the Energy to Lead

Paper Study on Review of Approaches for Preventing Catastrophic Events

Ernest Lever
R&D Director, Infrastructure
Gas Technology Institute

gti

Content

1. Executive summary
2. Review of past catastrophic events
3. Existing methodologies , strengths and weaknesses
4. Stakeholder Interviews
5. State of the art in risk assessment
6. Risk governance frameworks
7. Conclusions
8. Questions

Project Objective

Executive Summary

A lot is being done to assess risk

- 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.

Events have complex causal factors

- Human
- Technological
- Organizational
- Political and societal
- Uncertainty
- Complex systems
- Lack of familiarity with emergent risks:

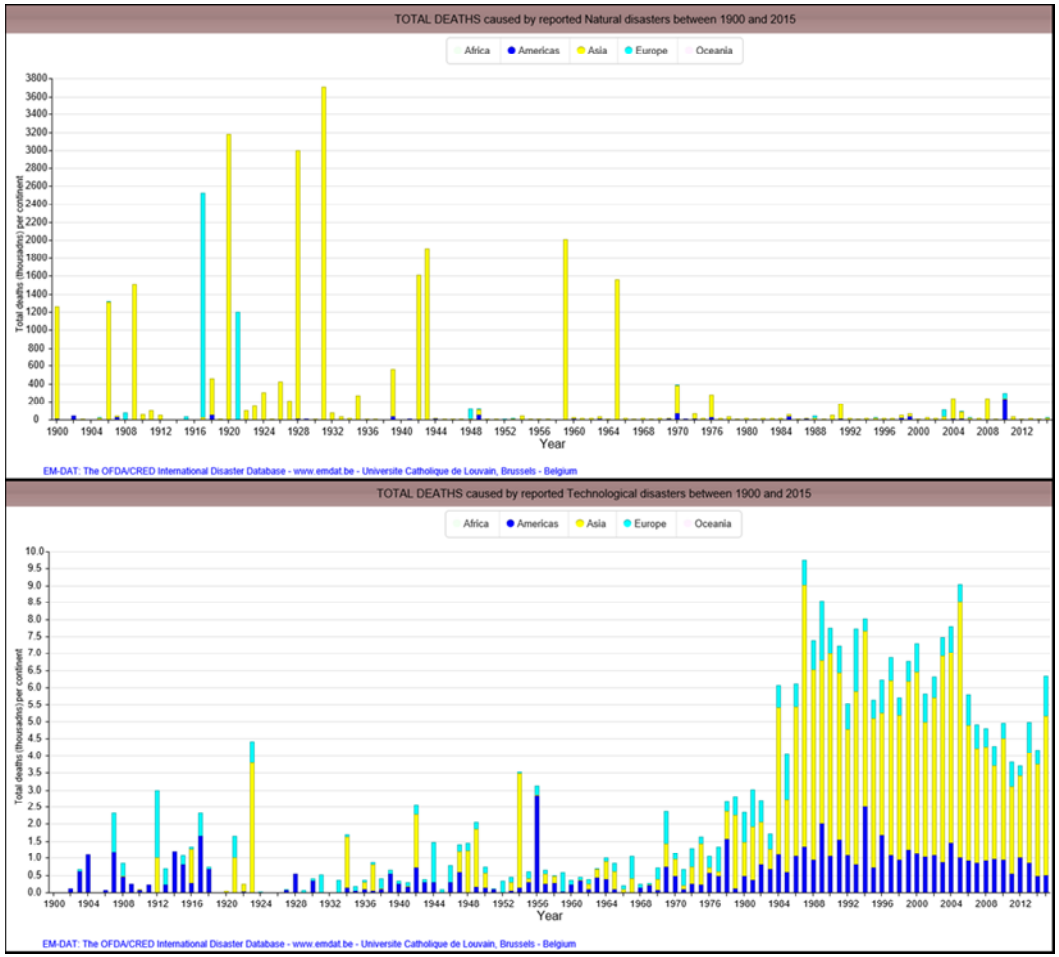
  Rare interactions lead to recognition of hidden risk

No Silver Bullet – Diversity is Key

- 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.

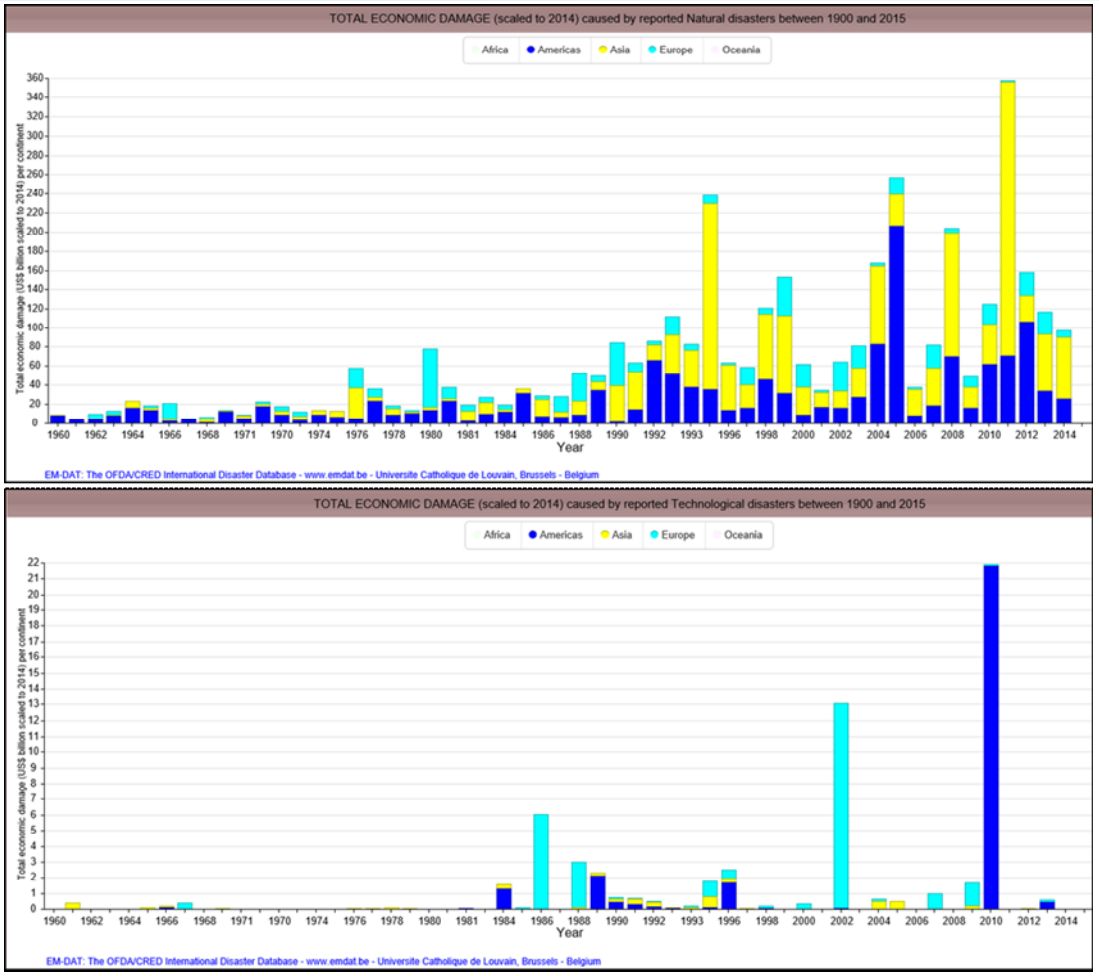
Past Catastrophic Events

Deaths from Natural and Technological Disasters 1900-2015



CRED. *EM-DAT Disaster Trends*. The OFDA/CRED International Disaster Database 2016 [cited 2016 May 17]; http://www.emdat.be/disaster_trends/index.html.

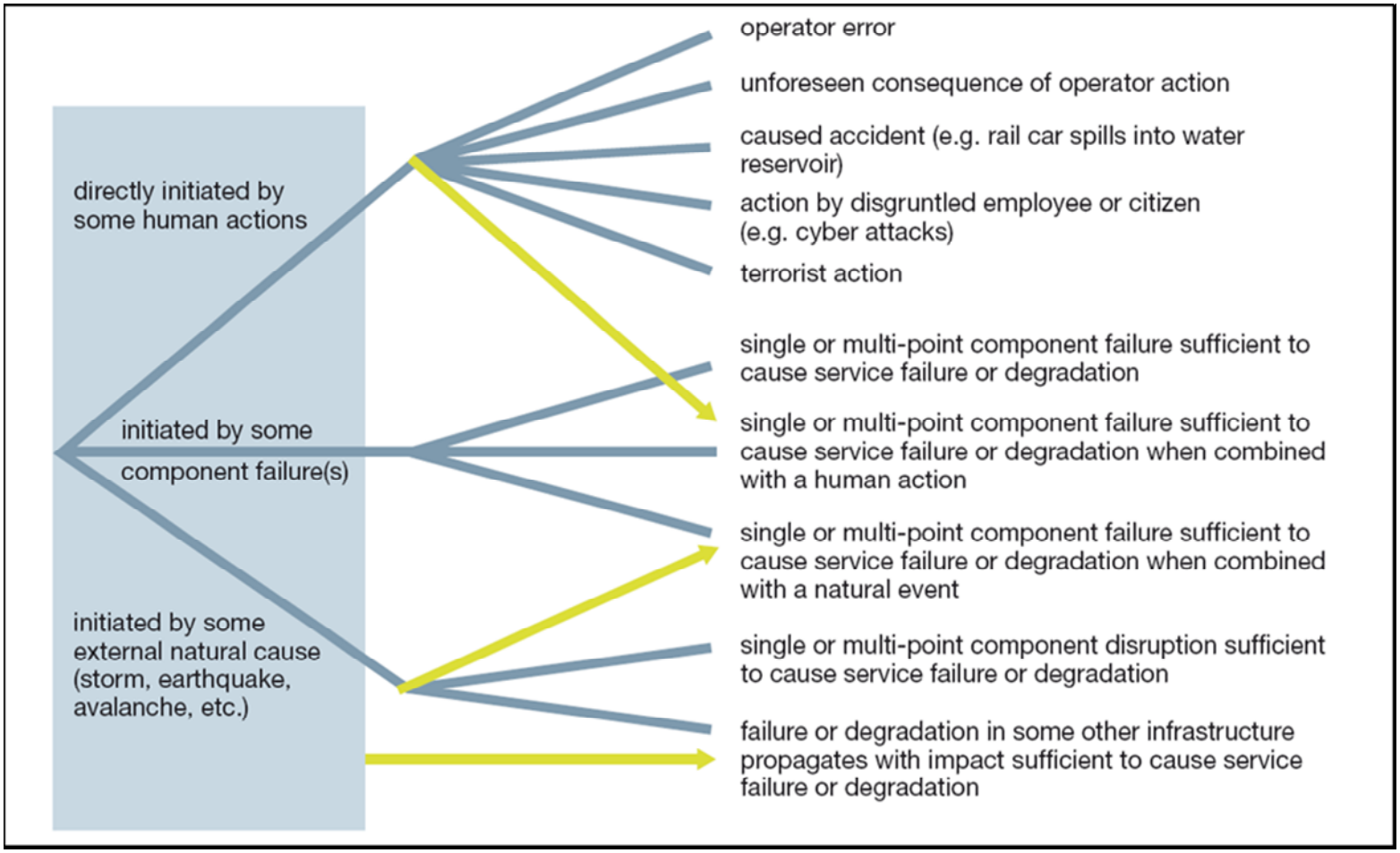
Economic Impact of Natural and Technological Disasters 1900-2015



CRED. *EM-DAT Disaster Trends*. The OFDA/CRED International Disaster Database 2016 [cited 2016 May 17]; http://www.emdat.be/disaster_trends/index.html.

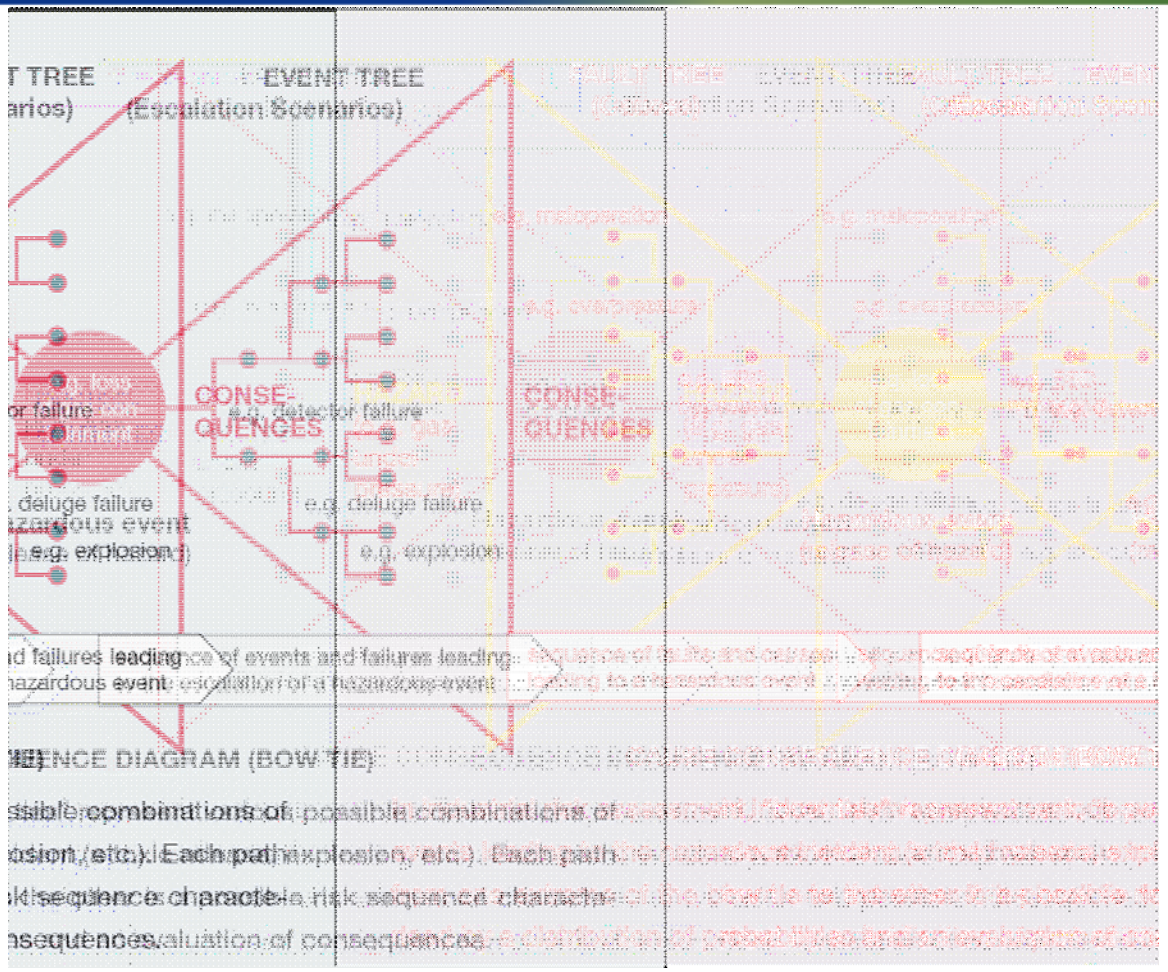
Causal Factors in Catastrophic Events

Causal Factors in Industrial Catastrophes - Simplified



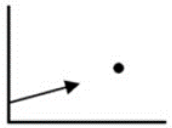
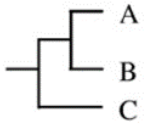
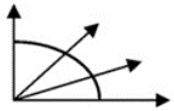
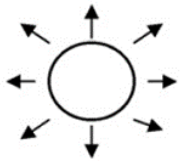
IRGC, *Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures*. 2006, International Risk Governance Council: Geneva. p. 68.

Causal Factors in Industrial Catastrophes – Bow Tie



IRGC, *IRGC (2015). Guidelines for Emerging Risk Governance.* 2015, International Risk Governance Council (IRGC): Lausanne.

Uncertainty - The Rumsfeld Revelation

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	

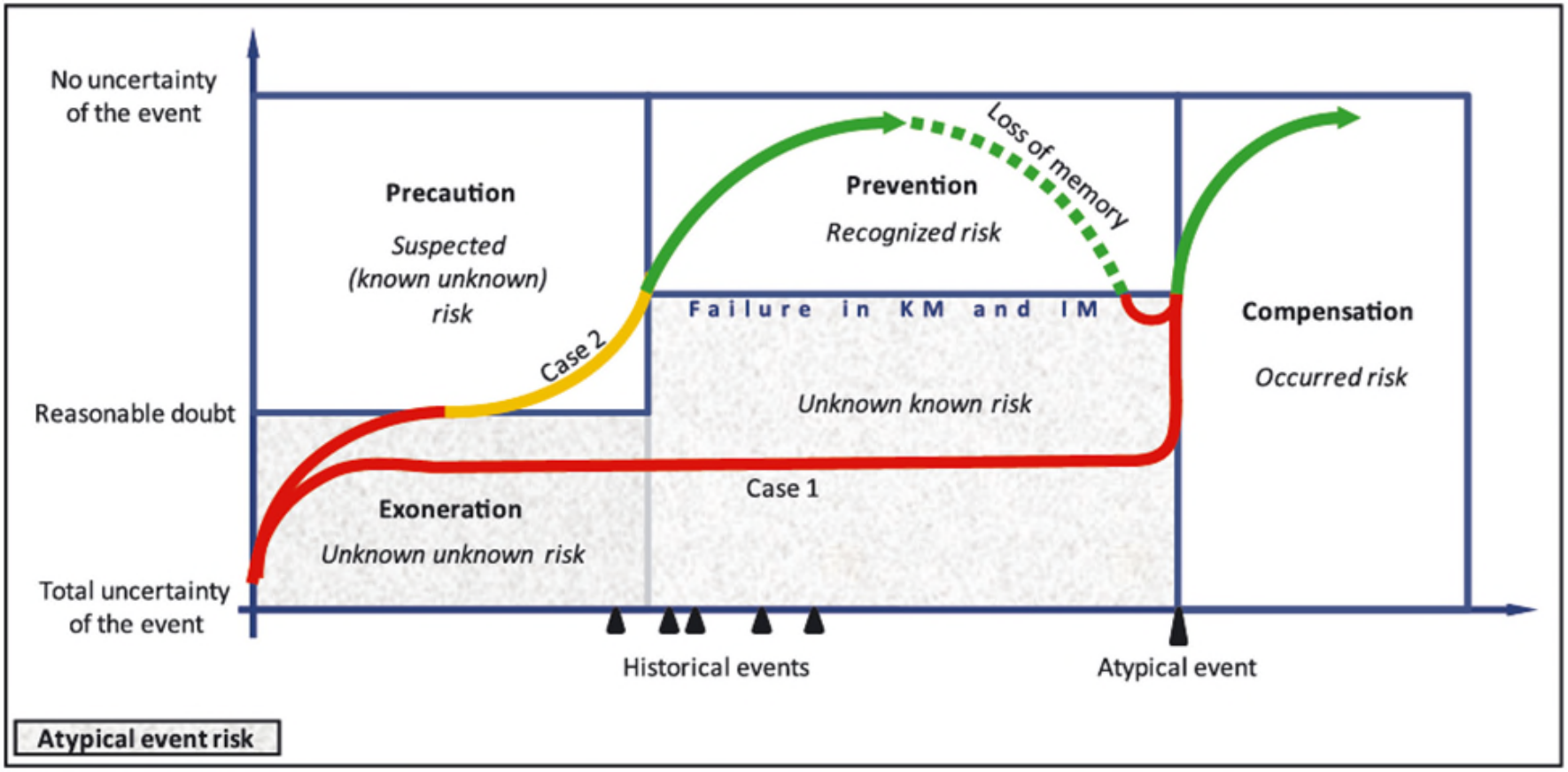
	Knowledge	Lack of Knowledge
Awareness	Known Known	Known Unknown
Unawareness	Unknown Known	Unknown Unknown

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.

Rumsfeld, D.H., *Defense.gov Transcript: DoD News Briefing - Secretary Rumsfeld and Gen. Myers.* 2002, U.S Department od Defense.

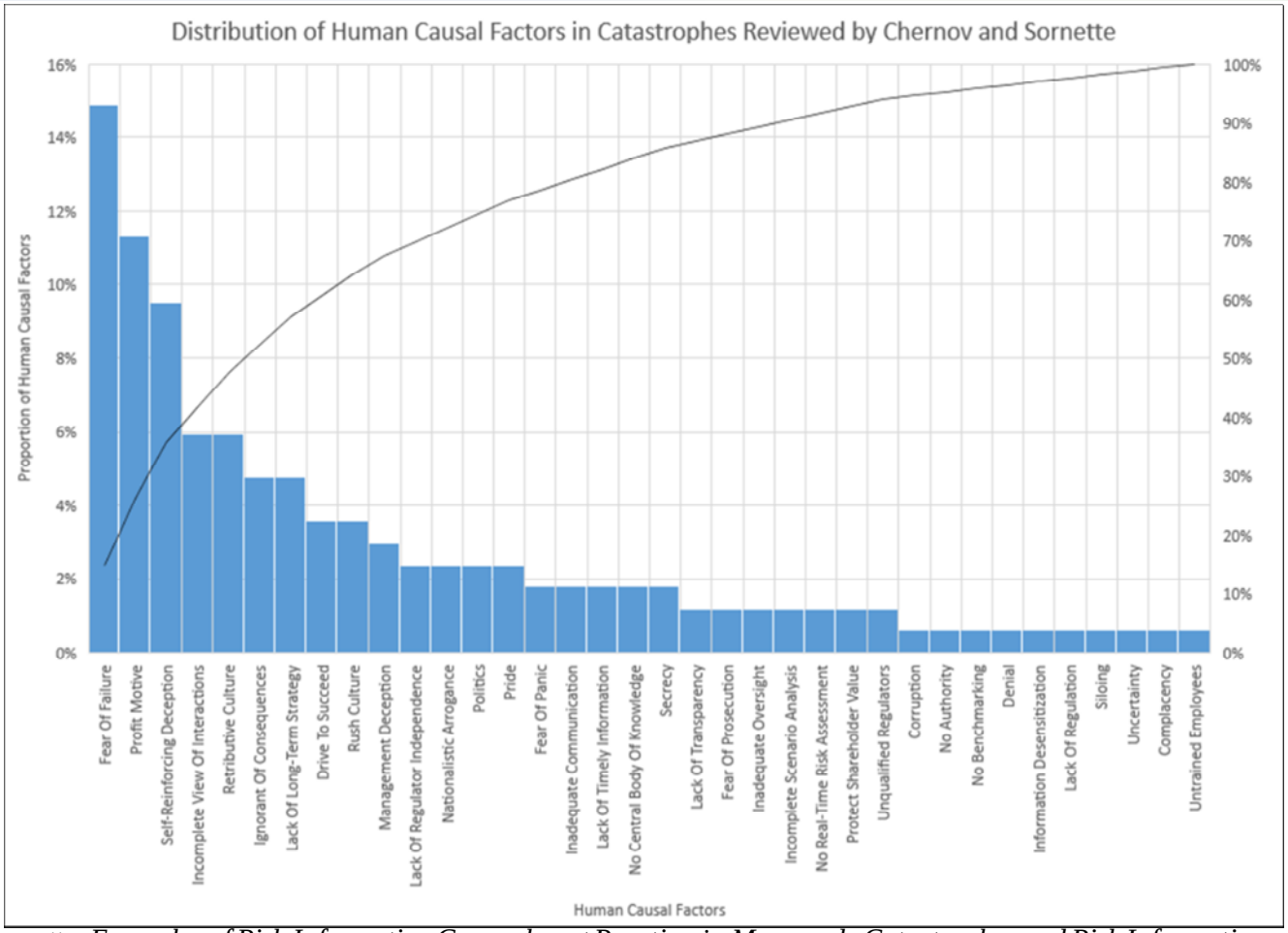
Walker, W.E., V.A. Marchau, and D. Swanson, *Addressing deep uncertainty using adaptive policies: Introduction to section 2.* Technological Forecasting and Social Change, 2010. **77**(6): p. 917-923.

Risk Management Cycle



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. – Adapted from:
Myriam, M., *Aide à la décision et expertise en gestion des risques*. 2010: Lavoisier.

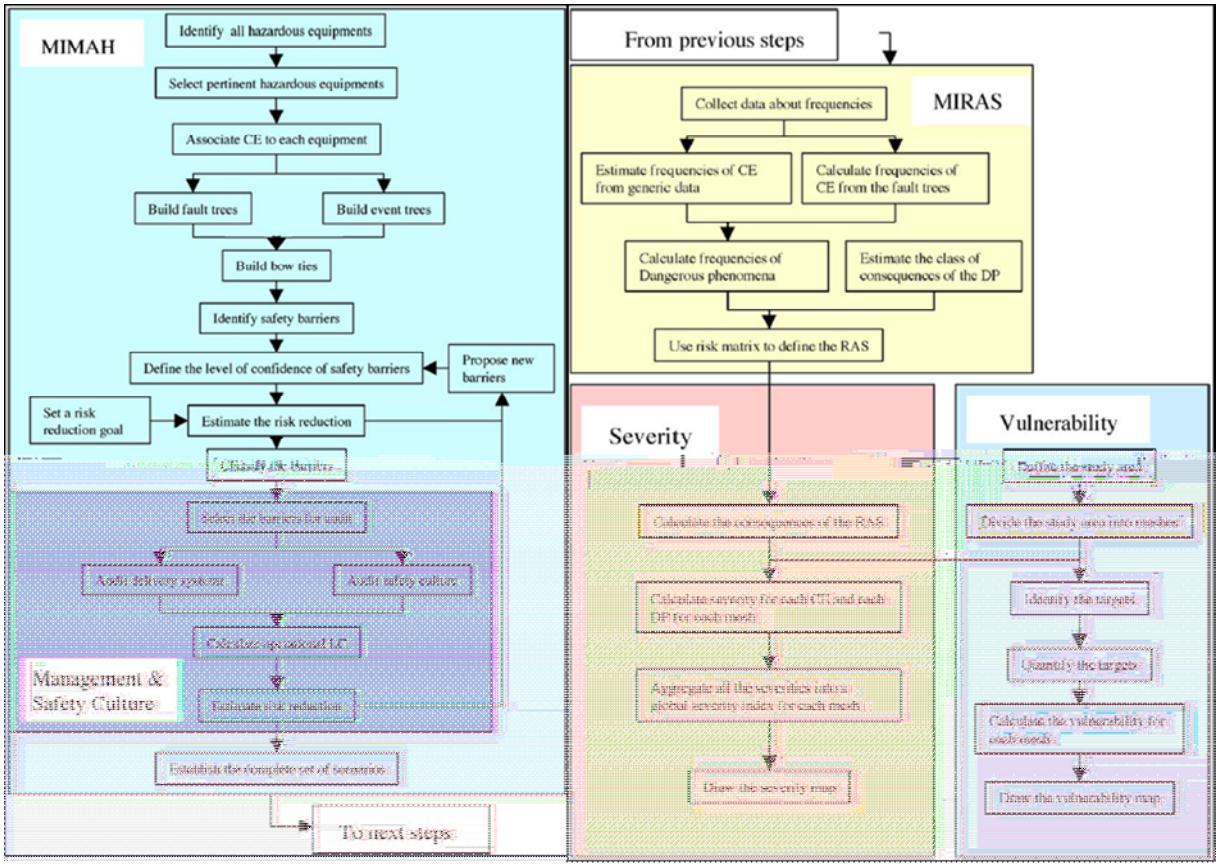
Distribution of Human Causal Factors in Industrial Catastrophes

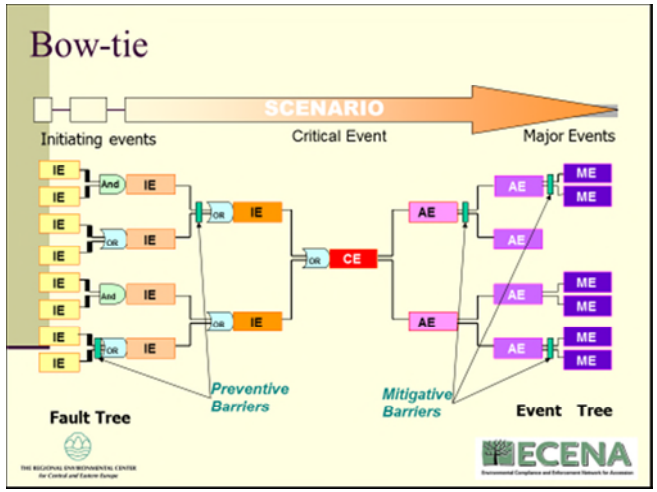


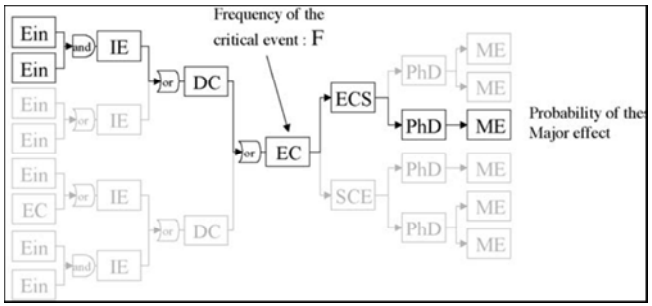
Chernov, D. and D. Sornette, *Examples of Risk Information Concealment Practice*, in *Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human Fallibility*. 2016, Springer International Publishing: Cham. p. 9-245.

Existing Risk Assessment Methodologies

Barrier Approach



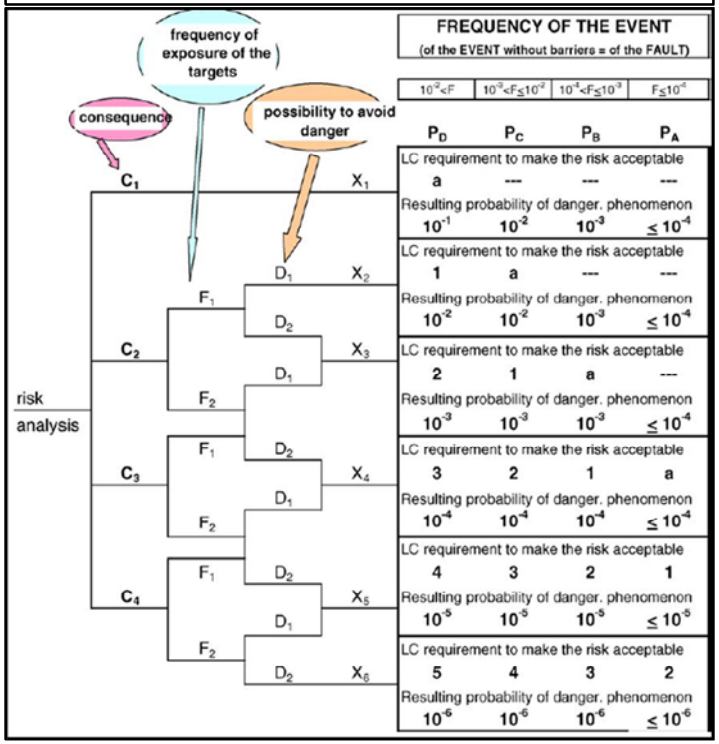


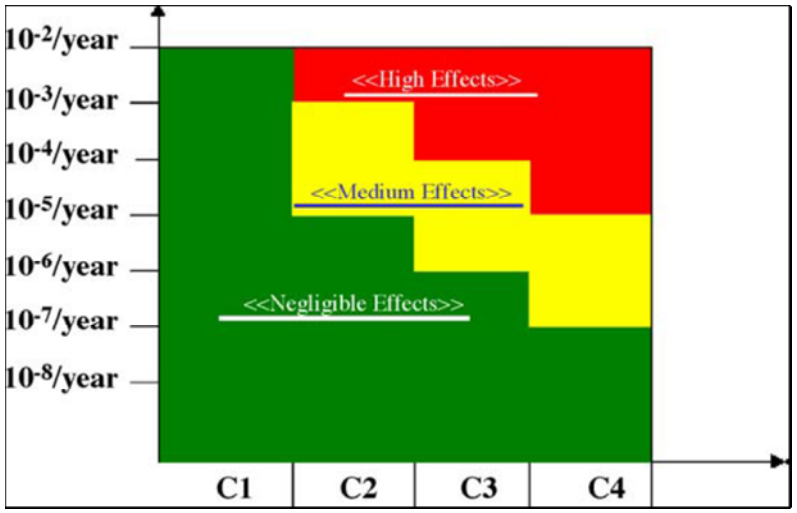


Salvi, O. and B. Debray, *A global view on ARAMIS, a risk assessment methodology for industries in the framework of the SEVESO II directive.* Journal of Hazardous Materials, 2006. **130**(3): p. 187-199.

Quantitative Risk Assessment

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 $<10^{-5}$

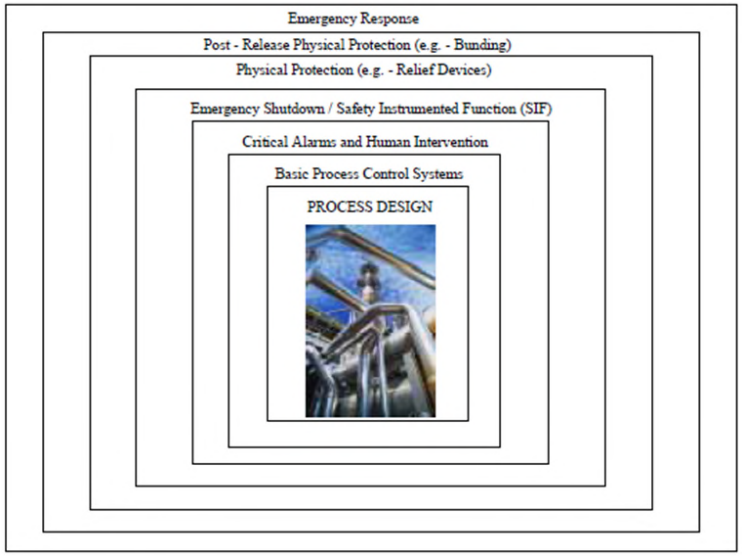


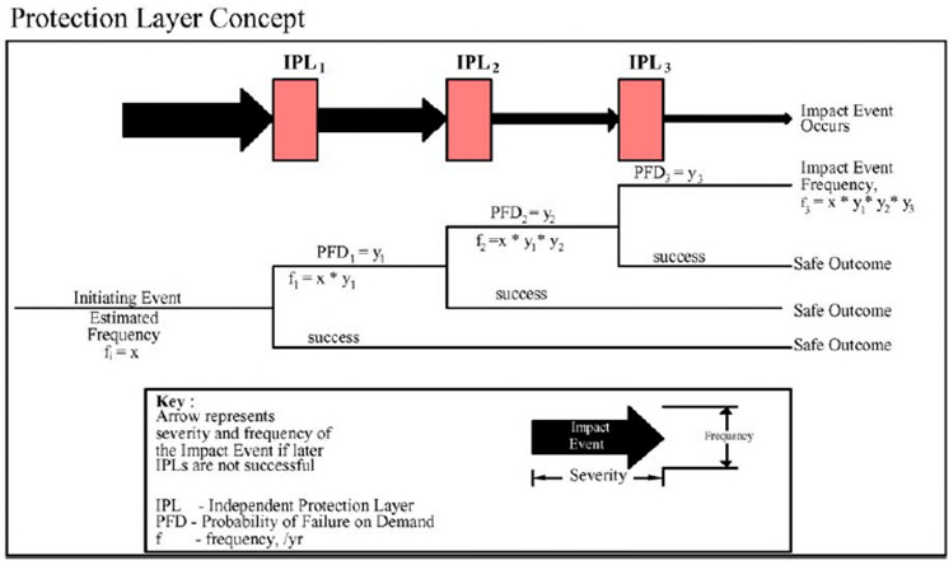


Several items that are not handled well by current QRA processes:

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

Layers of Protection





Potential advantages of the LOPA process as a simplified QRA are that it addresses a wider range of issues in addition to process control:

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

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 [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, and Herbert's review of the December 2005 explosion at the Buncefield storage site in the UK [34]. These two events occurred at facilities addressed by the Seveso directives and many years into the implementation of the methodologies

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

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

gti

Toulouse - September 21st, 2001

- 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.
- 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 now recognized as an explosive hazard.

Toulouse – Recommendations 1

- Need to improve knowledge of risks:
  - increased knowledge in the areas of technical risk prevention,
  - town planning control, and
  - crisis management measures.
- A specific emphasis was placed on improving feedback, 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

Toulouse – Recommendations 2

- Improvements are needed to improve the quality of hazard studies and their homogeneity between different industries
- 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.

Note: **Diversity and multi-disciplinary approaches needed**

gti

Buncefield – December 11th,2012

- 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.
- 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 Reinforces Safety Management Principles

- **An understanding of major accident risks**
- **Systems and a culture in place to detect signals of failure**
- **Time and resources for process safety**
- **An effective auditing system**
- **Board level engagement**
- **Constant engagement.**

History still repeats itself: Two almost identical events, to the Buncefield incident, 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 India 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.

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.

Figure 24

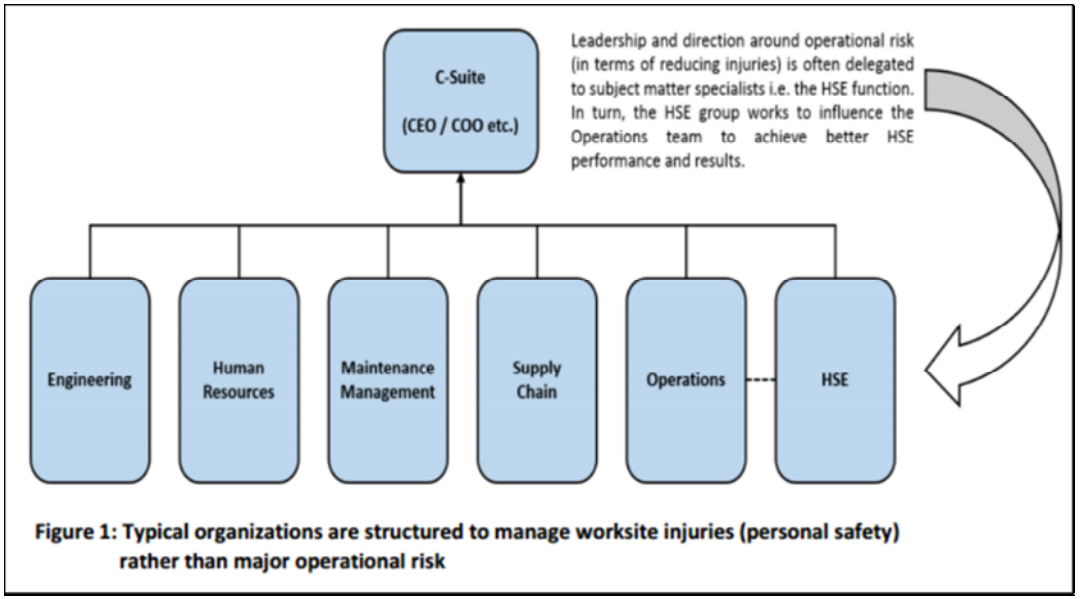


Figure 1: Typical organizations are structured to manage worksite injuries (personal safety) rather than major operational risk

"… 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!"

Figure 25

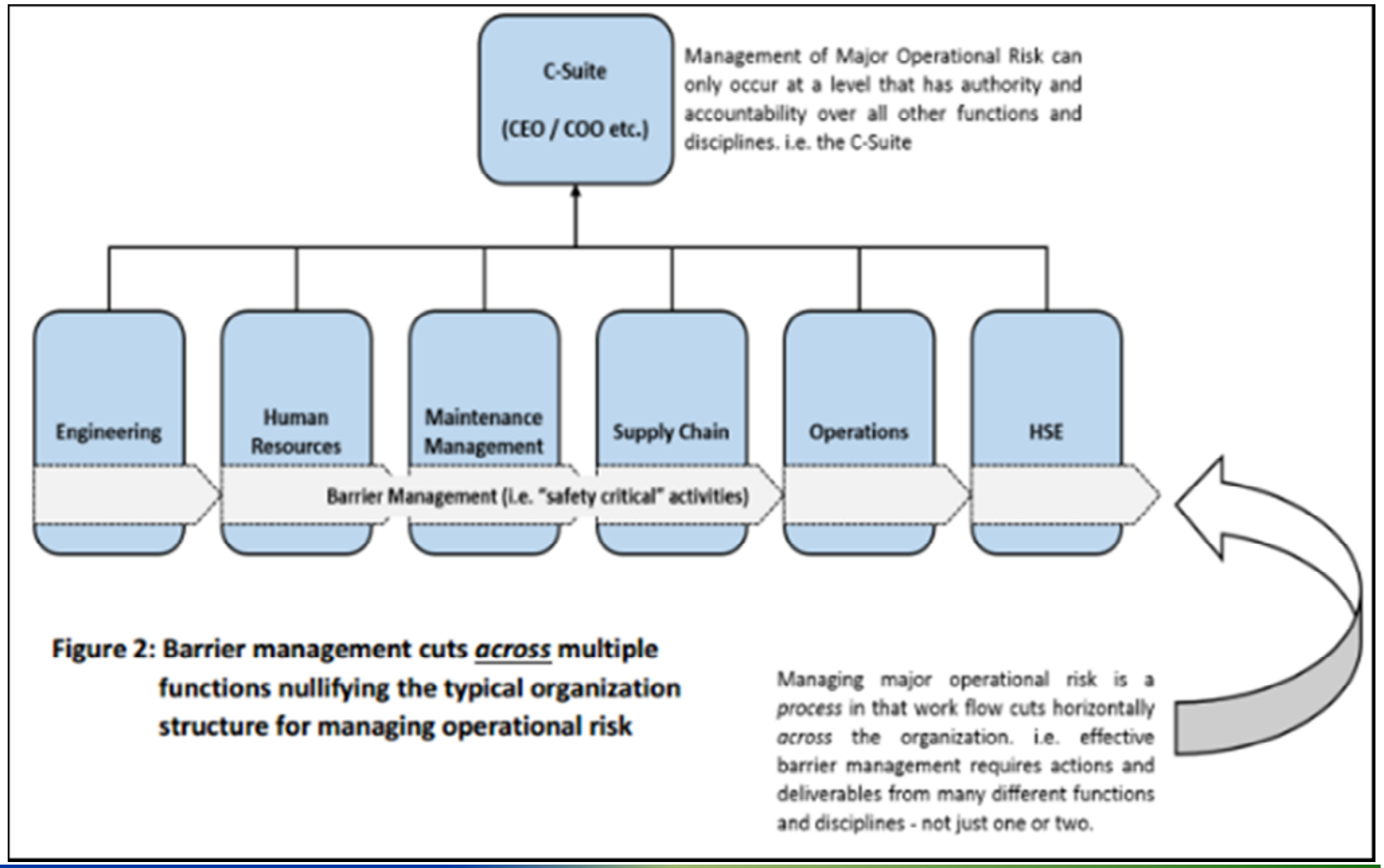


Figure 2: Barrier management cuts *across* multiple functions nullifying the typical organization structure for managing operational risk

Stakeholder Interviews

Stakeholder Interview Highlights 1

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.

Stakeholder Interview Highlights 2

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.

Stakeholder Interview Highlights 3

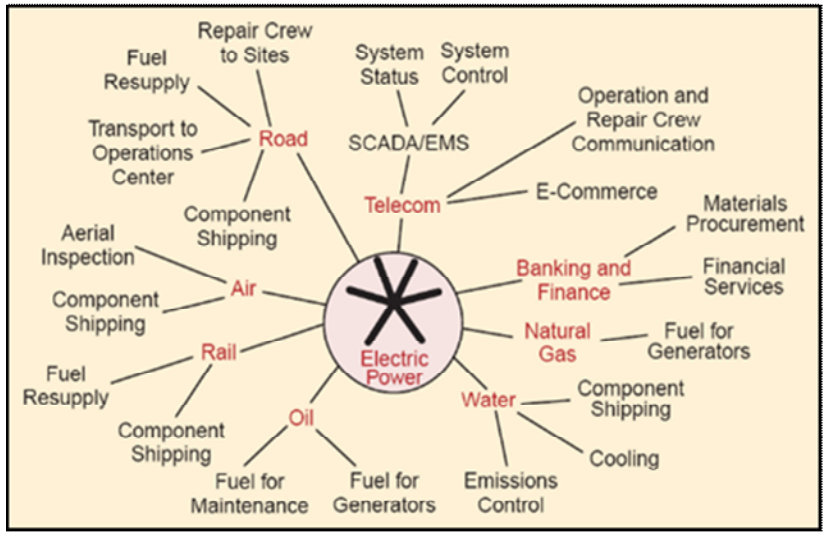
6. **Lack of Lessons Leaned, Transparency, and Internal Audits.** Not following up with lessons learned – history repeats itself. The industry needs to get better at sharing root cause information within a company and across companies. There is a lack of transparency and fear of doing internal audits 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.

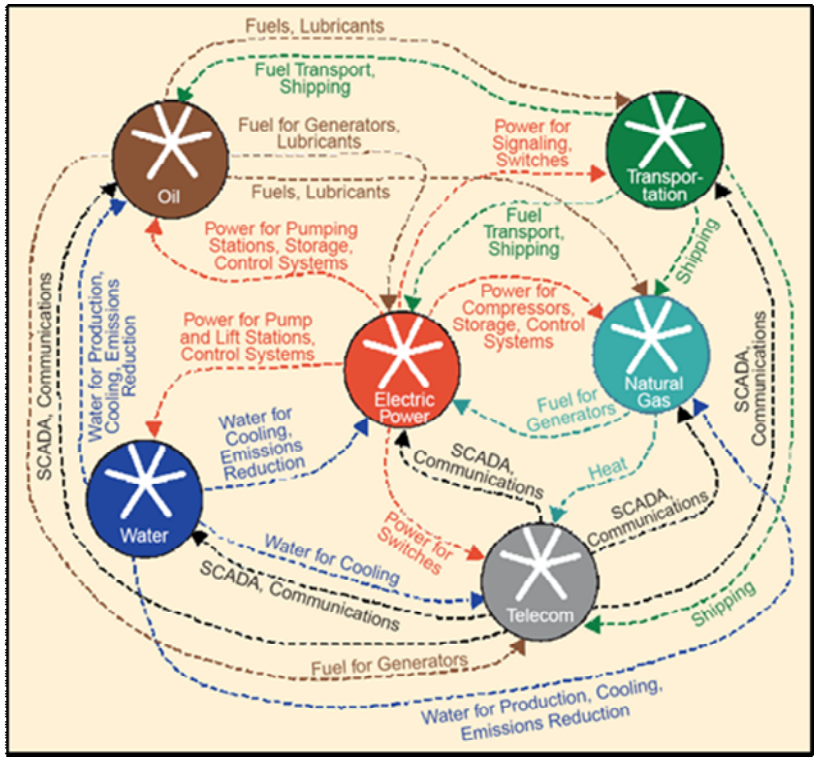
State of the Art in Risk Assessment

Moving away from linear methods

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 preventing the "black or grey swan" interactions between multiple systems that trigger 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.**

Systems of Systems thinking





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

The Good Judgment Project (GJP)

The GJP was variable based and addressed the following:

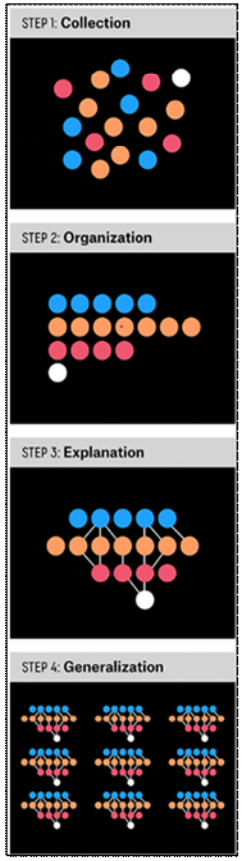
- Links between how people think and what they get right,
- Counterfactuals in the decision-process,
- Risk tolerance, and
- How to assess performance in the face of subjectivity and relativism.

Foxes and Hedgehogs

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

Addressing Deep Uncertainty Through Adaptation

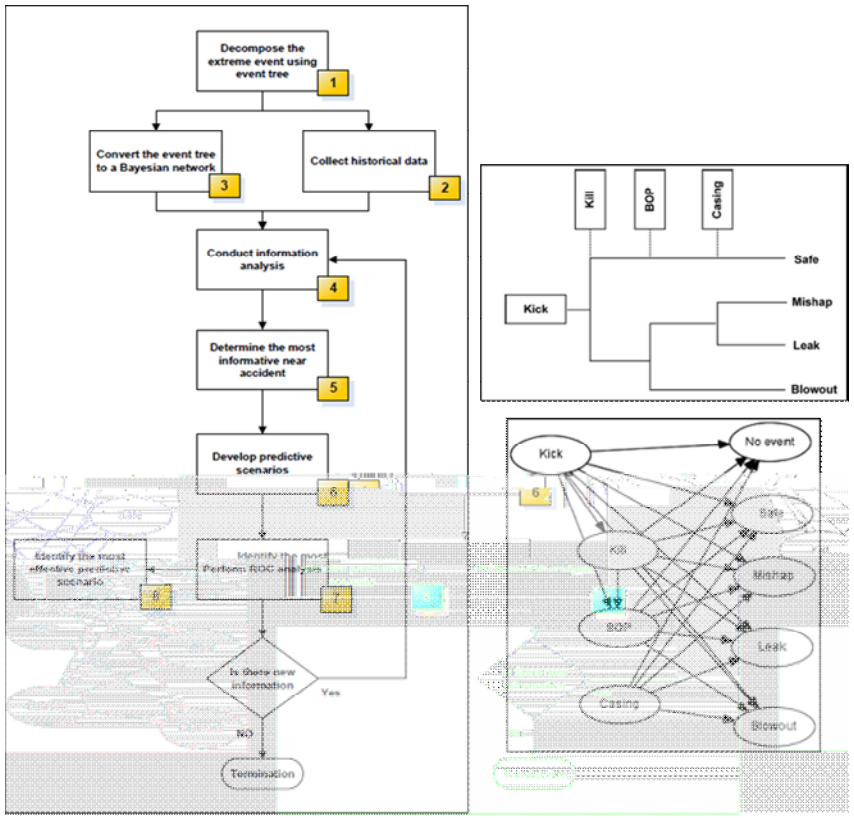


> I do not pretend to start with precise questions. I do not think you can start with anything precise. You have to achieve such precision as you can, as you go along.

1. *Integrated and forward-looking analysis*
2. *Built-in policy adjustment*
3. *Formal policy review and continuous learning*
4. *Multi-stakeholder deliberation*
5. *Enabling self-organization and social networking*
6. *Decentralization of decision making*
7. *Promoting variation*

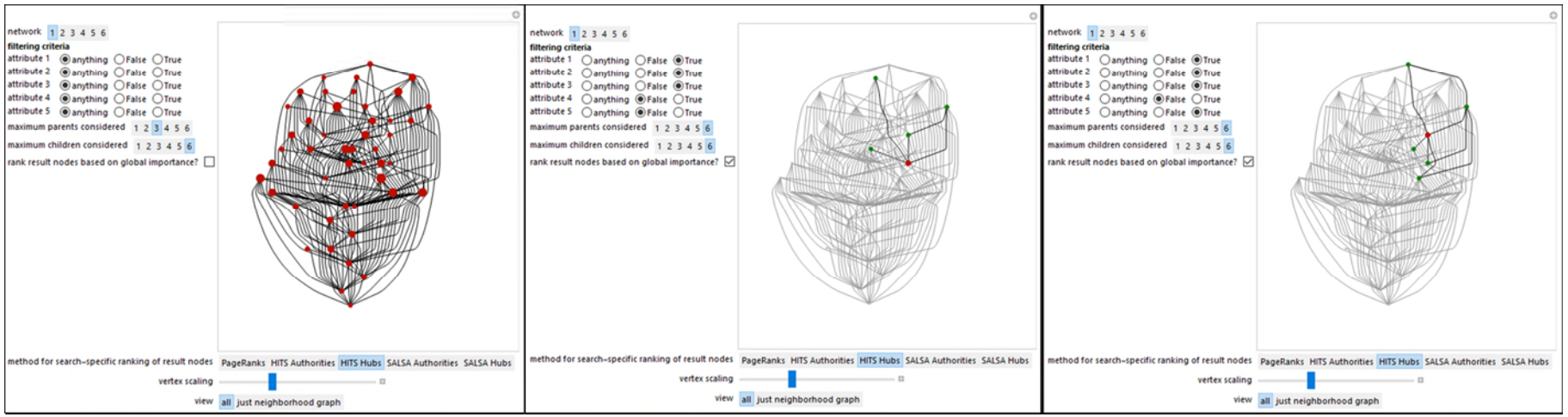
Walker, W.E., V.A. Marchau, and D. Swanson, *Addressing deep uncertainty using adaptive policies: Introduction to section 2.* Technological Forecasting and Social Change, 2010. **77**(6): p. 917-923.

Likelihood Modeling Using Accident Precursors and Approximate Reasoning



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.

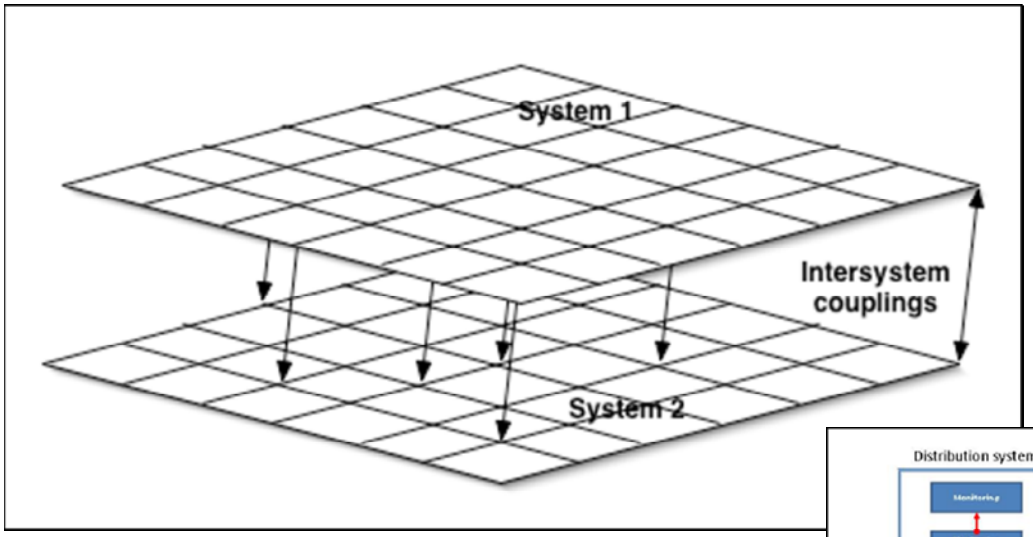
Understanding Complex System Interactions

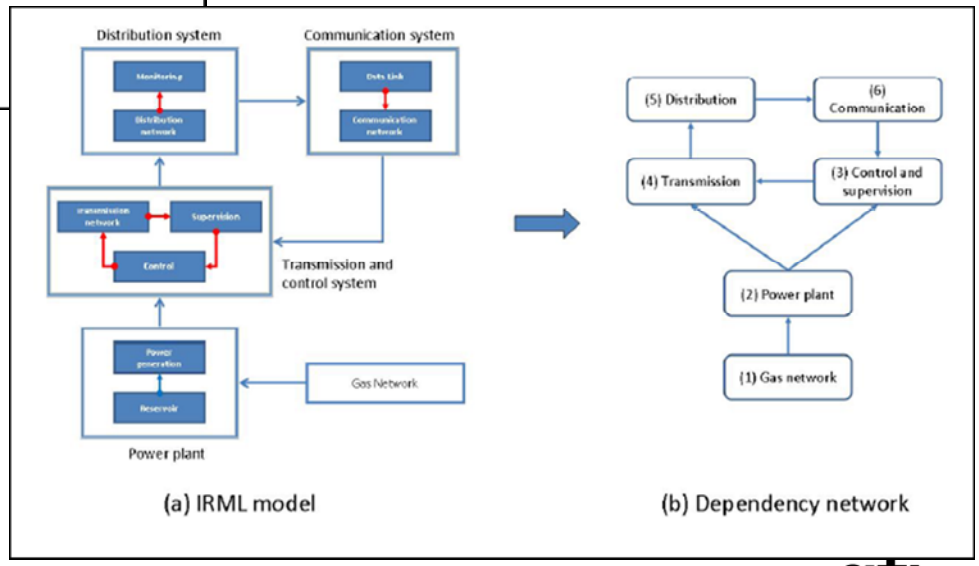


Klein et al. and Bar-Yam [64, 65] have written about how the methods and science of complex systems can be applied to the collaborative design and how evolutionary approaches based on biological systems can be helpful in breaking down the enormous task of trying to balance the design requirements of 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.

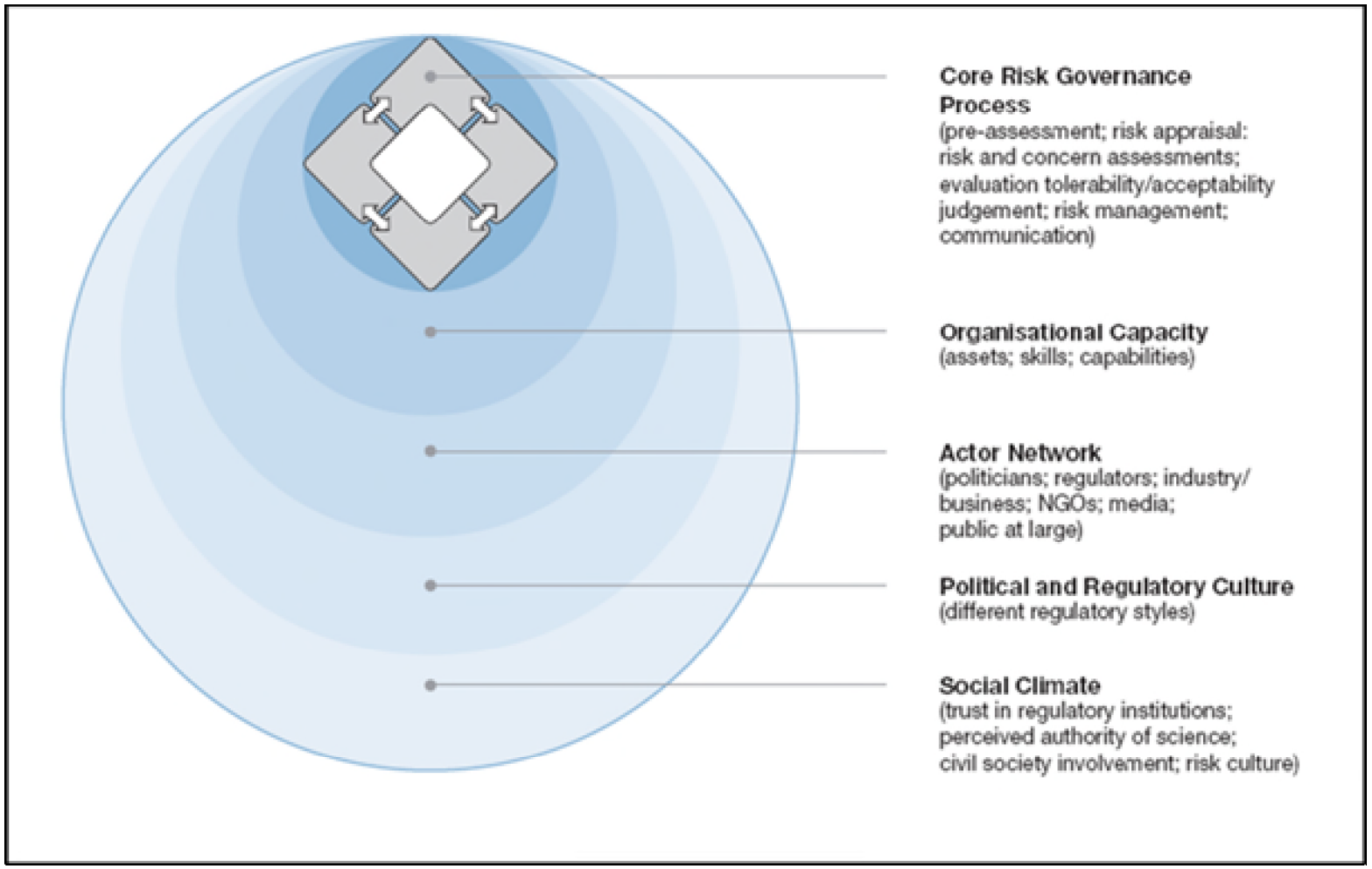
Understanding Coupled Systems



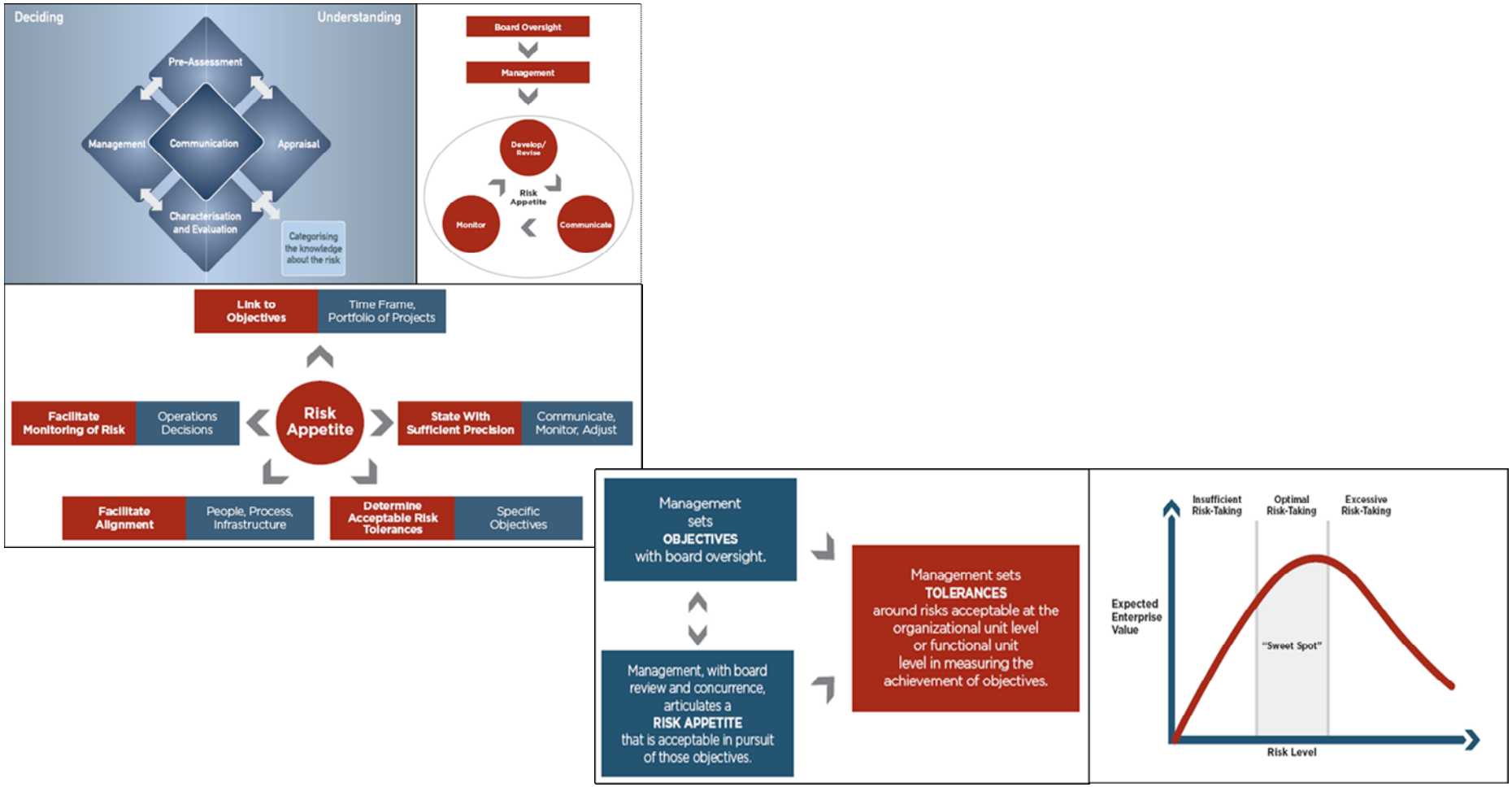


Risk Governance Frameworks

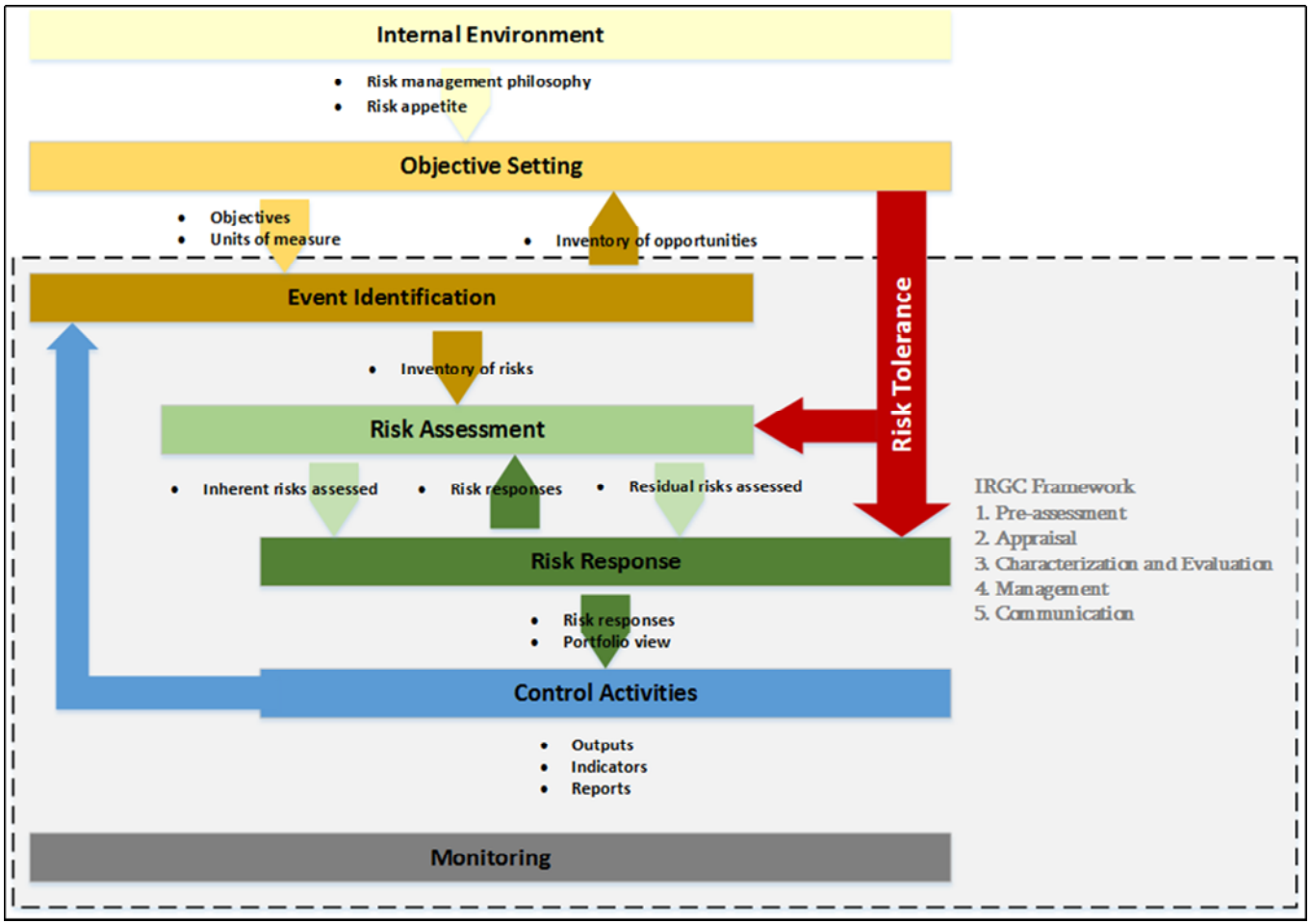
Risk Governance Frameworks



Risk Appetite, Tolerance, Management



Enterprise Risk Management



What are the enhancements?

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.

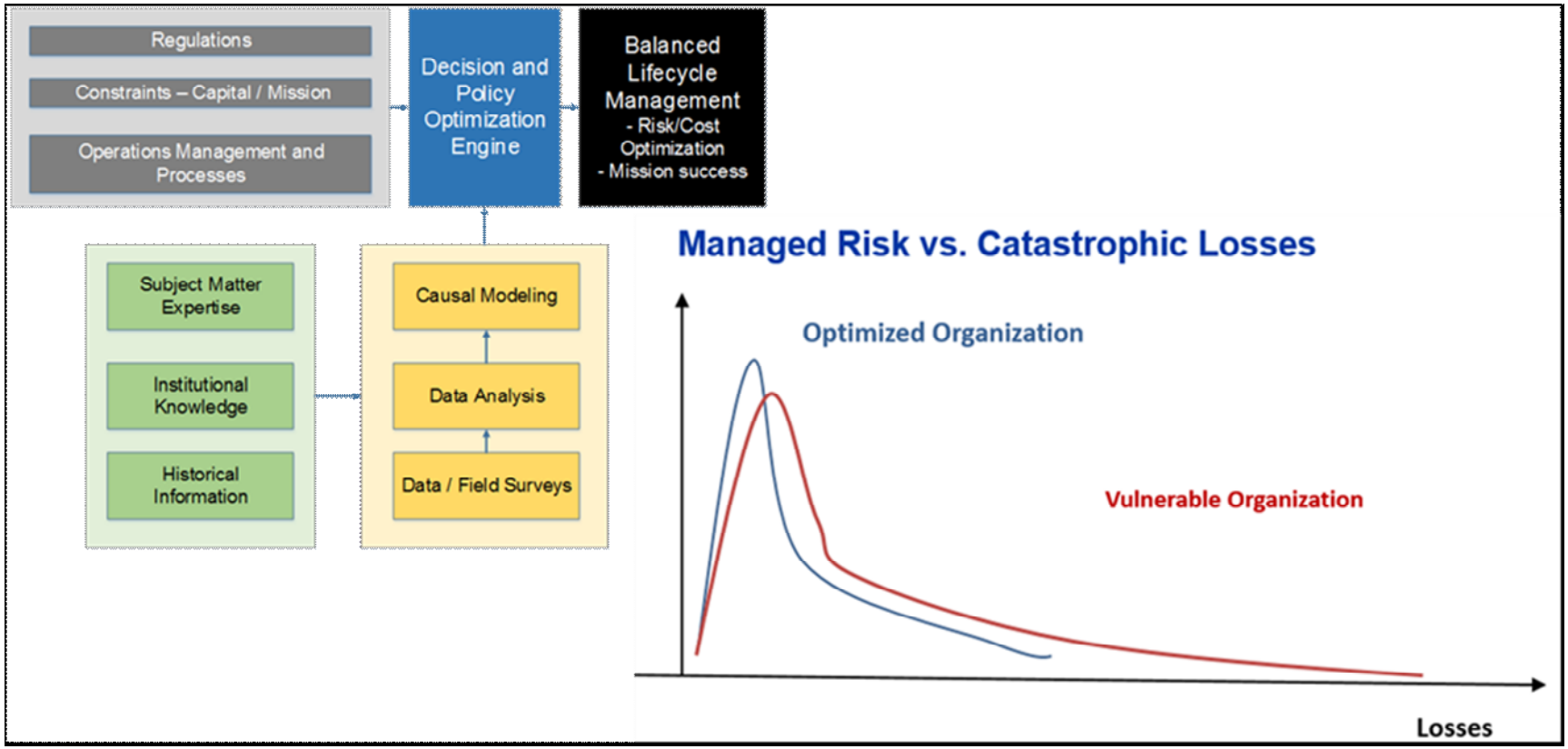
Conclusions

Conclusions

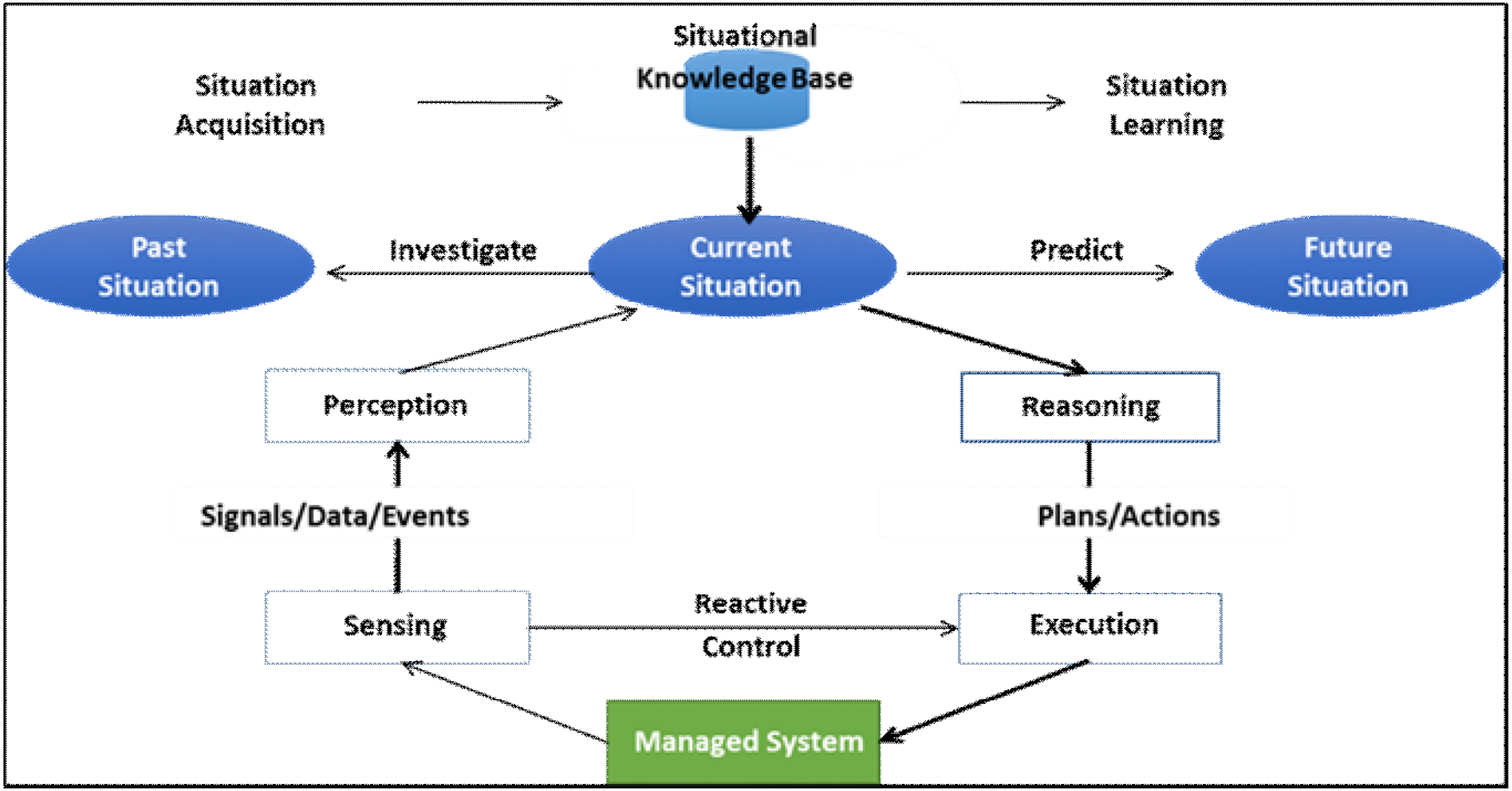
At the macro level, frameworks to achieve these ambitious goals have been proposed in the United States by the National Science and Technology Council (NTSC) and in Europe by the International Risk Governance Council (IRGC). These frameworks do an adequate job of covering the aspects of an improved worldwide,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

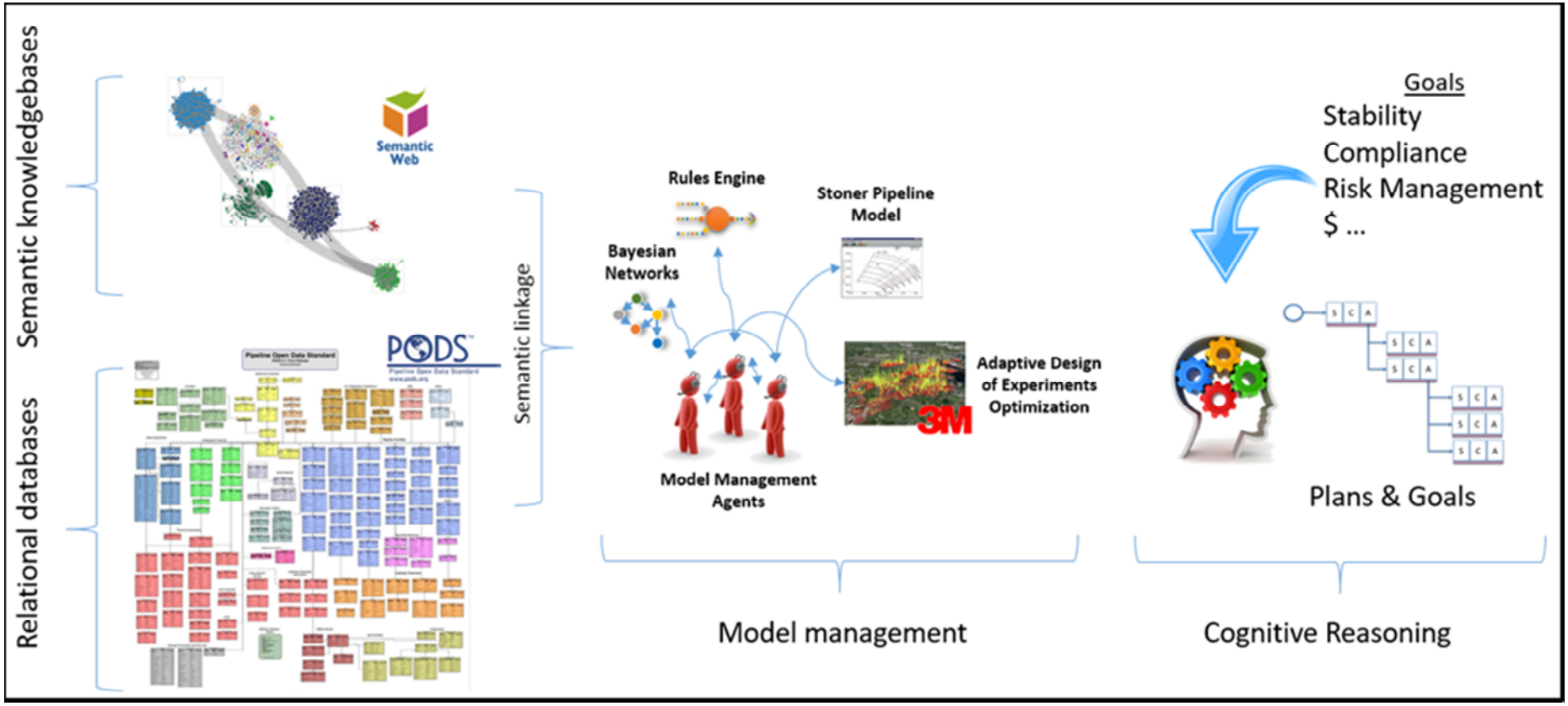
Potential System Architecture



Cognitive Reasoning Framework



Integration of Data into Cognitive Reasoning Framework



Questions?