which competent specialists may differ.

b. Assumes any liability with respect to the use of, or for any and all damages resulting from the use of, any information, apparatus, method, or process disclosed in this report; any other use of, or reliance on, this report by any third party is at the third party's sole risk.

c. The results within this report relate only to the items researched.

Table of Contents

Page

Signature Page i

Legal Notice ii

Table of Contents iii

Table of Figures v

List of Tables vii

Executive Summary 1

Overview 1

The Pathway Forward 3

Steps *3*

1. Pre-assessment *3*

2. Appraisal *4*

3. Characterization and Evaluation *5*

4. Management *5*

5. Communication *6*

What is different in this Process? *6*

A. Introduction 7

B. Background 8

C. Data on Disasters and Catastrophes 12

D. Causal Factors in Industrial Catastrophes 23

E. Common Approaches to Risk Management in Industry 37

Barrier Approaches to Risk Prevention and Mitigation 37

Shortcomings of the Quantitative Risk Assessment (QRA) process *41*

Layers of Protection (LOPA) *41*

A recent critique on Major Hazard Event (MHE) management 43

Toulouse Ammonium Nitrate Fertilizer Explosion, Sep. 21, 2001[1, 35] *43*

Buncefield Vapor Cloud Explosion on Dec. 11, 2005 [1, 38, 39] *46*

The Bridle Critique *48*

Summary of Stakeholder interviews 54

F. Transitioning from Risk Analysis to Preventing Catastrophic Events 56

Addressing the Uncertainties in Risk Analysis 57

Diversity of Approach and Bayesian Updating 58

Addressing Deep Uncertainty Through Adaptation 63

Agent Supported Cooperative Work in Complex Systems 66

G. Framework for Risk Governance 71

The IRGC Risk Governance Framework [10, 13, 14] 73

Pre-assessment *76*
Appraisal *77*
Characterization and Evaluation *78*
Management *78*
Communication *79*
H. Conclusions 80
I. References 82
J. List of Acronyms 86
Appendix 1: Interviews of Stakeholders 87
Appendix 2: A Brief Review of Defense in Depth Concepts 94
Military Underpinnings 94
Non-military Use 94
Engineering 94
Extremely Complex Systems 94
Nuclear Industry Overview 95
Defense in Depth Nuclear Industry Concepts - Adapted to Pipeline Systems 96
General Concepts *97*
Summary of Defense-in-Depth 97
Objectives *98*
Strategy *98*
Interrelated Prerequisites *98*
Levels of Defense-in-Depth *99*
Defense in depth implementation in operations [73] *102*
Observability in Depth – A Suggested Compliment to Defense in Depth 103
Appendix 3: Analysis of Human Causal Elements in Catastrophic Events 105
Brief Summaries of Past Catastrophic Events 106
Industrial Sector *106*
Financial Sector *125*
Military, Social and Natural Disasters *130*
Retail Production Industry *134*
Analysis of Human Causal Factors in Catastrophes Reviewed by Chernov and Sornette *136*

Table of Figures

Page

Figure 1. Total number of disasters by type 1900-2015. Natural top, Technological bottom. [11] 14
Figure 2. Total number of disasters by continent 1900-2015. Natural top, Technological bottom. [11] 15
Figure 3. Total number of people affected by disasters by type 1900-2015. Natural top, Technological bottom. [11] 16
Figure 4. Total number of people affected by disasters by continent 1900-2015. Natural top, Technological bottom. [11] 17
Figure 5. Total number of deaths from disasters by type 1900-2015. Natural top, Technological bottom. [11] 18
Figure 6. Total number of deaths from disasters by continent 1900-2015. Natural top, Technological bottom. [11] 19
Figure 7. Economic impact of disasters by type 1900-2015. Natural top, Technological bottom. [11] 20
Figure 8. Economic impact of disasters by continent 1900-2015. Natural top, Technological bottom. [11] 21
Figure 9. Natural catastrophes 2012 – World map. Source: Munich Re, 2013, and The 11th March 2011 Tohoku tsunami striking the eastern coast of Japan. Source: Newscom/Kyodo/WENN taken from [12] 22
Figure 10. Simplified illustration of events that can lead to infrastructure system failure. An example of interacting causes is highlighted in yellow. Source IRGC [13]. 23
Figure 11. The components of a bow tie diagram. Source IRGC [14]. 24
Figure 12. Progressive transition of uncertainty from determinism to total ignorance. Source [15]. 25
Figure 13. Tabulation of Rumsfeld quote [16], per Paltrinieri [1]. 26
Figure 14. Risk Management Cycle KM=Knowledge Management, IM=Information Management. Source [1] adapted from [18]. 27
Figure 15. Analysis of Human Causal Factors in Catastrophes Reviewed by Chernov and Sornette 32
Figure 16. Grouping of factors underlying the concealment of information per Sornette and Chernov. Source [22] 33
Figure 17. The steps of the ARAMIS process. Source [29] 38
Figure 18. Bow tie and risk path in an ARAMIS type risk assessment. Source [29] 39
Figure 19. Location of Barriers in an ARAMIS type risk analysis. Source 39
Figure 20. Risk graph per ARAMIS for determining the required level of confidence to make risk acceptable (medium effect in Figure 21). Source [29] 40
Figure 21.Risk matrix used for ranking the dangerous phenomena and selecting 41

Figure 22. Layers of Protection. Source [32] 42
Figure 23. The LOPA concept. Source [31] 42
Figure 24. Functional silos in a typical organization. Source [33] 49
Figure 25. Functional silos and barrier management. Source [33] 51
Figure 26. Interactions in Infrastructure Systems. Source [42] 56
Figure 27. Process for transforming anecdote into data and information [48] 61
Figure 28. Methodology proposed by Khakzad et al. left, Bayesian Network model for offshore blowout and related near accidents, right. Source [55] 62
Figure 29. Graph of Complex Interacting System. Source Seth J. Chandler 66
Figure 30. Graph of interacting nodes given specific constraints. Source Seth J. Chandler 67
Figure 31. Graph of interactions with one constraint changed. Source Seth J. Chandler 68
Figure 32. Cartoon of two homogenous systems with heterogeneous coupling. Source [66] 69
Figure 33. From System of Systems to dependency network. Source [67] 69
Figure 34. Emerging risk governance at the intersection of various disciplines and theoretical frameworks. Source [14] 74
Figure 35. IRGC recommended structure for stakeholder involvement. Source [10] 75
Figure 36. Risk governance in context. Source [10] 75
Figure 37. Components of the IRGC risk governance framework. Source [10] 76
Figure 38. The defense in depth concept: purposes, methods and means (INSAG-10). 96
Figure 39. Schematic Illustration of an Accident Sequence, Defense-in-depth, and the Causal Dimension of “Depth” in Observability-in-depth 104
Figure 40. Graph of relationship between catastrophes reviewed and causal factors 145

List of Tables

	Page
Table 1. Grouping of factors underlying the concealment of information prior to major catastrophes per Sornette and Chernov. Source [22]	34
Table 2. Definition of the level of confidence in barriers per ARAMIS. Source [29]	40
Table 3 Comparison of Risk and Resilience Perspectives. Source [63]	65
Table 4. List of Acronyms	86
Table 5. Levels of Defense, Objective, and Essential Means	99
Table 6. Listing of causal factors	136
Table 7. Statistical analysis of causal factors	146

Executive Summary

This project is one of three R&D projects funded by PHMSA aimed at improving the risk management process for pipeline operators. The other two complementary projects include 1) "Critical Review of Candidate Pipeline Risk Models"[1] by C-FER technologies and 2) "White Paper on Risk Tolerance"[2] by Kiefner/Applus-RTD. Collectively these three research projects will provide valuable information to PHMSA and the pipeline industry for improving risk management practices and ultimately the safety and reliability of the nation's pipeline infrastructure.

Overview

The goal of this white paper is to present a thorough and critical review of approaches for preventing catastrophic events, both within and outside the natural gas industry, in order to be able to select the most appropriate approaches and models, develop them further, and ultimately issue guidelines for effective implementation in risk models and integrity management programs. A structured review of past catastrophic events, the existing methodologies for risk assessment, and their strengths and weaknesses was undertaken. A review of the state of the art in risk assessment, system of systems research and probabilistic methods related to the prediction of catastrophic events was completed. The latest approaches to developing frameworks for resilience in the face of catastrophes, and risk governance were reviewed.

What was found is that industries in both the United States and Europe use sophisticated and mature methodologies to identify and assess risks associated with hazardous system components. A wide variety of preventive and mitigative measures are employed across all critical infrastructure systems. Safety culture is an important component of all operating policies. In spite of these facts, industrial accidents still occur, sometimes with devastating consequences.

Careful investigation of dozens of major events reveals a complex web of causal factors covering all aspects of human organization and endeavor. On the human side we have: political and social structures, management cultures, incentives and censure, our desire to succeed and fear of failure, our passions and skepticism of the unfamiliar, our tendency to imprint, followed by a very long laundry list of human failings. People tend to believe that what happened yesterday will happen tomorrow, and if an event is not in our collective memory it is probably not a threat.

---

1 https://primis.phmsa.dot.gov/matrix/PrjHome.rdm?prj=656&s=39054EBE070846C0B97C439CD7670644&c=1

2 https://primis.phmsa.dot.gov/matrix/PrjHome.rdm?prj=639&s=39054EBE070846C0B97C439CD7670644&c=1

On the technological side, we have our ability to conceive and build systems that meet our various needs, we also have scientific prowess and the constant expansion of knowledge and potential that allow us to tap into more and more unexplored resources. This scientific, engineering and technological ability has led to exponential growth of human populations, systems of systems, and daunting complexity as we continue to weave our intricate web. Unfortunately, our lack of understanding of the full implications of the complex interactions associated our infrastructures has exposed us to infrequent, yet catastrophic risks when failures occur along convoluted pathways through human and technological systems. We have difficulty identifying new and emergent risks, in part due to our enslavement to the familiar risks we think we understand.

There is a growing realization that the pathway to solving the problem of complexity with unfamiliar risks might lie in embracing diversity and bringing it in to our processes at all levels of our systems and culture. Diversity means multidisciplinary approaches involving all stakeholders at multiple levels, allowing local autonomy of decision making while enforcing communication between the lowest and highest strata in an organization and its surroundings.

At the macro level, frameworks to achieve these ambitious goals have been proposed in the United States by the National Science and Technology Council (NTSC) and in Europe by the International Risk Governance Council (IRGC). These frameworks do an adequate job of covering the aspects of an improved worldwide, nationwide, region wide and system of systems wide, risk-aware and informed decision making process that brings all social and technological aspects into the picture.

At the micro level, we have to develop a synthesis of classic risk assessment and management approaches, but ensure that they are guided by system of systems thinking. It is essential to adopt the emerging disciplines of complex system analysis and collaborative agent based design as they have the greatest potential for enlightening us on how risk is driven by difficult to visualize interactions. We need to learn from the various approaches that demonstrate the power of diverse teams at the micro level, and constant updating of our approaches and policies based on new evidence as it becomes available. There is a vibrant and emerging body of research exploring these techniques that demonstrate how it is possible to function under great uncertainty with sparse data. A good proportion of this research is aimed at interacting infrastructures and how to model their emerging risks, as well as how to use readily available precursors as reasonable predictors of catastrophic failure.

These techniques need to become familiar, everyday activities; embracing these will help us design and operate systems of systems that are both more resilient in the face of the unexpected, and less prone to extreme events. We need to accept that our styles of management and regulation may have to change dramatically as we become more aware of, and better understand, the likelihood and consequences of extremely rare events, and how to reduce their probability of ever occurring.

Our training curricula, both internal to the organizations and in our educational institutions need to reflect this shift in perception and facilitate the necessary cultural changes to truly grapple with the prevention of catastrophic events in our technological systems.

The Pathway Forward

Using the IRGC[3] framework as a basis, below is a process outline for an operator to reinforce their risk management framework to better address the potential for catastrophic events.

Steps

1. Pre-assessment
2. Appraisal
3. Characterization and Evaluation
4. Management
5. Communication

1. Pre-assessment

Risk pre-assessment addresses early warning and "framing" of the risk in order to provide a structured definition of the problem and how it may be handled. Pre-assessment clarifies the various perspectives on a risk, defines the issue to be looked at, and forms the baseline for how a risk is assessed and managed. Operators typically start with a risk assessment of their systems, both physical and human. This includes identifying threats and their potential interactions, and how preventative and mitigative measures tie in. This step typically uses a bow-tie analysis to lay out the perceived failure modes and consequences, their composite risks, leading indicators, regulatory requirements, and then prioritizes actionable items for risk management activities.

This process needs to be enhanced by bringing in more stakeholders and a multidisciplinary approach that includes the social and engineering sciences. This step needs to include

3 See section: The IRGC Risk Governance Framework [10, 13, 14] on p73 for detail

adjacent systems and events that could interact with the operator's system precipitating failures in either system. Secondly, the evaluation needs to assume a worst case failure and address how this failure will impact adjacent systems. *System of Systems* approaches based on networks of interacting agents are particularly effective in helping us understand the scope of the detailed risk assessment needed.

This pre-assessment will form the foundation and drive the detailed appraisal of risks in Step 2.

2. Appraisal

The risk appraisal develops and synthesizes the knowledge base for the decision on whether or not a risk should be taken and, if so, how the risk can possibly be reduced or contained. The risk appraisal comprises both, (i) a Scientific Risk Assessment – a conventional assessment of the risk's factual, physical and measurable characteristics including the probability of it happening; and (ii) a Concern Assessment – a systematic analysis of the associations and perceived consequences (benefits and risks) that the various stakeholders perceive.

Scientific Risk Assessment deals with the following types of questions:

- What are the potential damages or adverse effects?
- What is the probability of occurrence?
- How ubiquitous could the damage be? How persistent? Can it be reversed?
- How clearly can cause-effect relationships be established?
- What scientific, technical and analytical approaches, knowledge and expertise should be used to better assess these impacts?
- What are the primary and secondary benefits, opportunities and potential adverse effects?

Concern Assessment deals with such questions as:

- What are the public's concerns and perceptions?
- What is the social response to the risk? Is there the possibility of political mobilization or potential conflict?
- What role are existing institutions, governance structures and the media playing in defining public concerns?
- Are risk managers likely to face controversial responses arising from differences in stakeholder objectives and values, or from inequities in the distribution of benefits and risks?

3. Characterization and Evaluation

This step addresses the amalgam of the operators, regulators, and publics risk tolerance. Questions to address include:

- What are the societal, economic and environmental benefits and risks?
- Are there impacts on quality of life?
- Are there ethical issues to consider?
- Is there a possibility of substitution? If so, how do the risks compare?
- Does a choice of a particular technology impact on the risk? How?
- What are the possible options for risk compensation, or reduction?
- What are the societal values and norms for making judgements about tolerability and acceptability?
- Do any stakeholders – government, business or other – have commitments or other reasons for wanting a particular outcome of the risk governance process?

4. Management

Steps 1 to 3 feed this step which develops an adequate risk management plan. Risk management involves the design and implementation of the actions and remedies required to avoid, reduce, transfer or retain the risks. Risk management includes the generation, assessment, evaluation and selection of appropriate risk reduction options as well as implementing the selected measures, monitoring their effectiveness and reviewing the decision if necessary. Operators typically us a PDCA- Plan, Do, Check, and Act process coupled with a RACI – Responsible, Accountable, Consulted, and Informed chart to accomplish this. This is complemented with a MOC – Management of Change, as well as a CPI – Continuous Process Improvement plans.

The various management plans need to be frequently reassessed on the basis of new evidence that is constantly being gathered. This process need to be sensitive to new emerging risks that were previously not identified. Additionally, risks that were previously deemed acceptable, may become unacceptable in the light of new information, including additional interaction pathways that are recognized.

Management step questions include:

- Who is, or should be, responsible for decisions within the context of the risk and its management?
- Have they accepted this responsibility?
- What management options could be chosen (technological, regulatory, institutional, educational, compensation, etc.)?
- How are these options evaluated and prioritized?
- What are the secondary impacts of particular risk reduction options?

- What potential trade-offs between risks, benefits and risk reduction measures may arise?
- What measures are needed to ensure effectiveness in the long term (compliance, enforcement, monitoring, adaptive management plans, etc.)?

5. Communication

Communication, both internal and external, enables all stakeholders to understand the risks involved. Once risk management decisions are made, communication should explain the rationale for the decisions and allow stakeholders to make informed choices about the risks and their management, including their own responsibilities. Effective communication is the key to creating trust in risk management through transparency.

What is different in this Process?

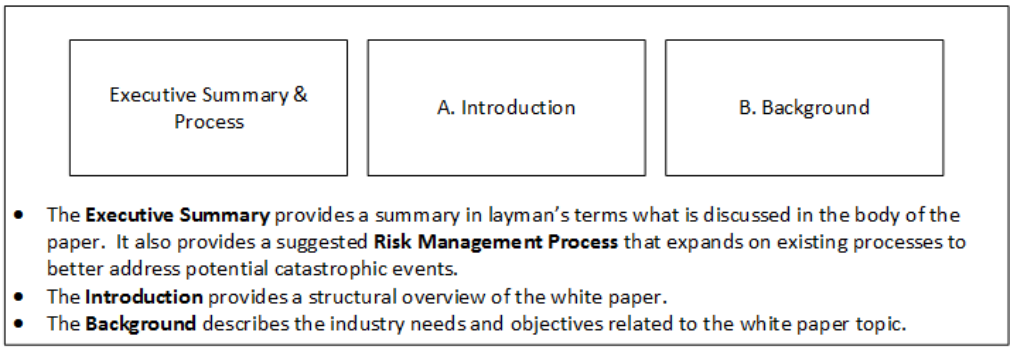
The process template above is very similar to risk management processes already used by operators.

The enhancements are:

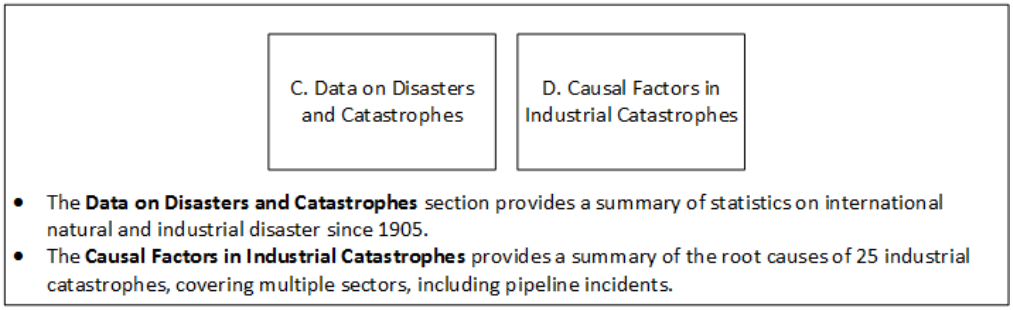
- The inclusion of a multi-disciplinary team approach at all levels:
    - Recent research has found that diversity of approach and frequent revisiting of assumptions greatly enhance our ability to make predictions under extreme uncertainty,
    - Using multiple models with diverse approaches increases the robustness of our decisions under extreme uncertainty,
- Introducing complex system approaches help us:
    - Gain a more complete understanding of possible causal pathways that lead to extreme events,
    - Develop probabilities of extreme events based on the appropriate precursor analysis
- The process is modular and scalable, in that the same approach can be applied to individual systems, systems of systems, interacting infrastructures and the regulatory process in turn.

The concepts and terms laid out in the process above are explained in detail in the body of this white paper. Further details can be found in the references.

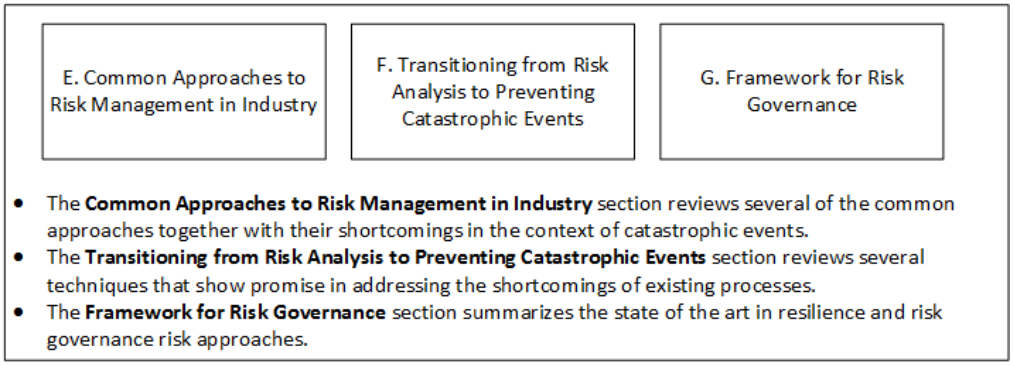
A. Introduction



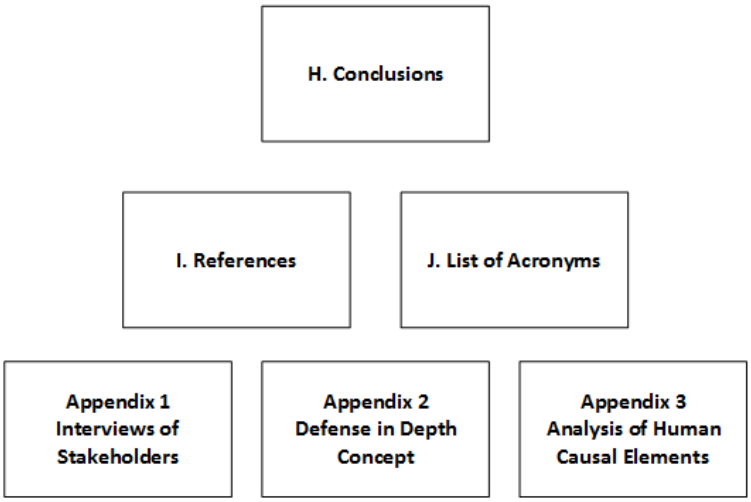
- The **Executive Summary** provides a summary in layman's terms what is discussed in the body of the paper. It also provides a suggested **Risk Management Process** that expands on existing processes to better address potential catastrophic events.
- The **Introduction** provides a structural overview of the white paper.
- The **Background** describes the industry needs and objectives related to the white paper topic.



- The **Data on Disasters and Catastrophes** section provides a summary of statistics on international natural and industrial disaster since 1905.
- The **Causal Factors in Industrial Catastrophes** provides a summary of the root causes of 25 industrial catastrophes, covering multiple sectors, including pipeline incidents.



- The **Common Approaches to Risk Management in Industry** section reviews several of the common approaches together with their shortcomings in the context of catastrophic events.
- The **Transitioning from Risk Analysis to Preventing Catastrophic Events** section reviews several techniques that show promise in addressing the shortcomings of existing processes.
- The **Framework for Risk Governance** section summarizes the state of the art in resilience and risk governance risk approaches.



B. Background

The goal of this white paper is to present a thorough and critical review of approaches for preventing catastrophic events, both within and outside the natural gas industry, in order to be able to select the most appropriate approaches and models, develop them further, and ultimately issue guidelines for effective implementation in risk models and integrity management programs. The aim is to obtain a structured review of the existing methodologies, identify gaps, and establish the groundwork for the adoption and/or development of a suitable approach for the sector. There is an extensive list of approaches and methodologies. Each might have a unique scope, address different sectors or stakeholders (policy makers, researchers, operators etc.), aim at differing objectives, use various applied techniques and standards, and quantify risk uniquely.

Catastrophic events are notoriously hard to predict and prepare for. These are low-probability high-impact events that do not "behave" well with standard probabilistic tools. They are rare and thus cannot properly inform a probability distribution function. They arealso unique, offering only limited learning opportunities from one such event to the next.

Paltrinieri et al. [1] explain that the classic risk analytic paradigm, which begins with hazard identification, is an exercise that is problematic in the context of complex systems and emergent threats, because hazards may be largely unknown. Park et al. [2] postulate a better catastrophe management plan combines risk analysis with resilience analysis: resilience approaches require preparing for the unexpected, whereas risk analysis proceeds from the premise that hazards are identifiable. Recognizing there are not enough available resources to reduce all risks, government agencies such as the Department of Homeland Security (DHS) are "moving increasingly to risk analysis and risk-based resource allocation, a process designed to manage the greatest risks instead of attempting to protect everything" Willis, [3].

More specifically, several mature approaches seem to capture the essence of catastrophic risk fairly well, but sometimes fail in properly propagating actionable results to any relevant supporting decision-making mechanisms. For example, the National Research Council's Committee to Review the DHS's Approach to Risk Analysis [4] reports while "DHS has established a conceptual framework for risk analysis… that, generally speaking, appears appropriate for decomposing risk and organizing information, and it has built models, data streams, and processes for executing risk analyses for some of its various missions… the committee did not find any DHS risk analysis capabilities and methods that are yet adequate for supporting DHS decision making, because their validity and reliability are untested."

The dramatic emergence in recent years of "big data" along with new modeling methodologies offer novel ways of dealing with risk from catastrophic events. The DHS has a number of relevant Calls to Action (detailed in the 2013 NIPP), among them:

- "Enable risk-informed decision making through enhanced situational awareness
- Analyze infrastructure dependencies, interdependencies, and associated cascading effects
- Identify, assess, and respond to unanticipated infrastructure cascading effects during and following incidents
- Strengthen coordinated development and delivery of technical assistance, training, and education."

These could all take advantage of novel modeling methodologies incorporating big data and the interconnectedness of modeling systems, such as Bayesian networks, semantic webs, and graph trace analysis.

An additional complication arising with catastrophic events is that they most often do not strike only one installation or even sector. On the contrary, technical installations, human operators, and organization represent diversity in any system. Nonetheless, a new challenge exists, which is represented by complex systems continuously enlarging. For instance, a natural gas delivery system is an infrastructure which does not work in isolation anymore. The same holds for the communication networks, Internet, railway transport, and so forth. A disruption of service is not confined but instead is propagating, and thus rendering the whole network more vulnerable. The modeling scope has changed accordingly, from the concept of complex system to the System of Systems (SoS). While complex systems still have boundaries and defined architecture, a SoS is blurrier in boundaries and may evolve in time. These topics are discussed in detail in the sections: **Diversity of Approach and Bayesian Updating p58, Addressing Deep Uncertainty Through Adaptation p63**, and **Agent Supported Cooperative Work in Complex Systems p66**.

These complications indicate a need for sophisticated use of distributed data. This can be achieved through data mining applications or semantic web implementations, which provide "a common framework that allows data to be shared and reused across application, enterprise, and community boundaries"[4][5]. In addition, various Knowledge Management Frameworks can facilitate accumulated knowledge across the industry, or even from multiple industries – if set up properly and used correctly.

"W3C Semantic Web Activity". World Wide Web Consortium (W3C).

The major challenge addressed herein is most catastrophic events (such as hurricanes and terror attacks) cannot be prevented per se, at least not by the actors in the natural gas industry or their regulators. However, preparations can go a long way in minimizing those events' probabilities and in containing their consequences – namely, in managing the risks and maximizing resilience.

Catastrophic events are typically low-probability, high-consequence events. The associated engineering systems must confront dynamic and unpredictable environments, causing estimates of likelihood to be unreliable, if at all available. Even more difficult to forecast is the joint probability of the confluence of two or more major events (which is not rare in the context of catastrophic events such as the Fukushima nuclear disaster). They have a far greater combined impact or synergy than when they occur independently. Similarly, we have a poor understanding of how failures propagate and are amplified within and across a complex systems and the SoS.

Mathematically, these events may be associated with the probability distributions having asymmetrical long tails, especially difficult to characterize because their frequency is so low that historical data sets, if extant at all, will be sparsely populated. Available data often represent a distally (far from the center) truncated probability distribution function (pdf), leading to an underestimation of unobserved low-probability, but potentially high-consequence risks. Such problems are exacerbated for distributions with "heavy tails" (e.g., power law), which have an indeterminate mean and variance of the pdf, Pisarenko and Rodkin [6]. This implies the risks with heavy tailed pdfs in complex systems are inherently impossible to fully quantify because their moments (e.g., mean, variance) are indeterminate Aban et al., [7]. Insurance companies sometimes use subjective judgments by experts in lieu of frequency-based estimates of probability Morgan, Henrion, and Small, [8]. However, advanced methodologies such as Bayesian networks can resolve many of these issues, by integrating multiple inputs, however uncertain, and subsequently producing meaningful posterior distributions. The Bayesian view is useful for informing decisions when existing information is vague or uncertain, yet may lead experts to have a prior belief of probabilities that can later be updated as new information becomes available. Bayesian decision theory allows for the incorporation of subjective probability judgments into assessments that may include frequentist calculations.

Moreover, at least two attributes of complex engineering systems complicate risk analysis:

1. Nonstationarity, wherein path dependencies, changing boundary conditions, or interdependencies generate different responses to identical stimuli that happen at

different times; i.e. past record is not a reliable predictor of future performance Ben-Haim [9], and

2. Unexpected shocks, wherein extreme (i.e., low-frequency, high- consequence) events lead to failure of the engineered systems.

Both of these issues can be resolved, at least to a certain extent, by various methods. The goal of this project is to examine proposed and applied solutions to these and similar problems, which can ultimately be applied to the natural gas sector.

C. Data on Disasters and Catastrophes

The Centre for Research on the Epidemiology of Disasters (CRED) provides a publically available database (EM-DAT)[5] that conveniently summarizes various statistics on both natural and technological disasters going back to 1905. There is no consensus on best practices for collecting such data, and there is considerable variation in definitions and methodologies associated with the reporting of this data. Notwithstanding these caveats, the database provides a very convenient tool for understanding the orders of magnitudes of the various disaster types measured by human and economic costs, the geographic spread and trends over time. A selection of graphs generated by this tool is presented in **Figure 1** to **Figure 8** below to provide some insights on the relative scale and trending of both natural and technological disasters across the globe.

It is immediately apparent that the number of natural and technological disasters recorded has increased dramatically over the last seventy years. The shape of the distribution of disasters over time is very similar for both types and the ratio between natural and technological disasters is approximately 2-3 over this time span (**Figure 1** and **Figure 2**). The increase in the number of recorded disasters is more than likely a reflection of the increasing concentration of people in urban areas that is strongly related to technological development over this time span. The number of people affected by natural disasters is orders of magnitude higher than the number affected by technological disasters for obvious reasons, geographically disperse impacts from natural disasters as opposed to highly localized impact for the majority of technological disasters, (**Figure 3** and **Figure 4**). However, it is interesting to note that there is a dramatic downward trend in the number of deaths from natural disasters and an increase in the number of deaths from technological disasters (**Figure 5** and **Figure 6**). This opposite trending likely reflects the advances in communication technology, heightened awareness and improving logistical capabilities for natural disasters, and the increasing proximity of human habitat to industrial facilities for technological disasters. The overall economic impact of natural disasters is an order of magnitude higher than that of technological disasters (**Figure 7** and **Figure 8**).

Having noted this difference in scale of economic impact, the year 2010 is a good illustration of the significant impact technological catastrophes can have. The Deep Water Horizon oil rig disaster in the Gulf of Mexico and the San Bruno pipeline explosion account for the very significant economic impact depicted in the graphs for 2010.

---

5 D. Guha-Sapir, R. Below, Ph. Hoyois - EM-DAT: The CRED/OFDA International Disaster Database – www.emdat.be – Université Catholique de Louvain – Brussels – Belgium

We cannot ignore the possible coupling of natural and technological catastrophes. The Tohoku earthquake and Fukushima Daiichi nuclear disaster are recent examples of such a coupling[6]. **Figure 9** is a world map showing the geographic distribution of potential for natural disasters. Few countries are exempt from natural disasters and North America has significant exposure to climatological, meteorological, hydrological and geophysical events. All of these naturally occurring events can have significant impact on infrastructure systems, hence disaster recovery and resilient system design are significant areas of focus in the modern world[7,8,9]. The focus on disaster recovery and resilience has led to the realization that collaboration between diverse disciplines across the full risk reduction cycle that includes prevention, prediction, early detection, response and recovery [10], is essential. We will draw on these collaborative approaches and discuss their relevance to the prevention of catastrophic events in subsequent sections of this white paper.

6 https://en.wikipedia.org/wiki/Fukushima_disaster_cleanup

7 https://www.dhs.gov/topic/disaster-response-and-recovery

8 http://ncdp.columbia.edu/

9 http://www.unisdr.org/

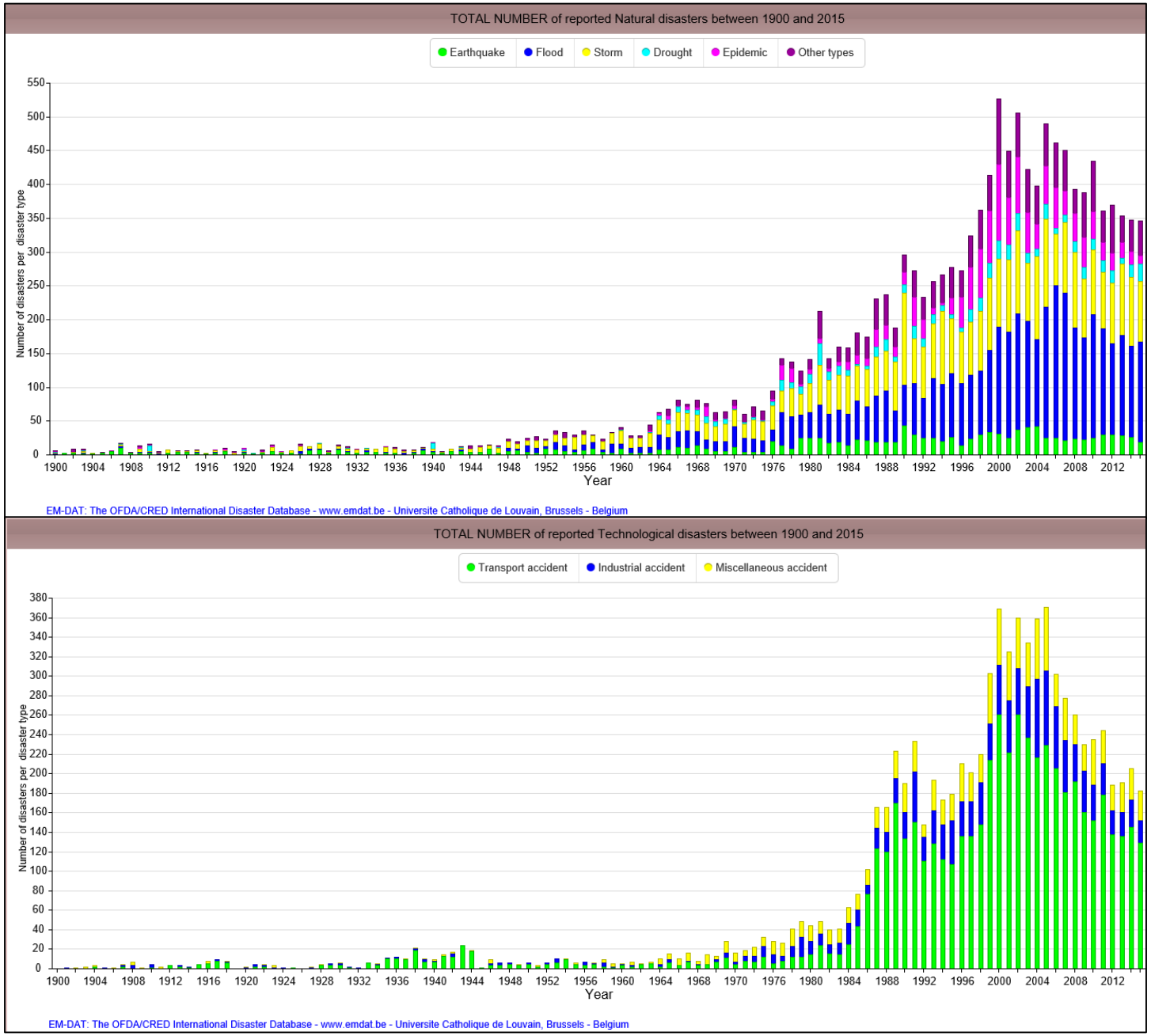


Figure 1. Total number of disasters by type 1900-2015. Natural top, Technological bottom. [11]

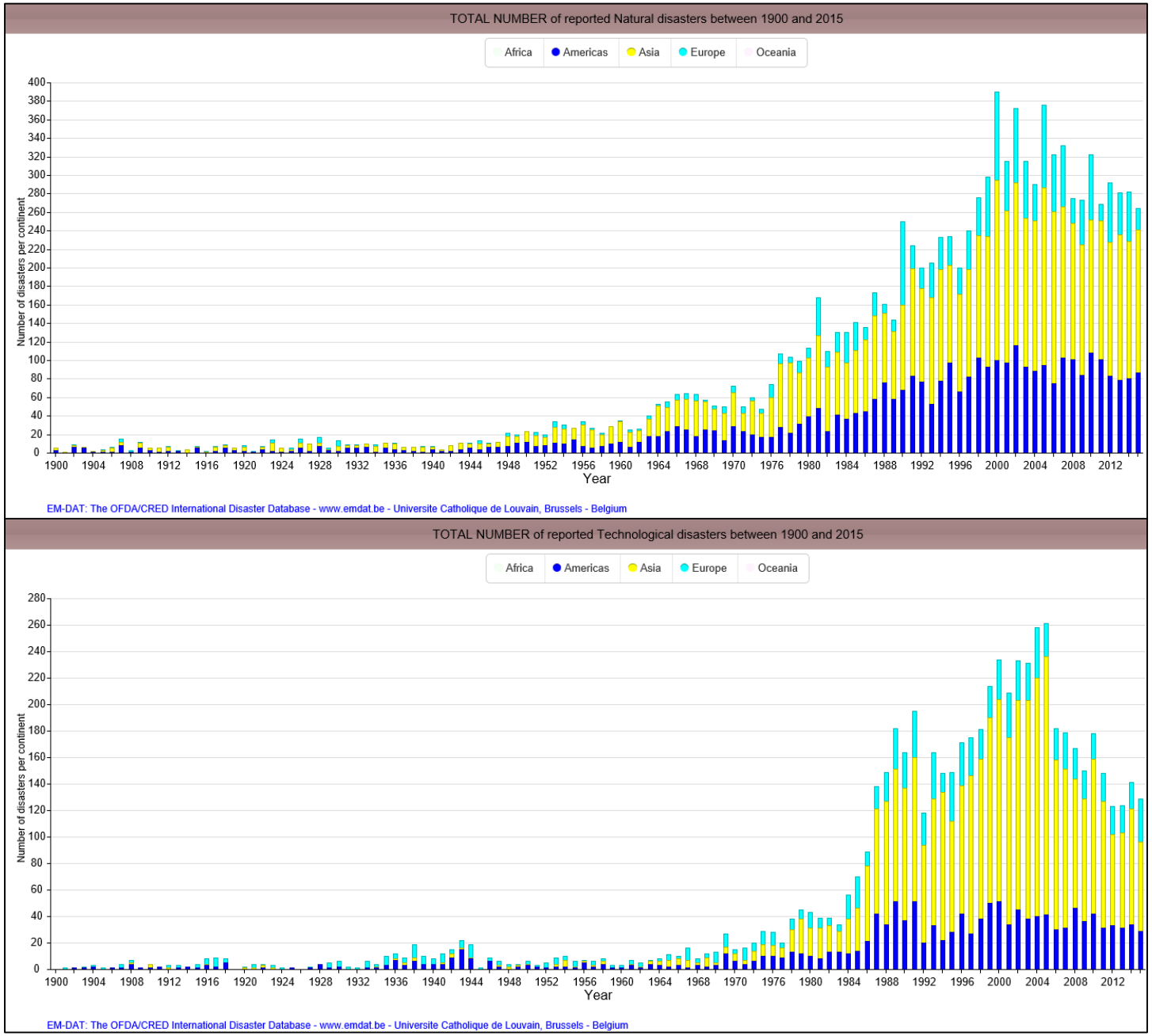


Figure 2. Total number of disasters by continent 1900-2015. Natural top, Technological bottom. [11]

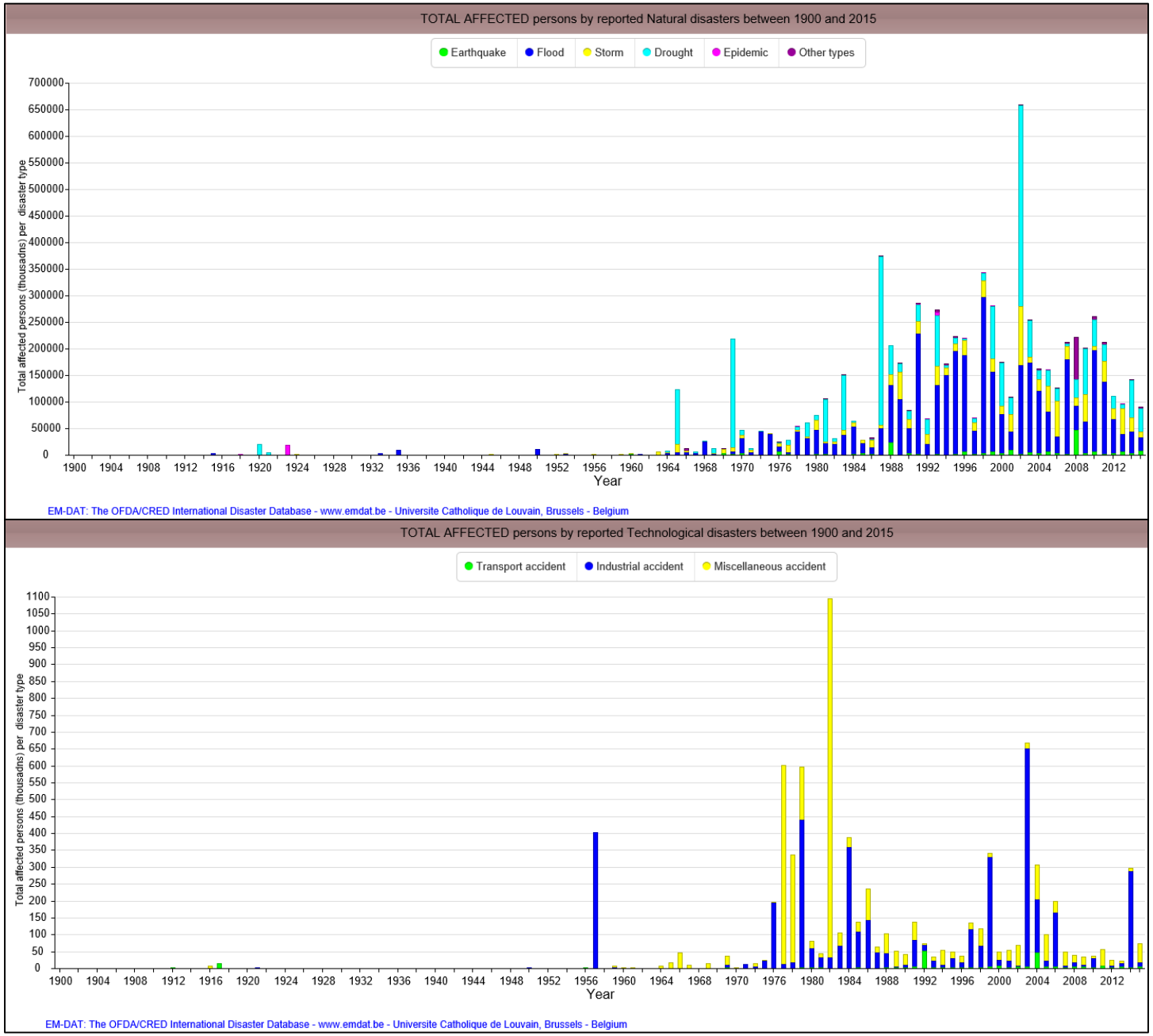


Figure 3. Total number of people affected by disasters by type 1900-2015. Natural top, Technological bottom. [11]

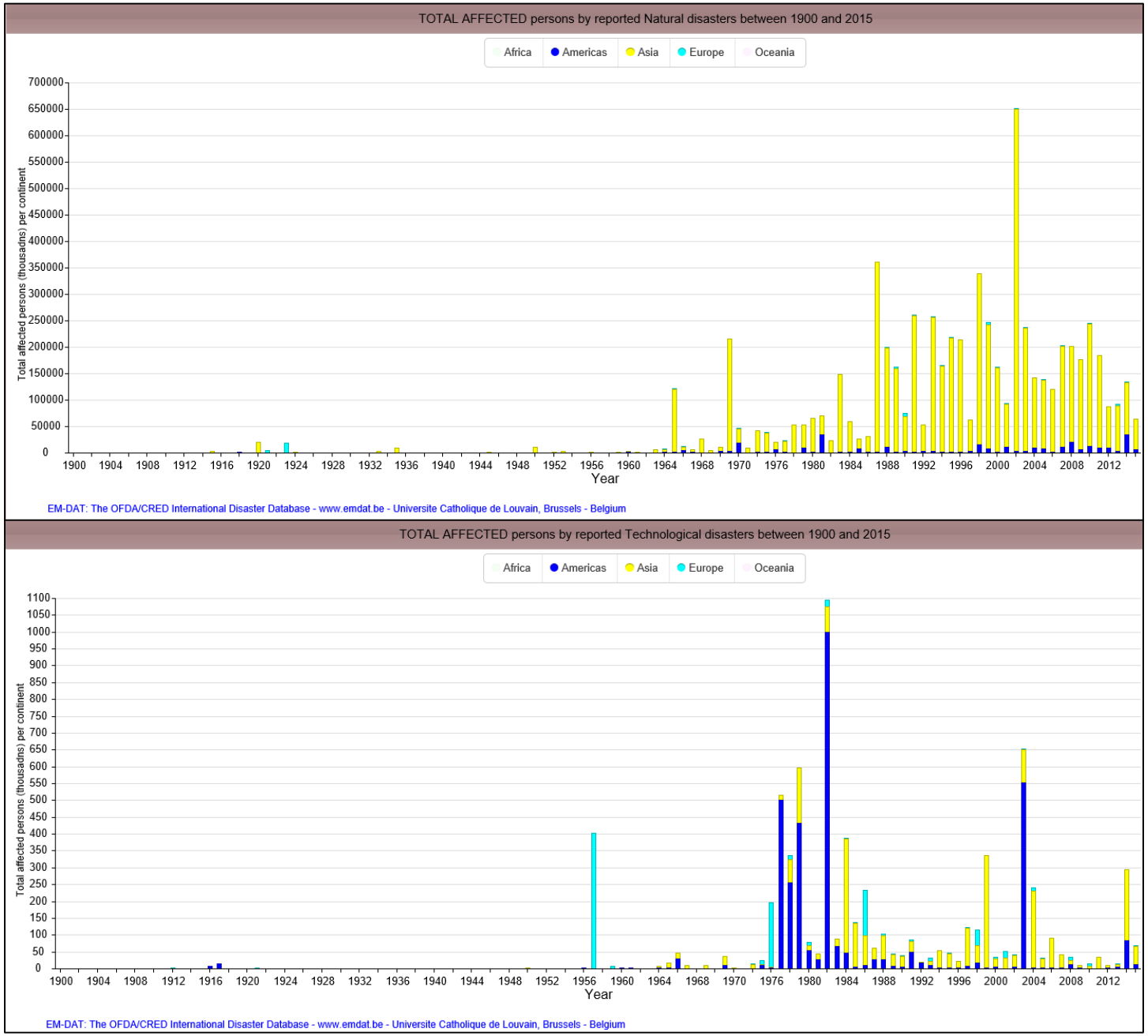


Figure 4. Total number of people affected by disasters by continent 1900-2015. Natural top, Technological bottom. [11]

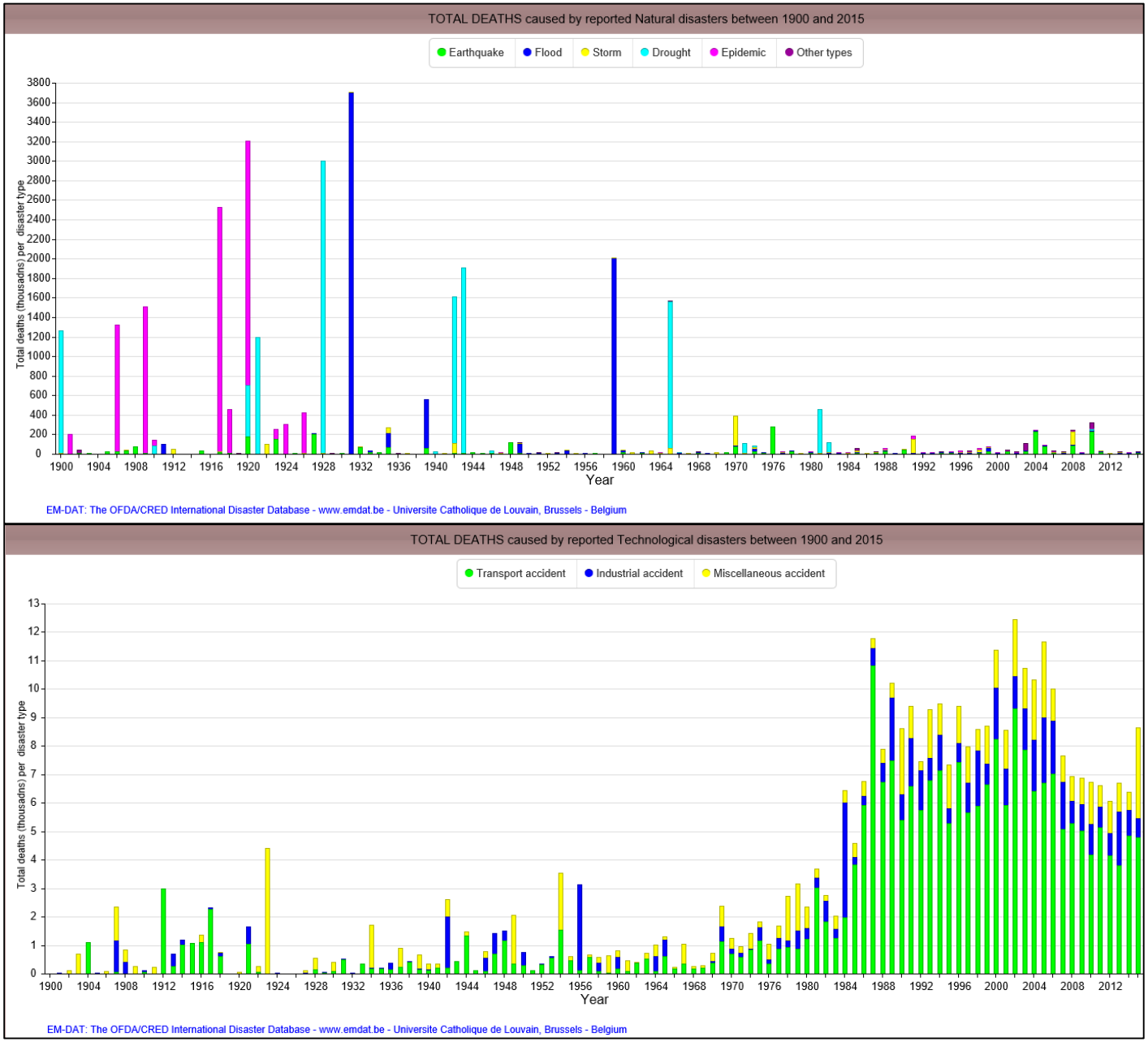


Figure 5. Total number of deaths from disasters by type 1900-2015. Natural top, Technological bottom. [11]

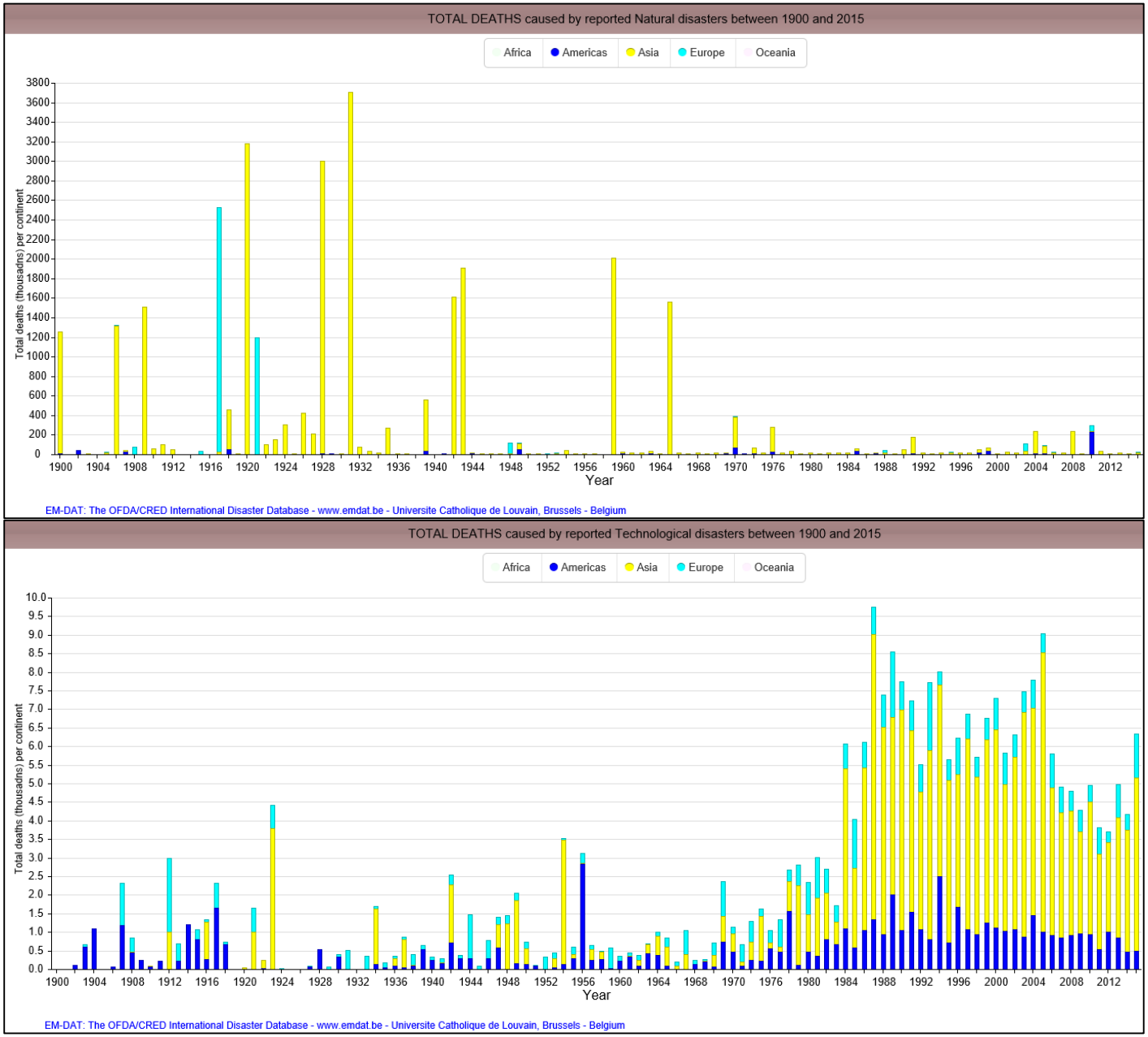


Figure 6. Total number of deaths from disasters by continent 1900-2015. Natural top, Technological bottom. [11]

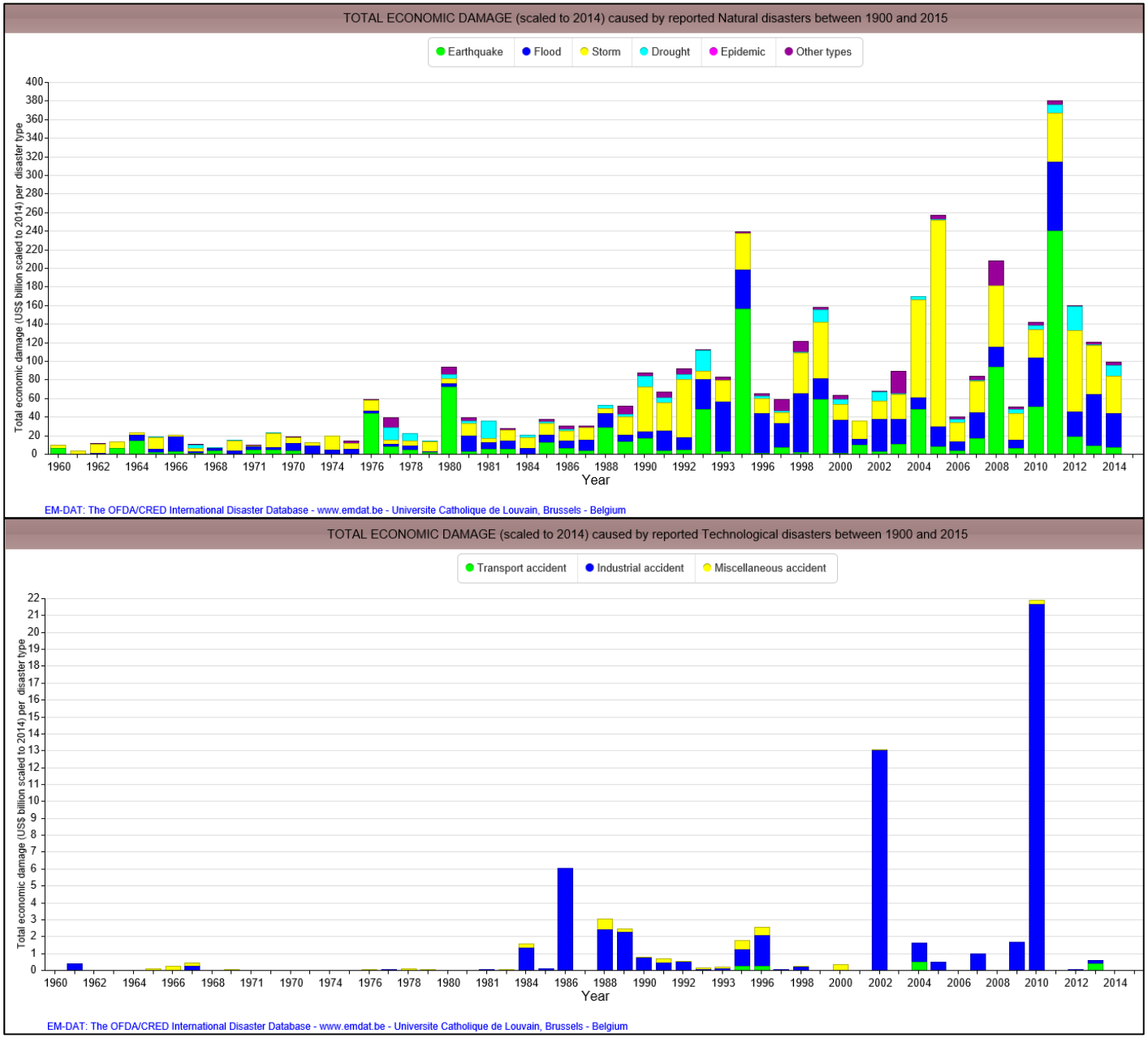


Figure 7. Economic impact of disasters by type 1900-2015. Natural top, Technological bottom. [11]

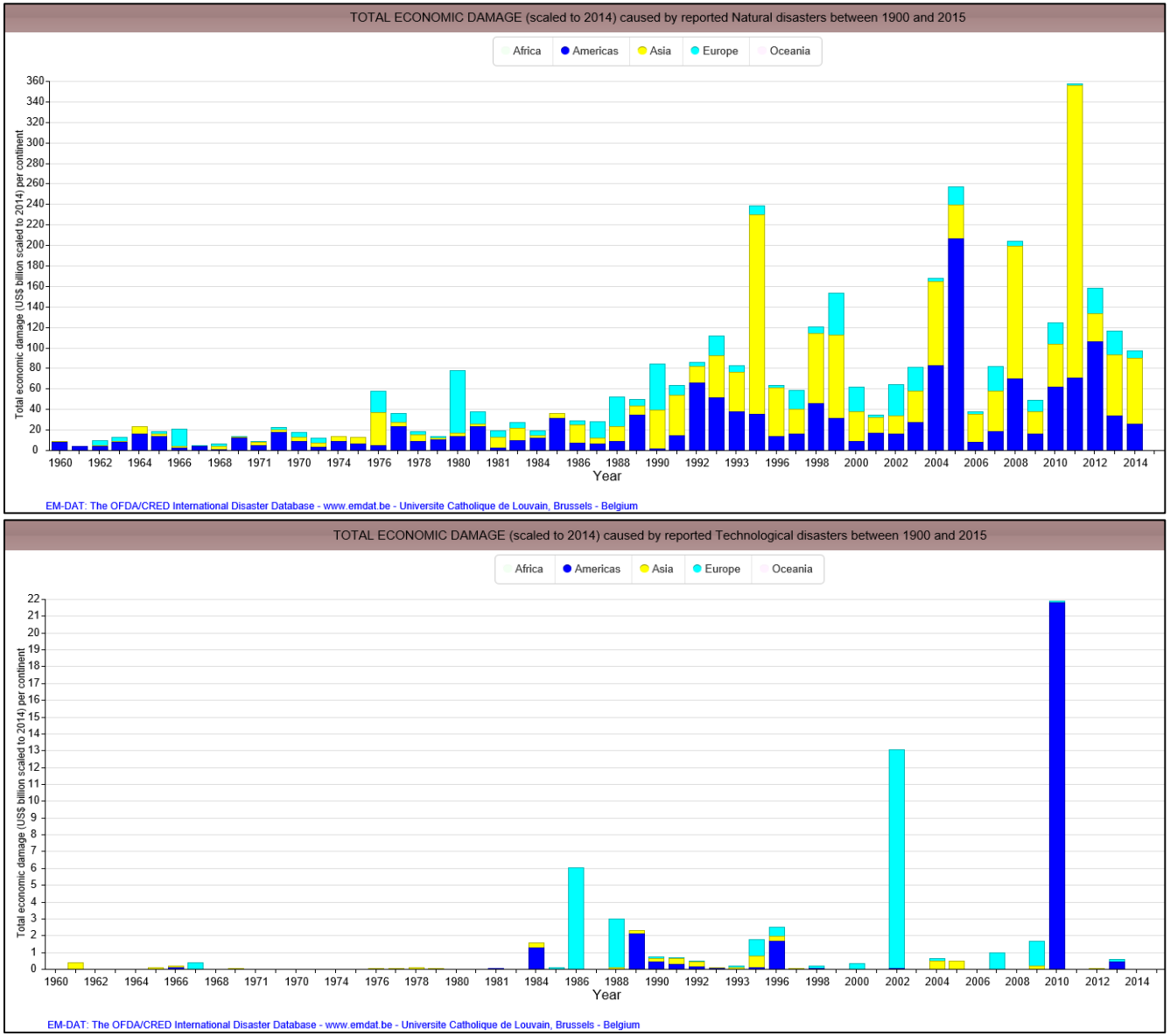


Figure 8. Economic impact of disasters by continent 1900-2015. Natural top, Technological bottom. [11]

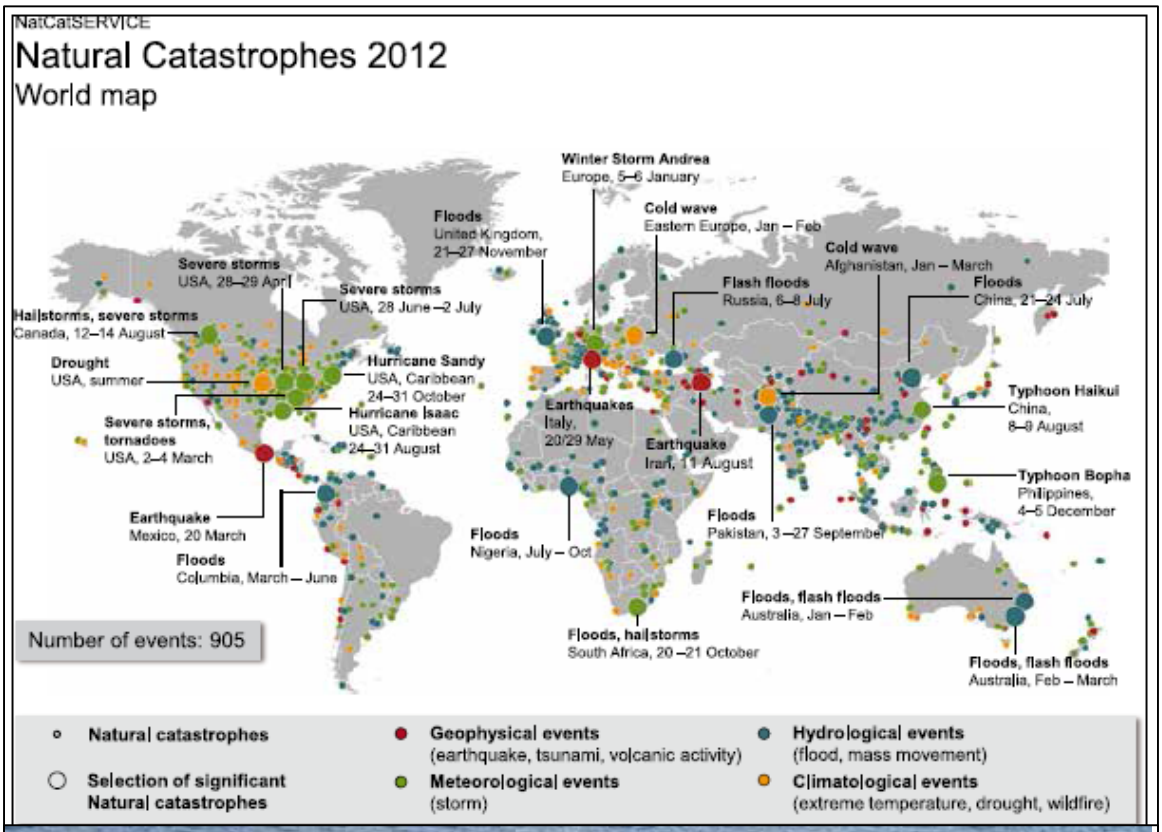


Figure 9. Natural catastrophes 2012 – World map. Source: Munich Re, 2013, and The 11th March 2011 Tohoku tsunami striking the eastern coast of Japan. Source: Newscom/Kyodo/WENN taken from [12]

D. Causal Factors in Industrial Catastrophes

Industrial malfunctions have at least one system, or component failure amongst their root causes. Incidents that rise to the level of a catastrophic failure are often the product of multiple low probability interacting causes. **Figure 10** provides a simplified illustration of some of the events that can lead to an infrastructure system failure.

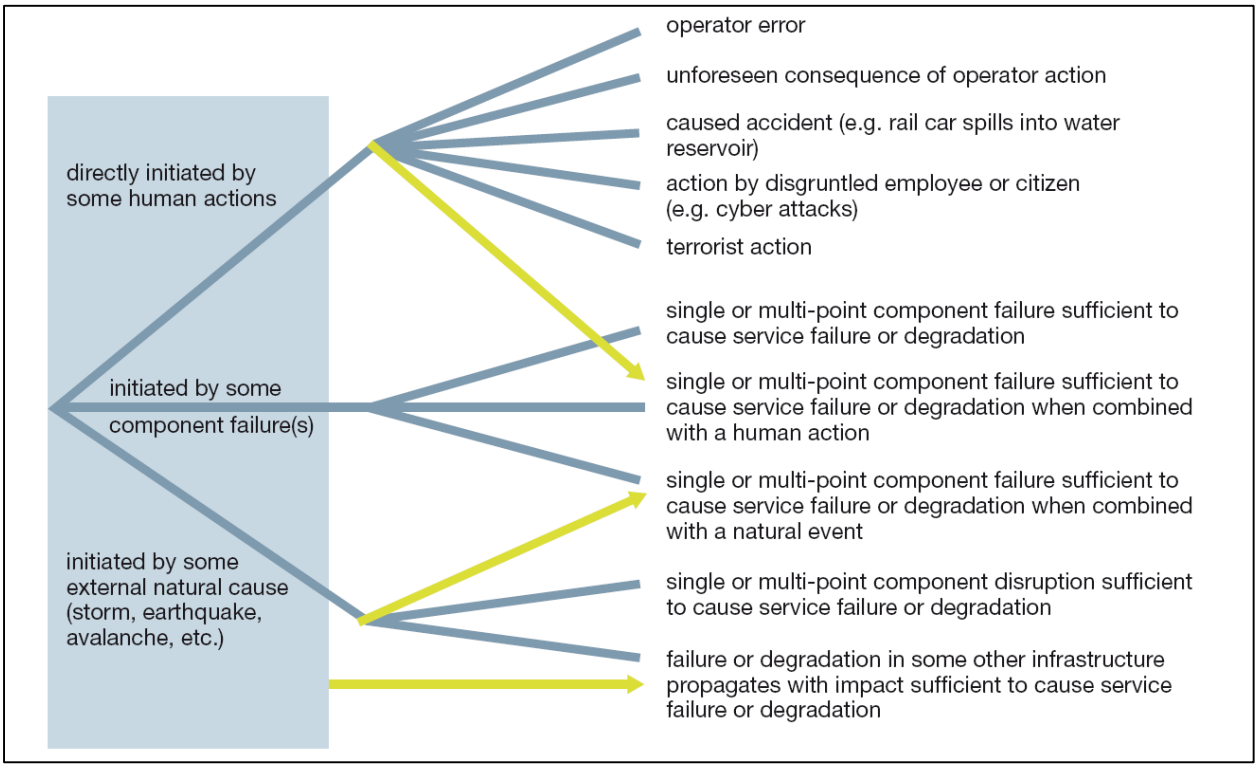


Figure 10. Simplified illustration of events that can lead to infrastructure system failure. An example of interacting causes is highlighted in yellow. Source IRGC [13].

The occurrence of a failure event provokes an effort to prevent future similar events and to anticipate the consequences of a future occurrence of the same event, i.e. a risk assessment process is carried out. There are many approaches to conducting a risk assessment. One commonly used approach in quantitative risk assessment is a rigorous analysis of the causes of a fault condition that can be extended to include estimates of the probability of occurrence of each of the underlying causes and the nature of their interaction, i.e. do two or more causal factors in a given failure pathway have to act in conjunction (and gate), or are each of them independent causal factors capable of triggering a causal condition (or gate). The aggregation of the causal factors underlying a single fault condition is known as a **fault tree** and defines a **hazard**, which is surrounded by a temporal boundary when events considered plausible and characterized by a probability distribution are studied [14]. The fault tree does not consider what the results of a failure event might be. An analysis of how the system may evolve after a fault occurs, and what the potential consequences related to each event precipitated by the fault might be, is performed by constructing an **event tree**. The event tree

fans out from the initial fault event as different event escalation pathways are defined, together with their associated probabilities of occurrence. The event tree is encapsulated by a boundary that reflects the constraints that were placed on the imagination of the analyst due to practical limitations or lack of knowledge.

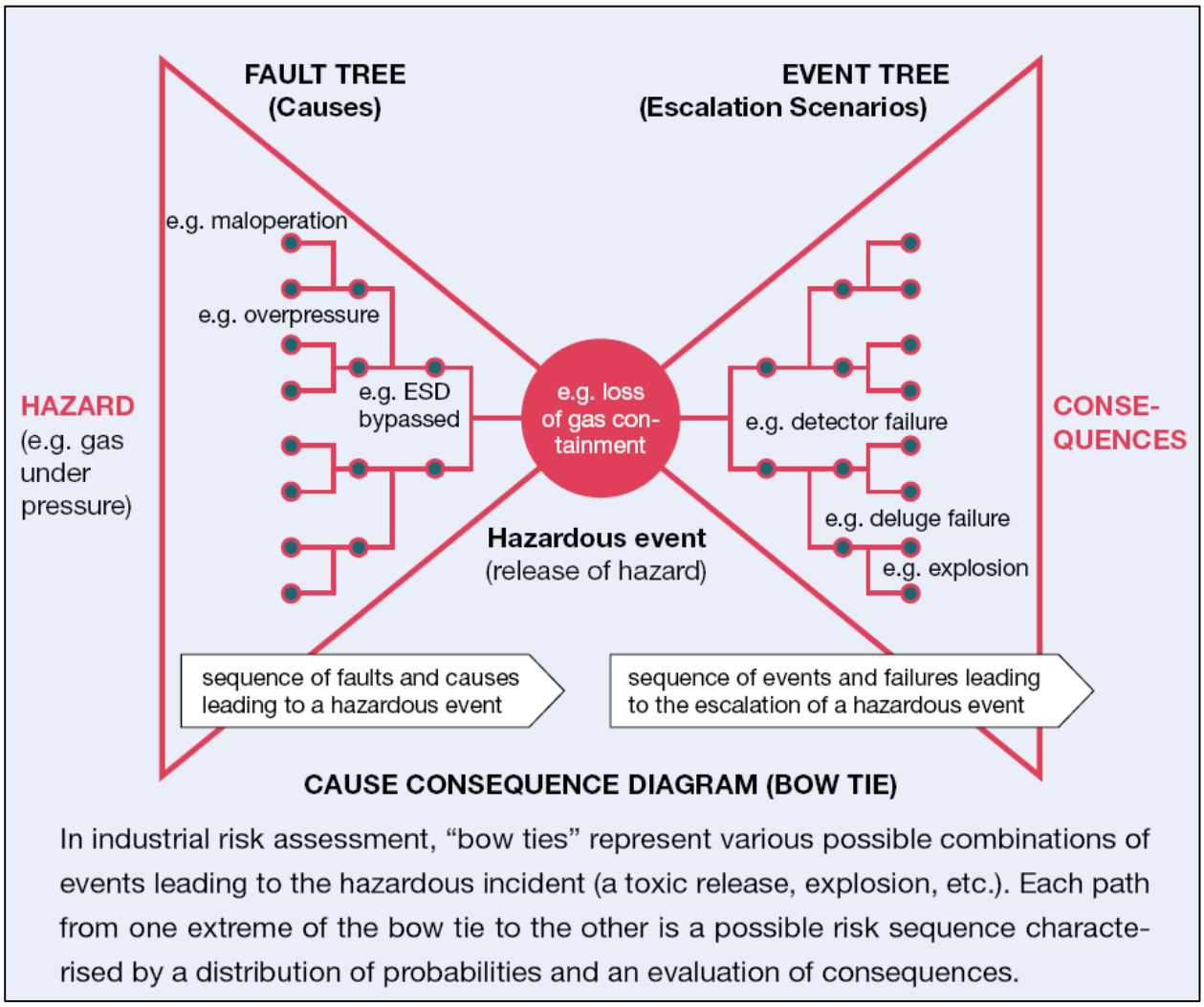


Figure 11. The components of a bow tie diagram. Source IRGC [14].

The combined fault and event trees associated with a given fault condition are known as a **bow tie** diagram. The bow tie diagram, **or its conceptual equivalent**, form the basis of any risk assessment process. Knowledge of the cause and effect relationships associated with any system component drive risk management policies, which in turn drive the preventive and mitigative measures taken by the operators of an industrial system in their efforts to prevent, or contain the consequences of system failures.

The risk assessment approach encapsulated within a bow tie diagram implies a level of predictive capability, but looking into the future involves varying degrees of uncertainty [14]. Walker et al. [15] point out that policy failures often follow from a failure to take uncertainties into account and they have tabulated a progressive transition of uncertainty from determinism to total ignorance as depicted in **Figure 12**.

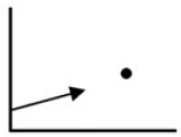
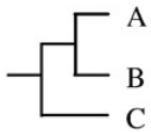
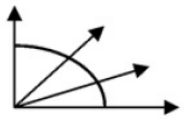
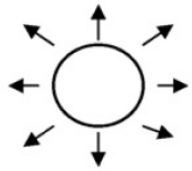
Determinism		Level 1	Level 2	Level 3	Level 4	Total ignorance
				Deep Uncertainty		
	Context	A clear enough future 	Alternate futures (with probabilities) 	A multiplicity of plausible futures 	Unknown future 	
	System model	A single system model	A single system model with a probabilistic parameterization	Several system models, with different structures	Unknown system model; know we don't know	
	System outcomes	A point estimate and confidence interval for each outcome	Several sets of point estimates and confidence intervals for the outcomes, with a probability attached to each set	A known range of outcomes	Unknown outcomes; know we don't know	
	Weights on outcomes	A single estimate of the weights	Several sets of weights, with a probability attached to each set	A known range of weights	Unknown weights; know we don't know	

Figure 12. Progressive transition of uncertainty from determinism to total ignorance. Source [15].

Paltrinieri [1] extends the discussion of uncertainty to atypical events that were not captured by standard hazard identification (HAZID) techniques, such as generation of bow tie diagrams, because of deviation from normal expectations of unwanted events or worst-case reference scenarios. He carries on to use the exquisite Donald Rumsfeld quote from 2002 [16] that very succinctly captures the transition of uncertainty from determinism to total ignorance:

"Reports that say that something hasn't happened are always interesting to me, because as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns -- the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones."

	Knowledge	Lack of Knowledge
Awareness	Known Known	Known Unknown
Unawareness	Unknown Known	Unknown Unknown

Figure 13. Tabulation of Rumsfeld quote [16], per Paltrinieri [1].

Paltrinrieri also discusses the strong predisposition to hindsight bias in humans, where events that have occurred are considered more predictably than they were before they took place. We also have a tendency to fall into the trap of believing that what is unknown is impossible and then being very surprised when "black swan events" [17] occur. Atypical events are sometimes preceded by early warning signals, or similar past events, but lessons are not properly learned and recorded, or are forgotten as time passes and we become complacent in the absence of reoccurrence of the events. Paltrinieri defines two separate groups of atypical accidents on the basis of available information:

- Events that we are not aware we do not know because they have never occurred or there are no records. These events can be defined as "Unknown Unknowns."
- Events that we are not aware we know because they have already occurred in the past and/or there are records of them. These events can be defined "Unknown Knowns."

He goes on to present a useful graphic of the risk management cycle adapted from [18] that captures the elements of the Rumsfeld quote and is shown in **Figure 14**.

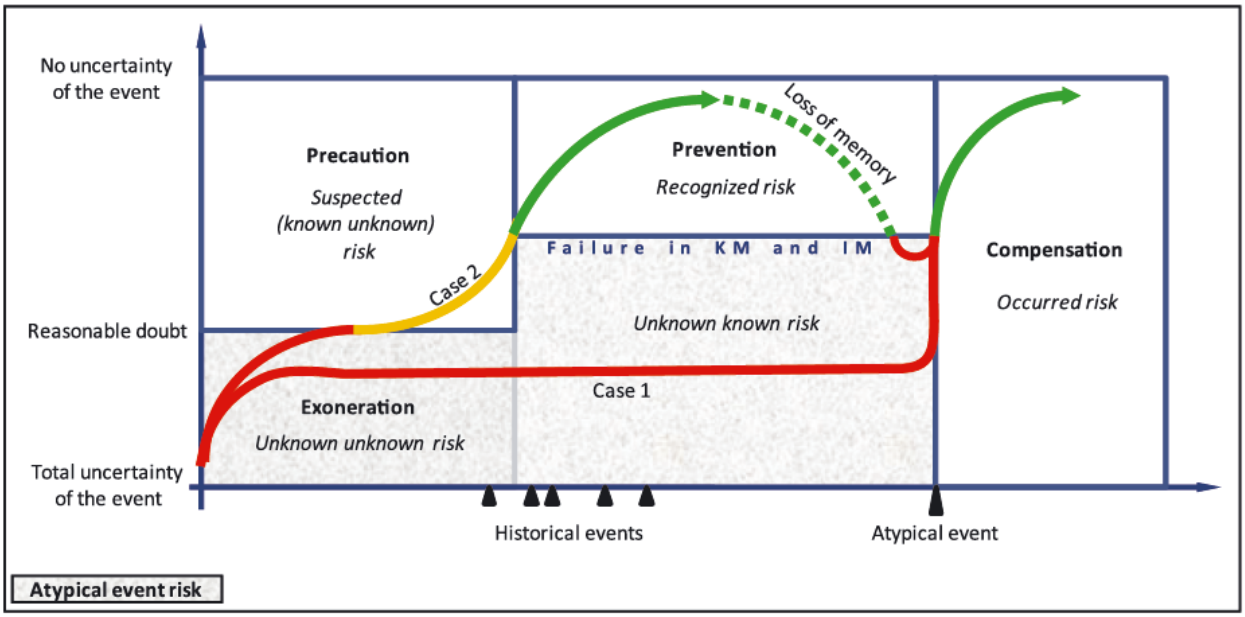


Figure 14. Risk Management Cycle KM=Knowledge Management, IM=Information Management. Source [1] adapted from [18].

All of the concepts discussed above, and the problematic aspects of uncertainty in defining the risks of unwanted events, or predicting their occurrence underpin two very enlightening presentations delivered by members of the NTSB at recent public workshops sponsored by DOT PHMSA[10,11].

On august 5, 2014 Robert J. Hall, Director - Office of Railroad, Pipeline and Hazardous Materials Investigations gave a presentation titled "*What are you looking for? Missed opportunities*" in which he discussed several recent accident investigations and recurring themes in the findings. He noted that in all of the cases there was information relevant to the eventual catastrophic failure available to the operators, but that there had been a failure to connect the dots and develop an awareness and understanding of a pending problem. These events all had failures of knowledge and information management in their underlying root

---

10 Robert J. Hall P.E., Director - Office of Railroad, Pipeline and Hazardous Materials Investigations, NTSB, Managing Pipeline Cracking Challenges Workshop, August 5, 2014

http://primis.phmsa.dot.gov/meetings/FilGet.mtg?fil=630

https://www.youtube.com/watch?v=0HTgewhmLvw&index=1&list=PL4wHDsuQ-uKlGhWt0LZbd3qpPEuJsMLAk

11 Christopher A. Hart, Chairman, NTSB, Pipeline Safety: Risk Modeling Methodologies Public Workshop, September 9, 2015

http://primis.phmsa.dot.gov/meetings/FilGet.mtg?fil=698

https://www.youtube.com/watch?v=C71wdgzT2bc&list=PL4wHDsuQ-uKk9o1mPhxfwghl5A3ERG--F&index=6

causes putting them in the unknown known category of risks. He ended his presentation with the following points:

- Defects often disguised
- Expect the unexpected
- Use all available information
- Know all there is to know
- Inspect comprehensively

The entire discussion was a tactful recognition of the pitfalls of uncertainty and the Rumsfeld quartet of knowledge/awareness groupings.

On September 9, 2015 Christopher A. Hart, Chairman, NTSB gave a presentation titled "*Pipeline Integrity Management: Next Steps*". Chairman Hart discussed how to transition to improved risk management by addressing the knowledge and information management frameworks. He referenced the 2015 NTSB Safety study "*Integrity Management of Gas Transmission Pipelines in High Consequence Areas*", in which it was recognized that since the implementation of the PHMSA Gas Pipeline Integrity Management Requirements in 2004 the significant incident rate has continued to trend upwards. He recognized the strength of system of systems approaches where it is recognized that safety issues are more likely to involve interactions between parts of large, complex interactive systems that are often tightly coupled. He pointed out the advantages of diverse, cross-functional teams in developing fact based approached to risk reduction.

Both of these NTSB presentations addressed lack of proper knowledge, incomplete knowledge management frameworks, and shortfalls in dissemination of lessons learned from the history of operations. This status quo exists in spite of well formulated risk assessment methodologies implemented by pipeline operators.

The NTSB presentations did not explicitly call out management or human failures, but these two categories of causal factors are noted in the executive summary of their accident investigation report [19]:

"Several deficiencies revealed by the National Transportation Safety Board investigation, such as PG&E's poor quality control during the pipe installation and inadequate emergency response, were factors in the 2008 explosion of a PG&E gas pipeline in Rancho Cordova, California. (See Explosion, Release, and Ignition of Natural Gas, Rancho Cordova, California, December 24, 2008, Pipeline Accident Brief NTSB/PAB-10/01 [Washington, DC: National Transportation Safety Board, 2010].) This 2008 accident involved the inappropriate installation of a pipe that was not intended for operational use and did not meet applicable pipe specifications. PG&E's response to that event was inadequate; PG&E initially dispatched an unqualified person to the emergency, causing an unnecessary delay in dispatching a properly trained and equipped technician. Some of these deficiencies were also factors in the 1981 PG&E gas pipeline leak in San Francisco, which involved inaccurate record-keeping, the dispatch of first responders who were not trained or equipped to close valves, and unacceptable delays in shutting down the pipeline. (See Pacific Gas & Electric Company Natural Gas Pipeline Puncture, San Francisco, California, August 25, 1981, Pipeline Accident Report NTSB/PAR-82/01 [Washington, DC: National Transportation Safety Board, 1982].) The National Transportation Safety Board concluded that PG&E's multiple, recurring deficiencies are evidence of a systemic problem.

The investigation also determined that the California Public Utilities Commission, the pipeline safety regulator within the state of California, failed to detect the inadequacies in PG&E's integrity management program and that the Pipeline and Hazardous Materials Safety Administration integrity management inspection protocols need improvement. Because the Pipeline and Hazardous Materials Safety Administration has not incorporated the use of effective and meaningful metrics as part of its guidance for performance-based management pipeline safety programs, its oversight of state public utility commissions regulating gas transmission and hazardous liquid pipelines could be improved. Without effective and meaningful metrics in performance-based pipeline safety management programs, neither PG&E nor the California Public Utilities Commission was able to effectively evaluate or assess PG&E's pipeline system."

The record keeping and knowledge management deficiencies were further corroborated in the testimony of Duller and North [20] to the CPUC after their independent review of the records management practices of PG&E where they found wide ranging and systemic problems over many decades of operation.

> "The article focuses on five distinct and unrelated regulatory disasters: the construction of 'leaky buildings' in New Zealand in the late 1990s-2000s, the explosion at the Buncefield chemical plant in the UK in 2005, the events leading up to the bail out of the Royal Bank of Scotland in the UK in 2008, the Macondo oil well blow out at the Deepwater Horizon oil rig in the Gulf of Mexico in 2010, and Pike River mining tragedy in New Zealand, also in 2010.6 These are chosen because they are uncontroversial examples of regulatory disasters – significantly adverse impacts on human health, financial position or the environment which arose from the design and operation of a regulatory regime intended to manage the very risks which materialised. They also have the advantage that each was subject to extensive investigation by an independent body established specifically to inquire into the causes of the disaster, thus providing a wealth of factual information. Whilst there are always inherent biases in any investigation, those which followed each of these disasters have not been significantly criticised as biased or 'captured' by any particular interest."

The quick review of the San Bruno catastrophe presented above illustrates that many of these events are failures of systems of systems that interact to generate an unexpected event that would not have been deemed probable by subject matter experts prior to the occurrence. The systemic failures include the regulators, which leads to the definition used by Black [21] where she examines several recent industrial (meaning generated by human endeavor with underlying technical failures in this context) catastrophes that she classifies as regulatory disasters:

Black focuses on the regulators as the major problem. This is a biased viewpoint, but several interesting connections worthy of discussion are made by Black when she lists contributory factors that are common to many industrial disasters:

- The incentives on individuals or groups,
- The organizational dynamics of regulators, regulated operators and the complexity of the regulatory system,
- Weaknesses, ambiguities and contradictions in the regulatory strategies adopted,
- Misunderstandings of the problem and the potential solutions,
- Problems with communication about the conduct expected or conflicting messages, and
- Trust and accountability structures.

Sornette and Chernov [22] provide a more thorough analysis, than Black, of 25 detailed case studies and a further 20 superficial reviews of manmade disasters from across the globe. They identify the concealment of information as a major underlying issue in all of the disasters studied. The root causes of the information concealment are varied, but several are very common and can be readily identified.

A summary of the catastrophes reviewed and a statistical breakdown of the human causal factors they attributed to each of the catastrophes is presented in **Appendix 3: Analysis of Human Causal Elements in Catastrophic Events.** The contributory factors listed by Black are a subset of the factors listed by Sornette and Chernov, a Pareto ranking of these factors is presented in **Figure 15.**

Figure 16 shows how Sornette and Chernov group the underlying factors contributing to risk concealment prior to major catastrophes.

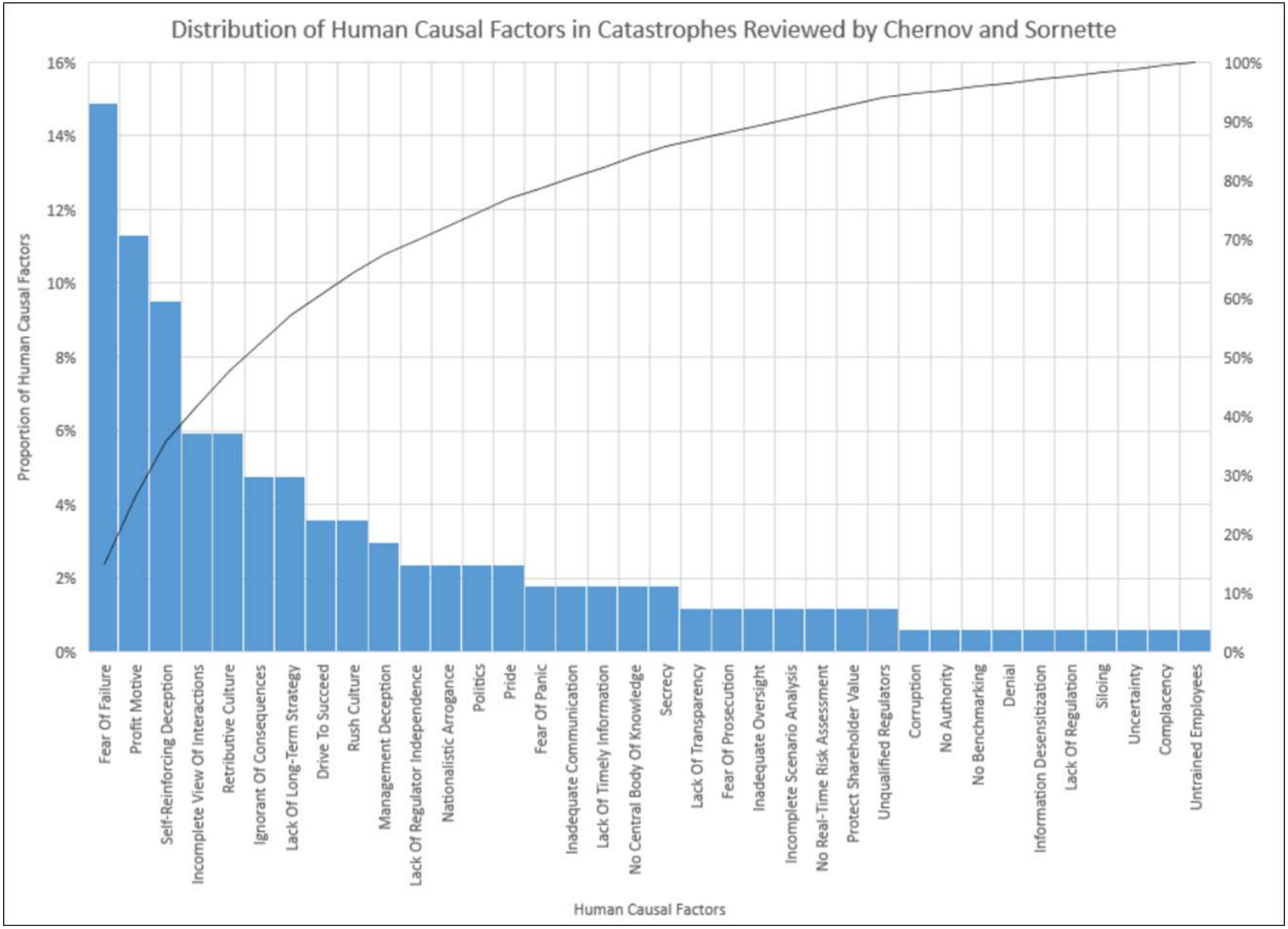


Figure 15. Analysis of Human Causal Factors in Catastrophes Reviewed by Chernov and Sornette

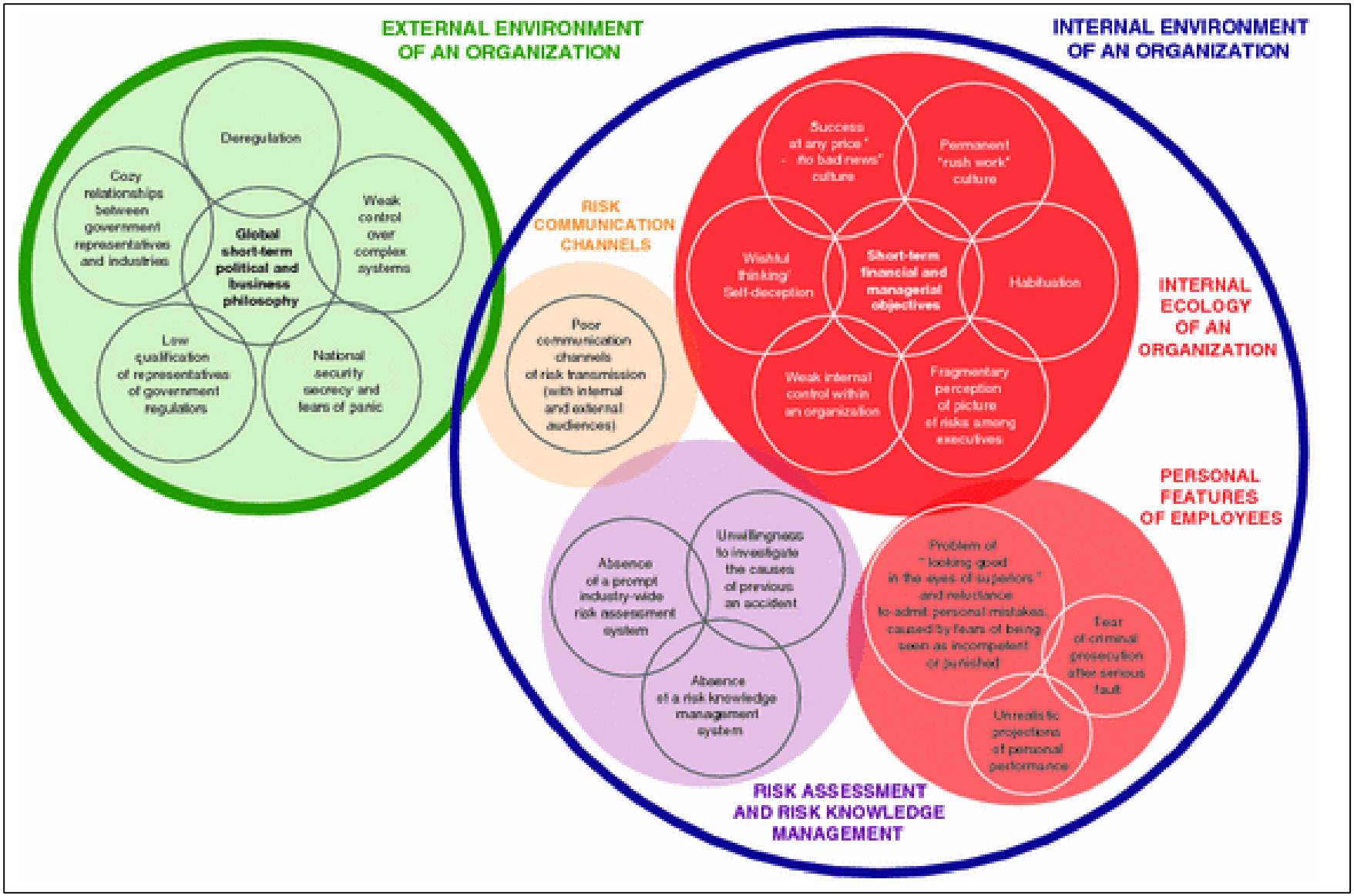


Figure 16. Grouping of factors underlying the concealment of information per Sornette and Chernov. Source [22]

The groupings are tabulated in **Table 1** below.

Table 1. Grouping of factors underlying the concealment of information prior to major catastrophes per Sornette and Chernov. Source [22]

Internal Environment of an Organization	External Environment of an Organization
1. Internal Ecology of an Organization	1. Global short-term political and business philosophy
a. Short term financial and managerial objectives	2. Deregulation
b. Permanent "rush work culture"	3. Cozy relationship between government representatives and industries
c. Success at any price "no bad news" culture	4. Low qualification of representatives of government regulators
d. Wishful thinking self-deception	5. National security secrecy and fear of panic
e. Weak internal control within an organization	6. Weak control over complex systems
f. Fragmentary perception of picture of risks among executives	
g. Habituation	
2. Personal Features of Employees	
a. Problem of "looking good in the eyes of superiors" and reluctance to admit personal mistakes, caused by fears of being seen as incompetent, or punished	
b. Fear of criminal prosecution after serious fault	
c. Unrealistic projections of personal performance	
3. Risk Assessment and Risk Knowledge Management	
a. Unwillingness to investigate the causes of previous accidents	

Internal Environment of an Organization	External Environment of an Organization
b. Absence of prompt industry-wide risk assessment system	
c. Absence of a risk knowledge management system	
4. Risk Communication Channels	
a. Poor communication channels of risk transmission (with internal and external audiences)	

Looking at the viewpoints of Black, Chernov and Sornette, in conjunction with the NTSB and CPUC reports it becomes very clear that human causal factors can dominate the lead up to a catastrophic event. It is evident that in the industrial world we are confronted with increasingly complex and interacting systems of systems that are difficult to comprehend. The relationship between system complexity and accidents was recognized in as far back as the early 1980's as can be seen in the work of Perrow, a sociologist, who applied a social science perspective to industrial accidents [23-25]. "Normal" accidents, or system accidents, as defined by Perrow, are viewed as inevitable in extremely complex systems. Perrow identifies three conditions that make a system likely to be susceptible to Normal Accidents. These are:

- The system is complex
- The system is tightly coupled
- The system has catastrophic potential

Three Mile Island nuclear accident (1979) was an example of a normal accident because it was "unexpected, incomprehensible, uncontrollable and unavoidable". Perrow concluded that the failure at Three Mile Island was a consequence of the system's immense complexity. Such modern high-risk systems, he realized, were prone to failures however well they were managed. It was inevitable that they would eventually suffer a normal accident involving multiple failures that interact with each other, despite efforts to avoid them. Perrow noted that operator error is a very common problem, many failures relate to organizations rather than technology, and big accidents almost always have very small beginnings [24]. Such events appear trivial to begin with, before unpredictably cascading through the system to create a large event with severe consequences [26]. This body of work made the case for examining technological failures as the product of highly interacting systems, and highlighted organizational and management factors as the main causes of failures.

Technological disasters could no longer be ascribed to isolated equipment malfunction, operator error or acts of God. [27]. The work of Black, Chernov and Sornette looking at dozens of catastrophic industrial failures corroborate Perrow's view and emphasize that the underlying problems are still endemic in the twenty first century more than three decades after Perrow's early work was published.

The human tendency to look backwards at recent history, and extrapolate lessons learned into the future behavior of our managed systems, misses the potential for unexpected interactions between coupled engineering and management systems simply because they have never shown any evidence of interacting in problematic ways in the past. We also have difficulty in properly defining uncertainty and understanding how this uncertainty propagates through a complex interacting system of systems. The categorization of causal factors provided by Chernov and Sornette, and the comments of Black, show that we need to extend our definition of systems beyond engineering systems to managerial systems, social systems and political systems to capture the full scope of human interaction with physical infrastructure systems and how this interaction can contribute to the evolution of catastrophes.

E. Common Approaches to Risk Management in Industry

The review of catastrophic events in previous section makes it abundantly clear that there is a very wide scope of, technical, managerial, societal and political, problems to address if we want to find ways to reduce the likelihood of catastrophic events occurring. One of the best thought out approaches to begin this massive undertaking appears to be defense-in-depth that incorporates barrier approaches to risk prevention and mitigation.

Barrier Approaches to Risk Prevention and Mitigation

An overview of the development of defense in depth thinking and methods is provided in **Appendix 2: A Brief Review of Defense in Depth Concepts**. A review of the development of the concepts in the US after the Three Mile Island accident is presented, but here we will focus on the outcome of the Seveso directives in Europe as they have led to a detailed application of defense in depth methods, focused on barrier approaches, in the industrial context over several decades. On July10, 1976 there was a major accident at a chemical plant in the town of Seveso, a suburb of Milan in Northern Italy. A significant quantity of dioxin gas was released into the atmosphere and while there was no loss of life, the land and vegetation were contaminated, 2000 people received treatment and millions of animals were destroyed. This accident exhibited many of the problems we have listed above, up to and including the concealment of information. In 1982 European regulations were changed by the passing of the Seveso directive that incorporated as a key principle the preventive transmission of information concerning existing risks of a hazardous object to all associated internal and external audiences [22]. The directives have been regularly updated and are currently at the Seveso III version of the directive. In 2002 the Accidental Risk Assessment Methodology for Industries (ARAMIS) project was initiated with the objective of answering the specific requirements of the Seveso II directive.

One of the outputs of the ARAMIS project is a user guide [28] that gives a detailed explanation of the major components of the methodologies developed by the project:

- Identification of major accident hazards (MIMAH)
- Identification of the safety barriers and assessment of their performances
- Evaluation of safety management efficiency to barrier reliability
- Identification of Reference Accident Scenarios (MIRAS)
- Assessment and mapping of the risk severity of reference scenarios
- Evaluation and mapping of the vulnerability of the plant's surroundings

Salvi and Debray, two of the ARAMIS project members, and contributors to the User Guide cited above, published a global view of the process [29] that provides a concise overview for easy reference. The fundamental approach is based on an extended definition of risk:

1. frequency × intensity = severity,
2. intensity × vulnerability = damages,
3. risk = frequency × intensity × vulnerability

Severity and Vulnerability are assessed separately to allow decision makers to better assess the resulting risk. **Figure 17** to **Figure 21** and **Table 2** depict the ARAMIS process.

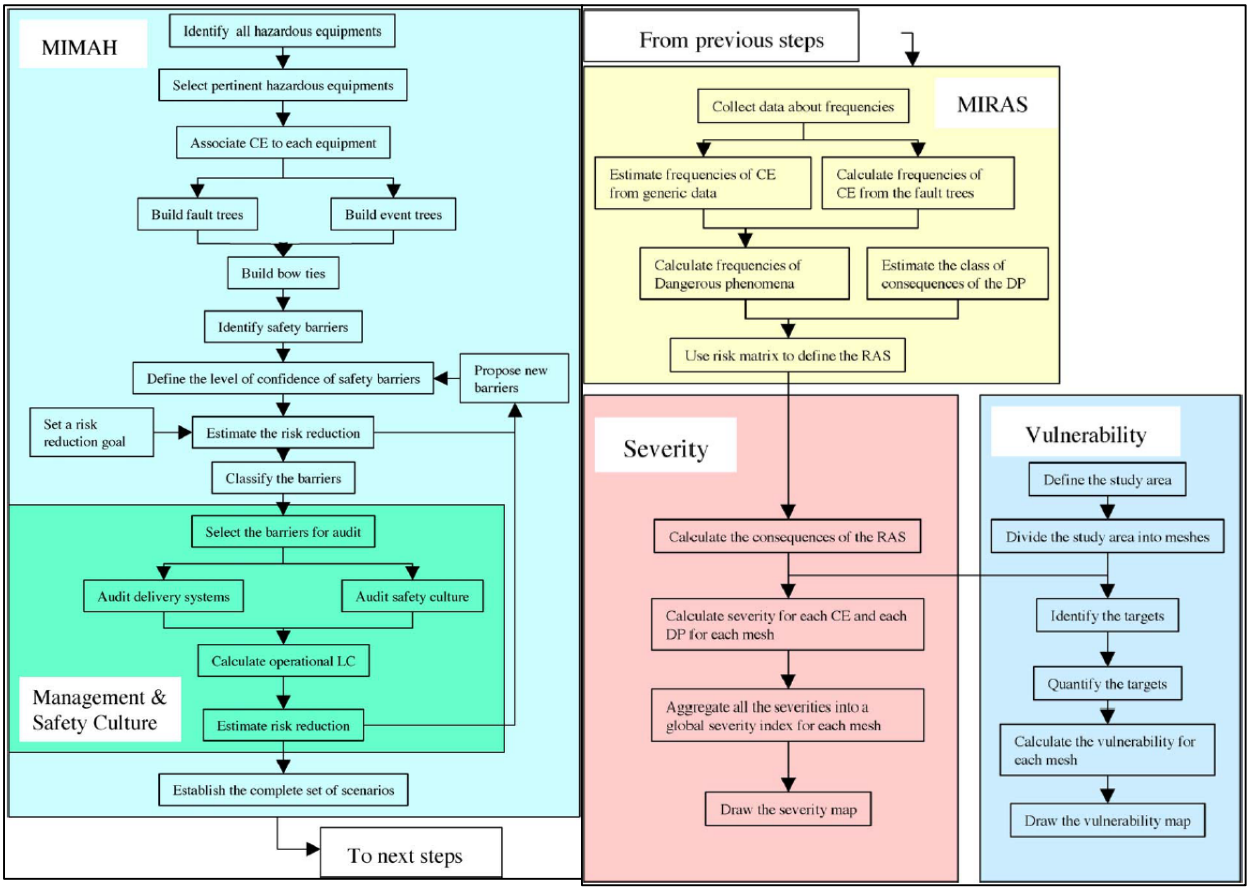


Figure 17. The steps of the ARAMIS process. Source [29]

During the course of the ARAMIS project is was recognized that there is limited true probabilistic data available for source events, that it is not always in the proper format and when there is statistical data available in may be from a very different geographic location, or a different industry with somewhat similar processes. For this reason, an alternative approach based on generic values for safety systems defined according to the initial risk level without barriers. The risk assessed from these initial assumptions helps the user define the safety barriers and strategies for the implementation of a given a safety function.

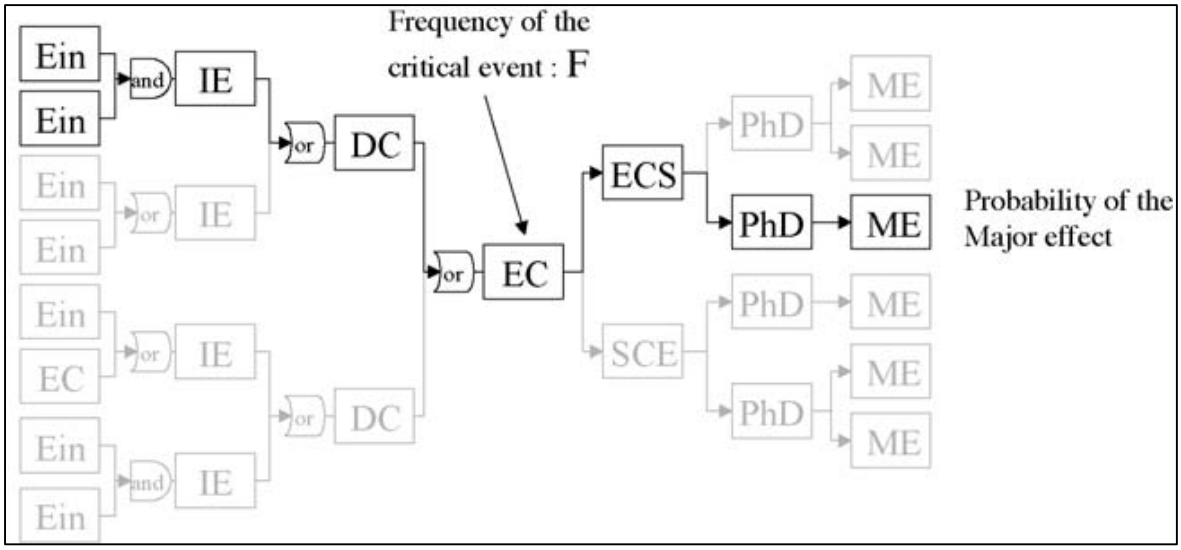


Figure 18. Bow tie and risk path in an ARAMIS type risk assessment. Source [29]

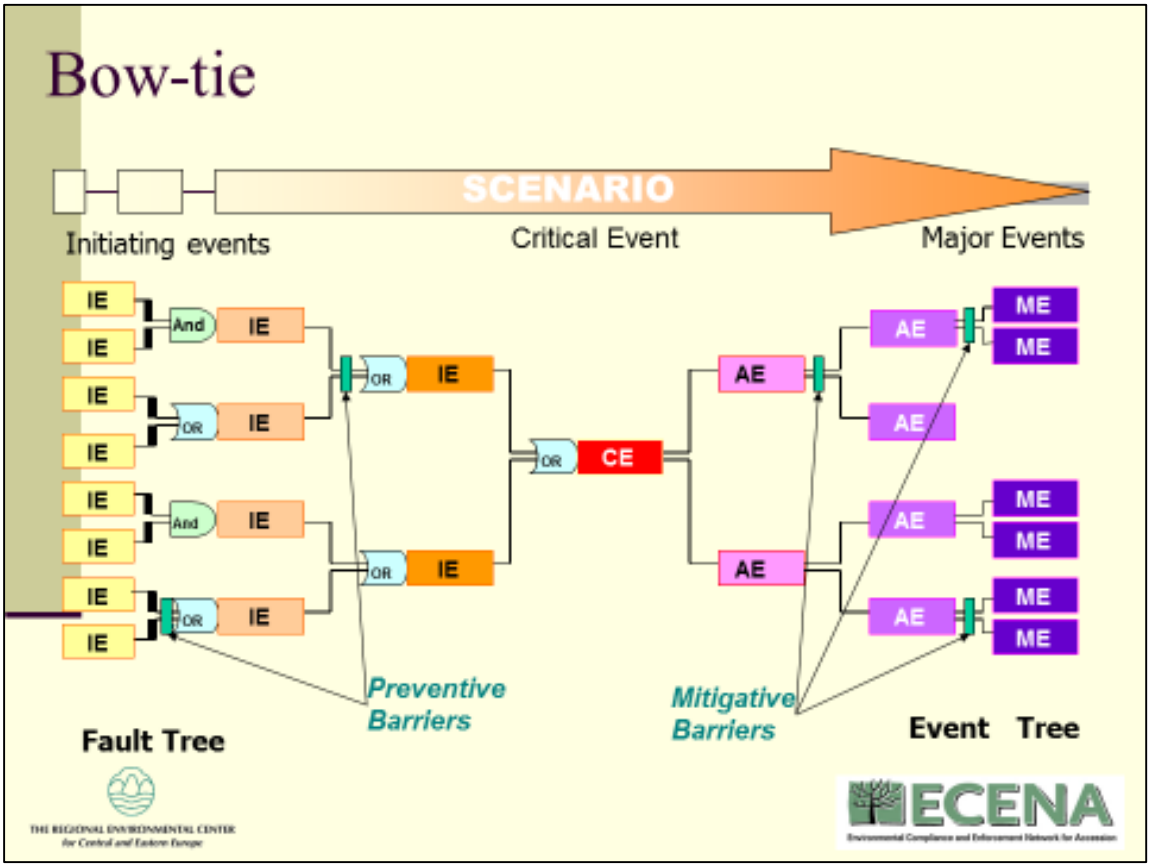


Figure 19. Location of Barriers in an ARAMIS type risk analysis. Source [12]

12 *web.rec.org/documents/**ECENA**/training_programmes/.../06_**overview**_of_ra1.ppt* Accessed 6/11/2016 from google search: overview of risk assessment ecena

Table 2. Definition of the level of confidence in barriers per ARAMIS. Source [29]

Level of confidence in a barrier	Risk reduction factor	Equivalent probability of failure on demand (PFD)	Equivalent probability of failure per hour
4	10000	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	1000	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	100	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$to $< 10^{-6}$
1	10	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

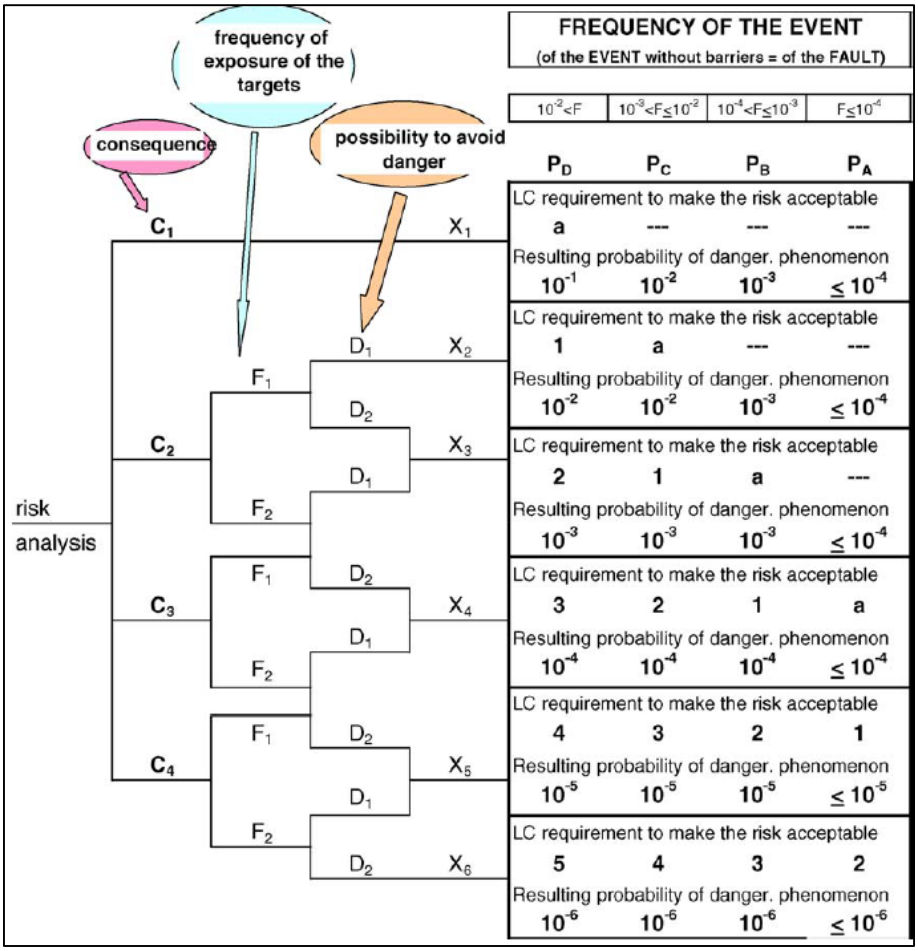


Figure 20. Risk graph per ARAMIS for determining the required level of confidence to make risk acceptable (medium effect in Figure 21). Source [29]

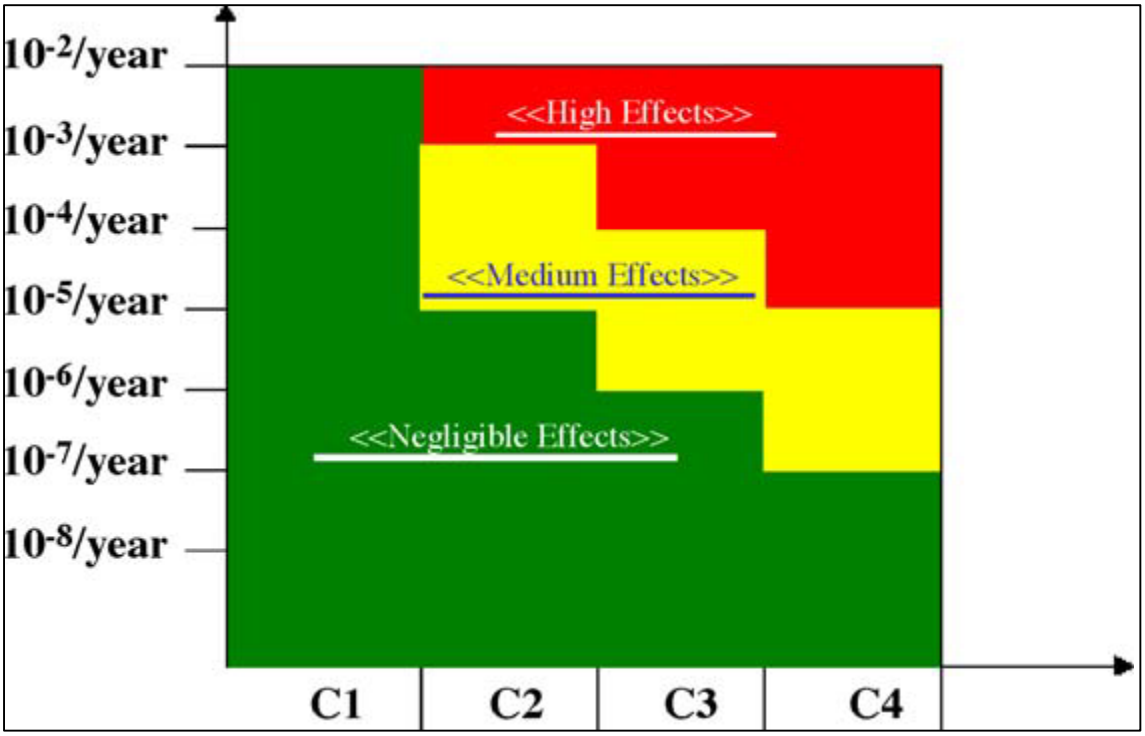


Figure 21.Risk matrix used for ranking the dangerous phenomena and selecting the reference accident scenarios for the risk severity mapping. Source [29]

Shortcomings of the Quantitative Risk Assessment (QRA) process

Apostolakis published a paper entitled "How useful is Quantitative Risk Assessment" [30] in which he argues for formal peer review as an essential part of the QRA process. He also emphasizes the importance of *risk informed* as opposed to *risk based* decision making i.e. factors other than those engineering insights provided by the risk analysis can have an important impact on management decisions. He points out several items that are not handled well by current QRA processes:

- Human errors
- Software failures
- Safety culture
- Design and manufacturing errors

He also points out common criticisms of the QRA approach such as uncertainty making the results useless, difficulties in calculating probabilities.

Layers of Protection (LOPA)

Gowland [31] discusses the LOPA approach as a simplified form of quantitative risk assessment that can potentially be used to carry out the assessment of barriers required in ARAMIS. **Figure 22** and **Figure 23** illustrate the LOPA concept.

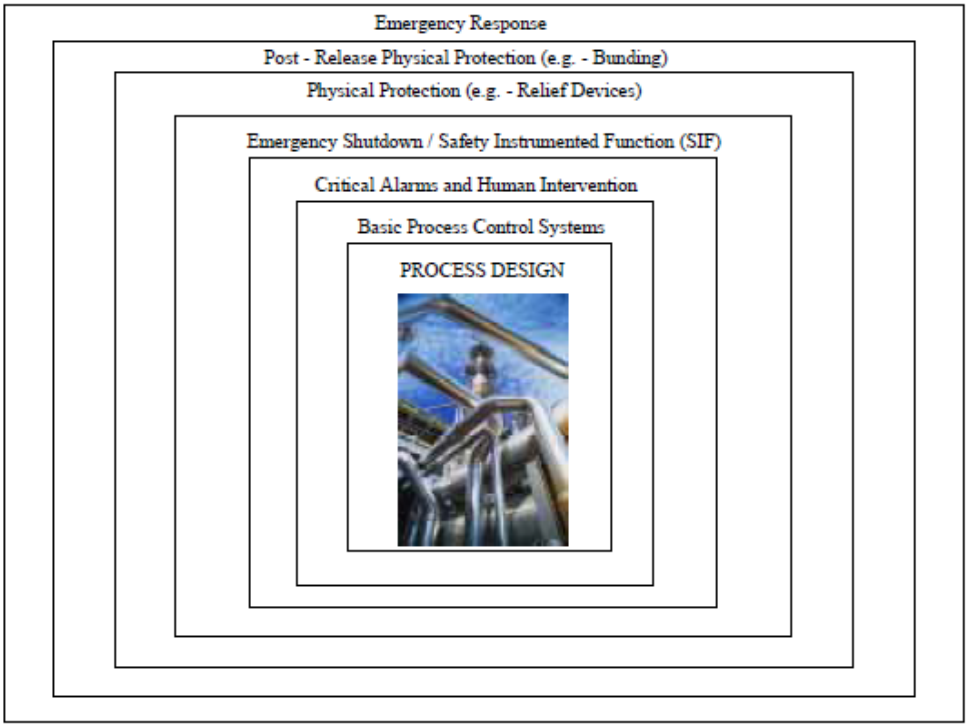


Figure 22. Layers of Protection. Source [32]

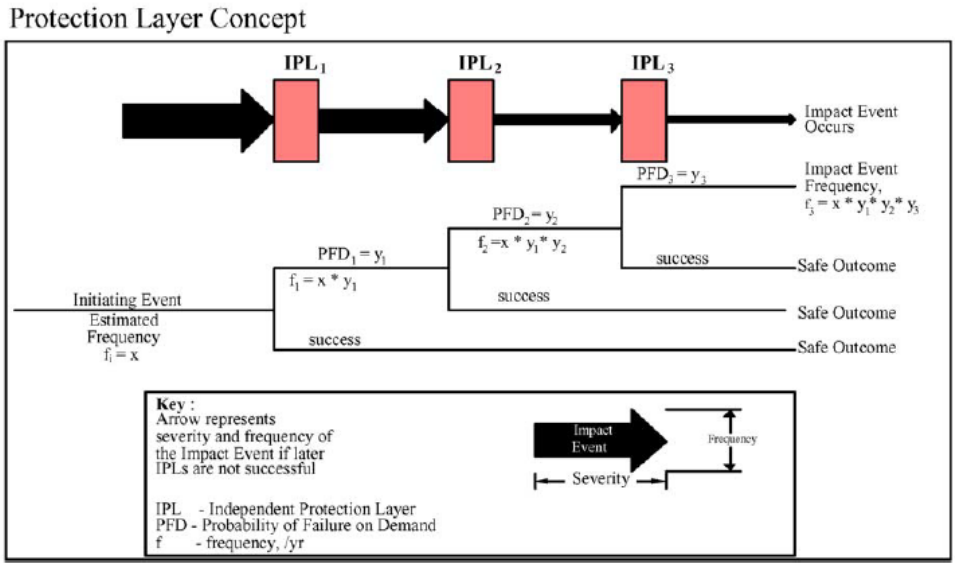


Figure 23. The LOPA concept. Source [31]

Typically, LOPA is used to evaluate scenarios that have been identified in a prior hazard identification exercise. A scenario comprises a single initiating event/consequence pair. The protective layers are a device, system, or action capable of preventing a scenario from proceeding to its undesired consequence independent of the initiating event.

Gowland [31] points out some potential advantages of the LOPA process as a simplified QRA in that it addresses a wider range of issues in addition to process control:

- Human error,
- Procedural failures,
- Operator response,
- Management systems.

He points out that the ARAMIS method is wider than LOPA and offers the user the opportunity to close the loop by assessing uncertainty, sensitivity and carrying out risk mapping. He concludes by pointing out that the two approaches are compatible and that LOPA can be readily incorporated into an ARAMIS approach.

A recent critique on Major Hazard Event (MHE) management

In May 2016, Peter Bridle, Executive Director at Pegasus Risk Management posted an interesting critique of current risk and safety management practices in the exploration and production industry on OILPRO.com[13] [33]. It is instructive to read this critique in conjunction with a report on the September 21, 2001 explosion of a fertilizer plant in Toulouse, France[14], and Herbert's review of the December 2005 explosion at the Buncefield storage site in the UK [34]. These two events all occurred at facilities addressed by the Seveso directives and many years into the implementation of the methodologies.

Toulouse Ammonium Nitrate Fertilizer Explosion, Sep. 21, 2001[1, 35]

The AZF chemical factory in Toulouse, France, exploded on 21 September 2001[36]. The blast was equivalent to 20-40 tons of TNT, measuring 3.4 on the Richter scale, and was heard 80 km away (50 miles). Steel girders were found 3 km away from the explosion. The incident resulted in 29 deaths and left 2,500 wounded. Damages paid by insurance exceed 1.5 billion euros.

An *explosion* scenario was not considered in safety studies, setup of perimeter, or emergency response plans. It was thought that the unconfined storage conditions would not lead to an explosion. Rather, consideration was given to a fire and toxic releases of gases. In addition, the Seveso II directive did not address the risk of "off-specification" ammonium nitrate. This type of material can be similar to technical grade ammonium nitrate used for explosives and is hence now recognized as an explosive hazard.

---

13 http://oilpro.com/post/24614/getting-serious-major-hazard-event-mhe-management accessed 05/27/2016

14 http://www.hse.gov.uk/landuseplanning/toulouse.pdf accessed 06/11/2016

The fertilizer storage facility did not have fire detection systems or nitrogen oxide detectors. The explosion resulted in multiple tanks containing ammonium nitrate leading to pollution of the same, as well as nitric acid leaks.

Seveso I, II, III Directives[37]

The Seveso Directives are the main EU legislation dealing specifically with the control of on-shore major accident hazards involving dangerous substances.

The Seveso I Directive of 24th June 1982 required operators to carry out hazard studies for installations that presented the risk of major accidents. It also required them to organize inspections, and to inform the public what to do in the event of accidents.

The Seveso II Directive of 9th December 1996 also requires those responsible to set up a safety management system and to carry out a periodic re-examination of the hazard studies every 5 years. It also requires them to set up emergency plans and to control urban development.

The Seveso III Directive came into force on 1 June 2015, replacing the Seveso II Directive. To implement this Directive, the COMAH Regulations 1999 (as amended) have been revoked and replaced by the COMAH Regulations 2015.

There is a long history of the implementation and updating of the SEVESO directives and the associated directives put in place. Readers are directed to the references if they want more detail.

1. Some post explosion recommendations/proposals

General knowledge of the risks – expert reports.

Need to improve knowledge of risks. This includes increased knowledge in the areas of technical risk prevention, town planning control, and crisis management measures. A specific emphasis was placed on improving feedback, of the Bureau d'analyse des risques et pollutions industrielles (BARPI)/Industrial Pollution and Risk Analysis Bureau, to record serious incidents or small accidents which may be the forerunners of more serious ones, i.e. they could be leading indicators or precursors to a larger accident. The example of such an industrial/government feedback system that is strong was given – the French nuclear industry and government oversight.

Knowledge of risks – hazard studies.

Improvements are needed to improve the quality of hazard studies and their homogeneity between different industries. Rules on what kinds of accident scenario to take into account, on external threats, on methods of hazard analyses and on the criteria for defining the effects on people should be put in place. The studies should not be slanted to avoid conflicts over the consequences of very serious accident scenarios that require public disclosure or control of urban development., that would be difficult to accept in terms of informing the public or controlling urban development, understandable as such a concern may be. These studies should specify the basic assumptions concerning:

- Rupture of various systems and piping.
- External threats like earthquakes, floods (100 and 1,000 year), sabotage, airline crashes, dam failures, and domino effects from neighboring facilities.
- The failure of safety systems, i.e., even when installed, must consider that they will not work.
- Comparisons to international accident assumptions and methods to learn from other countries.
- Full understanding of the numbers of people and establishments that could be affected by the accident scenario.

2. **Measures to reduce the risks: confinement, breaking up into smaller amounts, operating without stock.**

Recommendations included use of double confinement whenever possible. This includes isolating systems, e.g., defense in depth and multiple barriers. Another approach is to produce only what is needed immediately and carry no stock/storage. For explosive materials, stocks should be broken down into smaller amounts and isolated from each other.

3. **New urban and industrial projects.**

Federal, state, and local authorities and manufacturers should engage in a multifaceted process beyond just defining protective areas - a process in which the socio-economic stakes (both in industrial and land terms) are considerable. This should include:

a) Size of the danger area populations affected
b) Possibility of reducing stores and confining them
c) Where there is a fatal risk and substantial population, then ask if it can be made safer, as well as if it is a good idea to carry on in any event.

4. **Informing the public.**

   Industry must give information to public beyond what is required by regulation, which then tends to be fragmentary in nature. This is important for both new construction and extensions of facilities. There should be national guides on what information should be given under what scenarios. Information should include, in a clear and concise manner, the level of risks. This might include at least a map showing the risk zones: 1% lethal risk (LC 1) and risk of irreversible effects, together with the number of people affected for each zone. The composition of the information exchange between the various parties should include: manufacturers, authorities, elected representatives, associations and scientists in the field of major risks, under calm conditions.

Buncefield Vapor Cloud Explosion on Dec. 11, 2005 [1, 38, 39]

The Buncefield fire [40] was a major conflagration caused by a series of explosions on 11 December 2005 at the Hertfordshire Oil Storage Terminal, an oil storage facility located near the M1 motorway by Hemel Hempstead in Hertfordshire, England. The terminal was the fifth largest oil-products storage depot in the United Kingdom, with a capacity of about 60,000,000 gallons of fuel. Explosions eventually overwhelmed 20 large storage tanks. The initial explosion appears to have been an unconfined vapor cloud explosion of unusually high strength—also known as a fuel-air explosion. The explosions were heard up to 125 miles (200 km) away; there were reports that they were audible in Belgium, France, and the Netherlands and measured 2.4 on the Richter scale. There were 43 reported injuries.

The compulsory Seveso II safety reports completed for the Buncefield site did not predict the scenario of a vapor cloud from overfilling of a fuel tank and resulting explosion and the domino effect. It was felt that this scenario was not probable or reasonably realistic so it was not taken into account. However, vapor cloud explosions of gasoline due to loss of containment have occurred about every five years since the mid 1960's.

Failures of design and maintenance in the overfill protection systems and liquid containment systems were the technical causes of the initial explosion and the seepage of pollutants to the environment. Underlying these immediate failings lay root causes based in broader *management* failings:

- **Management systems** relating to tank filling were both deficient and not properly followed, even though the systems were independently audited.
- **Pressures on staff** had been increasing before the incident. The site was fed by three pipelines, two of which control room staff had little control over in terms of flow rates and timing of receipt. Staff did not have information easily available to them to manage the storage of incoming fuel.

- **Throughput had increased at the site.** This put more pressure on site management and staff and degraded their ability to monitor the receipt and storage of fuel. The pressure on staff was made worse by a lack of engineering support from Head Office.
- **A culture** where keeping the process operating was the primary focus and process safety did not get the attention, resources or priority required.

Buncefield explosion reinforces the importance of process safety management principles:

1. **An understanding of major accident risks** and the safety critical equipment and systems designed to control them. This understanding should be from the senior management down to the shop floor, and between all organizations involved in supplying, installing, maintaining and operating these controls.
2. **Systems and a culture in place to detect signals of failure** in safety critical equipment and to respond to them quickly and effectively. In Buncefield's case, there were clear signs that the equipment was not fit for purpose but no one questioned why, or what should be done about it other than ensure a series of temporary fixes.
3. **Time and resources for process safety** should be made available. The pressures on staff and managers should be understood and managed so that they have the capacity to apply procedures and systems essential for safe operation.
4. **An effective auditing systems** in place which test the quality of management systems and ensure that these systems are actually being used on the ground and are effective.
5. **Board level engagement.** At the core of managing a major hazard business should be clear and positive *process* safety leadership with board-level involvement and competence to ensure that major hazard risks are being properly managed.
6. **Constant engagement.** In particular, there should be regular reviews of the site risk assessments to ensure that learning from the Buncefield event and other incidents/guidance/standard changes are incorporated and that the Basis of Safety for a site is soundly maintained.
7. **History still repeats itself.** Two almost identical events, to the Buncefield incident, have occurred in 2009. These were the events in Puerto Rico at the Caribbean Petroleum Corporation (CAPECO) site on 23rd October 2009 (US Chemical Safety Board, 2009), and in Indian at the Indian Oil Corporation (IOC) depot in Jaipur on the 29th October 2009 (Indian Oil Industry Safety Directorate). Both sites had significant releases of petrol and blast effects were felt over considerable distances.

The Bridle Critique

The lessons learned from the Buncefield and Toulouse incidents can all be viewed as a subset, or particular manifestation of the issues noted by Bridle relating to barrier type approaches to risk informed management. Bridle first points out the functional silos reporting to the typical C-suite in the oil and gas industry depicted graphically in **Figure 24** and **Figure 25**. He goes on to describe a feature of safety and risk management we heard often in our discussions with risk management professionals in the industry; the policies of the organization are geared towards workplace safety defined in terms of injuries to people and damage to equipment. The responsibility for the implementation of the safety policies falls on the Health and Safety Executive (HSE) who are expected to influence line managers to achieve the specified metrics. Senior management are supportive of these efforts, but the HSE does not have the requisite authority, or empowerment, to make the operations do anything different in order to manage major operational risk.

Following the Piper Alpha disaster in 1988 in was advocated that the oil and gas industry should establish a safety case regime to ensure that major operational risks should be identified, assessed and controlled with appropriate barriers. Today, a quarter of a century later, bow tie methods are commonly accepted as the principal mechanism for conducting MHE management. However, a compliance focused culture and the difficulties encountered in integrating the requirements of the safety cases into day to day work activities, result in major events still occurring in cases where the facilities are nominally compliant with the regulations.

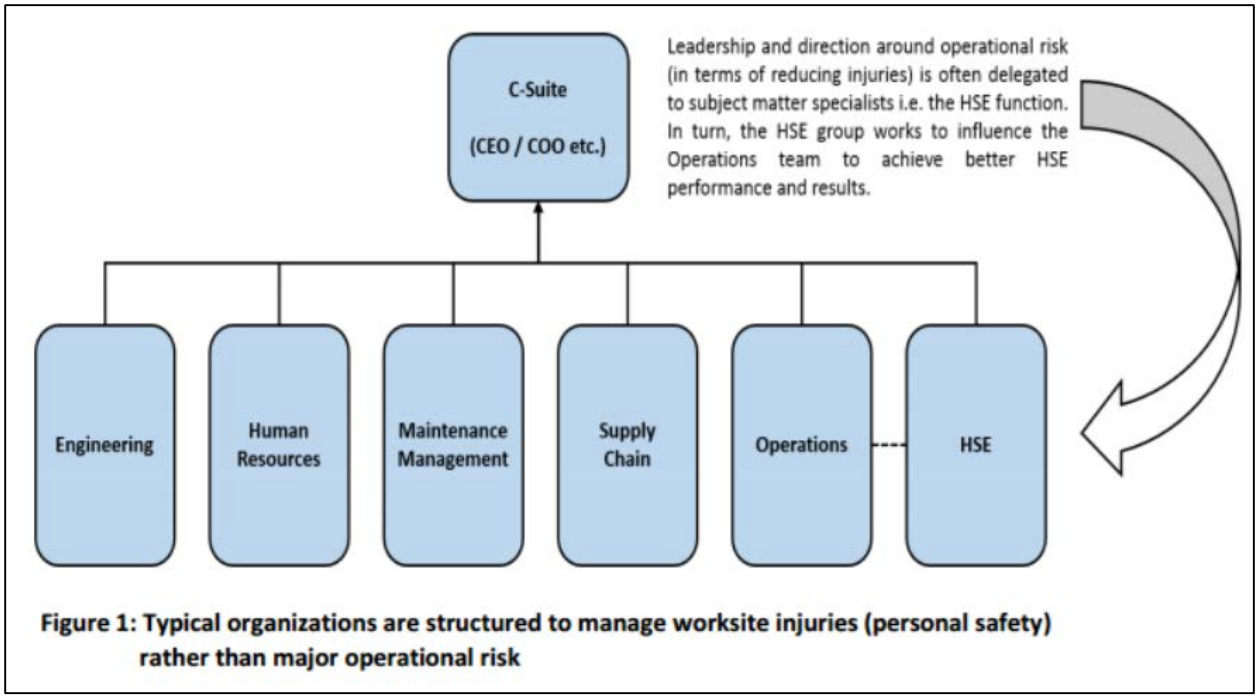


Figure 24. Functional silos in a typical organization. Source [33]

Bridle goes on to point out that it is difficult gain a full understanding of the overall effectiveness of a risk management program. He offers a simple anecdote to illustrate the point:

> "… Let's say an employee was performing a maintenance routine on a fire and gas detection system (i.e. barrier management) and during the course of the work they slipped, tripped, fell and twisted their ankle. Works out the sprain incurred was sufficient that the employee was unable to be fit for duty the following day. As a result, a Lost Time Incident (LTI) or a Days Away From Work Case (DAFWC) was incurred.
>
> Such an event (needless to say) would undoubtedly find its way to the top of the organization right quick!
>
> …
>
> But now comes the critical distinction…
>
> It is unlikely that the status of this barrier would also find its way to the top of the organization in the same way as the LTI or DAFWC!"

Clearly the integrity and availability of a key barrier is essential in the grand scheme of operational risk management, but senior management do not "own" the problem and are rarely held to account for failings in the same way that they are for personal safety. A

precursor to moving towards this accountability is generating the appropriate set of metrics and cultural expectations for which, senior management will be held accountable.

Bridle points out that functional silos work against an effective operational risk management culture. He gives an example of a fire and gas detection barrier.

Barrier: Fire and Gas Detection System (Major Operational Risk Recovery Preparedness Measure)		
#	**"Safety Critical" Activity**	**Typical Accountable Function**
1	Designed to predefined operating requirements	Engineering
2	Be installed and strategically placed in such a way that the equipment will perform as intended;	Engineering / Operations
3	Ensure any person(s) performing work on the equipment are competent to do so;	Human Resources / Training
4	The equipment (including any additional and / or replacement parts) must be sourced from approved vendors supplying genuine like for like replacements parts;	Supply Chain
5	The equipment must be routinely inspected, tested and where necessary calibrated to ensure the equipment will perform as intended;	Maintenance Management
6	Establish and implement QA/QC requirements to demonstrate that any work performed on the equipment is always completed to the correct standard;	HSE / Operations

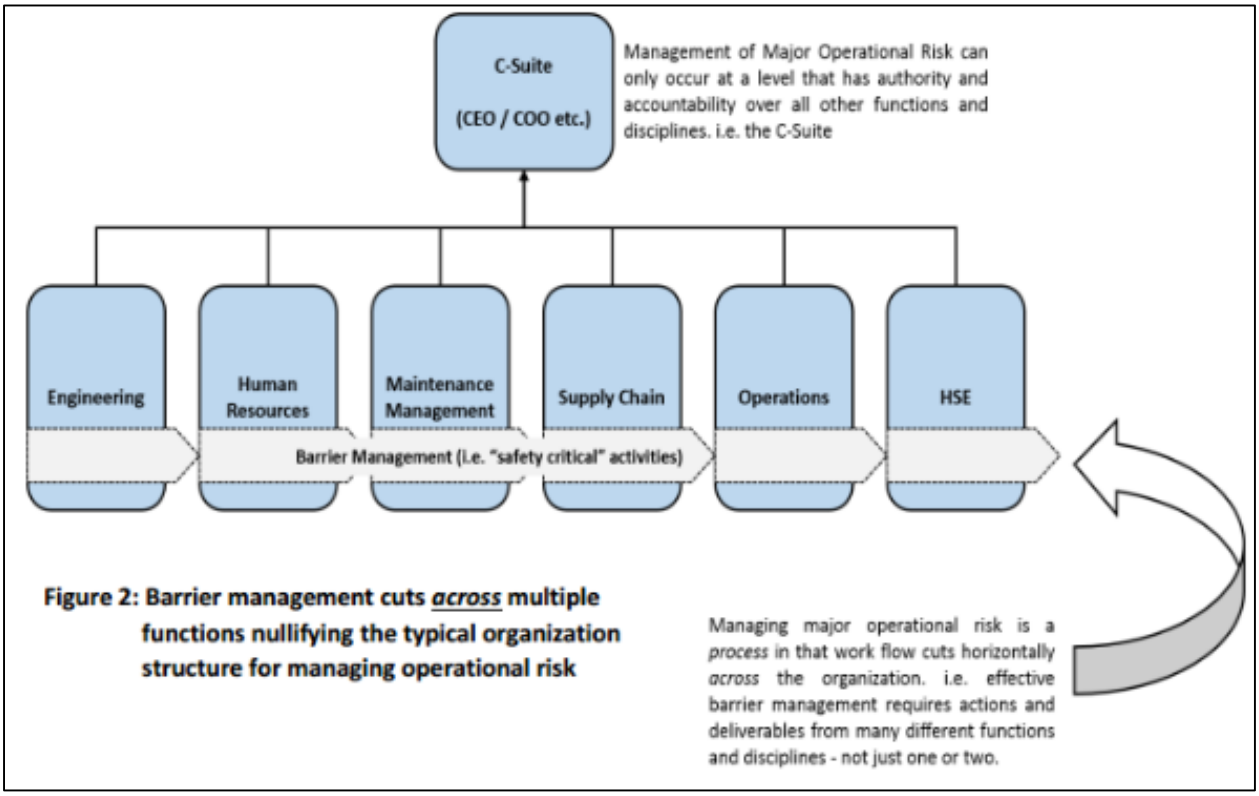


Figure 25. Functional silos and barrier management. Source [33]

"But unfortunately - and precisely at a time when the E&P industry can least afford it - the ongoing status and routine monitoring of key barriers still doesn't get the necessary attention from the highest levels in the organization. In many cases it's only when the last barrier fails and the prospect of a serious consequence begins to loom, do organizations really force themselves to examine the size and number of holes that may exist within their barriers (preventative controls and recovery preparedness measures) for managing major operational risk.

The point being that the cumulative functionality of multiple key barriers is not always known at a sufficiently high level within the organization and when combined with the failure to rigorously monitor their ongoing availability and integrity, means that any early warnings signs that should otherwise flag elevated levels of risk, often simply come too late.

This all of course represents one big vicious circle. Gaining a detailed understanding of how barriers work interdependently (for any given Major Hazard Event scenario), combined with poor overall monitoring, are products of often insufficient and inadequate metrics generating enough key data points for C-suite executives to act on. The consequence of this being the potential for complacently and cultures of "casual compliance" begin to manifest. In other words, if no one is telling a middle manager or line supervisor to do anything different (i.e. because of the absence of relevant data), then why would they even think to change their current behaviors when they've served them so well in the past? And again as the US CSB put it "One individual didn't cause the Macondo event. A multitude of decisions and actions up and down the organizational chains of both bp and Transocean led to this disaster."

But should suitable and sufficient metrics become well established, such that each and every time a barrier didn't perform as expected it was flagged and communicated to the highest necessary level within the organization such that coordinated action would result, then a very different picture of performance could be established. From there, C-suite executives would once again be able to ask the right (read tough) questions, shrug off their complacency and finally begin to turn their organizations toward one that resembles high reliability in terms of managing major operational risk. Until that point, organizations can expect more Major Hazard Events (MHE) in the future, while at the same time continuing to exhort their ongoing exemplary safety performance.

A further complication is pointed out by Bridle; companies and functions within a company often have different definitions of what constitutes "critical" e.g. engineering and operations managers can differ when asked to interpret a given safety case in order to establish critical activities for the organization. Trying to resolve these differences is an overwhelming task for any organization in the current management culture. In spite of this difficulty it is clear

that establish consistent definitions for “safety critical” will help organizations move forward cohesively. Bridle summarizes as follows:

> Organizations would do well to take on the following measures:
>
> •Establish consistent definitions of “safety critical” across all functions / disciplines - anchored in barrier management and tied to the Safety Case;
>
> •Establish a suite of metrics (KPI’s) that enables routine monitoring of barriers designed to manage Major Hazard Events (MHE) - and at a minimum, held at the same level of importance as metrics for determining personal safety performance (LTI’s, DAFWC etc.);
>
> •Align the organization structure such that ultimate authority and accountability for barrier management (Safety Case implementation) is not delegated to any one particular function, but resides at a level that has ultimate authority and accountability over all functions;
>
> •Establish practices at the worksite that enables “safety critical” activities to be clearly flagged and labelled such that all persons - not just those performing the work, but also those supervising/managing the work - recognize the importance of completing the job to the correct standard and in doing so, contribute to the overall management of major operational risk (as opposed to simply executing the job safely to avoid any LTI’s, DAFWC etc.);
>
> •Introduce effective QA/QC practices to ensure sufficient checks and balances exist to demonstrate the ongoing availability and integrity of any barriers remains (following any work performed on such equipment);
>
> •Expand the unplanned event (incidents, Near Misses etc.) reporting process to include missteps or breakdowns related to the QA/QC assurance protocols for all “safety critical” activities. And if such a process is risk based, it should easily be able to distinguish between low risk personal injuries (including those carrying high consequence classifications such as LTI’s) and high risk barrier failures that may or may not have resulted in any specific consequences. Such weightings should subsequently result in the correct level of scrutiny and at the right level of the organization.”

Summary of Stakeholder interviews

A cross section of this white paper's potential end users and stakeholders were interviewed. The questions posed, and a summary of the answers is provided in Appendix 1.

The interviews included: private and public natural gas distribution companies, transmission pipeline operators, combination gas/electric companies, state commissioners, nuclear consultants, and risk consultants. The issues raised by the interviewees was very consistent with all of the critiques summarized above.

Interview Highlights

1. **Defining Catastrophic Events.** Catastrophic events are defined in different ways depending on the industry, culture, and size of the operator. There are regulatory definitions, insurance definitions, and operator tolerance biases.
2. **Safety Culture.** The gas industry safety culture has been improving over the last 2-3 years. However, there are two areas that need major improvement: (a) industry is better at personal safety than process safety – it must focus more on process safety, and (b) there is a large disconnect from the "corner office to the ditch" and between department; both areas are not making connections related to enterprise risk and safety.
3. **Probability vs. Consequence.** It is sometimes very hard to predict an event probability; when this is the case some operators default to consequence as a deciding factor on risk decisions. However, engineers focus on probability and struggle with proper consequence considerations. This leads to a catch-22.
4. **Hiding Behind the Code.** Senior management tends to "hide behind the code", i.e., "if we are code compliant (even minimally) then we are OK" vs. Integrity Management personnel look at sub-quantitative risk estimates and integrity, and focus on managing risks themselves.
5. **Threat Interactions.** Interactive defects, threats, and circumstances are progressively difficult to plan for.
6. **Lack of Lessons Leaned, Transparency, and Internal Audits.** Not following up with lessons learned – history repeats itself. The industry needs to get better at sharing root cause information within a company and across companies. There is a lack of transparency and fear of doing internal audits on regular basis from their own legal people; fear of what they find, recording it, and that it could be used against them in the future.
7. **Lack of Imagination.** Planning for catastrophic events requires imagination, but that requires spending time on this - pressed for productivity, so this type of activity gets cut or put on a back burner.
8. **Lack of System Understanding.** Leadership will say that we do things well, we have a procedure and we follow it perfectly every time; but they do not follow it every time;

industry is good on specifics of what is done, but poor on the basis and process on how and why things are/were done.

F. Transitioning from Risk Analysis to Preventing Catastrophic Events

Giannopoulos et al., in their review of the state-of-the-art of risk assessment methodologies [41], point out the linear nature of the approaches that form the backbone of most systems: identification and classification of threats, identification of vulnerabilities, and evaluation of impact. These methods are well defined and have been tested and validated for many classes of assets over decades. However, the discussion of several catastrophic failures above, highlights the inadequacy of the approach for prevent the "black or grey swan" interactions between multiple systems that trigger these disasters. It is clear that we have to address complex interactions between engineering, management, supply chain and human systems over several different infrastructure systems that operate in proximity to one another, or physically interact at specific touch points.

Rinaldi et.al. [42] capture the touch points between infrastructures in their 2001 article on critical infrastructure interdependencies as shown in **Figure 26**.

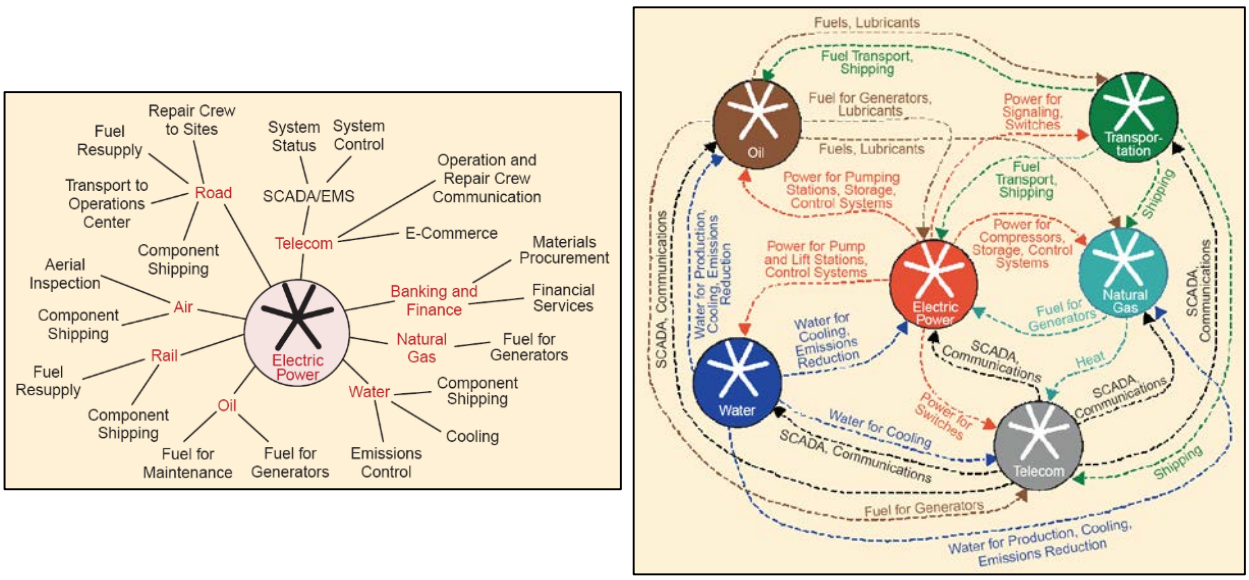


Figure 26. Interactions in Infrastructure Systems. Source [42]

The realization that we are in fact dealing with Systems of Systems is clearly not recent, but has not yet made its way into how industry build and manage their risk management systems. In the sections that follow we will introduce a number of tools and concepts that will be helpful, by slowly introducing network approaches that encourage diversity, in any effort to move towards an operational risk management approach that addresses some the shortcomings listed above.

Addressing the Uncertainties in Risk Analysis

In his essay "Why Risk Analysis is Difficult, and Some Thoughts on How to Proceed", Ben Haim [9] expands on the sources of uncertainty in risk analysis over and above those noted above. He covers the history of the axiomatic method invented by the ancient Greeks and the evolution of the understanding that uncertainty exists. He mentions the modern idea of conditional probability formalized bu Bayes in the mid-18th century and the emergence of probability theory and uncertainty theories in the 20th century. There is a plethora of approaches to uncertainty and their diversity reflects the variety of uncertainty itself. Ben-Haim explains the philosophical problem inherent in using the past to predict the future;

> "Given the richness of future discovery, (or conversely, the richness of our current ignorance), future behavior is incompletely determined by the past. The patterns and laws of behavior will grow or evolve in time as agents make discoveries. These laws cannot be known ahead of time. Indeed, they don't exist at all until they emerge because, by definition, discoveries cannot be predicted and the laws of behavior depend in part on discoveries that will be made."

tomorrow's discovery is by definition unknown today and therefore tomorrow's behavior is not entirely predictable today.

Ben-Haim goes on to discuss the philosophical problems with induction:

> "Furthermore, one cannot prove empirically that past experience is a guide to the future. By the time one tests the regularity of the future, that future has become the past. The future can never be tested, just as one can never step on the rolled up part of an endless rug unfurling always in front of you."

In the face of massive uncertainty there is a natural human reaction to reject any attempt to address the underlying issues because they seem insurmountable. This is epistemic paralysis as depicted by John Locke[43]:

> "If we will disbelieve everything, because we cannot certainly know all things; we shall do much what as wisely as he, who would not use his legs, but sit still and perish, because he had no wings to fly."

Ben-Haim points out our moral imperative to sweep aside this paralysis and advance our knowledge and understanding through the use of diverse sets of models in spite of their imperfection. He introduces the concepts of robustness in the face of uncertainty, and

satisficing as opposed to optimization, i.e. it is often a more robust approach (less sensitive to uncertainty) to choose a decision path that will satisfy some of our requirements rather than to try and optimize a probabilistic model that could be based on models that could prove to be completely incorrect due to massive uncertainty in their formulation. The satisficing approach leads to a tension between innovation (in the quest for continuous improvement) with uncertain outcome, and opting for a sure bet by taking better understood approaches known to be sub-optimal, but his point is well made in that we cannot allow ourselves to do nothing.

Diversity of Approach and Bayesian Updating

At this juncture it is instructive to reference the work of Tetlock [44-46] on what makes some people better predictors of future outcomes than others. The work comes out of an extensive set of studies that were part of The Good Judgment Project (GJP) [46]:

> " … a project "harnessing the wisdom of the crowd to forecast world events". It was co-created by Philip E. Tetlock (author of Superforecasting and of Expert Political Judgment: How Good Is It? How Can We Know?), decision scientist Barbara Mellers, and Don Moore… It was a participant in the Aggregative Contingent Estimation (ACE) program of the Intelligence Advanced Research Projects Activity (IARPA) in the United States… Predictions are scored using Brier scores… The top forecasters in GJP are "reportedly 30% better than intelligence officers with access to actual classified information"

The GJP was variable based and addressed the following:

- Links between how people think and what they get right,
- Counterfactuals in the decision-process,
- Risk tolerance, and
- How to assess performance in the face of subjectivity and relativism.

Tetlock found that individuals who met the requirements of being classified as a "superforecaster" were in many aspects very ordinary people, but they had a particular way of gathering information, processing information and updating forecasts on the basis of new information gathered. They tend to be extremely open minded, access diverse sets of information and synthesize the inputs in a fashion very similar to formal Bayesian updating. Their forecasts were always conditional on the basis of information available up to the point of forecasting. They tended to update their forecasts frequently, constantly revisiting assumptions. Tetlock adopts the term "Foxes and Hedgehogs" to differentiate between people with and without real foresight (see Excerpt 1 below).

In the EPJ results, there were two statistically distinguishable groups of experts. The first failed to do better than random guessing, and in their longer-range forecasts even managed to lose to the chimp. The second group beat the chimp, though not by a wide margin, and they still had plenty of reason to be humble. Indeed, they only barely beat simple algorithms like "always predict no change" or "predict the recent rate of change." Still, however modest their foresight was, they had some. So why did one group do better than the other? It wasn't whether they had PhDs or access to classified information. Nor was it what they thought— whether they were liberals or conservatives, optimists or pessimists. The critical factor was how they thought. One group tended to organize their thinking around Big Ideas, although they didn't agree on which Big Ideas were true or false. Some were environmental doomsters ("We're running out of everything"); others were cornucopian boomsters ("We can find cost-effective substitutes for everything"). Some were socialists (who favored state control of the commanding heights of the economy); others were free-market fundamentalists (who wanted to minimize regulation). As ideologically diverse as they were, they were united by the fact that their thinking was so ideological. They sought to squeeze complex problems into the preferred cause-effect templates and treated what did not fit as irrelevant distractions. Allergic to wishy-washy answers, they kept pushing their analyses to the limit (and then some), using terms like "furthermore" and "moreover" while piling up reasons why they were right and others wrong. As a result, they were unusually confident and likelier to declare things "impossible" or "certain." Committed to their conclusions, they were reluctant to change their minds even when their predictions clearly failed. They would tell us, "Just wait." The other group consisted of more pragmatic experts who drew on many analytical tools, with the choice of tool hinging on the particular problem they faced. These experts gathered as much information from as many sources as they could. When thinking, they often shifted mental gears, sprinkling their speech with transition markers such as "however," "but," "although," and "on the other hand." They talked about possibilities and probabilities, not certainties. And while no one likes to say "I was wrong," these experts more readily admitted it and changed their minds. Decades ago, the philosopher Isaiah Berlin wrote a much-acclaimed but rarely read essay that compared the styles of thinking of great authors through the ages. To organize his observations, he drew on a scrap of 2,500-year-old Greek poetry attributed to the warrior-poet Archilochus: "The fox knows many things but the hedgehog knows one big thing." No one will ever know whether Archilochus was on the side of the fox or the hedgehog but Berlin favored foxes. I felt no need to take sides. I just liked the metaphor because it captured something deep in my data. I dubbed the Big Idea experts "hedgehogs" and the more eclectic experts "foxes." Foxes beat hedgehogs. And the foxes didn't just win by acting like chickens, playing it safe with 60% and 70% forecasts where hedgehogs boldly went with 90% and 100%. Foxes beat hedgehogs on both calibration and resolution. Foxes had real foresight. Hedgehogs didn't.

…

Tetlock, Philip E.; Gardner, Dan. Superforecasting: The Art and Science of Prediction (pp. 68-69). Crown/Archetype. Kindle Edition.

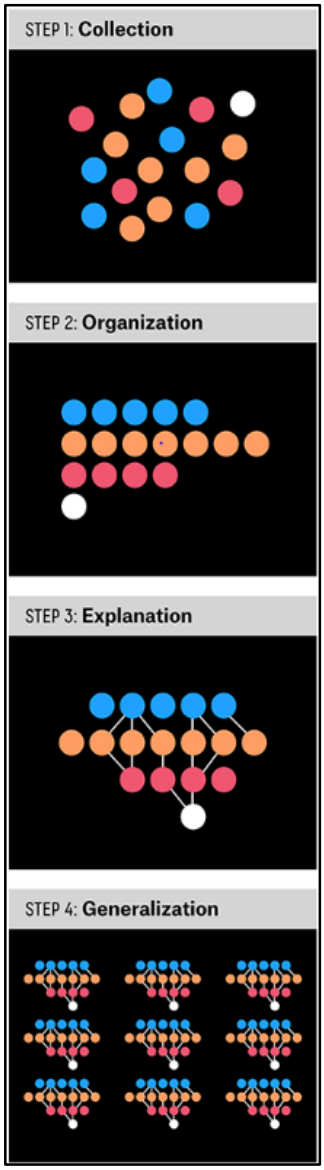
Excerpt 1. Foxes and Hedgehogs

The “Fox” approach is aptly captured by Ben-Haim [9]:

> “If we remain dispassionate and abjure demagoguery, then our mastery of the unknown will continue to grow”.

When “superforecasters” where assembled into teams they quickly became cohesive units and outperformed individuals on a regular and sustainable basis. One of the underlying reasons for this success is diversity of approach and the absence of territorial or egotistical behavior amongst these individuals. McChrystal [47] in his book “Team of Teams” describes how he was able to cultivate a similar success story when he took command of the Joint Special Operations Task Force in 2004. He quickly realized that conventional military tactics were failing. Al Qaeda in Iraq was a decentralized network that could move quickly, strike ruthlessly, then seemingly vanish into the local population. The allied forces had a huge advantage in numbers, equipment, and training that proved ineffective in preventing catastrophic attacks on their forces. They were fighting yesterday’s war, once again proving that the past is a poor predictor of the future. McChrystal and his colleagues discarded a century of conventional wisdom and remade the Task Force, in the midst of a grueling war, into something new: a network that combined extremely transparent communication with decentralized decision-making authority. The walls between silos were torn down. Leaders looked at the best practices of the smallest units and found ways to extend them to thousands of people on three continents, using technology to establish a oneness that would have been impossible even a decade earlier. Much of the success of the approach was contingent on banishing egotistical and hierarchical approaches, encouraging diversity, constantly updating the conditional probabilities of outcomes based on the most recent data, and empowering local experts to act independently knowing that they had grasped enough of the big picture objectives to understand how their local actions would impact the whole.

Nate Silver has also adopted the “Fox and Hedgehog” analogy in his approach to forecasting under uncertainty that is very much based on plausible, sometimes simplistic, but effective models, coupled to Bayesian updating, based on diverse sets of information [48, 49]. In his post “What the Fox Knows” [48] Silver provides a concise depiction of how he goes about gathering information and building models in the face of uncertainty. A graphical depiction of the approach is shown in Figure **27** below, together with a quote from Bertrand Russell that embodies Ben-Haim’s entreaty not to succumb to epistemic paralysis in the face of great uncertainty.



> I do not pretend to start with precise questions. I do not think you can start with anything precise. You have to achieve such precision as you can, as you go along.

Figure 27. Process for transforming anecdote into data and information [48]

Bearfield [50, 51] has formalized the use of Bayesian networks to realize bow-tie diagrams and capture local variability of inputs and constraints in his treatment of safety problems in the British rail network. His work was precipitated by a rash of catastrophic accidents in the network post privatization. Fenton and Neil [52, 53] have developed an extensive set of risk analysis and management tools based on Bayesian networks. Martins [54] has applied the Fenton and Neil tools to develop quantitative risk assessments of offshore LNG platforms in Brazil. Khakzad et al. [55], in their paper entitled "Major Accidents (Gray Swans) Likelihood Modeling Using Accident Precursors and Approximate Reasoning", present a novel approach to identify the most informative near accidents for developing likelihood estimates for major accidents. The method incorporates the use of Bayesian networks to estimate the likelihoods of future events, see **Figure 28**. Wheatley et al. [56], Guo et al [57] , and Li et al [58, 59]

provide various examples of using precursor events as indicators of future catastrophic events. The latter references incorporate Bayesian networks. Lathrop [60] provides methods for validating models in the absence of observed events.

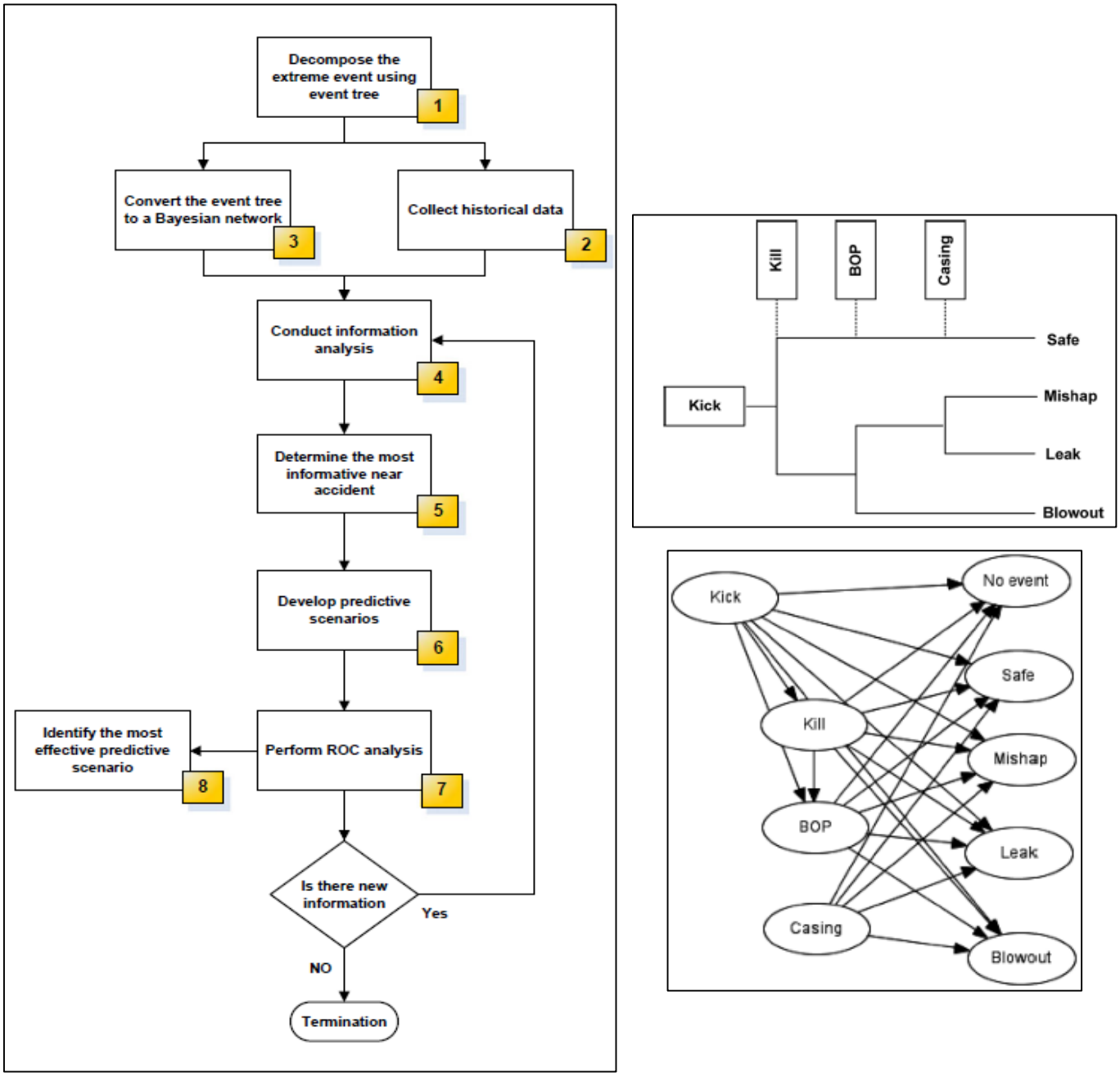


Figure 28. Methodology proposed by Khakzad et al. left, Bayesian Network model for offshore blowout and related near accidents, right. Source [55]

Bayesian network models are able to function with very sparse input data and provide reasonable initial estimates of likelihood that can be updated by rerunning the model each

time an additional data point becomes available. Fenton and Neil [53] demonstrate how hybrid Bayesian networks are very capable of synthesizing engineering models, behavioral models, historic data, or any anecdotal information synthesized by a process such as that illustrated by Silver, into a coherent model that provides meaningful insights.

Addressing Deep Uncertainty Through Adaptation

As already noted above in our discussion of the Rumsfeld quote, uncertainty in risk analysis is not only due to random fluctuations around expected values, but includes different parameterizations of the system model, uncertainties about mechanisms and functional relationships being studied and us not knowing what we don't know. We need to find ways to make the policies we follow and decisions we make robust under a range of plausible futures [9, 15, 61, 62].

Walker et al. [15] list three ways of dealing with uncertainties in this context:

1. *Resistance*: plan for the worst possible case or future situation
2. *Resilience*: whatever happens in the future, make sure that you can recover quickly
3. *Adaptation*: prepare to change the policy, in case conditions change

They go on to identify different types of adaptation:

1. Purposefulness, divided into:
    - *Planned adaptation*, which is the result of deliberate policy decisions, based on an awareness that conditions might change or have changed and that action is required to return to, maintain, or achieve a desired state.
    - *Autonomous adaptation*, which is adaptation that is not a planned external response to a situation, but is an internal system reaction due to changes within the system.
2. Timing, divided into:
    - Anticipatory adaptation, which takes place before negative impacts are observed.
    - Reactive adaptation, which takes place after negative impacts are observed.

Next they list a series of tools for adaptive policy development:

1. *Integrated and forward-looking analysis*

    This involves participatory scenario planning for policymaking and is an effective tool for anticipatory/planned types of policy adaptation.
2. *Built-in policy adjustment*

Some necessary policy improvements can be anticipated in advance and signposts monitored to trigger their implementation. This is a tool that facilitates anticipatory/planned adaptation.

3. *Formal policy review and continuous learning*

   Systematic review of policy is an important tool for anticipatory/planned adaptation. Treating policies as hypotheses for which assumptions must be continually tested also makes it more likely to detect surprises before they occur.

4. *Multi-stakeholder deliberation*

   Dialogue among stakeholders strengthens policy design in many ways. This tool facilitates anticipatory/planned adaptation, as well as autonomous/reactive adaptation undertaken by stakeholders most directly affected by policy.

5. *Enabling self-organization and social networking*

   A policy that does not undermine existing social capital and actively facilitates the sharing of good practices strengthen the potential for autonomous adaptation in the face of deep uncertainty.

6. *Decentralization of decision making*

   Autonomous adaptation can also be enabled by placing the authority and responsibility for decision making at the lowest effective and accountable unit of governance.

7. *Promoting variation*

   Implementing a variety of policies to address the same issue increases the likelihood of achieving desired outcomes and is illustrative of planned/anticipatory adaptation. Additionally, such diversity creates opportunity for autonomous response to surprise.

The concepts and methods briefly discussed in the section **Diversity of Approach and Bayesian Updating** above, are well suited for developing the tools and approaches listed above. Recognizing the value of diversity, in teams, models and solution approaches; that hybrid Bayesian networks are an ideal tool for coherent, forward and backward reasoning, and adopting their use will allow operators to take small steps towards a potentially robust networked system of systems approach to risk management. The Bayesian network approach is also well suited to rapid adaptation of the decision networks being developed for risk analysis in that nodes are readily added or deleted from the network as our knowledge of the system interactions increases.

There is a very large body of literature addressing the use of network and complex system of systems approaches in the study of resilience and emergent behavior of interacting infrastructures in the aftermath of catastrophic events. Giannopoulos et al. [41] point out that these approaches stretch the current understandings of risk analysis, but that **there is enormous room for innovation in this field**. **Table 3** lists some of the differences in perspective between the risk management and resilience approaches.

Table 3 Comparison of Risk and Resilience Perspectives. Source [63]

	Risk Management	Resilience
Design principles	Preservation of status quo, that is, avoid transformative change; minimize risk of failures	Adaptation to changing conditions without permanent loss of function (e.g., changing paths, if not destinations) Acknowledgment of unknown hazards. Intentional failure may be allowed at subsystem level to reduce the possibility of permanent loss of function in larger system
Design objectives	Minimization of probability of failure, albeit with rare catastrophic consequences and long recovery times	Minimization of consequences of failure, albeit with more frequent failures and rapid recovery times
Design strategies	Armoring, strengthening, oversizing, resistance, redundancy, isolation	Diversity, adaptability, cohesion, flexibility, renewability, regrowth, innovation, transformation
Relation to sustainability	Security, longevity	Recovery, renewal, innovation
Mechanisms of coordinating response	Centralized, hierarchical decision structures coordinate efforts according to response plans	Decentralized, autonomous agents respond to local conditions
Modes of analysis	Quantitative (probability-based) and semi quantitative (scenario-based) analysis of identified hazards in context of utility theory (i.e., costs & benefits)	Possible consequence analysis involving scenarios with unidentified causes

Agent Supported Cooperative Work in Complex Systems

In the previous section we noted that network approaches are very useful in developing a better understanding how multiple systems of systems interact in non-linear ways. It was pointed out that there is a large body of work addressing resilience in infrastructure systems based on network approaches and that there is room for innovation with regard to risk management. A potential area for innovative work is the realization that network based resilience approaches can be applied to the control methodologies for the systems themselves. Klein et al. and Bar-Yam [64, 65] have written about how the methods and science of complex systems can be applied to the collaborative design and how evolutionary approaches based on biological systems can be helpful in breaking down the enormous task of trying to balance the design requirements of very large interacting systems.

The key realization is that in any large complex network each node should be in a state that is compatible with its adjacent nodes only, we do not need to be looking at the full network. There is a simple demonstration [15] on the "Wolfram Demonstrations Project" from an unrelated field that gets this point across. **Figure 29** depicts a complex system and potential critical interactions (red nodes):

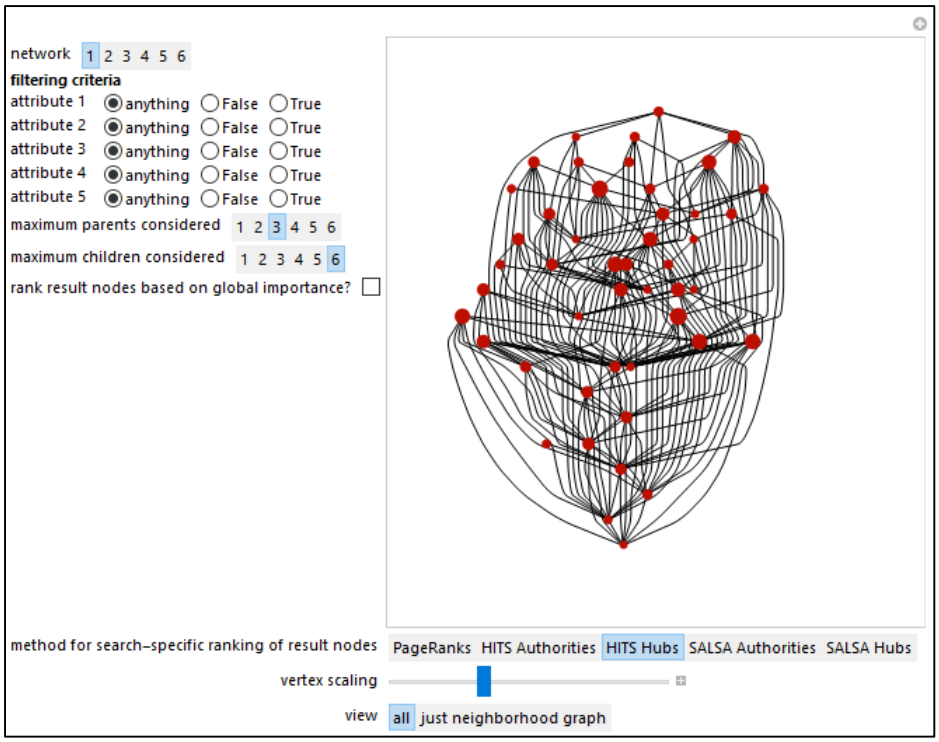


Figure 29. Graph of Complex Interacting System. Source Seth J. Chandler

15 "Neighborhood Graphs with HITS and SALSA" from the Wolfram Demonstrations Project
http://demonstrations.wolfram.com/NeighborhoodGraphsWithHITSAndSALSA/
Contributed by: Seth J. Chandler

If we apply constraints on the condition of the 5 system attributes, we get a very different picture of node (system component) connectivity:

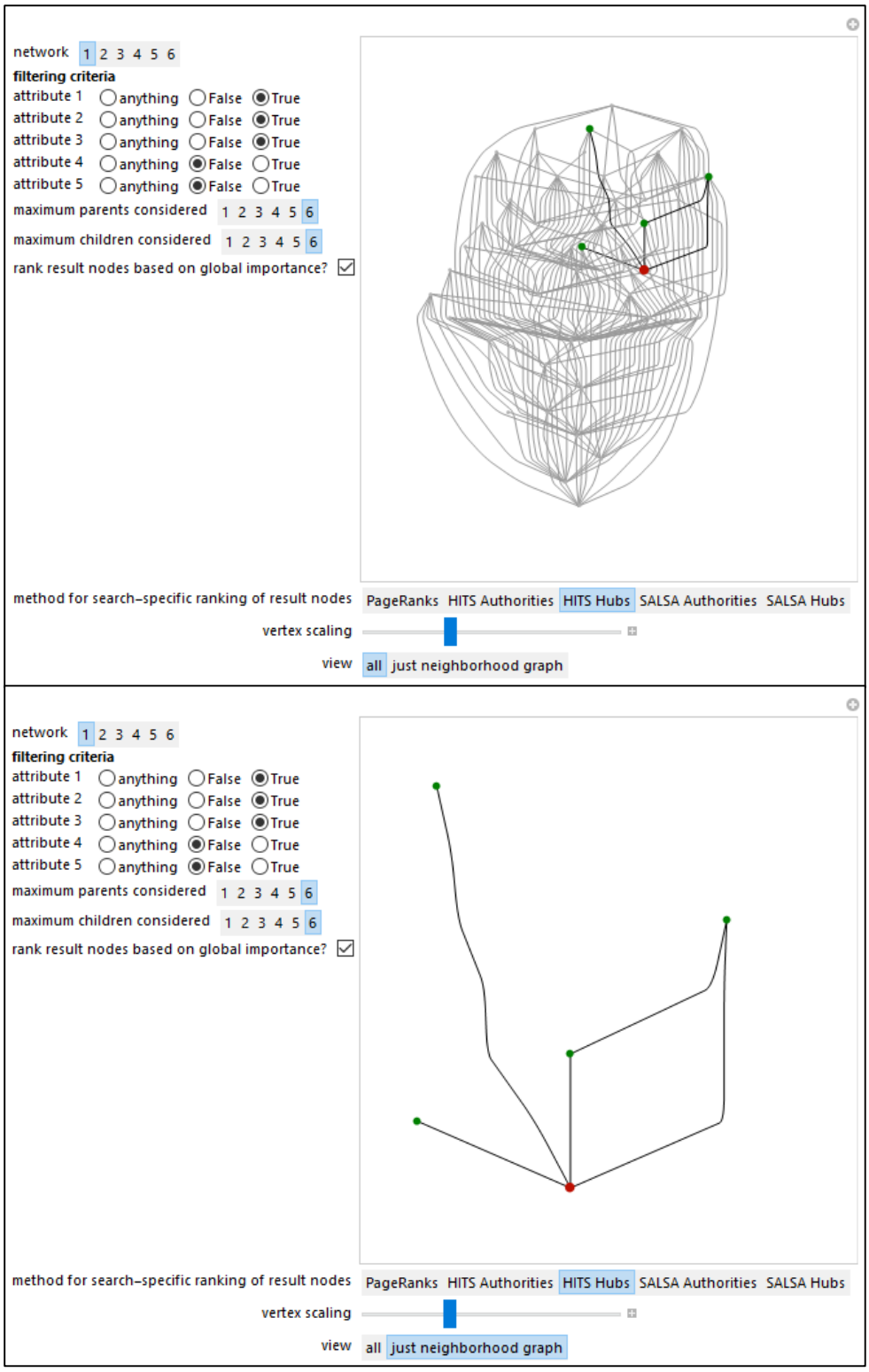


Figure 30. Graph of interacting nodes given specific constraints. Source Seth J. Chandler

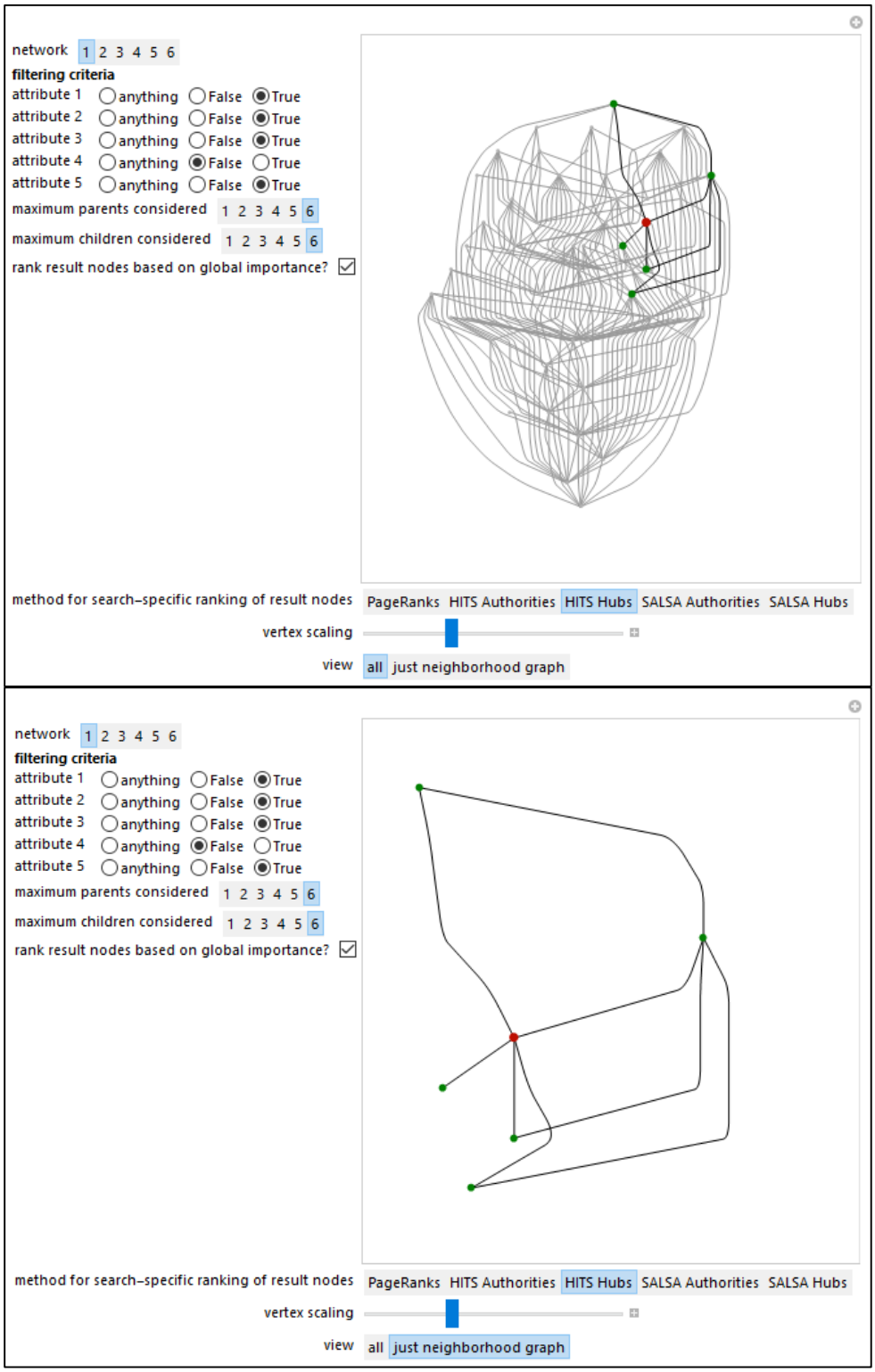


Figure 31. Graph of interactions with one constraint changed. Source Seth J. Chandler

Moving from **Figure 30** to **Figure 31** we see that changing one system wide attribute drops one node from the picture, brings in two nodes and changes the system focus (red node).

This could be the critical interaction leading to a catastrophe that was completely lost using traditional control approaches, because it was buried in the maze of possible interactions. Newman et. al [66] provide a conceptual cartoon (**Figure 32**) of how agents in adjacent systems can interact and Filippini and Silva [67] provide a specific example of such system of systems coupling and how to depict them as a dependency graph, see **Figure 33**.

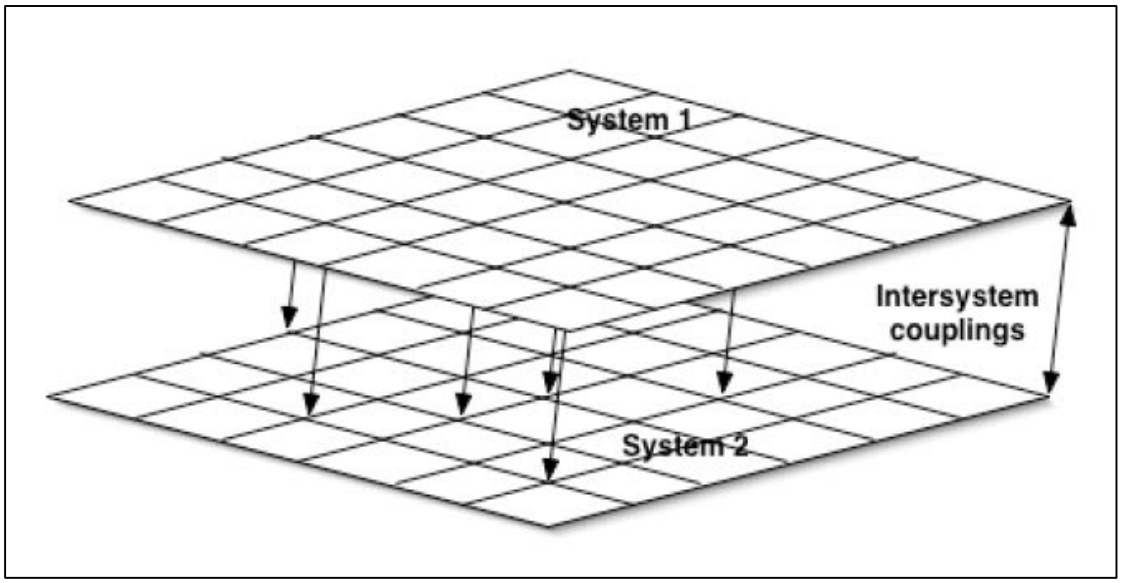


Figure 32. Cartoon of two homogenous systems with heterogeneous coupling. Source [66]

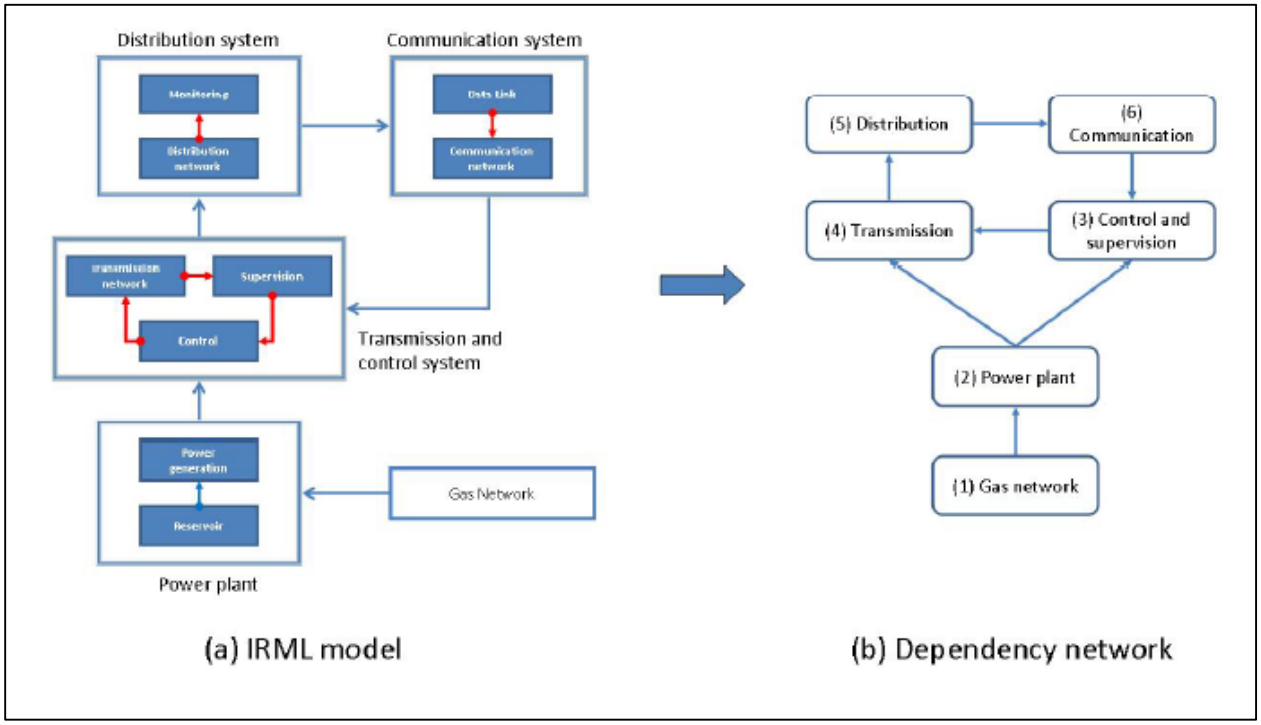


Figure 33. From System of Systems to dependency network. Source [67]

An important concept in complex systems is that of an agent. Russel et al.[68] in their book "Artificial intelligence: A Modern Approach" define the main unifying theme of artificial intelligence as the idea of an **intelligent agent**. Agents implement functions that map the basic components of a system concept to actions i.e. they perform very specific tasks at specific points in the system of systems. Each node in the figures above can be viewed as a single agent; they perform specific system functions given the inputs they receive and the control logic programmed into them. Once again Bayesian networks are a key tool in defining the conditional probabilistic behavior of systems of agents. Complex system theory has a lot to offer in this regard and needs to be properly explored.

G. Framework for Risk Governance

In the United States the National Science and Technology Council (NSTC) through their Committee on Environment, Natural Resources and Sustainability (CENRS) established The Subcommittee on Disaster Reduction (SDR) with the following charter:

1. Establish clear national goals for Federal science and technology programs aimed at disaster reduction.
2. Coordinate Federal research and policy related to natural and technological hazards and disasters, including with other NSTC committees and subcommittees where appropriate.
3. Create working groups to improve interagency collaboration in addressing Federal disaster risk reduction and resilience issues.
4. As permitted by law, identify and coordinate opportunities for the U.S. Government to collaborate with state, local, and foreign governments; international organizations; and private/academic/industry groups in the science and technology of disaster reduction.
5. Provide information to senior policymakers that summarizes relevant resources and scientific work within the member departments and agencies of the SDR.
6. Provide scientific and technical information to senior policymakers in response to current disaster situations.
7. As permitted by law, communicate with Administration officials, Congress, nongovernmental organizations, and other policy development bodies as appropriate about the science and technology of disaster reduction.
8. Promote disaster reduction preparedness and practices.
9. Facilitate the fusion of classified and unclassified data streams and research for disaster reduction applications.

Through its Co-chairs, the SDR will recommend action on policy and R&D issues to the CENRS for approval.

In July 2003 the SDR published an interim report "Reducing Disaster Vulnerability Through Science and Technology " [16] in which they list the following important areas for hazard risk reduction for the nation:

1. Leverage existing knowledge of natural and technological hazards to address terrorism events
2. Improve hazard information data collection and prediction capability
3. Ensure the development and widespread use of improved hazard and risk assessment models and their incorporation into decision support tools and systems

16 http://www.sdr.gov/docs/SDR_Report_ReducingDisasterVulnerability2003.pdf

4. Speed the transition from hazard research to hazard management application
5. Increase mitigation activities and incentives
6. Expand risk communication capabilities, especially public warning systems and techniques.

In June 2005 the SDR published a report entitled "Grand Challenges for Disaster Reduction" [17] with a second printing in 2008. In this report they identify the following "Grand Challenges":

1. Provide hazard and disaster information where and when it is needed
2. Understand the natural processes that produce hazards
3. Develop hazard mitigation strategies and technologies
4. Recognize and reduce vulnerability of interdependent critical infrastructure
5. Assess disaster resilience using standard methods
6. Promote risk-wise behavior

The report goes on to state:

> "Advances in science and technology alone cannot fully protect the Nation from all hazards. In support of these Grand Challenges, key research and major technology investments must be linked to effective "risk-wise" policy decisions at all levels. Change must occur at both the policy level and in the societal perception of risk so that adoption and adaptation keep pace with advances in science and technology. A sustained emphasis on risk mitigation and public/private partnerships is essential throughout all aspects and at all levels of the community. Within this integrated planning context, improved coordination of sustained Federal science and technology investment to address the Grand Challenges for Disaster Reduction will enhance disaster resilience and national safety."

These SDR reports do a good job of formulating the scope of the problem and highlighting the difficult challenges we have to grapple with if we want to extend classic risk analysis and management concepts to address the prevention of catastrophic events. Although their focus is resiliency, the general concepts are directly applicable to risk management that is focused on preventing the catastrophes to begin with. The tools and methods reviewed above, ARAMIS, LOPA and collaborative frameworks based on complex systems approaches are all consistent with those laid out by the SDR.

---

17 http://www.sdr.gov/docs/GrandChallengesSecondPrinting.pdf

The International Risk Governance Council (IRGC)[18] was established by the Swiss Federal Assembly in 2003. The risk management and regulatory failures of the 1990's (some of which we have reviewed above) were the driving force behind the established of the council, which is an independent and international body to bridge increasing gaps between science, technological development and the public. In July 2012 the IRGC was granted special consultative status with the United Nations Economic and Social Council (ECOSOC) and in July 2014 became a member of Sustainable Development Solutions Network (SDSN).

The IRGC has published a risk governance framework that addresses many of the issues we have noted above, and is consistent with the approach of the SDR.

The IRGC Risk Governance Framework [10, 13, 14]

A key concept in the IRGC risk governance framework is that of **emerging risk**, which is defined as new risks, or familiar risks that become apparent in new or unfamiliar circumstances. The aim of the framework is to support public and private organizations in dealing proactively with these emerging risks. Processes capable of dealing with emerging risks need two attributes: the ability to anticipate risks and the ability to respond to risks. It is understood from the outset that emerging risks develop in complex environments that display high levels of uncertainty, therefore conventional frameworks for familiar risks are not appropriate. It is understood that opportunities and emerging risks are interrelated and that the organizations need to manage these two concepts in conjunction. The decision support systems used by upper management need to be multi-disciplinary and capable of dynamically adapting as the environment changes. **Figure 34** to **Figure 37** graphically illustrate the IRGC framework.

18 https://en.wikipedia.org/wiki/International_Risk_Governance_Council (accessed 6/14/2016)
https://www.irgc.org/

Figure 34. Emerging risk governance at the intersection of various disciplines and theoretical frameworks. Source [14]

The framework recommends that decision makers consider using the dominant characteristic of a risk as the basis for deciding the appropriate level of stakeholder involvement in the process. Simple risks may require little consultation, while high complexity, uncertainty and ambiguity are candidates for more diverse stakeholder interaction to reconcile the various framings that different stakeholders may have when interpreting a risk or evaluating the options for its management.

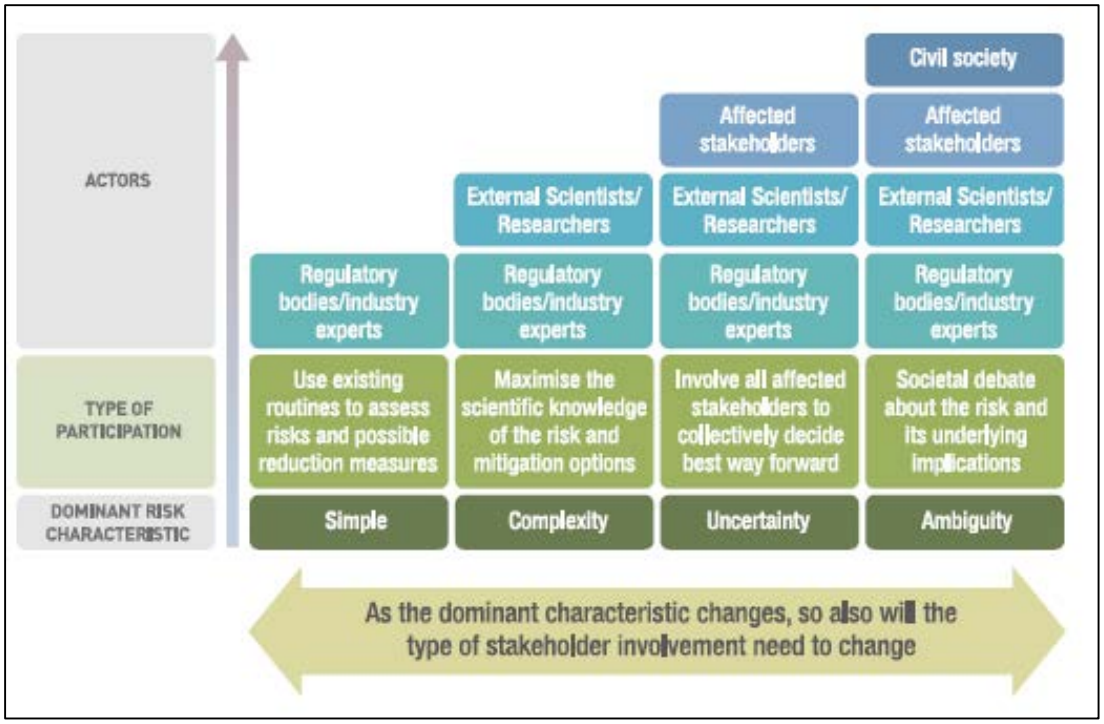


Figure 35. IRGC recommended structure for stakeholder involvement. Source [10]

Alongside the conventional elements of risk assessment, risk management, and risk communication, the framework stresses the broader social, institutional, political and economic contexts that must be taken into account in risk-related decision-making.

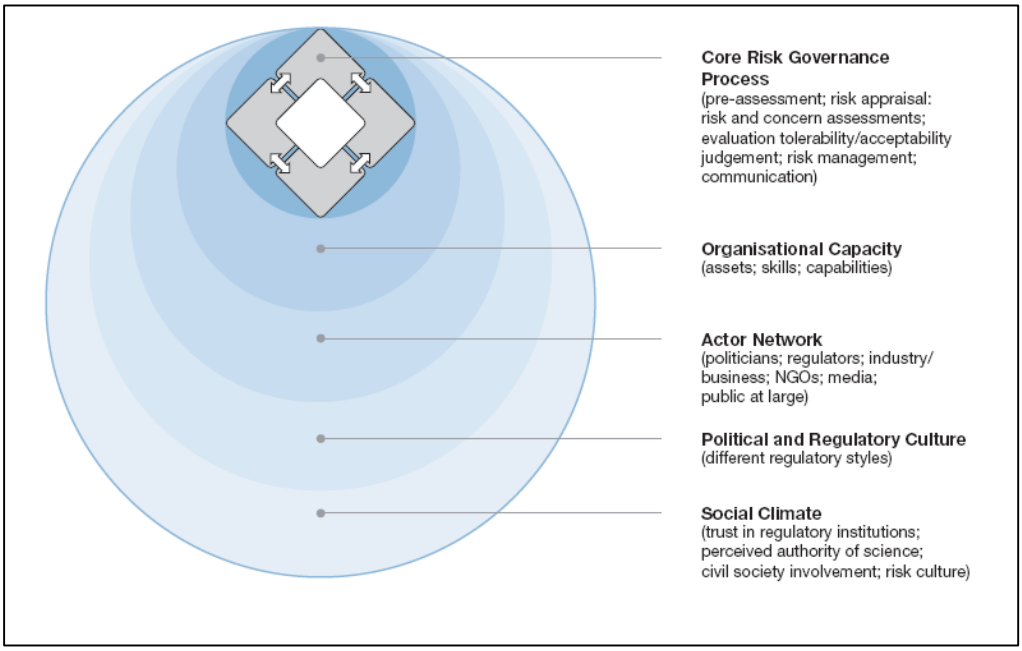


Figure 36. Risk governance in context. Source [10]

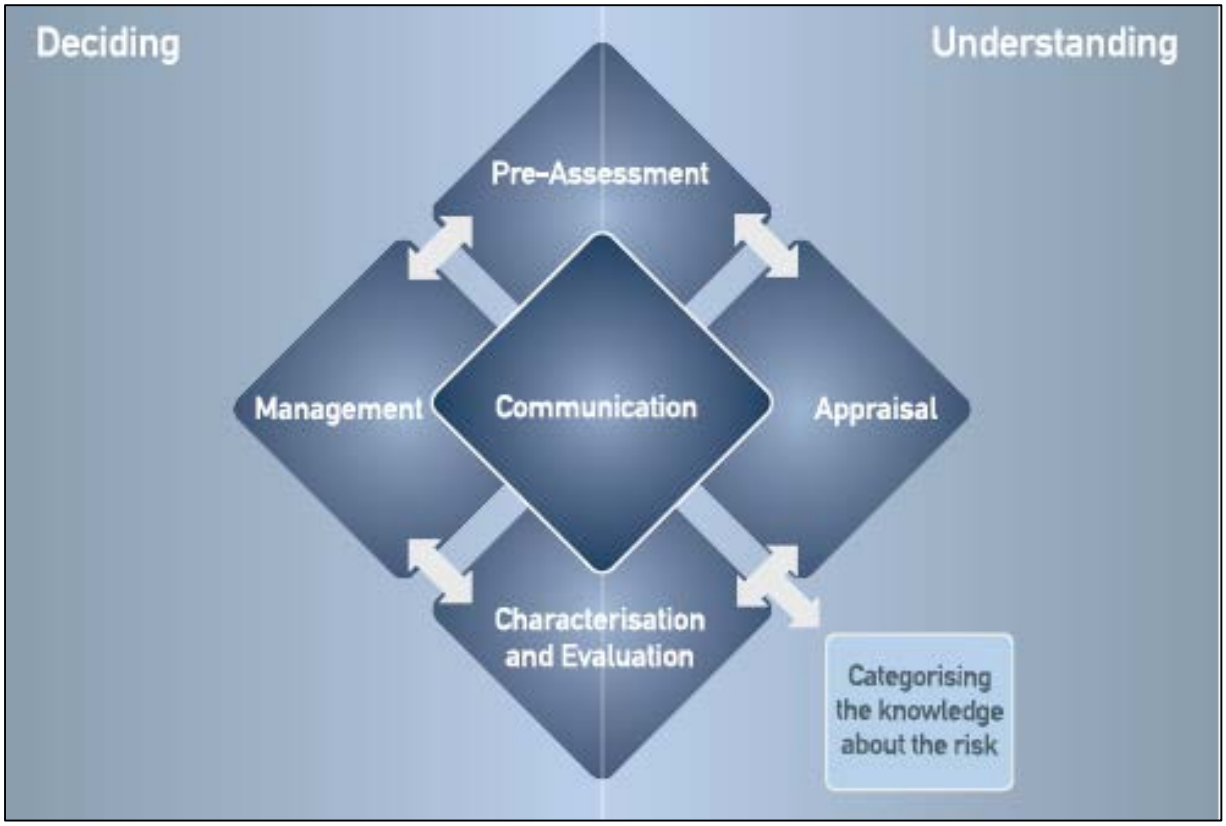


Figure 37. Components of the IRGC risk governance framework. Source [10]

There are five components to the IRGC framework: pre-assessment, appraisal, characterization and evaluation, management and communication.

Pre-assessment

Risk pre-assessment addresses early warning and "framing" the risk in order to provide a structured definition of the problem and how it may be handled. Pre-assessment clarifies the various perspectives on a risk, defines the issue to be looked at and forms the baseline for how a risk is assessed and managed. Crucially, it captures and brings to the open both:

- The variety of issues that stakeholders and society may associate with a certain risk (and the related opportunities), and
- Existing indicators, routines and conventions that may help narrow down what is to be addressed as the risk, as well as the manner in which it should be addressed.

The main questions in pre-assessment are:

- What are the risks and opportunities we are addressing?
- What are the various dimensions of the risk?
- How do we define the limits for our evaluations?

- Do we have indications that there is already a problem? Is there a need to act?
- Who are the stakeholders? How do their views affect the definition and framing of the problem?
- What are the established scientific/analytical tools and methods that can be used to assess the risks?
- What are the current legal/regulatory systems and how do they potentially affect the problem?
- What is the organizational capability of the relevant governments, international organizations, businesses and people involved?

Appraisal

Risk appraisal develops and synthesizes the knowledge base for the decision on whether or not a risk should be taken and, if so, how the risk can possibly be reduced or contained. Risk appraisal comprises both a scientific risk assessment – a conventional assessment of the risk's factual, physical and measurable characteristics including the probability of it happening – and a concern assessment – a systematic analysis of the associations and perceived consequences (benefits and risks) that stakeholders, individuals, groups or different cultures may associate with a hazard or cause of hazard. The concern assessment is a particular innovation of the IRGC framework, ensuring that decision makers account for how the risk is viewed when values and emotions come into play.

Scientific risk assessment deals with the following types of questions:

- What are the potential damages or adverse effects?
- What is the probability of occurrence?
- How ubiquitous could the damage be? How persistent? Can it be reversed?
- How clearly can cause-effect relationships be established?
- What scientific, technical and analytical approaches, knowledge and expertise should be used to better assess these impacts?
- What are the primary and secondary benefits, opportunities and potential adverse effects?

Concern assessment deals with such questions as:

- What are the public's concerns and perceptions?
- What is the social response to the risk? Is there the possibility of political mobilization or potential conflict?
- What role are existing institutions, governance structures and the media playing in defining public concerns?

- Are risk managers likely to face controversial responses arising from differences in stakeholder objectives and values, or from inequities in the distribution of benefits and risks?

Characterization and Evaluation

IRGC's inclusion of this element is deliberately intended to ensure that the evidence based on scientific facts is combined with a thorough understanding of societal values when making the sometimes controversial judgement of whether or not a risk is "acceptable" (risk reduction is considered unnecessary), "tolerable" (to be pursued because of its benefits and if subject to appropriate risk reduction measures) or, in extreme cases, "intolerable" and, if so, to be avoided. This phase involves making a judgement based on such questions as:

- What are the societal, economic and environmental benefits and risks?
- Are there impacts on quality of life?
- Are there ethical issues to consider?
- Is there a possibility of substitution? If so, how do the risks compare?
- Does a choice of a particular technology impact on the risk? How?
- What are the possible options for risk compensation, or reduction?
- What are the societal values and norms for making judgements about tolerability and acceptability?
- Do any stakeholders – government, business or other – have commitments or other reasons for wanting a particular outcome of the risk governance process?

Management

All tolerable risks will need appropriate and adequate risk management. Risk management involves the design and implementation of the actions and remedies required to avoid, reduce, transfer or retain the risks. Based on the development of a range of options and a consideration of the most appropriate of them, risk management decision are taken and put into practice. Risk management includes the generation, assessment, evaluation and selection of appropriate risk reduction options as well as implementing the selected measures, monitoring their effectiveness and reviewing the decision if necessary.

The questions are:

- Who is, or should be, responsible for decisions within the context of the risk and its management?
- Have they accepted this responsibility?
- What management options could be chosen (technological, regulatory, institutional, educational, compensation, etc.)?
- How are these options evaluated and prioritized?

- Is there an appropriate level of international cooperation and harmonization for global or transboundary risks?
- What are the secondary impacts of particular risk reduction options?
- What potential trade-offs between risks, benefits and risk reduction measures may arise?
- What measures are needed to ensure effectiveness in the long term (compliance, enforcement, monitoring, adaptive management plans, etc.)?

Communication

Communication is of the utmost importance. It enables stakeholders and civil society to understand the risk itself. It also allows them to recognize their role in the risk governance process and, through being deliberately two-way, gives them a voice in it. Once the risk management decision is made, communication should explain the rationale for the decision and allow people to make informed choices about the risk and its management, including their own responsibilities. Effective communication is the key to creating trust in risk management

H. Conclusions

Industries in both the United States and Europe use sophisticated and mature methodologies to identify and assess risks associated with hazardous system components. A wide variety of preventive and mitigative measures are employed across all critical infrastructure systems. Safety culture is an important component of all operating policies. In spite of these facts, industrial accidents still occur, sometimes with devastating consequences.

Careful investigation of dozens of major events reveals a complex web of causal factors covering all aspects of human organization and endeavor. On the human side we have: political and social structures, management cultures, incentives and censure, our desire to succeed and fear of failure, our passions and skepticism of the unfamiliar, our tendency to imprint, followed by a very long laundry list of human failings. People tend to believe that what happened yesterday will happen tomorrow, and if an event is not in our collective memory it is probably not a threat.

On the technological side, we have our ability to conceive and build systems that meet our various needs, we also have scientific prowess and the constant expansion of knowledge and potential that allow us to tap into more and more unexplored resources. This scientific, engineering and technological ability has led to exponential growth of human populations, systems of systems and daunting complexity as we continue to weave our intricate web. Unfortunately, our understanding of the full implications of the complex interactions associated our infrastructures has exposed us to infrequent, yet catastrophic risks when failures occur along convoluted pathways through human and technological systems. We have difficulty identifying new and emergent risks, in part due to our enslavement to the familiar risks we think we understand.

There is a growing realization that the pathway to solving the problem of complexity with unfamiliar risks might lie in embracing diversity and bringing it in to our processes at all levels of our systems and culture. Diversity means multidisciplinary approaches involving all stakeholders at multiple levels, allowing local autonomy of decision making while enforcing communication between the lowest and highest strata in an organization and its surroundings.

At the macro level, frameworks to achieve these ambitious goals have been proposed in the United States by the National Science and Technology Council (NTSC) and in Europe by the International Risk Governance Council (IRGC). These frameworks do an adequate job of covering the aspects of an improved worldwide, nationwide, region wide and system of

systems wide, risk aware and informed decision making process that brings all social and technological aspects into the picture.

At the micro level, we have to develop a synthesis of classic risk assessment and management approaches, but ensure that they are guided by system of systems thinking. It is essential to adopt the emerging disciplines of complex system analysis and collaborative agent based design as they have the greatest potential for enlightening us on how risk is driven by difficult to visualize interactions. We need to learn from the various approaches that demonstrate the power of diverse teams at the micro level, and constant updating of our approaches and policies based on new evidence as it becomes available. There is a vibrant and emerging body of research exploring these techniques that demonstrate how it is possible to function under great uncertainty with sparse data. A good proportion of this research is aimed at interacting infrastructures and how to model their emerging risks, as well as how to use readily available precursors as reasonable predictors of catastrophic failure.

These techniques need to become familiar, everyday activities; embracing these will help us design and operate systems of systems that are both more resilient in the face of the unexpected, and less prone to extreme events. We need to accept that our styles of management and regulation may have to change dramatically as we become more aware of, and better understand, the likelihood and consequences of extremely rare events, and how to reduce their probability of ever occurring.

Our training curricula, both internal to the organizations and in our educational institutions need to reflect this shift in perception and facilitate the necessary cultural changes to truly grapple with the prevention of catastrophic events in our technological systems.

I. References

1. Paltrinieri, N., et al., *Lessons learned from Toulouse and Buncefield disasters: from risk analysis failures to the identification of atypical scenarios through a better knowledge management.* Risk Analysis, 2012. **32**(8): p. 1404-1419.
2. Park, J., et al., *Integrating risk and resilience approaches to catastrophe management in engineering systems.* Risk analysis, 2013. **33**(3): p. 356-367.
3. Willis, H.H., *Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection*. 2007: RAND.
4. Council, N.R., *Review of the Department of Homeland Security's Approach to Risk Analysis.* 2010, Washington, DC: The National Academies Press. 160.
5. W3C. *Semantic Web - W3C*. 2016; Available from: http://www.w3.org/standards/semanticweb/.
6. Pisarenko, V. and M. Rodkin, *Distributions of characteristics of natural disasters: Data and classification*, in *Heavy-Tailed Distributions in Disaster Analysis*. 2010, Springer. p. 1-22.
7. Aban, I.B., M.M. Meerschaert, and A.K. Panorska, *Parameter estimation for the truncated Pareto distribution.* Journal of the American Statistical Association, 2006. **101**(473): p. 270-277.
8. Morgan, M.G. and M. Small, *Uncertainty: a guide to dealing with uncertainty in quantitative risk and policy analysis*. 1992: Cambridge University Press.
9. Ben-Haim, Y., *Why risk analysis is difficult, and some thoughts on how to proceed.* Risk Analysis, 2012. **32**(10): p. 1638-1646.
10. IRGC, *An Introduction to the IRGC Risk Governance Framework*. 2008, International Risk Governance Council: Geneva.
11. CRED. *EM-DAT Disaster Trends*. The OFDA/CRED International Disaster Database 2016 [cited 2016 May 17]; Available from: http://www.emdat.be/disaster_trends/index.html.
12. Southgate, R., et al., *Using Science for Disaster Risk Reduction*. 2013, UNISDR Scientific and Advisory Group: New York.
13. IRGC, *Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures*. 2006, International Risk Governance Council: Geneva. p. 68.
14. IRGC, *IRGC (2015). Guidelines for Emerging Risk Governance.* 2015, International Risk Governance Council (IRGC): Lausanne.
15. Walker, W.E., V.A. Marchau, and D. Swanson, *Addressing deep uncertainty using adaptive policies: Introduction to section 2.* Technological Forecasting and Social Change, 2010. **77**(6): p. 917-923.
16. Rumsfeld, D.H., *Defense.gov Transcript: DoD News Briefing - Secretary Rumsfeld and Gen. Myers*. 2002, U.S Department od Defense.
17. Taleb, N.N., *The black swan: The impact of the highly improbable*. 2007: Random House.
18. Myriam, M., *Aide à la décision et expertise en gestion des risques*. 2010: Lavoisier.
19. NTSB, *Pacific Gas and Electric Company Natural Gas Transmission Pipeline Rupture and Fire San Bruno, California, September 9, 2010*. 2011, National Transportation Safety Board: Washington DC.
20. Duller, P. and A. North, *Records Management within the Gas Transmission Division of Pacific Gas and Electric Company prior to the Natural Gas Transmission Pipeline Rupture and Fire, San Bruno, California September 9, 2010*. 2012: San Francisco.
21. Black, J., *Learning from regulatory disasters.* 2014.
22. Chernov, D. and D. Sornette, *Examples of Risk Information Concealment Practice*, in *Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human Fallibility*. 2016, Springer International Publishing: Cham. p. 9-245.

23. Perrow, C., *The President's Commission and the Normal Accident*, in *Accident at Three Mile Island: The Human Dimensions*, D. Sils, C. Wolf, and V. Shelanski, Editors. 1982, Shelarski Westview Press: Boulder, CO.
24. Perrow, C., *Normal Accidents: Living with High-Risk Technologies*. 1984, New York, NY: Basic Books.
25. Wikipedia. *Normal Accidents*. 2016 [cited 2016 April 6, 2016]; Available from: https://en.wikipedia.org/wiki/Normal_Accidents.
26. Perrow, C. and D.E. Whitney, *Normal Accidents by Charles Perrow - Reviewed by Daniel E. Whitney*. 2003, MIT-Engineering Systems Division: Massachesetts Institute of Technology.
27. Pidgeon, N., *In Retrospect: Normal Accidents.* Nature, 2011. **477**.
28. Anderson;, H., et al., *Accidental Risk Assessment Methodology for Industries in the Context of the Seveso II Directive: User Guide*. 2004, Community Research: Energy, Environment and Sustainable Development: Brussels. p. 110.
29. Salvi, O. and B. Debray, *A global view on ARAMIS, a risk assessment methodology for industries in the framework of the SEVESO II directive.* Journal of Hazardous Materials, 2006. **130**(3): p. 187-199.
30. Apostolakis, G.E., *How Useful Is Quantitative Risk Assessment?* Risk Analysis, 2004. **24**(3): p. 515-520.
31. Gowland, R., *The accidental risk assessment methodology for industries (ARAMIS)/layer of protection analysis (LOPA) methodology: A step forward towards convergent practices in risk assessment?* Journal of Hazardous Materials, 2006. **130**(3): p. 307-310.
32. Franks, A., *Lines of Defence/Layers of Protection Analysis in the COMAH Context*. 2003, HSE: Warrington. p. 56.
33. Bridle, P., *Getting Serious About Major Hazard Event (MHE) Management*, in *Oilpro*.
34. Herbert, I., *The UK Buncefield incident – The view from a UK risk assessment engineer*. Journal of Loss Prevention in the Process Industries, 2010. **23**(6): p. 913-920.
35. Barthélémy, F., et al., *Usine de la société Grande Paroisse à Toulouse Accident du 21 septembre 2001*. Rapport de l'Inspection générale de l'environnement, Paris, 2001.
36. Wikipedia. *AZF Factory*. 2016 [cited 2016 6/12/2016]; Available from: https://en.wikipedia.org/wiki/AZF_(factory).
37. HSE. *Seveso Directive*. 2016 [cited 2016 6-12-2016]; Available from: http://www.hse.gov.uk/seveso/.
38. COmAH, C., *Buncefield: Why did it happen*. 2011, HSE Books.
39. Herbert, I., *The UK Buncefield incident–the view from a UK risk assessment engineer*. Journal of Loss Prevention in the Process Industries, 2010. **23**(6): p. 913-920.
40. Wikipedia. *Buncefield Fire*. 2016 [cited 2016 6/12/2016]; Available from: https://en.wikipedia.org/wiki/Buncefield_fire.
41. Giannopoulos, G., R. Filippini, and M. Schimmer, *Risk Assessment Methodologies for Critical Infrastructure Protection, Part I: A state of the art.* JRC Technical Notes, 2012.
42. Rinaldi, S.M., J.P. Peerenboom, and T.K. Kelly, *Identifying, understanding, and analyzing critical infrastructure interdependencies.* Control Systems, IEEE, 2001. **21**(6): p. 11-25.
43. Locke, J., *An essay concerning human understanding*. 1841.
44. Tetlock, P.E. and D. Gardner, *Superforecasting: The Art and Science of Prediction*. 2015: Crown/Archetype.
45. Tetlock, P.E., *Expert Political Judgment: How Good Is It? How Can We Know?* 2009: Princeton University Press.
46. Wikipedia. *The Good Judgement Project*. [cited 2016 6/10/2016]; Available from: https://en.wikipedia.org/wiki/The_Good_Judgment_Project.
47. McChrystal, S.A., et al., *Team of Teams: New Rules of Engagement for a Complex World*. 2015: Penguin Publishing Group.
48. Nate Silver, *What the Fox Knows | FiveThirtyEight*. 2016, FiveThirtyEight.

49. Silver, N., *The Signal and the Noise: Why So Many Predictions Fail-but Some Don't*. 2012: Penguin Publishing Group.
50. Bearfield, G. and W. Marsh, *Generalising event trees using bayesian networks with a case study of train derailment*, in *Computer Safety, Reliability, and Security*. 2005, Springer. p. 52-66.
51. Bearfield, G.J., *Using Bayesian networks to represent parameterised risk models for the UK railways*. 2009, Queen Mary, University of London.
52. Fenton, N. and M. Neil, *Making decisions: using Bayesian nets and MCDA.* Knowledge-Based Systems, 2001. **14**(7): p. 307-325.
53. Fenton, N. and M. Neil, *Risk assessment and decision analysis with Bayesian networks*. 2012: CRC Press.
54. Martins, M.R., A.M. Schleder, and E.L. Droguett, *A Methodology for Risk Analysis Based on Hybrid Bayesian Networks: Application to the Regasification System of Liquefied Natural Gas Onboard a Floating Storage and Regasification Unit.* Risk Analysis, 2014: p. n/a-n/a.
55. Khakzad, N., F. Khan, and P. Amyotte, *Major Accidents (Gray Swans) Likelihood Modeling Using Accident Precursors and Approximate Reasoning.* Risk Analysis, 2015. **35**(7): p. 1336-1347.
56. Wheatley, S., B. Sovacool, and D. Sornette, *Of Disasters and Dragon Kings: A Statistical Analysis of Nuclear Power Incidents and Accidents.* Risk Analysis, 2016: p. n/a-n/a.
57. Guo, Z. and Y.Y. Haimes, *Risk Assessment of Infrastructure System of Systems with Precursor Analysis.* Risk Analysis, 2016: p. n/a-n/a.
58. Li, L., et al., *Assessment of Catastrophic Risk Using Bayesian Network Constructed from Domain Knowledge and Spatial Data.* Risk Analysis, 2010. **30**(7): p. 1157-1175.
59. Li, L., et al., *A Bayesian Method to Mine Spatial Data Sets to Evaluate the Vulnerability of Human Beings to Catastrophic Risk.* Risk Analysis, 2012. **32**(6): p. 1072-1092.
60. Lathrop, J. and B. Ezell, *Validation in the Absence of Observed Events.* Risk Analysis, 2016. **36**(4): p. 653-665.
61. Ben-Haim, Y., *Info-Gap Decision Theory: Decisions Under Severe Uncertainty*. 2006: Elsevier Science.
62. Ben-Haim, Y., *Doing Our Best: Optimization and the Management of Risk.* Risk Analysis, 2012. **32**(8): p. 1326-1332.
63. Park, J., et al., *Integrating Risk and Resilience Approaches to Catastrophe Management in Engineering Systems.* Risk Analysis, 2013. **33**(3): p. 356-367.
64. Klein, M., et al., *The dynamics of collaborative design: insights from complex systems and negotiation research.* Concurrent Engineering, 2003. **11**(3): p. 201-209.
65. Bar-Yam, Y., *About engineering complex systems: Multiscale analysis and evolutionary engineering*, in *Engineering Self-Organising Systems*. 2004, Springer. p. 16-31.
66. Newman, D.E., et al. *Risk assessment in complex interacting infrastructure systems*. in *System Sciences, 2005. HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on*. 2005. IEEE.
67. Silva Vazquez, A. and R. Filippini, *Resilience analysis of networked systems-of-systems based on structural and dynamic interdependencies.* 2012.
68. Russell, S.J., P. Norvig, and E. Davis, *Artificial intelligence : a modern approach*. 3rd ed. Prentice Hall series in artificial intelligence. 2010, Upper Saddle River: Prentice Hall. xviii, 1132 p.
69. Sagan, S.D., *Learning from Normal Accidents.* Organization and Environment, 2004. **17**(1): p. 15-19.
70. Commission, U.N.R. *Defense in Depth*. 2016 [cited 2016 April 6, 2014]; Available from: http://www.nrc.gov/reading-rm/basic-ref/glossary/defense-in-depth.html.
71. (INSAG), I.N.S.A.G., *Defence in Depth in Nuclear Safety INSAG-10*. 1996, INSAG: Austria. p. 1-33.

72. Satorius, M.A., *SECY-13-0132 U.S. Nuclear Regulatory Commission Staff Recommendation for the Disposition of Recommendation 1 of the Near-Term Task Force Report; Enclosure 3: Defense-In-Depth Observations, and Detailed History (ML13277A421)*, Operations, Editor. 2013, U.S. NRC: Washington D.C.
73. IAEA. *Assessment of Safety*. 2016 [cited 2016 April 6, 2016]; Available from: https://www.iaea.org/ns/tutorials/regcontrol/chapters/assess.pdf.
74. Favaro, F.M. and J.H. Saleh, *Observability-in-depth: an essential complement to the defense-in-depth safety strategy in the nuclear industry.* Nuclear Engineering and Technology, 2014. **46**(6): p. 803-816.

J. List of Acronyms

Table 4. List of Acronyms

Acronym	Description
GTI	Gas Technology Institute
NTSB	National Transportation Safety Board
CPUC	California Public Utilities Commission
IRGC	International Risk Governance Council
PG&E	Pacific Gas and Electric
QRA	Quantitative Risk Assessment
ARAMIS	Accidental Risk Assessment Methodology for Industries
MIMAH	Identification of major accident hazards
MIRAS	Identification of Reference Accident Scenarios
LOPA	Layers of Protection Analysis
HSE	Health and Safety Executive
MHE	Major Hazard Event
NSTC	National Science and Technology Council
CENRS	Committee on Environment, Natural Resources and Sustainability
SDR	Subcommittee on Disaster Reduction
SoS	System of Systems

Appendix 1: Interviews of Stakeholders

Interview Questions – Summary of Answers
[contains all eight interviews through 4/15/2016]

1. How does your company/organization define a "Catastrophic Event (CE)"?

- Unlikely events with high consequences.
- Multiple fatalities.
- Prolonged and sustained resource impact.
- Prolonged and sustained ecosystem damage.
- Threatens the business itself.
- Defined as event that requires emergency actions.
- Do not have a detailed definition.
- Different and dependent on size of company.
- Not expected, not recognized as a risk, do not see it coming, miss assess.
- Extended outage could be a CE
- Preserve life and property
- There is a regulatory answer (based on Part 192 and 195) and a practical answer.
- There are events that do not reach reportable status, but are significant to the organization, e.g., a large leak when you had multiple events in the past; if it was a little worse it would have had a great $ impact and/or if reportable a large enforcement action.
- Say had rupture and fire, but no one hurt or major damage: 15yrs ago hand slap, 10 years ago corrective action issued, now any leak they get into your business and issue a safety order to reduce pressure ($ impact).
- A double guillotine rupture in a critical class of piping.

2. What is the measure or metric for a CE, e.g., threshold number of injuries and/or loss of life, property damage, environmental damage, stock devaluation, fines, lawsuits, etc.? For instance, the insurance industry currently classifies a CE as > $25M (million). Katrina for instance was $41.1B (billion). [combine with #3 below].

3. Does your company carry CE insurance, such as excess line insurance?

- Depends on risk tolerance; different companies of diff. sizes, impact on enterprise, size of consequence (esp. when cannot predict likelihood).

- For larger company, say BP, they were self-paid up to $1M so less than that was not a big issue since the insurance company didn't get into your business and ask what they did beyond the regulatory requirements.
- For the nuclear industry any violation of a pressure boundary is tracked and addressed by the operator and regulator, regardless of consequence or impact in dollars or lives.

4. How do you define safety culture related to CEs?

- Culture, e.g., highly reliable organizations: nuclear, aircraft, maybe medical, all preoccupied by failure; Commonly use FTA and ETA, threat interactions, unknown-unknowns = black swans.
- Gas industry is good at responding to CE and gets better as the practice.
- It is evolving, especially seeing some improvement the last 2-3 years. Still poor, but getting better.
- Huge disconnect between guy in the ditch and the one in the corner office; also disconnect between departments – both areas not making connections related to enterprise/process safety and risk.

5. What probability of event occurring is low enough that you do not consider it as a potential CE (from a planning perspective)? For example, once in every 1,000 years, 500 years, etc. or one in a million, one in a billion, etc.

- Falls from corporate memory, people forget; especially with large M&A's – this has been a real problem.
- When cannot determine likelihood, use consequence to determine what to do: replace, repair, etc. Sometimes very hard to predict event probability.
- Exact numbers do not really matter, if it happens in my congressional district it is a CE.
- Systems run by engineers so they focus on likelihood, they can calculate the probabilities and pdfs; but they struggle if it happens what the consequence is.
- The non-technical folks like lawyers and leaders focus on consequences.
- Can back-calculate tolerable likelihood as a function of consequence through the risk relationship; the low end of the range with significant consequences is 1x10-8/yr*mile or a 1 in 100 million tolerance for ruptures.
- In the nuclear industry follows a leak before break philosophy. Use deterministic models coupled with Monte Carlo simulations; desire a very low probability of failure, less than one in a million.

6. How do you combine the technical, managerial, leadership, process, and cultural aspects of the risks of a CE occurring? The core question is how do build the connection between organizational to technical factors related to CEs?

- Management issue, Challenger O-Rings, technical against lift-off but management team gave OK, the technical guys do not speak the enterprise risk language of the final decision makers.
- Small companies may have an advantage because all this resides in a few people with multiple management, leadership, and technical hats.
- Senior management tends to "hide behind the code", i.e. if we are code compliant (even minimally) then we are "OK" vs. Integrity Management personnel look at sub-quantitative risk estimates and integrity and focus on managing risks.
- In the nuclear industry the NRC has authority for safety. A Relief Request is required to depart from prescriptive codes. The requests are reviewed by an autonomous technical group, and any technical person who has concerns can issue a DPO – Differing Professional Opinion. The DPO must be addressed through the chain of command and resolved. This means that an engineer can have a form of "veto power". It slows things down, but is a solid and good practice as far as safety is concerned.

7. How do you consider and plan for interactive threats that could combine and trigger a CE?

- Process issue, FMEA, need formal system, Flint water Pb issue tried to save money but should have added inhibitor so Pb did not come out, connect the dots
- Watch single supply points and reliability.
- These are hard to identify and consider, not something we do.
- Three categories of interactions
    - Interactive Defects: gouge in a dent, industry is good with this, can run calculations, and they can control this. PHMSA sometimes only calls these interactive threats (should be defects).
    - Interactive Threats: EC, IC, SCC combo, industry struggles a little with this, they have to relate this to how they do P&M; partially control this.
    - Interactive Circumstances: PG&E example, rupture takes out water main to fight fire, do not control this (like the trees outside of ROW for hurricanes and change in flood plain outside of ROW that washes out pipeline). These can and often are location specific.
- The nuclear industry is focused on Beyond-Design-Basis. Post Fukishima the industry is focused on interactions, earthquakes, floods, tsunamis, and other external factors that could challenge the design basis of the plants. Supports are added if the probability of failure is greater than one in a million frequency.

8. Recent surveys show that human interactions, communications, teamwork, and cultural factors contribute to technical breakdowns that trigger CEs - what are your organizations strengths and weaknesses in these areas?

- Need management systems, new PHMSA pipelines are failing early, lack of process.
- This is a soft area for engineers, they do not really understand this well.
- Not following up with lessons learned; need to get better at sharing root cause information within company and across companies. There is a lack of transparency.
- Big companies are dispersed, in many states; therefore, dependent on localized leadership.
- Not strong on follow up of problems with human issues, lessons learned, and how to fix and prevent in the enterprise.
- Fear of doing internal audits on regular basis from own legal people, fear of what they find, recording it and that it could be used against them in the future.
- Trying to build consensus among leaders that the risk of what we find is less than the risk of not understanding what is happening.
- Having a license to do something (like drive) does not mean you are really qualified and confirmed competent; there is a difference between training and passing and exam and a real transfer of knowledge to ensure competency.
- Very difficult to break out human error and interactions into a probabilistic model – we do it by increasing the uncertainty in specific portions of the risk model. In effect the human factors contaminate the probabilistic model.
- Combination of inadequate worker training and very old infrastructure is a problem. Need to ramp up integrity management requirement and use state of the art technology when ready.
- Nuclear industry has checks and balances on the technical side – multiple cross checks. The industry uses a very rigorous root cause failure analysis method that includes human interactions, communications, etc. They apply the lessons industry-wide, not just at one plant.

9. How does your organizations leadership perform "Anticipation", which is the practice of enhancing organizational sensitivity to the "weak signals" that may indicate increased risk to a CE (could also be labeled weak "leading indicator")?

- Vigilance, sensitivity, mindfulness, culture of nuclear and aircraft folks.
- Don't let small things become big.
- Debrief events and do root causes.
- Have confirmation bias; tend to be reactive vs. proactive.

- Trying to combat confirmation bias that results in coming to a conclusion that is equal to your preconceived idea of what it would be.
- There is a big disconnect between personnel/personal safety and process safety.
- Industry is good at personnel safety and poor at process; they can use leading indicators for personnel safety, but are stuck with lagging indicators on process safety.
- We look at leaks, even small ones, as leading indicators that could relate to major leaks or ruptures, i.e., any leak event is in the "wrong direction", especially if it is in an HCA.
- In the nuclear industry new threats are addressed by a combination and cooperation from industry, operators, and regulators. The resources provided by industry and the regulator are significant to solve these new threats.

10. How does your organizations leadership approach "Inquiry" which is the practice of making effective use of information to analyze, understand, and plan mitigation for the risks of CEs?

- Deference to technical experts, leaders should find knowledge centers and defer to that, understand what is at stake.
- Industry does great RCFA with reasons something happened, but is poor at applying lessons learned across the enterprise to prevent new/next event.
- Have done this for events that have happened, but not for events that have not happened yet.
- Requires imagination, but that requires spending time on this – pressed for productivity, so this type of activity gets cut or put on a back burner.
- The model must accept new information, need to weight historic vs. SME vs. analytical information, some information will change the model, reinforce the model, and/or make the model obsolete.
- Have data overload, i.e. too much data and not enough people or time to review it. The data is also disperse and dissimilar and not sure what value it is.

11. How does your organizations leadership assess "Execution" which is the practice of ensuring that hazard identification, assessment, and control efforts are followed as intended?

- PDCA the check part of the management system.
- Leadership will say that we do things well, we have a procedure and we follow it perfectly every time; but they do not follow it every time; industry is good on specifics of what is done, but poor on the basis and process on how and why things are/were done.
- Periodic audits and drills help.

12. How does your organizations leadership plan for "Resilience" which is the organizations ability to react in ways that prevent upset conditions from becoming CEs, and then learning from the experience (prevent and then lessons learned)?

- Ability to respond and adapt to a crisis, understand risks, understand consequences, table top drills, barrier management, multiple barriers, defense in depth.
- Poor at lessons learned, history repeats itself.
- We try to design to the ways that the pipeline actually fails, not just Barlow's equation. We design to the threats like third party damage and try to design for leak vs. rupture failures by controlling pressure, etc.

13. Does your organization constantly maintain a sense of vulnerability towards CEs? This means you do not become comfortable over time as typical events (not CEs) and safety issues reduce or no longer occur?

- See #5
- Trying to teach new engineers that the safety requirements were put in the 50-70's and more needs to be done than just the regulations and requirements. Trying to convince people that compliance does not mean you are safe and/or risk free.

14. How does your organization leverage and maintain its Institutional Knowledge related to CEs? As your experts retire, what is your organization doing to maintain their engineering controls and data analysis skills required to optimize risk decisions?

- Letting Sr. people go, or retiring, cannot replace deep experts with process and structure, need apprenticeship program for engineering excellence.
- Industry will lose 70% of core folks in 7 years, understands this, but is not doing anything about it.
- May be able to offset this loss with process to a degree, but not all of it.
- New generation comes up to speed faster using computer/internet tools; but wisdom and common sense and judgement come with time and experience.

15. What metrics does your company currently measure as precursors to CEs? What data is reviewed that impacts on-the-ground-realities? How do you know what information to look for and what questions to ask related to dealing with CEs?

- Only doing and reporting what PHMSA asks, minimum compliance and tracking, need to track near misses like aircraft industry, etc.
- Do not have good data and information on trends.
- Need to focus on leading vs. lagging indicators.

- Canada does a better job (maybe British influence) than U.S. for some reason. Canada focuses on process more and U.S. focuses on people more.

16. What are your organizations practices related to these core principles of prevention of catastrophic risks and CEs:

- Redundancy (i.e., diversification of systems) to prevent CEs
- Reliability Management (testing and preventative maintenance) to prevent CEs
- Safety Features in Control Systems to prevent CEs
- Multiple Barriers/Lines of Defense (if it occurs)
- Mitigation (if it occurs)

17. What technical risk methods does your organization currently employ? Here are some examples:

- Failure Modes and Effect Analysis (FMEA)
- Failure Modes and Effect Criticality Analysis (FMECA)
- Hazard and Operability Analysis (HAZOPS)
- Fault Tree Analysis (FTA)
- Event Tree Analysis (ETA)
- Monte Carlo Simulations
- Qualitative Risk Analysis
- Quantitative Risk Analysis
- Defense in Depth
- Structural Reliability Analysis and Methods

Appendix 2: A Brief Review of Defense in Depth Concepts

Military Underpinnings

The concept of defense in depth (DID) originates in military strategy where one wants to delay as opposed to prevent the advance of an attacker. The concept is centered around the principle that an attacker loses momentum with time as it covers a large area. A defender can therefore give up some territory in effort to stress an attacker's logistics supplies and/or spread out their numerically superior force. Then defensive counter-attacks can be waged against the enemy's weak points and drive them back. It is recognized that "buying time" causes additional casualties by yielding space.

Non-military Use

The idea of DID is now used to describe multi-layered (multi-barrier) or redundant protections for non-military situations, such as nuclear operations, fire preventions, engineering systems, information security, and others. We will focus on two areas in this white paper, first and briefly, engineering systems and fire prevention and then go into more detail on DID in the nuclear industry, which has a- mature DID culture and implementation.

Engineering

Defense in depth may also mean engineering which emphasizes redundancy – a system that keeps working when a component fails – over attempts to design components that will not fail in the first place. For example, an aircraft with four engines will be less likely to suffer total engine failure than a single-engine aircraft no matter how much effort goes into making the single engine reliable. However, Charles Perrow, author of Normal accidents, has said [69] that sometimes redundancies backfire and produce less, not more reliability. This may happen in three ways:

1. Redundant safety devices result in a more complex system, more prone to errors and accidents.
2. Redundancy may lead to shirking of responsibility among workers.
3. Redundancy may lead to increased production pressures, resulting in a system that operates at higher speeds, but less safely.

Extremely Complex Systems

"Normal" accidents, or system accidents, are so-called by Perrow because such accidents are inevitable in extremely complex systems. Given the characteristic of the system involved, multiple failures which interact with each other will occur, despite efforts to avoid them. Perrow said that operator error is a very common problem, many failures relate to

organizations rather than technology, and big accidents almost always have very small beginnings. [24] Such events appear trivial to begin with before unpredictably cascading through the system to create a large event with severe consequences. [26]

This body of work made the case for examining technological failures as the product of highly interacting systems, and highlighted organizational and management factors as the main causes of failures. Technological disasters could no longer be ascribed to isolated equipment malfunction, operator error or acts of God. [27]

Nuclear Industry Overview

U.S. non-military nuclear material is regulated by the U.S. Nuclear Regulatory Commission, which uses the concept of defense in depth when protecting the health and safety of the public from the hazards associated with nuclear materials. The NRC defines defense in depth [70] as creating multiple independent, and redundant, layers of protection, and response, to failures, accidents, or fires in power plants, see **Figure 38** [71]. For example, defense in depth means that if one fire suppression system fails, there will be another to back it up. The idea is that no single layer, no matter how robust, is exclusively relied upon; access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures are used. Defense in depth is designed to compensate for potential human and mechanical failures, which will occur. Any complex, close-coupled, system, no matter how well-engineered, cannot be said to be failure-proof. That is especially true if people operate controls that determine how the system performs.

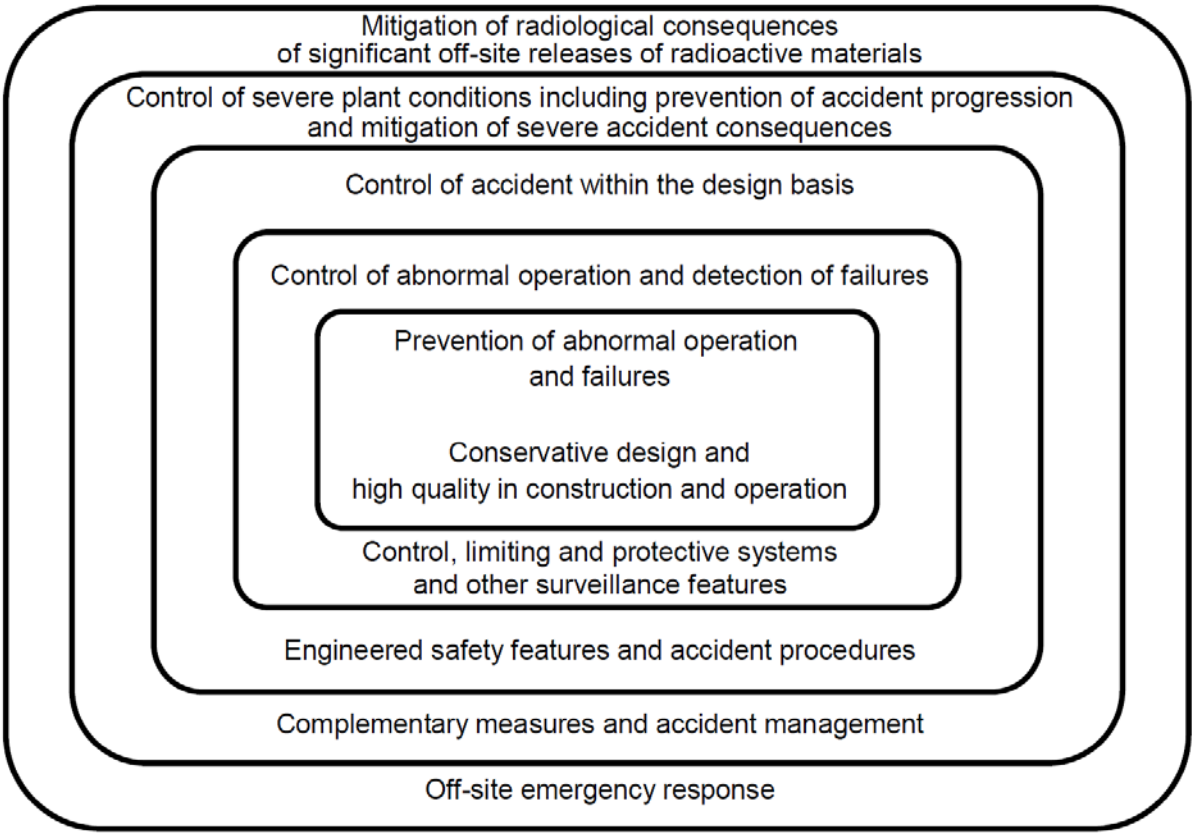


Figure 38. The defense in depth concept: purposes, methods and means (INSAG-10).

The nuclear industry will be used as an example to discuss defense in depth in greater detail and the related concepts will be mapped into the pipeline industry.

Defense in Depth Nuclear Industry Concepts - Adapted to Pipeline Systems

In this section we map the DID concept from the nuclear industry into the area of pipeline systems.

Two key references for DID in the U.S. and International nuclear industries are the International Nuclear Safety Advisory Group (INSAG) report, Defense in Depth in Nuclear Safety, INSAG-10 [71] and the U.S. Nuclear Regulatory Commission document SECY-13-0132 U.S. Nuclear Regulatory Commission Staff Recommendation for the Disposition of Recommendation 1 of the Near-Term Task Force Report; Enclosure 3: Defense-In-Depth Observations, and Detailed History (ML13277A421)[72].

General Concepts

A summary of the major concepts of these two documents along with other references is presented below as it might apply to the pipeline (natural gas and hazardous liquids) sector below:

1. Leverage continuous growth in knowledge, development of safety concepts, and the increase in expertise and experience gained from operating pipeline systems under normal and abnormal conditions, including accidents.
2. Consider both prevention and mitigation of incidents and accidents.
3. Consider Concepts of: design, operations, protection systems, safety features, external hazards, human factors, human-machine interfaces, training, quality assurance, automation, monitoring, diagnostic tools, accident management, multiple failures, emergency procedures and response, regulatory regime, safety culture, and probabilistic safety analysis.
4. Defense in depth can be implemented through design and operation to provide a graded protection against a wide variety of transients, incidents and accidents, including equipment failures and human errors within the pipeline system and events initiated outside the pipeline system.
5. A single failure at one level of defense or combinations of failures at more than one level of defense, will not propagate to jeopardize the defense in depth at subsequent levels.
6. The strength of the lines of defense depend on the specific risk posed by the pipeline system.

Summary of Defense-in-Depth

There is a common recognition that there is a lack of knowledge (or uncertainty) with regard to the design, construction, maintenance and operation of the pipeline system. We ask four questions related to defense in depth in pipeline systems:

1. Why is defense in depth needed?
2. What are the objectives of defense in depth?
3. What approaches or strategies should we adopt?
4. What are the Criteria for implementing defense in depth?

In answering the first question of why there is a need for defense-in-depth; it is to address the uncertainties in the design, construction, maintenance and operation of the pipeline system.

The objective of defense-in-depth is to avert damage to the system thereby ensuring the protection of public health and safety while maintaining an acceptably low probability of accidents.

Regarding approaches or strategies that have been defined for defense-in-depth; there are similar concepts of basic protections which involve, at a high level, prevention of accidents and mitigation of accidents. Prevention of accident can be defined as preventing the occurrence of an event to preventing the progression of an accident sequence. Mitigation of an accident can be defined from ending the progression of a severe accident, containing the effects of a severe accident, to mitigating the consequences of a severe accident. This approach or strategy is similar to the concept of *multiple barriers* which are achieving the same goal.

The criteria for implementing the approaches or strategies that have been defined for defense-in-depth, there are very similar criteria that include, for example, quality assurance, redundancy, independence, oversight, containment, and emergency planning.

Objectives

1. Compensate for potential human and component failures,
2. Maintain effectiveness of barrier by averting damage to the system and the barriers themselves, and
3. Protect the public and the environment from harm in the event these barriers are not fully effective.

Strategy

1. First, prevent accidents, and
2. Second, if prevention fails, to limit (mitigate) potential consequences and prevent evolution to more serious conditions.

Interrelated Prerequisites

Conservatism

1. Broadly applied at the first three levels of defense.
2. Made for site selection, design, construction, commissioning, and operation.
3. Conservative assumptions and safety margins are also considered in the review of modifications, the assessment of ageing effects on the systems, periodic safety reassessment, and the development of emergency plans.
4. At Levels 4 and 5, best estimate considerations are increasingly important.

Quality Assurance

1. Each Level of defense is effective only if the quality of design, materials, components, systems, operations, and maintenance can be relied upon.
2. Quality assurance programs can ensure development of a safe design, as well as the intent of the design is achieved as built, operated, and maintained.

Safety Culture

1. Organizations and individuals involved in activities that may have an impact at each Level of defense need to be committed to a strong safety culture.
2. Some aspects of system safety are difficult to assess quantitatively by probabilistic methods. Examples include the influence of operator organization and safety culture, as well as aspects such as common cause effects, reliability of software, some types of human error, and internal and external hazards. It is therefore an essential task of deterministic system design to limit the influence of such aspects of safety.

Levels of Defense-in-Depth

Table 5. Levels of Defense, Objective, and Essential Means

Level of Defense in Depth	Objective	Essential Means
Level 1	Prevent abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control abnormal operations and detect failures	Control, limiting, and protection systems and other surveillance features
Level 3	Control accidents within design basis	Engineered safety features and accident prevention
Level 4	Control severe system conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of significant consequences and releases	Off-site emergency response

Level 1. Prevention of abnormal operation and failures

1. Conservative design to confine the hazardous material and minimize deviations from normal operating conditions, including normal transients.
2. Safety provisions at Level 1 include choice of pipeline location, design, manufacturing, construction, commissioning, operating, and maintenance.
3. Clearly define normal and abnormal operating conditions.
4. Provide adequate margins of design for the system and components, including robustness and resistance to accidents. Focus on preventing the need for Levels 2 and 3.
5. Careful selection of materials and fabrication processes, include extensive testing.
6. Comprehensive training of the properly selected personnel, all consistent with a sound safety culture.
7. Adequate operating instructions/manuals and reliable system monitoring of status and operating conditions.
8. Record, evaluate, and utilize operator experience.
9. Comprehensive preventative maintenance prioritized by safety significance and reliability requirements of the system.
10. Level 1 provides initial basis for external and internal hazards (e.g., earthquakes, lighting strikes, fire, flooding, third party damage, etc.).

Level 2. Control of abnormal operation and detection of failures

1. Incorporate inherent system features and systems to control abnormal operation, with focus on items capable of causing further deterioration in system status.
2. Objective is to bring the system back to normal operating conditions as soon as possible.
3. Automatic control systems can provide acute actions before system limitations are met, e.g. remote control and automatic shutting valves, relief valves, etc.
4. Ongoing surveillance of quality and compliance through in-service inspection and periodic testing of systems and components to detect degradation of equipment and systems.

Level 3. Control of accidents within the design basis

1. Level 3 is when accidents occur despite prevention efforts.
2. Engineered safety features and protection systems prevent evolution towards severe accidents and confine the hazardous material being transported.
3. Design and operating procedures are aimed at maintaining the effectiveness of barriers from product release in event of an accident. Design feature principles include:
    a. Redundancy,

b. Prevention of common failure modes due to internal or external hazards, by physical or spatial separation and protections,
c. Prevention of common failure modes due to human interventions related to design, manufacturing, construction, commissioning, maintenance, or other related factors; this is achieved by diversity or redundancy,
d. Automation to reduce vulnerability to human failure, at least in the initial phase of an incident or accident,
e. A system that is testable to performance standards,
f. Qualification of systems and components for specific environments that could result from an accident or external hazard.

Level 4. Control of severe conditions including prevention of accident progression and mitigation of the consequences of a severe accident

1. It is assumed that the first three levels will ensure maintenance of the system structural integrity and limit hazards for members of the public. The broad aim of the fourth level of defense is to ensure the likelihood of an accident with severe damage (e.g., large pipeline rupture and fire) is kept as low as reasonably achievable. This does not excuse prior level requirements, especially proper designs.
2. Consideration is given to severe system conditions that were not explicitly addressed in the original system designs (Levels 1 to 3), owning to their very low probabilities. These types of conditions are usually caused by multiple failures or extremely unlikely events. Ancillary and support systems are designed, manufactured, constructed, and commissioned to address these events.
3. Measures for accident management are also aimed to control the course of severe accidents and to mitigate their consequences. This could include preventative and mitigative measures for severe situations like double guillotine ruptures of transmission lines in high consequence areas.
4. For offsite emergency response, the measures are preventative.
5. Essential objectives of accident management are:
    a. Monitor the main system status,
    b. Regaining control of the system and delaying further deterioration, and implementing on-site and off-site emergency response.
6. The role of the operator is vital in actuating hardware features for accident management and to take action beyond the originally intended functions of the system or using temporary or ad hoc systems.
7. Adequate staff preparation and training for such conditions is a prerequisite for effective accident management.

8. Managerial provisions like an on-site emergency plan are also necessary.

Level 5. Mitigation of the consequences of significant external releases of hazardous materials

1. Even if Levels 1 to 4 limit consequences of severe accidents, one must address off-site emergency plans.
2. The responsible authorities take the corresponding actions on the advice of the operating organization and the regulatory body.
3. Off-site emergency procedures are prepared in consultation with the operating organization and the authorities in charge and comply with agreements.
4. Both on-site and off-site emergency plans are exercised periodically to the extent necessary to ensure the readiness of the organizations involved.

Defense in depth implementation in operations [73]

The defense in depth concept is fully applicable for operational activities. An outline of this mapping to operational activities (and associated documents) is presented below.

Level 1: Prevention

- Plant organization, staff selection and training;
- Normal operation procedures;
- Implementation of the technical specifications.

Level 2: Surveillance

- Periodic testing program;
- Preventive maintenance program;
- Incident detection and analysis.

Level 3: Mitigation

- Incident and accident procedures.

Level 4: Accident management

- Beyond design basis accident procedure;
- Internal emergency plan (links with external emergency plan).

Level 5: Emergency response

- External emergency plan.

Observability in Depth – A Suggested Compliment to Defense in Depth

Recent work out of the Georgia Institute of Technology [74] suggests some drawbacks with the concept of defense in depth, which include its potential for concealing the occurrence of hazardous states in a system, and more generally rendering the latter more opaque for its operators and managers, resulting in safety blind spots.

This shrinks the time window for operators to identify an unfolding hazardous condition or situation and intervene. To prevent this drawback from materializing, a safety principle termed "observability-in-depth" has been developed. It is a set of provisions technical, operational, and organizational designed to enable the monitoring and identification of emerging hazardous conditions and accident pathogens (latent failures) in real-time and over different time-scales.

Observability-in-depth requires the monitoring of conditions of all safety barriers that implement defense-in-depth; and supports sense making of identified hazardous conditions, and the understanding of potential accident sequences that might follow (i.e., how they can propagate). It is defined as:

1. The set of provisions, technical, operational, and organizational designed to enable the monitoring and identification of emerging hazardous conditions and accident pathogens in real-time and over different time-scales;
2. The monitoring / reliable estimation of the conditions and status of all safety barriers that implement the defense-in-depth strategy (especially if they are degraded or breached);
3. The sense making of the emerging hazardous conditions and the understanding of potential accident sequences that might follow (and how they can propagate).

In this sense, observability-in-depth should be thought of as a complement to the well-established defense-in-depth safety strategy

Observability-in-depth is an ***information***-a***centric*** principle, and its importance in accident prevention is in the value of the information it provides and actions or safety interventions it spurs.

To appreciate the causal dimension of "depth" in observability-in-depth, see Figure 2, which represents hazardous transition/escalation in an accident sequence (states, S) has a set of underlying causes, and Figure 2 includes the underlying causes of a transition from state Si to Sj in the form of a Fault Tree.

The condition Pi in the fault tree is a latent failure or accident pathogen; it does not have a visible effect on the system behavior or operation, until the second condition in its AND gate occurs. If the system reaches state Si, the hazardous transition to Sj will occur, thus further advancing the accident sequence.

The ability to observe such latent causal factors or accident pathogens in an accident sequence before they have a visible effect on the system operation is another aspect of the

depthness of observability. In other words, the "further down" a fault tree are adverse conditions identified, the more depth there is to the ob-servability-in-depth principle.

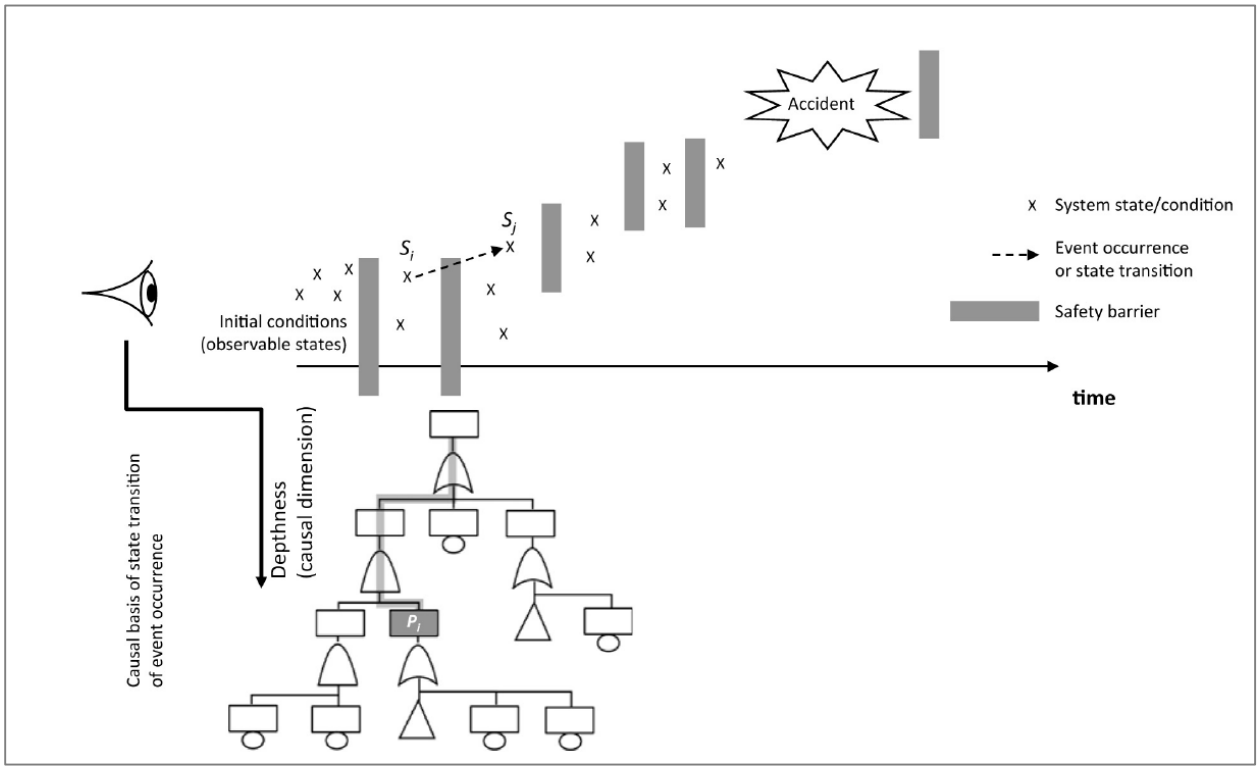


Figure 39. Schematic Illustration of an Accident Sequence, Defense-in-depth, and the Causal Dimension of "Depth" in Observability-in-depth

Appendix 3: Analysis of Human Causal Elements in Catastrophic Events

The summaries appearing in text boxes below are directly excerpted from: *Chernov, Dmitry; Sornette, Didier (2015-10-27). Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human Fallibility. Springer International Publishing. Kindle Edition*.

All **bold text accents** are those of the authors Chernov and Sornette.

These reviews provide an interesting review of 21 catastrophic events that occurred around the world in the industrial, financial, military and social sectors and natural disasters. Several more fiascos in the retail production industry are reviewed as well. Chernov and Sornette provide a useful summary of why risks were concealed in each of these catastrophes and fiascos. These summaries are useful in addressing the human element in catastrophes. An analysis of these underlying human causal elements provides insights into what a Knowledge Management Framework should provide if it is to be effective in identifying potential sequences of interactions that could result in catastrophes and thus help prevent them.

Three Mile Island Nuclear Accident (USA, 1979)

The Three Mile Island Nuclear Power Plant (NPP) is located 15 km from Harrisburg, Pennsylvania, 140 km from Washington, DC and 240 km from New York. The plant has two pressurized water reactors (PWRs) with a generating capacity of 1700 megawatts (MW). When the largest civil nuclear accident the world had ever seen occurred there at the end of March 1979, Unit 2 (TMI-2) had only been in commercial service for about three months and was operating at 97 % capacity. Unit 1 was shut down for refueling. The reactor core of TMI-2 contained around 100 tons of uranium fuel.

…

Three Mile Island Nuclear Accident: Why Risks Were Concealed

- The US government and the NRC shared an interest in developing the domestic civil nuclear industry, as part of a larger program to ensure the energy independence of the country after the severe oil crises of 1973 and 1979. This led to a perception among industry executives that **increasing the production of electricity took priority over safety matters**.
- **Wishful thinking/ self-deception among decision makers**, who persuaded themselves that minor accidents did not merit close scrutiny; that the probability of a multi-factor malfunction of hardware was marginal; that the influence of human factors on the operation of a reactor during an emergency was minimal; and that the worst-case scenario— meltdown or decapsulation of a reactor vessel— could never happen.
- Government and the nuclear industry had weak control over the complex systems involved, and had only a **fragmentary perception of the whole picture of risks**. Key decision makers were ignorant of other accidents or near-miss cases within the organization or the wider industry, nationally or abroad.
- There was **no system for managing knowledge about risks within the industry** (exchange, accumulation, systematization and transmission).
- There was **no industry-wide risk assessment system for timely evaluation of the condition of nuclear power plants**. Both operators and management at TMI-2 misjudged the status of the plant, causing them to give misleading information to other audiences and delaying the measures that needed to be taken to cool the reactor.

Chernov, Dmitry; Sornette, Didier (2015-10-27). Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human Fallibility. Springer International Publishing. Kindle Edition.

Bhopal Pesticide Plant Gas Leak (India, 1984)

During the night between December 2 and 3, 1984, at the pesticide plant in Bhopal, India, more than 40 tons of methyl isocyanide (MIC) and other gases leaked into the atmosphere. MIC is an intermediate in pesticide production processes and has an extremely toxic impact on human health. Over the days following the accident, from 3,000 to 10,000 citizens of Bhopal died, 100,000 were injured with irreversible changes in their health and more than 500,000 were exposed to toxic gases, [101] out of a total population of around 850,000 residents.

…

Bhopal Pesticide Plant Gas Leak: Why Risks Were Concealed

- The Indian government's desire to reach national industrial independence, and its negligence to reveal details of deliberate violations of safety rules at the plant. **The lack of experience or qualifications of government representatives**, which did not allow them to recognize the disastrous state of the plant years before the accident. In addition, without sufficient control by the parent corporation over Union Carbide India Limited, **management at the plant could manipulate data about real conditions at the plant** without fear to be punished by representatives of Union Carbide Corporation and Indian authorities.
- The **desire of Indian managers to appear in a good light** in the eyes of Union Carbide Corporation executives motivated them to **play down the existence of massive safety imperfections at the plant**.
- The chronic unprofitability of the Bhopal plant, and **reluctance of plant managers to reveal the risks involved to local authorities that would likely oblige them to incur additional expense on safety measures**, or to suffer from increased wages to reward employees for hazardous work that would be known as such, or to support the costs for relocating the shantytowns, and so on.
- The **reluctance of Union Carbide Corporation executives to reveal statistics of accidents** at the West Virginia MIC plant, and the extreme danger posed by MIC, to their international subdivisions.
- **False reassurance/ self-suggestion/ self-deception among American and Indian executives** about the maximum possible scale of any chemical accident at the plant.

Challenger Space Shuttle Disaster (USA, 1986)

On January 28, 1986 at 11: 39 a.m., the Space Shuttle Challenger exploded in the second minute after lift-off from the Kennedy Space Center. This resulted in the deaths of all seven astronauts.

…

Challenger Space Shuttle Disaster: Why Risks Were Concealed

- Unrealistic projections about the launch schedule and a **culture of continuously rushed organization**. NASA management's desire to demonstrate to Congress and the military that the Shuttle program could send any load to space in any weather conditions on a timely basis.
- **Habituation/ wishful thinking/ false reassurance/ self-suggestion/ self-deception** among NASA and MTI decision-makers about the supposedly minuscule probability of a failure of the Shuttle. This also led to an attitude of arrogance among NASA executives.
- MTI management's **fear of losing their main client** (NASA). General problem of incentives in risk management: if MTI had remained adamant and advised against the flight, how would the "success" of no disaster resulting from the flight cancellation be rewarded?
- The **reluctance of MTI management to confess their own mistakes** in the design of solid rocket boosters and in ignoring previous warnings (damage to the O-rings during previous launches).
- **"Success at any price" and "no bad news" culture**
- MTI management's **fear of being accused of incompetence**. This question was also connected to **national security secrecy** because MTI was the supplier of solid rocket boosters for several American ballistic missiles.

Chernov, Dmitry; Sornette, Didier (2015-10-27). Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human Fallibility. Springer International Publishing. Kindle Edition.

Chernobyl Nuclear Disaster (USSR, 1986)

On April 26, 1986 at 1: 23 a.m., during an experiment with the emergency power supply system at the Chernobyl nuclear power plant, a power excursion occurred in the RBMK-1000 Reactor #4 that led the reactor to burn uncontrollably. The plant was located in the Ukrainian Soviet Socialist Republic, which at the time was part of the Soviet Union. It was 700 km away from Moscow, 320 km from Minsk, and 140 km from Kiev. Because the reactor did not have a containment dome, the explosion led to the release into the atmosphere of 7.7 tons of uranium oxide fuel, amounting to 4 % of the total contained in the reactor; 96 % of the fuel, or 185 tons of uranium, stayed in the reactor. [190] Huge regions of Belarus, Russia and Ukraine were contaminated, [191] and traces of chemical elements from Chernobyl NPP were later found in Northern and Western Europe. The accident resulted in the release of approximately 5200 PBq (1 PBq (Penta Becquerels) = 1015 disintegrations per second) [192] of radioactive substances into the atmosphere. [193] This was the first accident since the beginning of the nuclear age to be classified as a level 7 event—the maximum level according to the International Nuclear Event Scale. More than 116,000 people were evacuated from the 30 km zone around the NPP. [194] Two workers died after the explosion, and 28 firefighters died in the first three months following the accident. Estimates from various sources of the total number of victims of the Chernobyl accident remain contradictory because of political indecisiveness, different scientific approaches and the unavailability of health statistics from Soviet officials. In 2005, the UN report "Chernobyl's Legacy: Health, Environmental and Socio-Economic Impacts" contained a statement from an international team of more than 100 scientists that up to about 4000 people could eventually die of radiation from the Chernobyl NPP accident. [195] The financial cost of the Chernobyl disaster remains controversial too. Mikhail Gorbachev, General Secretary of the Communist Party of the Soviet Union from 1985 until 1991, cited that the Soviet Union spent 18 billion rubles[196] (approximately US $ 27 billion[197]) on dealing with the consequences of the disaster. The government budget of the USSR was around 360 billion rubles from 1985– 1987,[198] and the GNP in that period was around 780– 800 billion rubles; so the expenses for the response to Chernobyl were 5 % of the annual Soviet budget, or approximately 2 % of GNP. According to estimates from academician Valery Legasov, a key member of the government investigation committee on the Chernobyl disaster, the total damage caused by the Chernobyl accident was in fact 300 billion rubles in pre-1990 prices, or approximately US $ 450 billion (of 1990 US $). This amount exceeds the combined profits of all Soviet nuclear power plants for the duration of their existence. [199]

Chernobyl Nuclear Disaster (USSR, 1986) continued

…

Chernobyl Nuclear Disaster: Why Risks Were Concealed

- **Short-term profitability**, and the production of cheap nuclear energy in the Soviet Union, **took priority over the long-term resilience of the Soviet nuclear industry** and the protection of the environment.
- **A "rush culture"** was established by the Politburo in order to increase the speed of construction of nuclear power plants to meet urgent domestic energy needs. This environment of constant haste encouraged people to ignore possible measures to correct minor shortcomings of the reactor, which were perceived by developers as insignificant and unlikely to cause a serious problem in practice.

Chernov, Dmitry; Sornette, Didier (2015-10-27). Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human Fallibility. Springer International Publishing. Kindle Edition.

Exxon Valdez Oil Spill (USA, 1989)

On March 24, 1989 at 12: 04 a.m., the oil tanker Exxon Valdez ran aground on Bligh Reef in Prince William Sound in Alaska (USA). The vessel was carrying approximately 1.2 million barrels of North Slope oil, which was loaded in port Valdez (40 km from the site of the accident). In the collision, eight of the ship's eleven cargo tanks were punctured, resulting in the leakage of around 250,000 barrels of oil during the first 3.5 h after the accident. [287] The total amount of leaked oil is estimated to be between 250,000 and 260,000 barrels. [288] The slow and inadequate response to the spill resulted in extensive oil contamination of 2000 km of pristine coastline on the Gulf of Alaska.

…

Exxon Valdez Oil Spill: Why Risks Were Concealed

- **Short-term profitability won priority over the long-term sustainability** of the Trans-Alaska Pipeline System and over environmental protection.
- **Habituation/ wishful thinking/ overconfidence/ self-suggestion/ self-deception** among representatives of the Alyeska consortium about the low probability of a severe oil spill in Prince William Sound after more than a decade of intensive shipping of supertankers. This led the consortium being reluctant to admit the importance of readiness in the case of a large oil spill and to pay for a high-capacity oil spill response team.
- **Lack of consideration of scenarios** that could lead to large oil spills, such as a super-tanker collision: only past spills that had occurred were considered as representative of possible future events. This is well-known as historical sampling bias.
- **Cozy relationships between the Alyeska consortium and representatives of the State of Alaska**, who allowed Alyeska to exert a strong influence on state government decisions concerning the regulations of the consortium's activity, the funding of the state government environmental regulator (ADEC) or heeding its warnings. This helped the Alyeska consortium to conceal for years and with impunity the risks resulting from the inadequately prepared oil spill

Exxon Valdez Oil Spill (USA, 1989) continued

- A **fragmented perception of risks** (i.e., the **absence of the whole picture of risks**) among decision-makers of the stakeholders led companies to resist revealing their own risks to members of the oil spill response team. Ultimately, nobody understood the risks existing in other involved organizations.
- A **permanent rush culture** among the crew of Exxon Valdez, because of unrealistic projections about the shipping schedule, which compelled the crew to conceal their chronic fatigue from employers. **Crew members were also afraid to lose their jobs** during the depression occurring in the oil supertanker market.

Chernov, Dmitry; Sornette, Didier (2015-10-27). Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human Fallibility. Springer International Publishing. Kindle Edition.

Ufa Train Disaster (USSR, 1989)

On the night of June 3– 4, 1989, about 50 km from the city of Ufa in the Bashkiria region of the Ural Mountains, the Western Siberia/ Ural/ Volga natural gas liquids pipeline ruptured, causing the build-up of a potentially explosive hydrocarbon-air mixture. At 1: 15 a.m., two passenger trains came into the zone of gas contamination, passing in opposite directions with a total of 37 railroad cars carrying 1284 passengers and 86 crew members. Apparently, a spark from a susceptor on one of the electric locomotives ignited the lethal gas mixture, causing an explosion in which 575 people perished and 623 were injured. [325] The explosion, equivalent to 300 tons of TNT, became the most deadly railway accident in the history of the Soviet Union and of the Russian Federation.

…

UFA Train Disaster: Why Risks Were Concealed

- **Short-term tasks** (timeline, productivity, carrier opportunities and awards) took priority over long-term consequences (quality of works, safety and reliability of the pipeline in the long term).
- There was a **rush work culture** prevailing during development and construction of the pipeline.
- **Executives of the Soviet Ministry of Petroleum were reluctant of to admit their own mistakes** during the redesigning and lobbying for the pipeline, or their negligence during its subsequent operation (long-term spending cuts on the maintenance of the pipeline; cancellation of the telemetry system for real-time monitoring of leaks; scrapping the helicopter and ground monitoring teams; poor quality of reconstruction works, and so on).
- The **lack or absence of communication between representatives of the pipeline, Soviet railways, and local residents**, in spite of the fact that the pipeline had 50 leakage incidents over 3 years and was constructed parallel to the railway for a length of more than 270 km. In addition, **nobody could imagine that such a catastrophic event could ever take place**.
- The fact that railway traffic controllers had **no authority** to preventively halt traffic on any section of the Trans-Siberian railway during the detailed investigation of the causes of the gas smell.

Chernov, Dmitry; Sornette, Didier (2015-10-27). Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human Fallibility . Springer International Publishing. Kindle Edition.

Sayano-Shushenskaya Hydropower Station Disaster (Russia, 2009)

The Sayano-Shushenskaya Hydropower Station (SSHPS), on the Yenisei River in south-central Siberia, is the largest hydroelectric power plant and the largest power producing facility in Russia in terms of its installed capacity (6400 MW). The station produces 2 % of all Russian electricity, and 15 % of the country's hydroelectricity. In 2009, the station was the sixth largest hydroelectric plant in the world, exceeded in average annual power generation only by Three Gorges in China, Itaipu in Brazil/ Paraguay, Guri in Venezuela, Tucuruí in Brazil, and Churchill Falls in Canada. On August 17, 2009, the rotor of SSHPS Turbine 2 shot out. This flooded the turbine hall of the station, damaged nine of SSHPS's ten turbines and killed 75 station workers. After the disaster, the Minister of Emergency Situations for the Russian Federation evaluated the event as "the biggest man-made emergency situation [in Russia] in the past 25 years [after Chernobyl] – for its scale of destruction, for the scale of losses it entails for our energy industry and our economy". [356] Recovery costs after the accident came to over US $ 1.5 billion and the reconstruction of the station took more than 5 years.

…

Sayano-Shushenskaya Hydropower Station Accident: Why Risks Were Concealed

- The Politburo and State Planning Commission **focused on the short-term reduction of safety costs** through the redesign of the station, **and demanded constant rush** during the construction phase, because they wanted to accelerate the introduction of new energy facilities to meet the needs of the national economy.
- There was a general **reluctance** within the Soviet and Russian electro-energetics industry **to investigate in detail the causes of previous accidents/ near-miss cases**, or to transmit the results among decision-makers, so that the remedies learned from the experience of previous accidents on other electro-energetical facilities could be implemented across the industry.
- After the collapse of the Soviet Union, the liberal-oriented government **gave priority to short-term financial results** in the operation of electro-energetical facilities, and to indicators of market capitalization, over the long-term reliability of Russian electro-energetics.
- **Habituation/ wishful thinking/ overconfidence/ self-suggestion/ self-deception**: engineers and management at the station believed that a severe turbine accident was highly unlikely, because of the station's 30-year history of generally safe operations.

Sayano-Shushenskaya Hydropower Station Disaster (Russia, 2009) continued

- **Habituation/ wishful thinking/ overconfidence/ self-suggestion/ self-deception**: engineers and management at the station believed that a severe turbine accident was highly unlikely, because of the station's 30-year history of generally safe operations.
- SSHPS managers were afraid of **potential criminal charges** for using questionable repair tender schemes, which they felt obliged to implement after the misguided reorganization imposed by RAO UES. They were also afraid to seem incompetent in the eyes of RusHydro's superiors.
- **The Russian government was unwilling to admit its own mistakes in pushing through unreasoned free-market reforms of Russian electro-energetics**, or to admit the evident failure of its reorganization of RAO UES. This led to a situation where only SSHPS staff faced criminal charges after the accident.

Chernov, Dmitry; Sornette, Didier (2015-10-27). Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human Fallibility. Springer International Publishing. Kindle Edition.

Deepwater Horizon Oil Spill (USA, 2010)

From January to April 2010, floating in the Gulf of Mexico 66 km from the coast of Louisiana State, the Deepwater Horizon oil platform was drilling the Macondo exploratory well. The total depth of the well was 6500 m: 1500 m below sea level and 4000 m beneath the seafloor in Block 252 of the Mississippi Canyon. The proven reserves of the field were 110 million barrels[424]; the potential income from extraction of this amount of oil was approximately US $ 10 billion. The platform was owned by Transocean Ltd., the largest offshore drilling operator in the world. BP (formerly known as British Petroleum) leased the rig for exploration of the Macondo field. Halliburton Company, one of the world's largest oilfields services companies, was engaged as the cementing contractor. On April 20th, 2010 at 9: 45 p.m. US Central Time, a blowout of oil, gas and concrete from the well occurred on the Deepwater Horizon platform, causing an explosion and a fire that sunk the platform. There were 126 crewmembers on the rig during the accident; 11 people perished and 17 were injured. The rest of the crew survived unharmed, but the accident led to oil being discharged from the well for 87 days— for a total of 3.19 million barrels. [425] This was the third largest oil spill in the history of the oil industry, after the Kuwaiti oil fires in 1991 where the approximate discharge was 10 million barrels and the blowout at Lakeview Gusher Number One oil well in Kern County, California, which was out of control for nine months in 1910– 1911 and led to the release of approximately 9 million barrels. BP was forced to cover all expenses incurred in shutting down the deepwater leak and in cleaning up the American part of the Gulf of Mexico coastline— an area where 14 million inhabitants reside— contaminated by spilled oil. In addition, they paid compensation to the fishing and coastal tourism industries in the area and a fine issued by the U.S. government. BP's total losses from the accident were estimated at US $ 46 billion (US $ 28 billion was spent on the accident and $ 18 billion on additional government fines and penalties[426]) and by June 2010, BP's stock market value had fallen by US $ 70 billion. [427] Because of the disaster, the U.S. government suspended any deepwater offshore activity in the United States for 6 months. In the middle of June 2010, the President of the United States Barack Obama declared: "this oil spill is the worst environmental disaster America has ever faced". More than 47,000 people and 7000 vessels[428] took part in the response to the spill.

…

Chernov, Dmitry; Sornette, Didier (2015-10-27). Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human Fallibility. Springer International Publishing. Kindle Edition.

Deepwater Horizon Oil Spil continued

Why Risks Were Concealed

- **Habituation/ wishful thinking/ false reassurance/ self-deception** among representatives of the Minerals Management Service, BP, Halliburton Company, and Transocean Ltd. in assuming that a massive well blowout on American deepwater oil fields was unlikely.
- The **nationalistic arrogance of American regulators and oil companies**: they ignored international experience of previous disasters on deepwater drilling platforms, and assumed that they could neglect advanced oil drilling requirements because the Americans were pioneers in deepwater oil drilling and had the most skilled staff.
- **Deliberate lobbying by the American oil industry to persuade government to deregulate the sector and massively reduce the budget of the regulators**: unattractive wages, lack of skilled staff, inadequately qualified government officers, and so on. This led to a situation where regulators began to rely on information concerning new technologies from, and on the experience of, oil companies and their contractors, the very entities they were supposed to independently assess and regulate; as a result, **regulators failed to identify systemic failures in risk management, which the industry was trying to hide from regulators and the public**.
- **Fragmentary risk perception (failure to see the whole picture of risks) and lack of communication among representatives of the different organizations** working on the project about the real risks involved.
- **Rush during drilling because of delays in the schedule and cost overrun**, which encouraged those involved to ignore warnings and conceal information from other participants about defects during the cementing job in order to save time and money.

Chernov, Dmitry; Sornette, Didier (2015-10-27). Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human Fallibility . Springer International Publishing. Kindle Edition.

Raspadskaya Coal Mine Burnout (Russia, 2010)

In 2006, the Raspadskaya coal mine together with other mines managed by the open joint stock company (OJS) "Raspadskaya" had 781 million tons of coal reserves, but only 22 million tons were extracted by 2008.[482] The company still had more than 750 million tons of coal reserves— assets that could lead to substantial profits for their owners for decades to come. The coal company was very profitable: in 2009, its profitability was an incredible 51 %, while Gazprom, the Russian natural gas giant, exhibited a profitability of 36 %, and Lukoil, the largest Russian private oil company, of only around 17 %. [483] The Raspadskaya coal mine itself was the largest underground mine in Russia with reserves of 450 million tons of coking coal: the mine produced up to 20 % of the coking coal in Russia and was among the top ten coking coal producers in the world. It was located in the Kuznetsk coal basin (Kuzbass) in the southern part of Western Siberia. On the night of 8 to 9 May 2010, two blowouts occurred at the mine. As a result, 91 people were killed and 94 injured. The blowouts ignited a huge underground fire, which continued to burn for years, destroying 300 km of coal roadways and making it one of the worst in the history of coal mining worldwide.

…

Raspadskaya Coal Mine Burnout: Why Risks Were Concealed

- The owners and management focused on **short-term profitability instead of the long-term resilience of the coal mining business**. They created a sophisticated unofficial payroll scheme, which motivated coalminers to knowingly break safety rules. As a result, miners were potentially implicated in any possible methane blowout. This approach ensured that miners kept quiet about risky working practices.
- **Government oversight over Russian coalmining had been deregulated**, which allowed the management of the coalmine to violate safety rules with impunity.
- **Habituation/ wishful thinking/ overconfidence/ self-suggestion/ self-deception**: the owners and management of the mine totally underestimated the impact of a possible blowout of methane/ coal-dust/ air mixture during the intensive exploration of methane-saturated coal belts by powerful coal-plow machines, in parallel with the systematic desensitization of the methane detectors.

Chernov, Dmitry; Sornette, Didier (2015-10-27). Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human Fallibility. Springer International Publishing. Kindle Edition.

Fukushima-Daiichi Nuclear Disaster (Japan, 2011)

On March 11, 2011 at 2: 46 p.m., a seaquake of magnitude 9.0– 9.2 on the Richter scale occurred 70 km from the east coast of the Tohoku region in Japan. This was the largest earthquake ever recorded in Japan, and the United States Geological Survey considered that it was the fifth largest recorded worldwide since 1900.[504] The earthquake generated a large-scale tsunami, which reached the coastlines of Iwate, Miyagi and Fukushima prefectures approximately 50 min after the main shock, destroying hundreds of kilometers of coastline infrastructure and killing more than 18,800 people. [505] There were five NPPs located in the disaster zone on the east coast of Japan. Several were hit by the tsunami but, at the Fukushima-Daiichi plant owned by Tokyo Electric Power Co. (TEPCO), the largest electric utility in Japan, it led to a severe nuclear disaster— level 7, the highest level on the International Nuclear Event Scale. The plant had 6 reactors (Units 1– 6) and large pools with spent nuclear fuel, but only Units 1– 3 were operating when the seaquake occurred: Units 5 and 6 were shut down for routine inspection, and Unit 4 was on reconstruction. The emergency shutdown (SCRAM) system on all operating reactors was activated successfully after the main shock. The maximum ground acceleration at the Fukushima-Daiichi plant was [550] Gal (550 cm/ s), [506] while the containment vessels were designed to retain functionality up to a seismic ground acceleration of 270 Gal and important buildings, structures, and equipment piping systems were designed to withstand 180 Gal. [507] Although the ground acceleration of the seaquake was beyond design limits, Unit 1 only had a leakage of coolant. [508] However, the plant lost all AC power sources because the earthquake had destroyed both external transmission lines and the Shin-Fukushima transformer station. DC power sources (diesel generators and batteries) generated electricity to cool the reactors for the next 51 min— until the tsunami reached the plant. [509] The maximum designed height of the protective seawall of the NPP was 5.7 m. [510] Vulnerable objects like seawater pumps were located beyond the seawall— 4 m above sea level; diesel-generators and batteries were inside the reactor buildings— 10 m above sea level. [511] But the tsunami waves generated by the Tohoku seaquake had built up to a height of 14–15.5 m by the time they hit the plant. [512] As a result, Fukushima-Daiichi NPP lost all sources of electricity to cool the reactors of Units 1, 2 and the spent fuel pool of Unit 4;

Fukushima-Daiichi Nuclear Disaster (Japan, 2011) continued 1

Unit 3 had battery power for about 30 h; emergency diesel engines provided emergency power only to Units 5 and 6. Damage to the reactor core – and the resulting meltdown of nuclear fuel— began on Unit 1 3 h and 15 min after the tsunami struck, on Unit 3 after 43 h and on Unit 2 after 76 h. [513] There were 257 tons of nuclear fuel in the three operational reactors— Units 1 and 2 were fuelled by low-enriched uranium (LEU) and Unit 3 was fuelled by mixed oxide (MOX) fuel that contained plutonium— and 264 tons of spent nuclear fuel in the pool of Unit 4 at time of the disaster. [514, 515] The accident resulted in the release of approximately 900– 940 PBq of radioactive substances into the atmosphere, [516, 517] compared with the 5200 PBq estimated for the 1986 Chernobyl accident. Thus, the Japanese government reported to the International Atomic Energy Agency (IAEA) that the release was 1/ 6 of the emissions from the Chernobyl accident when converted to iodine. One hundred and fifty thousand residents were evacuated for a long time[518] because of radioactive contamination: 1800 km2 of the Fukushima Prefecture have levels that would give a potential cumulative dose of 5 mSv/ year or more. [519]

Fukushima-Daiichi Nuclear Disaster: Why Risks Were Concealed

- The distinctive position of the nuclear industry within the Japanese economy and the **misplaced loyalty of regulators concerning shortcomings in the design and operation of Japanese NPPs**, which allowed plant operators to neglect basic safety rules and conceal the occurrence of many safety violations from regulators and the public with impunity.
- The **national arrogance of both executives and regulators in the Japanese nuclear industry**, who refused to learn from the experience of other countries that had faced nuclear accidents, or to implement IAEA's recommendations and advanced safety requirements. The Japanese preferred to rely on their supposed technical superiority over the rest of the world. They assumed that falsifying data about minor equipment faults would never lead to catastrophic results and that the Japanese attitude toward work would always compensate for minor imperfections in reactor design during natural disasters.
- **Habituation/ wishful thinking/ overconfidence/ self-suggestion/ self-suggestion/ self-deception** among representatives of the Japanese nuclear industry concerning the low probability of a severe nuclear accident caused by a tsunami.

Fukushima-Daiichi Nuclear Disaster (Japan, 2011) continued 2

- TEPCO's focus on the **short-term profitability of operations and on ongoing cost reduction** provoked reluctance among executives to reveal the risks of NPPs— whether to IAEA specialists, representatives of local authorities or emergency services, investors or local residents— because this would entail additional expenses on advanced safety measures.
- The **specific national risk perception and organizational culture**: Japanese corporate mentality is based on unconditional submission of employees to their supervisors and does not approve of employees asking embarrassing questions. This makes the working environment uncomfortable for whistleblowers.
- The **absence of a prompt risk assessment system**, and the long chain of communication between field staff and senior management, made urgent decision-making difficult during the disaster: field staff had no authority for even minor on-site decisions during the development of the critical situation.
- The **political struggle** between the Democratic Party and the Liberal Democratic Party, which generated massive distortion of information about the real condition of the plant after the disaster. Both parties used the accident in their own political interests.
- Misleading comments from the Kantei, NISA and TEPCO about the accident during the first days after the disaster to the Japanese people and the international community were caused by the following factors**: lack of information and misjudgment about the real scale of the disaster** in the first days; the **absence of objective estimates of possible consequences of the disaster; fear of massive panic** in Japan and in nearby countries because nuclear accidents and radiation are the most dangerous threats in public perception; **reluctance to confess that regulation of the Japanese nuclear industry had been defective**, and that concealing the imperfections and risks of Japanese NPPs had been common practice for decades.

Chernov, Dmitry; Sornette, Didier (2015-10-27). Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human Fallibility (Kindle Locations 3469-3485). Springer International Publishing. Kindle Edition.

Minamata Mercury Poisoning (Japan, 1932– 1968)

In 1956, in Minamata city in Japan, a strange epilepsy-like neurological disease was discovered among locals, as well as in their cats and dogs. They called the disease "dancing cat fever". Initially, scientists thought that it was an infectious disease but, when they tested marine creatures on the coast nearby, they discovered extremely high levels of mercury contamination, which was determined as being caused by industrial wastewater discharge from the adjacent Chisso Corporation chemical factory. The factory used mercury sulfate as a catalyst in the production of acetaldehyde, and had been discharging the compound into Minamata Bay for 25 years. And seafood from the bay had been the main diet of local residents and their domestic animals for decades. Chisso Corporation knew about the potential damage to the health of locals and to the environment, but was reluctant to construct expensive wastewater treatment facilities. Moreover, the company continued to discharge mercury-contaminated waste after the cause of the disease had been confirmed. It lobbied to cut back pollution control regulation, and obstructed detailed investigation by scientists and the media. Ultimately, 2265 victims have been officially certified— 1784 of whom died from the poisoning— and over 10,000 people have received financial compensation from the company, which paid out a total of more than US $ 170 million. [625] During the Fukushima-Daiichi nuclear disaster described above, many commentators compared the neglectful behavior of TEPCO with the actions of Chisso Corporation during the Minamata crisis. They concluded that, in the intervening 50 years, the Japanese industry had not changed in its willingness to risk the health, and even the lives, of local residents through its activities.[626, 627]

Minamata Mercury Poisoning: Why Risks Were Concealed

- Chisso Corporation prioritized **short-term profitability over the long-term resilience** of the chemical factory, or the protection of public health and the environment.

Chernov, Dmitry; Sornette, Didier (2015-10-27). Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human. Springer International Publishing. Kindle Edition.

Asbestos Crisis (Worldwide, 1970s)

Asbestos became a very popular construction material at the end of the 19th and the beginning of the 20th centuries because of its resistance to fire, heat, electrical and chemical damage, and its sound absorption, average tensile strength, and affordability. The first evidence that asbestos fibers cause lung cancer and mesothelioma was discovered among asbestos miners, and had been scientifically proven by the 1930s to 1940s. Nowadays, the World Health Organization estimates that about 125 million people around the world are annually exposed to asbestos in the workplace, and about 100,000 workers die each year from an asbestos-related disease. [628] In the United States, it took more than three decades for the government to impose strict regulations concerning the working conditions of employees dealing with asbestos. Regulations were finally developed as the consequence of a lawsuit during which specific documents were provided proving that industry officials knew of the dangers of asbestos and tried to conceal them from workers to avoid the costs of improving the safety conditions of workplaces. During an exemplary lawsuit, it was stated that "[t] he manufacturers put a lethal risk of harm in (the plaintiff's) work environment, then allowed him unwittingly to confront the risk with tragic results, on a daily basis". [629] The asbestos industry had also been hiding health risks from customers, because of the fear of losing whole markets. After the risks were revealed, dozens of American firms had to file for bankruptcy due to asbestos liabilities— and with 600,000 claims from individuals so far, the total cost of asbestos compensation is estimated to be more than US $ 200 billion. [630] Nevertheless, China and India still consume large amounts of asbestos imported from Russia, Canada and Kazakhstan. [631]

Asbestos Crisis: Why Risks Were Concealed

- The **priority of short-term profitability**, and the industry's reluctance to confess the harmfulness of asbestos, thereby destroying the market and generating millions of lawsuits seeking compensation for health damage.

Chernov, Dmitry; Sornette, Didier (2015-10-27). Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human Fallibility. Springer International Publishing. Kindle Edition.

Savar Building Collapse (Bangladesh, 2013)

On 24 April 2013, in Savar in the Greater Dhaka Area of Bangladesh, 1127 workers at garment factories died when the Rana Plaza building collapsed on them. There are more than 5000 competing garment factories in Bangladesh, which provide cheap labor for the tailoring of many world-famous brands. The average monthly salary of a sewing machine operator is only US $ 38, but the garment industry produces garments for up to US $ 20 billion and provides Bangladesh with 77 % of its exports. [632 , 633] The Rana Plaza was originally designed as a six-story building for shops and offices, but the owner of the plaza illegally constructed three additional floors using low-quality materials— and sited five garment factories there, deploying heavy machinery, which generated excessive vibrations. The day before the collapse, local authorities discovered cracks in the building and issued an order to evacuate the whole building. The personnel on the lower floors with shops and a bank were not permitted to their workplaces until inspectors had confirmed the safety of the building; but managers of the garment factories insisted that their staff should go to work, otherwise they would all lose their monthly salary. [634] Moreover, they misled the sewers by telling them that the building had been inspected and declared safe. [635] The motives of the managers were simple: if operations were shut down, they would be fined by their customers— world-famous high street clothing brands— for delays with shipping, and could lose contracts in a highly competitive market. Two years earlier in 2011, Walmart and GAP had refused to sign a new industry agreement to pay Bangladeshi factories a higher price, so the garment industry could not afford safety upgrades on their sewing factories. [636]

Savar Building Collapse: Why Risks Were Concealed

- **Short-term profitability** in a highly competitive market took priority over the safety of personnel.
- The owners of the garment factories were **afraid of losing customers** in case of a prolonged time-out of the factory.

Chernov, Dmitry; Sornette, Didier (2015-10-27). Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human Fallibility . Springer International Publishing. Kindle Edition.

Financial Sector

Barings Bank Collapse (Singapore-UK, 1995)

In February 1995, Barings PLC— the oldest and the most reputable bank in Britain— collapsed from the unauthorized trading of Nick Leeson, a Singapore-based trader at the bank, who single-handedly lost about US $ 1.4 billion (£ 827 million).

…

Barings Bank Collapse: Why Risks Were Concealed

- By authorizing the use of unfamiliar and risky financial instruments, Barings managers gave priority to **short-term profitability over the long-term financial stability of the oldest bank in the UK**.
- The **climate of wishful thinking** at the bank made it uncomfortable for people to spread warnings, or make a sober assessment of suspicious operations or phenomenal earnings.
- **Habituation/ false reassurance/ self-suggestion/ self-deception** among executives at the Bank of England and Barings Bank concerning the low probability of massive losses from **deregulation and innovative financial instruments** (derivatives). The tendency among decision-makers not to see the **whole picture about risks**.
- The widely accepted **"success at any price" organizational culture** within the investment banking industry, and the fear of being blamed as incompetent, forced Nick Leeson to start to hide his own losses, leading to a fatal spiral.
- **Ignorance about derivatives and their associated risks** among executives of the bank and representatives of the internal control department, which allowed Leeson to falsify data with impunity for 3 years.

Chernov, Dmitry; Sornette, Didier (2015-10-27). Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human Fallibility. Springer International Publishing. Kindle Edition.

Enron's Bankruptcy (USA, 2001)

In December 2001, the American company Enron went bankrupt, losing US $ 63.4 billion in assets.

…

Enron's Bankruptcy: Why Risks Were Concealed

- **Close and corrupting relationships between Enron executives and representatives of the US political elite led to deregulation changes** that allowed Enron to build a flawed business model. The risks of such a model could be hidden with impunity because of the absence of a strict regulatory framework, and extensive informal relationships between Enron executives, regulators and politicians. Employees of Enron and Arthur Andersen were afraid to reveal risks to the public because they feared they would not find support from regulators, who seemed to have a cozy relationship with Enron's management team.
- The business model was geared to constantly raising the earnings of Enron executives by maintaining the permanent growth of the company's market value. This growth could be achieved by a continual increase of Enron's short-term revenue figures and low debts. Therefore, **Enron's executives corrupted their auditors and several investment banks with lucrative years-long contracts for reaching the required figures**.
- **Wishful thinking of the board of directors, and among investors, employees and the media**— they preferred to believe only in what they wanted to believe, and ignored facts and early warnings. The unwillingness of the majority of investors to go deep into Enron's complex financial operations while the company was steadily expanding in the market.
- **Unfathomable complexity** of the financial engineering through which Enron generated its false financial results was key. This was a precursor to the absolute impossibility of penetrating the CDO-squared structure of the mid-2000s. It was not just an unwillingness; it was an inability.

Enron's Bankruptcy (USA, 2001) continued

In December 2001, the American company Enron went bankrupt, losing US $ 63.4 billion in assets.

- The **reluctance of Enron executives to confess any shortcomings of the created business model** in the early stages of Enron's ascent, because doing so could lead to accusations of incompetence and the collapse of capitalization. The **fear of criminal prosecution after the majority of the falsifications** had occurred caused Enron's management to continue distorting information about the real situation within the company until bankruptcy.
- **A "success at any price" and "no bad news" culture**, the **secrecy** of deals at Enron, the **absence of internal control within the company and its frequent labor turnover**: all these processes were consciously implemented by executives to provide a **fragmentary picture of risks among employees**.

Chernov, Dmitry; Sornette, Didier (2015-10-27). Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human Fallibility. Springer International Publishing. Kindle Edition.

Subprime Mortgage Crisis (USA, 2007– 2008)

During the 2000s, an American real estate bubble was forming, [769] which burst during 2007– 2008. More than eight million American households lost their homes due to foreclosure. More than US $ 17 trillion of household wealth was wiped out within 21 months after the burst. The American subprime mortgage crisis triggered a global financial and economic crisis in 2008– 2009,[770] which caused the most severe recession in over 50 years. Total stock market losses exceeded US $ 30 trillion worldwide. [771] In order to prevent a total collapse of the world financial system, governments imperiled trillions of taxpayers' money on bailouts of private financial institutions, which were "too big to fail". This global salvage operation disrupted the stability of government finance not only in the USA, but also in many European countries.

…

Subprime Mortgage Crisis: Why Risks Were Concealed

- **Deregulation** was implemented in the (mistaken) pursuit of long-term improvement in the efficient allocation of resources. In this respect, the transient triumph of the Efficient Market and Rational Expectations Hypotheses created an intellectual environment that rationalized and legitimized policy initiatives that created the opportunity for massive, unregulated pursuit of short-terms profits by all the intermediaries in the financial supply chain. So, **the captains of finance got carte blanche from the government to take further risks with derivatives**— and to conceal the risks they were taking— with near impunity.
- **Government representatives, and the executives and board members of financial institutions, did not fully understand the complexity of innovative financial instruments** and the potential consequences of deregulating the financial sector. Government control over these complex systems was too weak in the absence of a "mega-regulator", and there was only **fragmentary perception of the whole picture of risks** among representatives of the government and the top managers of companies in the mortgage pipeline.

Subprime Mortgage Crisis (USA, 2007– 2008) continued

- **Wishful thinking among borrowers, investors and the media**— they preferred to believe only what they wanted to believe and in particular in the illusion of a "perpetual money machine" promising endless wealth and prosperity for everyone based on the sure thing, the never ending growth of real-estate prices, and ignored known facts and early warnings about the real estate bubble and the low quality of CDOs.
- **Government executives were reluctant to admit mistakes in previous deregulation efforts**, which, together with the policy of low interest rates in 2002– 2003, had help create the real estate bubble. Any admission of oversight would massively reduce the value of assets and lower US economic figures. So, government decision-makers preferred not to respond to clear evidence of risk before the collapse of Bear Stearns and Lehman Brothers.

Chernov, Dmitry; Sornette, Didier (2015-10-27). Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human Fallibility. Springer International Publishing. Kindle Edition.

Unreadiness of the Soviet Red Army for the Nazi Invasion (1941)

On June 22, 1941 at 3: 30 a.m., the Nazi German armed forces (the Wehrmacht) together with Italian, Romanian, Finnish, Hungarian, and Slovakian forces invaded the Soviet Union. It was the most powerful invasion in world history in terms of the number of soldiers: more than 5.5 million fighters were amassed in 192 divisions for the Eastern campaign. The forces had more than 4300 tanks, 5000 military airplanes and 47,200 artillery guns and mortars. [882] The Soviet Red Army actually had numerical superiority over the Wehrmacht, but could not make use of it because of its unreadiness for the sudden attack. During the first day, the Wehrmacht penetrated between 25 and 50 km into Soviet territory. By the end of the first week, Minsk, the capital of the Soviet Republic of Belarus, was taken. By the third week, the depth of the invasion exceeded 600 km and the Wehrmacht was close to Leningrad (the former St. Petersburg) and Kiev (the capital of the Soviet Republic of the Ukraine). After 3 1/2 months of fierce battles, the Nazis had advanced up to 1000 km and reached the suburbs of Moscow, the capital of the Soviet Union. The first months of the war on the Eastern Front— a major part of the Second World War— turned out to be a military catastrophe for the Red Army: more than 850,000 soldiers died, more than 1 million soldiers were captured, and nearly 3500 military airplanes and 6000 tanks were lost. The Wehrmacht seized territory that normally produced up to 40 % of Soviet GDP. [883]

…

Unreadiness of the Soviet Army for the Nazi Invasion: Why Risks Were Concealed

- **The wishful thinking/ overconfidence/ self-suggestion/ self-deception** of Stalin, who convinced himself in 1941 that an attack on the Soviet Union by Nazi Germany was impossible.
- **A prevailing culture of "success at any price" and "no bad news"**: the fear among Soviet army officers of being punished (dismissed, criminally prosecuted or executed) for communicating any information about the situation on the battlefronts that did not match Stalin's perception and expectations.

Chernov, Dmitry; Sornette, Didier (2015-10-27). Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human Fallibility. Springer International Publishing. Kindle Edition.

Great Wildfires in the European Part of Russia (Russia, 2010)

In July 2010, gigantic wildfires and a drought occurred in the western part of Russia caused by a record-breaking heat wave. Fifty-four people perished and 458 were injured in the wildfires themselves and, according to Munich Re estimates, around 56,000 people died from the effects of the smog and heat wave cause by the fires. [941] More than 2000 buildings were destroyed and more than 9 million hectares of crops were lost. Total damages from the wildfires and drought were estimated at between US $ 15 billion and $ 50 billion. [942]

Massive Wildfires in the European Part of Russia: Why Risks Were Concealed

- **This propensity for hiding bad news** resulted in part from the change of the rules for appointing regional leaders: instead of being elected by popular vote, all heads of Russian regions were appointed by the President. This led to a situation where their performance was evaluated in Moscow, rather than in their regions by the citizens they were supposed to be serving. **Eager to make a favorable impression on Putin and ensure their continuation in power, regional leaders preferred to send only reassuring reports to the central government**. They always tried to convince the federal authorities that they could handle any situation. This led to massive distortion of information about the real situation concerning wildfires in several Russian regions and, as a result, delayed the reaction of Russian federal government to the threat. There is a prevalent Russian political culture, which motivated subordinates to conceal risks.
- This was further reinforce by the federal government's **shortsightedness in deregulating forest management**, leading to confusing and badly designed attribution of responsibilities among involved parties from local government to the private sector.

Chernov, Dmitry; Sornette, Didier (2015-10-27). Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human. Springer International Publishing. Kindle Edition.

Worldwide Spanish Flu and SARS Outbreaks (1918– 1919, 2003)

Severe acute respiratory syndrome (SARS) originated in Guangdong Province in China in November 2002. The Chinese authorities suppressed news of the outbreak of an unknown disease, concealing it both from residents of the province and specialists of the World Health Organization (WHO). As a result, large-scale preventive measures were delayed for four months. The WHO issued a global warning only in mid-March 2003. A unique collaboration of governmental organizations and research centers throughout the world made it possible to halt the last human chain of the transmission of SARS on 5 July 2003. But, by that time, the international spread of SARS had resulted in 8098 cases in 26 countries, with 774 deaths. [913] … global pandemic of 1918– 1919 (also known as the "Spanish flu"), when around 500– 600 million people— a third of the world's population at that time— were infected, and nearly 50 million lost their lives (some estimates put the figure at nearer 100 million casualties). [914] … In the USA alone, the disease claimed more than 650,000 lives during 1918– 1919.

Worldwide Spanish Flu: Why Risks Were Concealed

- The military requirement to keep up the morale of the US nation caused deliberate suppression of any information about the disease. Such **secrecy on the grounds of "national security" was common during the war period**.
- **The absence of scientific knowledge about viruses, the principles of their transmission and the associated risks meant** that decision-makers underestimated the need for urgent and decisive action.
- American (and other allied countries) politicians apparently **gave priority to their political interests over the lives of hundreds of thousands of their own citizens, and millions of people around the World**.

SARS Outbreak: Why Risks Were Concealed

- National security concerns: The Chinese authorities were **afraid of massive panic, and were worried about the threat to social stability and continued economic growth** if SARS caused a similar death rate as the Spanish flu pandemic.
- **The Chinese provincial authorities wanted to be seen in a good light by the central government**, which in turn tacitly approved of the "no bad news" culture that existed within the Chinese communist party.

Chernov, Dmitry; Sornette, Didier (2015-10-27). Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human Fallibility. Springer International Publishing. Kindle Edition.

Krymsk Flooding (Russia, 2012)

On July 7, 2012 from 2 until 4 a.m., a powerful flash flood with a 6.8-m water surge occurred in the Krymsk district of Southwestern Russia. Krymsk is in the Krasnodar region, just 30 km from the coast of the Black Sea and 200 km from Sochi, where the Winter Olympic Games took place in 2014. For two days before the disaster, the volume of rainfall exceeded the monthly average by three to five times. The torrential rain caused a sharp rise in the water level of rivers flowing from the nearby Caucasus Mountains, which led to the flooding of several districts and cities. However, it was only in the Krymsk district that the consequences of the flooding were dreadful. The disaster affected 34,650 people, 171 people died— 153 in the Krymsk district— and 2225 people (including 496 children) were injured. More than 7200 residential and public buildings in the district were destroyed or damaged by the flood. [947]

Krymsk Flooding: Why Risks Were Concealed

- **Habituation/ false reassurance/ overconfidence/ self-deception** among representatives of the local authorities about the low probability of a catastrophic flash flood in Krymsk district.
- **Regional authorities were unwilling to investigate the causes of previous flash floods in detail**, since this would inevitably lead to the lengthy and embarrassing process of passing on the lessons learnt and making recommendations to subordinates.
- **The high frequency of flood and severe weather warnings** previously received by local authorities, which were often not realized**, leading to a "crying wolf" psychological response and growing complacency**.
- **Russian regional bureaucrats and federal ministers wanted to appear in a good light in the eyes of the Russian president**. This led to massive distortion of information about the timeliness of the state of emergency during the disaster and the adequacy of crisis response measures after the disaster.

Chernov, Dmitry; Sornette, Didier (2015-10-27). Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human. Springer International Publishing. Kindle Edition.

Retail Production Industry

This sector produces consumer goods: foods and drinks, drugs, cosmetics, electronic gadgets, cars and so on. The majority of risk concealment cases in the sector are similar because of its specific business practice. Mutually competing manufacturers tend to produce similar goods in every product segment because each manufacturer is continually watching competitors for any innovations, which will be implemented as fast as possible in the products of all manufacturers. Prof. Leveson assessed the problem very clearly: "At the same time that the development of new technology has sprinted forward, the time to market for new products has greatly decreased, and strong pressures exist to decrease this time even further. The average time to translate a basic technical discovery into a commercial product in the early part of this century was thirty years. Today our technologies get to market in two to three years and may be obsolete in five. We no longer have the luxury of carefully testing systems and designs to understand all the potential behaviors and risks before commercial or scientific use. [This leads to] reduced ability to learn from experience". [964] Therefore, manufacturers try to launch new products as swiftly as possible to gain a competitive advantage during the first few months, and sometimes ignore defects in the design of innovative production.

Such problems have occurred in many cases with complex innovative products. The retail sector has seen the Ford-Firestone tire controversy (1990), the Intel Pentium FDIV Bug Crisis (1994), and problems with the antenna of the Apple iPhone 4 (2010) and with the brakes of the Toyota Prius (2010– 2013). In the industrial sector, notorious cases include the lithium ion batteries on the Boeing 787 Dreamliner (2012– 2013) [965] and the chassis of the Sukhoi SuperJet (2013). [966] To take just one of these examples: the management of Apple was aware of problems with the quality of signal reception of the iPhone 4 long before it was released, but Apple's co-founder Steve Jobs liked the design of the new phone so much that he personally gave an order to launch it into mass production without redesigning the antenna. He also cancelled real-world testing before the launch – the testing process usually takes a minimum of 14 weeks. [967] Within three weeks of the launch, Steve Jobs and Apple were denying that the new phone had flaws. This position angered many people and attracted media attention to the problem. Ultimately, the company had no choice but to admit the problem, issue a temporary solution for the 25 million customers who had already bought the phone (a free case for the phone) and update the software.

Cases Reviewed: Toyota's Cost Reduction Challenge, The Acceleration Pedal Problem, Genuine Cases of Concealments of Defects in Automotive Industry, The 17-Year Poly Implant Prothese Fraud (France, 1993-2010), Other Cases with Risk Information Concealment: Tobacco and Food Industries.

Retail Production Industry: Why Risks Were Concealed

- **Companies prioritised short-term profitability** and used all means necessary to gain a competitive advantage by launching products as quickly and cheaply as possible, at the expense of the quality of their products and the long-term health and loyalty of customers.
- This happened in some cases as the path of least (short-term) effort to **respond to the pressure from emerging competition or other appearing stressors**.
- In a capitalistic free market system, a narrow view is that firms aim at **maximizing shareholder value and nothing else counts**. In such rational optimization framework, additional considerations involving the physical health of consumers, if not directly impacting the financial well-being of business, will be relegated, ignored or simply negated. Of course, this is a short-term view, but humans tend to be biased towards short-term preferences.

Chernov, Dmitry; Sornette, Didier (2015-10-27). Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human Fallibility. Springer International Publishing. Kindle Edition.

Analysis of Human Causal Factors in Catastrophes Reviewed by Chernov and Sornette

Table 6. Listing of causal factors

Sector	Event	Human Causal Element	Standardized Human Causal Element
Industrial	Vajont Dam	Cozy relations between SADE executives and Italian government officials	Lack Of Regulator Independence
Industrial	Vajont Dam	The political struggle	Politics
Industrial	Vajont Dam	The short-term profitability	Profit Motive
Industrial	Vajont Dam	unwilling to admit mistakes	Fear Of Failure
Industrial	Vajont Dam	save the dam project and avoid the collapse of SADE's shares	Protect Shareholder Value
Industrial	Vajont Dam	reassurance/ self-suggestion/ self-deception	Self-Reinforcing Deception
Industrial	Vajont Dam	afraid of being accused of incompetence	Fear Of Failure
Industrial	Three Mile Island	increasing the production of electricity took priority over safety matters.	Profit Motive
Industrial	Three Mile Island	Wishful thinking/ self-deception among decision makers	Self-Reinforcing Deception
Industrial	Three Mile Island	fragmentary perception of the whole picture of risks	Incomplete View Of Interactions
Industrial	Three Mile Island	no system for managing knowledge about risks within the industry	No Central Body Of Knowledge
Industrial	Three Mile Island	no industry-wide risk assessment system for timely evaluation of the condition of nuclear power plants	No Benchmarking
Industrial	Bhopal	The lack of experience or qualifications of government representatives	Unqualified Regulators
Industrial	Bhopal	management at the plant could manipulate data about real conditions at the plant	Management Manipulation Of Data
Industrial	Bhopal	desire of Indian managers to appear in a good light	Fear Of Failure
Industrial	Bhopal	play down the existence of massive safety imperfections at the plant	Fear Of Failure
Industrial	Bhopal	reluctance of plant managers to reveal the risks involved to local authorities that would likely oblige them to incur additional expense on safety measures	Profit Motive
Industrial	Bhopal	False reassurance/ self-suggestion/ self-deception among American and Indian executives	Self-Reinforcing Deception
Industrial	Bhopal	absence of a prompt risk assessment system	No Real-Time Risk Assessment
Industrial	Challenger	culture of continuously rushed organization	Rush Culture
Industrial	Challenger	Habituation/ wishful thinking/ false reassurance/ self-suggestion/ self-deception	Self-Reinforcing Deception
Industrial	Challenger	fear of losing their main client	Fear Of Failure

Sector	Event	Human Causal Element	Standardized Human Causal Element
Industrial	Challenger	fear of losing their main client	Profit Motive
Industrial	Challenger	reluctance of MTI management to confess their own mistakes	Fear Of Failure
Industrial	Challenger	“Success at any price” culture	Fear Of Failure
Industrial	Challenger	“Success at any price” culture	Drive To Succeed
Industrial	Challenger	“no bad news” culture	Fear Of Failure
Industrial	Chernobyl	Short-term profitability	Profit Motive
Industrial	Chernobyl	took priority over the long-term resilience of the Soviet nuclear industry	Lack Of Long-Term Strategy
Industrial	Chernobyl	rush culture	Rush Culture
Industrial	Chernobyl	nationalistic arrogance	Nationalistic Arrogance
Industrial	Chernobyl	over-confidence	Pride
Industrial	Chernobyl	Habituation/ wishful thinking/ self-suggestion/ self-deception	Self-Reinforcing Deception
Industrial	Chernobyl	refused to believe that a serious disaster could happen	Denial
Industrial	Chernobyl	focused only on their narrow departmental interests	Siloing
Industrial	Chernobyl	prevented timely and adequate communication of risk information between different agencies	Lack Of Transparency
Industrial	Chernobyl	prevented timely and adequate communication of risk information between different agencies	Inadequate Communication
Industrial	Chernobyl	National security secrecy	Secrecy
Industrial	Chernobyl	operators at the plant did not receive any information about the accidents that had occurred previously	No Central Body Of Knowledge
Industrial	Chernobyl	reluctant to confess their own mistakes	Fear Of Failure
Industrial	Chernobyl	reluctant to confess their own mistakes	Pride
Industrial	Chernobyl	afraid of accusations of incompetence	Fear Of Failure
Industrial	Chernobyl	question of national security	Secrecy
Industrial	Chernobyl	organizational culture of “Success at Any Price”	Drive To Succeed
Industrial	Chernobyl	“No Bad News” within the industry	Retributive Culture
Industrial	Chernobyl	“No Bad News” within the industry	Pride
Industrial	Chernobyl	uncertainty about the real scale of the disaster	Lack Of Timely Information
Industrial	Chernobyl	uncertainty about the real scale of the disaster	Lack Of Timely Information
Industrial	Chernobyl	absence of objective estimates of the possible consequences of the disaster	Ignorant Of Consequences
Industrial	Chernobyl	fear of panic	Fear Of Panic
Industrial	Exxon Valdez	Short-term profitability won priority over the long-term sustainability	Lack Of Long-Term Strategy

Sector	Event	Human Causal Element	Standardized Human Causal Element
Industrial	Exxon Valdez	Short-term profitability won priority over the long-term sustainability	Lack Of Long-Term Strategy
Industrial	Exxon Valdez	Habituation/ wishful thinking/ overconfidence/ self-suggestion/ self-deception	Self-Reinforcing Deception
Industrial	Exxon Valdez	Lack of consideration of scenarios	Incomplete View Of Interactions
Industrial	Exxon Valdez	Cozy relationships between the Alyeska consortium and representatives of the State of Alaska	Lack Of Regulator Independence
Industrial	Exxon Valdez	fragmented perception of risks (i.e., the absence of the whole picture of risks)	Incomplete View Of Interactions
Industrial	Exxon Valdez	permanent rush culture	Rush Culture
Industrial	Exxon Valdez	Crew members were also afraid to lose their jobs	Retributive Culture
Industrial	Exxon Valdez	Crew members were also afraid to lose their jobs	Retributive Culture
Industrial	Ufa	Short-term tasks	Rush Culture
Industrial	Ufa	rush work	Rush Culture
Industrial	Ufa	Executives of the Soviet Ministry of Petroleum were reluctant of to admit their own mistakes	Fear Of Failure
Industrial	Ufa	Executives of the Soviet Ministry of Petroleum were reluctant of to admit their own mistakes	Retributive Culture
Industrial	Ufa	lack or absence of communication between representatives of the pipeline, Soviet railways, and local residents	Lack Of Transparency
Industrial	Ufa	lack or absence of communication between representatives of the pipeline, Soviet railways, and local residents	Inadequate Communication
Industrial	Ufa	nobody could imagine that such a catastrophic event could ever take place	Incomplete Scenario Analysis
Industrial	Ufa	no authority	No Authority
Industrial	Sayano-Shushenskaya	focused on the short-term reduction of safety costs	Profit Motive
Industrial	Sayano-Shushenskaya	and demanded constant rush	Rush Culture
Industrial	Sayano-Shushenskaya	reluctance … to investigate in detail the causes of previous accidents/ near-miss cases	No Central Body Of Knowledge
Industrial	Sayano-Shushenskaya	gave priority to short-term financial results	Profit Motive
Industrial	Sayano-Shushenskaya	Habituation/ wishful thinking/ overconfidence/ self-suggestion/ self-deception	Self-Reinforcing Deception

Sector	Event	Human Causal Element	Standardized Human Causal Element
Industrial	Sayano-Shushenskaya	afraid of potential criminal charges	Fear Of Failure
Industrial	Sayano-Shushenskaya	afraid of potential criminal charges	Fear Of Prosecution
Industrial	Sayano-Shushenskaya	The Russian government was unwilling to admit its own mistakes in pushing through unreasoned free-market reforms of Russian electro-energetics	Profit Motive
Industrial	Sayano-Shushenskaya	The Russian government was unwilling to admit its own mistakes in pushing through unreasoned free-market reforms of Russian electro-energetics	Fear Of Failure
Industrial	Sayano-Shushenskaya	The Russian government was unwilling to admit its own mistakes in pushing through unreasoned free-market reforms of Russian electro-energetics	Incomplete Scenario Analysis
Industrial	Deepwater Horizon	Habituation/ wishful thinking/ false reassurance/ self-deception	Self-Reinforcing Deception
Industrial	Deepwater Horizon	nationalistic arrogance of American regulators and oil companies	Nationalistic Arrogance
Industrial	Deepwater Horizon	Deliberate lobbying by the American oil industry to persuade government to deregulate the sector and massively reduce the budget of the regulators	Profit Motive
Industrial	Deepwater Horizon	Deliberate lobbying by the American oil industry to persuade government to deregulate the sector and massively reduce the budget of the regulators	Lack Of Regulator Independence
Industrial	Deepwater Horizon	regulators failed to identify systemic failures in risk management, which the industry was trying to hide from regulators and the public	Unqualified Regulators
Industrial	Deepwater Horizon	regulators failed to identify systemic failures in risk management, which the industry was trying to hide from regulators and the public	Management Deception
Industrial	Deepwater Horizon	Fragmentary risk perception (failure to see the whole picture of risks) and lack of communication among representatives of the different organizations	Incomplete View Of Interactions
Industrial	Deepwater Horizon	Fragmentary risk perception (failure to see the whole picture of risks) and lack of communication among representatives of the different organizations	Inadequate Communication
Industrial	Deepwater Horizon	Rush during drilling because of delays in the schedule and cost overrun	Profit Motive

Sector	Event	Human Causal Element	Standardized Human Causal Element
Industrial	Raspadskaya	short-term profitability instead of the long-term resilience of the coal mining business	Profit Motive
Industrial	Raspadskaya	short-term profitability instead of the long-term resilience of the coal mining business	Lack Of Long-Term Strategy
Industrial	Raspadskaya	Government oversight over Russian coalmining had been deregulated	Lack Of Regulation
Industrial	Raspadskaya	Habituation/ wishful thinking/ overconfidence/ self-suggestion/ self-deception	Self-Reinforcing Deception
Industrial	Fukashima	misplaced loyalty of regulators concerning shortcomings in the design and operation of Japanese NPPs	Lack Of Regulator Independence
Industrial	Fukashima	misplaced loyalty of regulators concerning shortcomings in the design and operation of Japanese NPPs	Pride
Industrial	Fukashima	misplaced loyalty of regulators concerning shortcomings in the design and operation of Japanese NPPs	Retributive Culture
Industrial	Fukashima	national arrogance of both executives and regulators in the Japanese nuclear industry	Nationalistic Arrogance
Industrial	Fukashima	Habituation/ wishful thinking/ overconfidence/ self-suggestion/ self-suggestion/ self-deception	Self-Reinforcing Deception
Industrial	Fukashima	short-term profitability of operations and on ongoing cost reduction	Profit Motive
Industrial	Fukashima	specific national risk perception and organizational culture	Nationalistic Arrogance
Industrial	Fukashima	specific national risk perception and organizational culture	Retributive Culture
Industrial	Fukashima	absence of a prompt risk assessment system	No Real-Time Risk Assessment
Industrial	Fukashima	political struggle	Politics
Industrial	Fukashima	lack of information and misjudgment about the real scale of the disaster	Uncertainty
Industrial	Fukashima	lack of information and misjudgment about the real scale of the disaster	Lack Of Timely Information
Industrial	Fukashima	the absence of objective estimates of possible consequences of the disaster; fear of massive panic	Ignorant Of Consequences
Industrial	Fukashima	the absence of objective estimates of possible consequences of the disaster; fear of massive panic	Fear Of Panic
Industrial	Fukashima	reluctance to confess that regulation of the Japanese nuclear industry had been defective	Fear Of Failure

Sector	Event	Human Causal Element	Standardized Human Causal Element
Industrial	Minamata	short-term profitability over the long-term resilience	Profit Motive
Industrial	Minamata	short-term profitability over the long-term resilience	Lack Of Long-Term Strategy
Industrial	Asbestos	priority of short-term profitability	Lack Of Long-Term Strategy
Industrial	Savar	Short-term profitability	Profit Motive
Industrial	Savar	afraid of losing customers	Fear Of Failure
Financial	Barings Bank	to short-term profitability over the long-term financial stability of the oldest bank in the UK.	Profit Motive
Financial	Barings Bank	to short-term profitability over the long-term financial stability of the oldest bank in the UK.	Lack Of Long-Term Strategy
Financial	Barings Bank	climate of wishful thinking	Fear Of Failure
Financial	Barings Bank	climate of wishful thinking	Retributive Culture
Financial	Barings Bank	Habituation/ false reassurance/ self-suggestion/ self-deception	Self-Reinforcing Deception
Financial	Barings Bank	“success at any price” organizational culture	Fear Of Failure
Financial	Barings Bank	“success at any price” organizational culture	Drive To Succeed
Financial	Barings Bank	Ignorance about derivatives and their associated risks	Incomplete View Of Interactions
Financial	Barings Bank	Ignorance about derivatives and their associated risks	Ignorant Of Consequences
Financial	Enron	Close and corrupting relationships between Enron executives and representatives of the US political elite led to deregulation changes	Profit Motive
Financial	Enron	Close and corrupting relationships between Enron executives and representatives of the US political elite led to deregulation changes	Politics
Financial	Enron	Enron’s executives corrupted their auditors and several investment banks with lucrative years-long contracts for reaching the required figures.	Profit Motive
Financial	Enron	Enron’s executives corrupted their auditors and several investment banks with lucrative years-long contracts for reaching the required figures.	Corruption

Sector	Event	Human Causal Element	Standardized Human Causal Element
Financial	Enron	Enron's executives corrupted their auditors and several investment banks with lucrative years-long contracts for reaching the required figures.	Management Manipulation Of Data
Financial	Enron	Wishful thinking of the board of directors, and among investors, employees and the media	Self-Reinforcing Deception
Financial	Enron	Unfathomable complexity	Incomplete View Of Interactions
Financial	Enron	Unfathomable complexity	Ignorant Of Consequences
Financial	Enron	reluctance of Enron executives to confess any shortcomings of the created business model	Fear Of Failure
Financial	Enron	fear of criminal prosecution after the majority of the falsifications	Fear Of Failure
Financial	Enron	fear of criminal prosecution after the majority of the falsifications	Fear Of Prosecution
Financial	Enron	"success at any price"	Fear Of Failure
Financial	Enron	"success at any price"	Drive To Succeed
Financial	Enron	"no bad news" culture	Retributive Culture
Financial	Enron	the absence of internal control within the company and its frequent labor turnover	Inadequate Oversight
Financial	Enron	the absence of internal control within the company and its frequent labor turnover	Untrained Employees
Financial	Enron	fragmentary picture of risks among employees.	Incomplete View Of Interactions
Financial	Enron	fragmentary picture of risks among employees.	Ignorant Of Consequences
Financial	Subprime Mortgage Crisis	Deregulation	Inadequate Oversight
Financial	Subprime Mortgage Crisis	the captains of finance got carte blanche from the government to take further risks with derivatives	Self-Reinforcing Deception
Financial	Subprime Mortgage Crisis	Government representatives, and the executives and board members of financial institutions, did not fully understand the complexity of innovative financial instruments	Incomplete View Of Interactions
Financial	Subprime Mortgage Crisis	fragmentary perception of the whole picture of risk	Ignorant Of Consequences
Financial	Subprime Mortgage Crisis	Wishful thinking among borrowers, investors and the media	Self-Reinforcing Deception

Sector	Event	Human Causal Element	Standardized Human Causal Element
Financial	Subprime Mortgage Crisis	Government executives were reluctant to admit mistakes in previous deregulation efforts	Fear Of Failure
Military	Soviet Red Army	The wishful thinking/ overconfidence/ self-suggestion/ self-deception	Self-Reinforcing Deception
Military	Soviet Red Army	A prevailing culture of “success at any price” and “no bad news”	Fear Of Failure
Military	Soviet Red Army	A prevailing culture of “success at any price” and “no bad news”	Retributive Culture
Social	Spanish Flu	secrecy on the grounds of “national security” was common during the war period.	Secrecy
Social	Spanish Flu	The absence of scientific knowledge about viruses, the principles of their transmission and the associated risks meant	Incomplete View Of Interactions
Social	Spanish Flu	The absence of scientific knowledge about viruses, the principles of their transmission and the associated risks meant	Ignorant Of Consequences
Social	Spanish Flu	gave priority to their political interests over the lives of hundreds of thousands of their own citizens, and millions of people around the World	Politics
Social	SARS	afraid of massive panic, and were worried about the threat to social stability and continued economic growth	Fear Of Panic
Social	SARS	afraid of massive panic, and were worried about the threat to social stability and continued economic growth	Profit Motive
Social	SARS	The Chinese provincial authorities wanted to be seen in a good light by the central government	Fear Of Failure
Social	SARS	The Chinese provincial authorities wanted to be seen in a good light by the central government	Retributive Culture
Natural Disaster	Great Wildfires	This propensity for hiding bad news	Fear Of Failure
Natural Disaster	Great Wildfires	Eager to make a favorable impression on Putin and ensure their continuation in power, regional leaders preferred to send only reassuring reports to the central government	Drive To Succeed
Natural Disaster	Great Wildfires	Eager to make a favorable impression on Putin and ensure their continuation in power, regional leaders preferred to send only reassuring reports to the central government	Management Manipulation Of Data

Sector	Event	Human Causal Element	Standardized Human Causal Element
Natural Disaster	Great Wildfires	shortsightedness in deregulating forest management	Incomplete View Of Interactions
Natural Disaster	Great Wildfires	shortsightedness in deregulating forest management	Ignorant Of Consequences
Natural Disaster	Krymsk Flooding	Habituation/ false reassurance/ overconfidence/ self-deception	Self-Reinforcing Deception
Natural Disaster	Krymsk Flooding	Regional authorities were unwilling to investigate the causes of previous flash floods in detail	Fear Of Failure
Natural Disaster	Krymsk Flooding	The high frequency of flood and severe weather warnings	Information Desensitization
Natural Disaster	Krymsk Flooding	leading to a “crying wolf” psychological response and growing complacency	Complacency
Natural Disaster	Krymsk Flooding	Russian regional bureaucrats and federal ministers wanted to appear in a good light in the eyes of the Russian president	Drive To Succeed
Natural Disaster	Krymsk Flooding	Russian regional bureaucrats and federal ministers wanted to appear in a good light in the eyes of the Russian president	Management Manipulation Of Data
Retail	Production	Companies prioritised short-term profitability	Profit Motive
Retail	Production	respond to the pressure from emerging competition or other appearing stressors	Lack Of Long-Term Strategy
Retail	Production	maximizing shareholder value and nothing else counts	Shareholder Protection

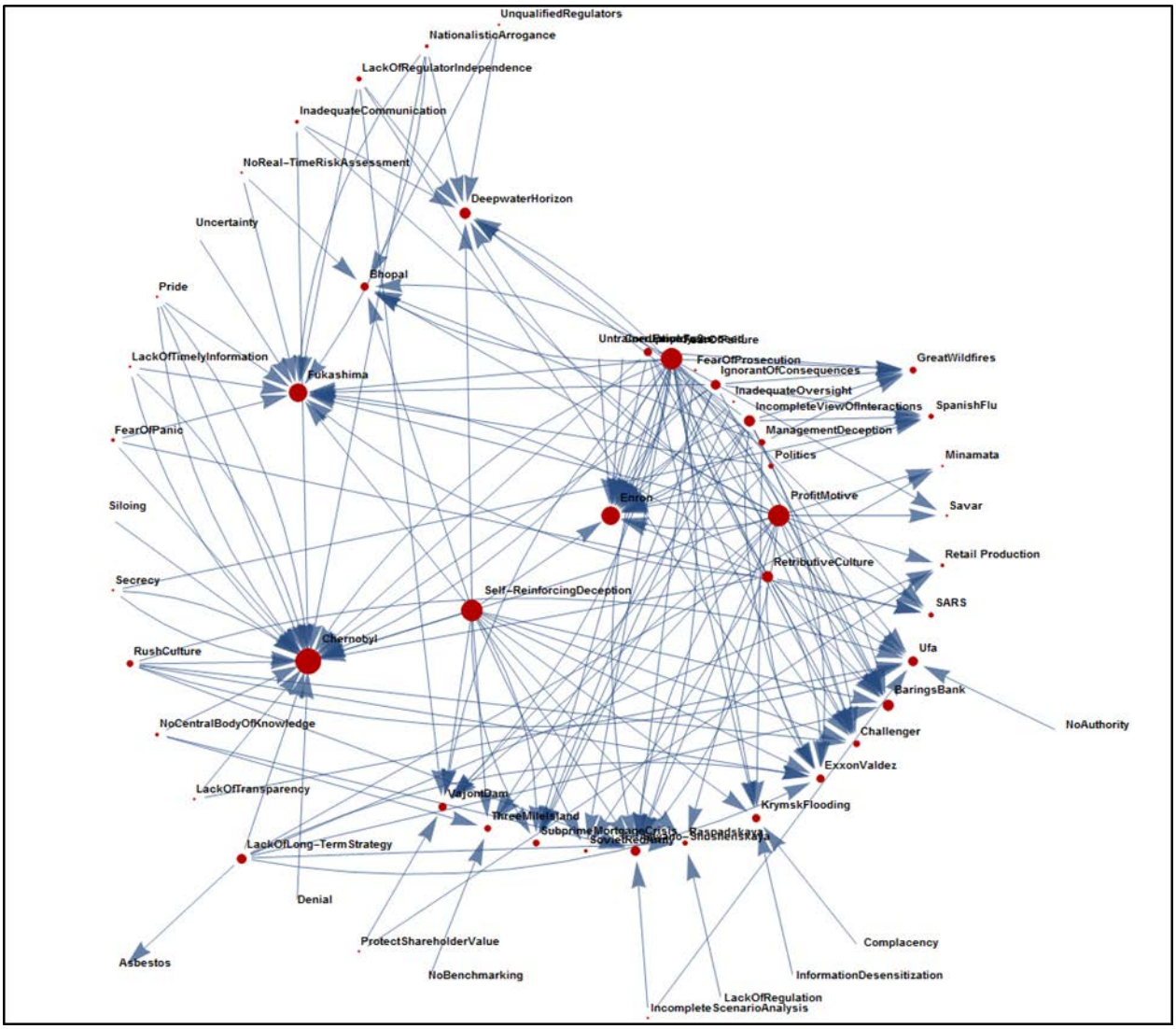


Figure 40. Graph of relationship between catastrophes reviewed and causal factors

Table 7. Statistical analysis of causal factors

Cause Rank	Number of Occurrences	Description of Cause	Proportion
1	25	Fear Of Failure	0.1488
2	19	Profit Motive	0.1131
3	16	Self-Reinforcing Deception	0.0952
4	10	Incomplete View Of Interactions	0.0595
5	10	Retributive Culture	0.0595
6	8	Ignorant Of Consequences	0.0476
7	8	Lack Of Long-Term Strategy	0.0476
8	6	Drive To Succeed	0.0357
9	6	Rush Culture	0.0357
10	5	Management Deception	0.0298
11	4	Lack Of Regulator Independence	0.0238
12	4	Nationalistic Arrogance	0.0238
13	4	Politics	0.0238
14	4	Pride	0.0238
15	3	Fear Of Panic	0.0179
16	3	Inadequate Communication	0.0179
17	3	Lack Of Timely Information	0.0179
18	3	No Central Body Of Knowledge	0.0179
19	3	Secrecy	0.0179
20	2	Fear Of Prosecution	0.0119
21	2	Inadequate Oversight	0.0119
22	2	Incomplete Scenario Analysis	0.0119
23	2	Lack Of Transparency	0.0119
24	2	No Real-Time Risk Assessment	0.0119
25	2	Protect Shareholder Value	0.0119
26	2	Unqualified Regulators	0.0119
27	1	Complacency	0.0060
28	1	Corruption	0.0060
29	1	Denial	0.0060
30	1	Information Desensitization	0.0060
31	1	Lack Of Regulation	0.0060
32	1	No Authority	0.0060
33	1	No Benchmarking	0.0060
34	1	Siloing	0.0060
35	1	Uncertainty	0.0060
39	1	Untrained Employees	0.0060
Total	168		

END OF REPORT