Conceptual Paper

Open Access CrossMark

What is safe?

Conceptual paper

Volume 1 Issue 1 - 2016

Robert Bea
Department of Civil & Environmental Engineering, University of California Berkeley, USA

Correspondence: Robert Bea, Department of Civil & Environmental Engineering, University of California Berkeley, USA, Email rmbeachy@yonsei.ac.kr

Received: September 14, 2016 | **Published:** September 22, 2016

Every day, I hear a word that makes me wince. That word is 'safe.'

I wince because I have listened to people who have insisted what they did was safe. Later, I learned what they did was not safe. I wince because I have asked many qualified people, including engineers, what the word safe means. Almost without exception, I have gotten muddled answers. If I pressed the discussion and asked how they could prove that something was safe, I either got dismissive answers like 'everybody knows it is safe,' it was done according to some 'prescribed' code or guideline, or 'take my word for it.'

In this paper, I will use a formal definition of the word safe: "freedom from undue exposure to injury or harm." There are two important parts to this definition. The first is "freedom from undue exposure." The second is "injury or harm."

The beginning

As a young engineer, I did not receive training in how to understand, evaluate, and manage different types of ambiguities; to understand and successfully cope with the uncertainties influencing how different types of systems were engineered, constructed, operated, and maintained. Frequently, Factors-of-Safety (ratio of Capacity to Demand) appeared magically in the engineering processes. Safety of the systems engineers designed was discussed; it was emphasized that engineers should hold public safety as a priority, but there was no instruction in how to determine if a system was safe or not safe. In many cases, it was assumed that something was safe if it was designed according to some generally accepted engineering code or guideline.

Types of uncertainties

I have learned there are different types of ambiguities - things that are doubtful or uncertain. These different types of ambiguities must be assessed and managed in different ways. There is not a 'one size fits all' approach to either characterize or manage uncertainties.

To provide organization and structure for classification, description, and analyses of the different types of ambiguities, they have been organized here into two fundamental categories (Table 1): 1) Intrinsic - belonging to the essential nature, and 2) Extrinsic - what comes from outside of something.

Table 1 Classification of sources of uncertainties

Intrinsic	Extrinsic
Type 1 – Natural, Inherent, Information Insensitive	Type 3 – Task Performance
Type 2 – Analytical, Information Sensitive	Type 4 – Knowledge Development
	(a) – Unknown Knowables
	(b) – Unknown Unknowables

There are two types of intrinsic uncertainties: Type 1- natural, inherent, information (data) insensitive, and Type 2 - analytical modeling (qualitative and quantitative), parametric, state, information sensitive. Knowledge and data can be used effectively to reduce Type 2 uncertainties. Other means like Factors-of Safety can be used to cope with Type 1 uncertainties.

There are two types of extrinsic uncertainties: Type 3 - human and organizational task performance; and Type 4 -human and organizational information development and utilization. Results from Extrinsic uncertainties frequently are identified as 'human errors.' Experience has amply demonstrated that such errors are results from human and organizational processes and are not the 'root causes' of accidents and failures.[1–3] Human errors are results, not causes.

Type 4 uncertainties have been divided into two sub-categories: a) Unknown Knowable - "Predictable Surprises"[4] or "Black Swans" (Table 2007),[5] and b) Unknown Unknowable's[6] not predictable or knowable before something is done. In the case of Unknown Knowables, the knowledge exists but has not been properly accessed, analyzed, and understood. In the case of Unknown Unknowables, the knowledge does not exist and the uncertainties and their effects are not predictable. In this case, the knowledge must be developed at different times and ways during the life of a system, properly analyzed, and appropriate actions taken to understand these uncertainties to enable preservation of the operational integrity of a system. Recognition of and preparation for Unknown Unknowable uncertainties makes it clear that processes to understand and manage uncertainties performed before a system exists and is operated can and never will be complete. Developing safe and reliable systems is a continuing 'improvement' process to properly recognize and defend systems for ambiguities.

Management of uncertainties

A primary method to manage Type 1 uncertainties is with Factors-of-Safety (FoS) incorporated into the different parts of a system. The FoS is the ratio of the element or system (assembly of elements) Capacity (force and displacement resistance) to the Demand (forces and displacements) imposed on or induced in the element or system. The Capacity (demand resistance) can be increased and/or the Demand decreased. Often, the element or system is deemed to be 'Safe' if the Capacity exceeds the Demand and 'Not Safe' if vice versa. Greater Type 1 uncertainties require larger FoS.

Frequently, the 'design Demand' conditions and FoS can be found in engineering codes and guidelines. In most cases, these design conditions and FoS have been developed by professional engineering

Submit Manuscript | http://medcraveonline.com

© 2016 Bea. This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and build upon your work non-commercially.

Copyright: ©2016 Bea et al.

societies. In these cases, there has been sufficient 'good experience' with certain types of systems so the design conditions and FoS can be developed from system performance 'hindcasts' (backward looking analyses).

The difficulties with this approach develop when the systems are modified or used in conditions that have not been included in the referenced 'good experience'. This difficulty becomes even more important when aging systems need to be addressed together with the aging processes that lead to greater Type 1 and Type 2 uncertainties. Additional challenges develop when the potential consequences of failures have increased as a result of changes in the natural or 'social' environments in which the systems exist. What was deemed Safe for the original environments can no longer be deemed for the changed environments.

A very important part of management of intrinsic uncertainties is properly addressing Type 2 uncertainties. These uncertainties are 'information sensitive.' Reliable data and information on the performance of elements and systems when they are subjected to intense Demands (e.g. load testing) can provide vital information needed to validate and calibrate analytical models. These data based validation processes can provide information that can be used to better define Type 2 uncertainties. Investments in gathering and analyzing data can be shown to pay substantial economic rewards. Explicit treatment of Type 2 uncertainties leads directly to rejection of unproven invalidated analytical models. This is an important wake up call for many who may not be taught to question the validity of the analytical models they use in their work; particularly, when these analytical models are embedded in complex computer programs.

Extrinsic uncertainties can be addressed with leadership and management developed by High Reliability Organizations (HROs)[7] with High Reliability Management[8] that develop High Reliability Systems.[2]

Three interrelated and interactive approaches are used by HROs to continually access and manage extrinsic uncertainties:

a. Proactive management performed before activities are conducted,
b. Interactive management conducted during activities, and
c. Reactive management conducted after activities are concluded.

Each of these approaches is based on three primary strategies:

i. Reduce the uncertainties,
ii. Reduce the effects of uncertainties, and
iii. Increase the proper detection, analysis, and correction of the adverse effects of uncertainties.

These three approaches and strategies are intended to develop effective 'barriers' to continually assess and manage system risks - barriers to maintain 'acceptable' likelihoods and consequences of failures.

Application of these HRO system management approaches is very dependent on the time and other resources available for their development, validation, and implementation. If there is a lot of time and other resources available (days, months), then the goal can be to develop approaches that can result in optimized solutions. If time is very limited (seconds, minutes, hours), then the goal is to implement approaches and mobilize resources that can result in survival - non-failure conditions. This is crisis management[9] Systems need to be prepared with people and system 'supports' that enable proper management of both types of situations.

Engineering approaches typically do not explicitly address Extrinsic uncertainties. Often, engineering approaches are premised on 'effective' assessment and management of Extrinsic uncertainties using 'specified' Quality Assurance and Control (QA/QC) and 'good' HRO leadership and management processes. Omission of explicit analysis of and provisions to cope with Extrinsic uncertainties is one of the primary reasons why traditional engineering approaches can result in significant underestimates of the likelihoods and consequences of major system failures and in overly optimistic evaluations of the 'safety' of such systems. Similarly, neglect of explicit consideration of Extrinsic uncertainties can lead to Root Cause Analyses that do not properly address the true root causes because they focus on 'what broke'. Rarely are specified QA/QC and good management processes perfect. Consequently, they can produce predictable and unpredictable undesirable outcomes. Of major importance is the definition and characterization of the particular 'system' that is being considered. Systems are comprised of seven primary parts:

a. Operating groups with daily responsibilities for the functionality and performance of the system,
b. Organizations that determine the means, methods, and resources used by the operating groups,
c. Hardware utilized by the operating groups and organizations,
d. Structures that provide the support and protection for the operators and operations,
e. Procedures and processes (formal, informal) used by the operators,
f. Environments in which the operations are conducted (external, internal, social), and
g. The interfaces among the foregoing. These components are highly interrelated, interconnected, and interdependent. Systems are highly dynamic and organic - adaptive. Systems are not uniform, homogenous, and static or unchanging.

These characteristics pose special challenges for assessment and management of ambiguity. Assessment and management of ambiguity is never complete, never perfect, and often not appreciated until it fails. These characteristics also pose special challenges for engineers and engineering. Engineers typically address some parts of systems-often, the hardware and structure components-sometimes the procedure components (e.g. computer programs). The behavior and performance of the entire system is rarely adequately understood or addressed by engineers and engineering. Engineers are typically taught to decompose a system into its parts and focus on the parts. The vast majority of engineering analytical models are 'static', not dynamic and organic - changing and adaptive to the multiple environments in which real systems exist.

Proactive management is intended to prepare systems so they are ready and able to cope with the hazards and threats they will face during their lives - to reduce the likelihoods and consequences of major system failures so the associated risks (combinations of likelihoods and consequences of failures) are maintained to be tolerable and acceptable. A key part of this work is to eliminate the potential for Unknown Knowable and to learn all that can be learned

Copyright: ©2016 Bea et al.

about the constitution and performance of a particular system.

Another key part of this work is to acknowledge and prepare for Unknown Unknowables. For many, if not most engineers, this is a foreign concept because the majority of engineering work is focused on predictability - knowability. Effective management of Unknown Unknowables requires two basic things: 1) people supports, and 2) system supports. Such management supports needs to be provided for the system operators who have daily responsibilities for the safety of the system.

People support strategies include such things as selecting personnel well suited to address unknown unknowable ambiguities, and then training them so they possess the required skills and knowledge to properly understand the ambiguities and implement corrective actions to mitigate their negative effects. Training needs to encompass normal daily situations, unusual situations, and 'unbelievable' unusual situations that require development of innovative methods that can return the system to a safe state. Re-training is important to maintain skills and achieve vigilance. The cognitive skills developed for management of unknown unknowable ambiguities degrade rapidly if they are not maintained and used.

Unknown Unknowable management teams should be developed that have the requisite variety to manage the crisis and have developed teamwork processes so the necessary awareness, skills and knowledge are mobilized when they are needed. Auditing, training, and re-training are needed to help maintain and hone skills, improve knowledge, and maintain readiness. Unknown Unknowables management teams need to be trained in 'divide and conquer' strategies that preserve situational awareness through organization of strategic and tactical commands and utilization of 'expert task performance' (specialists) teams. Unknown Unknowables management teams need to be provided with practical and adaptable strategies and plans that can serve as useful 'templates' in helping manage each unique situation. These templates help reduce the amount and intensity of cognitive processing that is required to manage the situation.

System support includes factors such as improved maintenance of the necessary critical equipment and procedures so they are workable and available as an unknown unknowable development unfolds. Data systems and communications systems are needed to provide and maintain accurate, relevant, and timely information in 'chunks' that can be recognized, evaluated, and managed. Adequate safe haven and life saving measures need to be provided to allow Unknown Unknowable management teams to face and manage the developments, and if necessary, escape. Hardware and structure systems need to be provided to slow escalation of the developments, and re-stabilize the system. Safety system automation needs to be provided for the tasks people are not well suited to perform in emergency situations.

Another key part of Proactive management is to develop systems that are Robust - damage and defect tolerant of the adverse effects from extrinsic uncertainties. These are not 'minimum' initial cost systems. These are not hemophiliac systems that when scratched, bleed to death and fail. These are 'hell for stout' systems designed to help people succeed in their operations.

Robust systems can safely tolerate the effects of large defects and damage developed by Extrinsic uncertainties. Experience has shown that robust systems result from a combination of four essential things:[2] 1) excess capacity to withstand system demands, 2) proper configuration so there are alternative ways to handle the system demands, 3) very high ductility or 'stretchability' so that the system can tolerate excess demands without loosing capacity, and 4) appropriate 'associations or correlations' - high and positive for 'series - weak link' system components and low for 'parallel' element components in which all of the elements must fail before there is failure. These robustness guidelines apply to all of the important parts of a system, particularly the human and organizational components. Since explicit assessment and management of Extrinsic uncertainties is traditionally not included in engineering, it is easy to understand how non-robust, first cost minimized hardware and structure systems often are developed by engineers.

Reactive assessment and management of ambiguity is intended to prepare systems to cope with failures - to reduce and control the short and long-term consequences associated with failures. Reactive management is based on the premise that systems can fail and that the goal is to make the failures have minimum consequences. System Reactive management also is intended to develop deep understanding of the lessons taught by near misses and system failures and then use this knowledge to help further defend or protect the system. Organizations that have good Reactive management are rapidly learning and highly adaptive organizations. They make the right decisions at the right times in the right ways.

Interactive assessment and management of ambiguity is performed during the operations conducted during the life of system; from the time the system is conceived until it is decommissioned. Interactive management frequently takes the form of QA/QC processes. Interactive management also frequently takes the form of Crisis Management and provides mechanisms that allow the effects of unknown unknowable uncertainties to be properly detected, analyzed, and managed. In this way, potential failures and hazards that are not foreseen or predicted can be managed to prevent major system failures. The people and system supports previously discussed provide the essential elements needed for successful Interactive assessment and management of uncertainty. Interactive assessment and management of ambiguity explicitly acknowledges the limitations in predictability of the performance of systems and prepares systems including the system operators to successfully cope with these ambiguities. These processes require significant investments to provide adequate people and system 'supports', resources, and protections. Properly preparing to manage unknown unknowable uncertainties is not quick, easy, or free. Proper preparations are essential to develop and maintain the performance of a system when faced with unpredictable - unknowable hazards and threats.

Risk assessment

Risk is characterized as the likelihood of 'failure' (undesirable performance) of an element or system (comprised of elements) and the consequences that result from such failures (Figure 1). Consequences of failure can be expressed using different metrics such as monetary, productivity, injuries to people and the environment. The 'risk space' is divided into two quadrants identified as 'Safe' and 'Not Safe'. The Safe quadrant contains combinations of likelihoods and consequences of failures that are 'acceptable' or 'tolerable'. The 'Not Safe' quadrant contains combinations of likelihoods and consequences not acceptable or tolerable.

Often, risk is expressed as the product of the likelihood and consequences of failure. This expression of risk can be interpreted as the 'expected' (or best estimate) of the risk if the expected values of the likelihood and consequences of failure are used. Because there are significant uncertainties associated with assessments of both

the likelihoods and consequences of failures, there are important uncertainties associated with risk assessments. This additional uncertainty dimension of results from risk assessments can have important effects on development of decisions about what constitutes tolerable or acceptable risks.

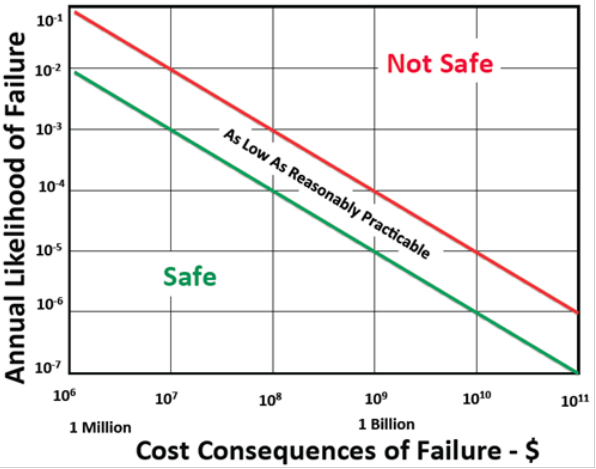

Figure 1 Example risk space identifying Safe and Not Safe risks based on the annual likelihoods of failure including Types 1-4 uncertainties and the consequences of failure measured in 2010 U.S. dollars.

Earlier, the concept of the engineering FoS and the assumption that an element or system was safe if the FoS was greater than unity were introduced. This is the traditional engineering definition of what constitutes something that is safe. But, there is a major problem with this definition when it is recognized that both the element and system Capacity and Demand are uncertain and that these uncertainties can change substantially during the life of the element or system.

Typically, engineers are not taught how to determine the safety or 'Reliability' (likelihood of developing desirable system performance) of the things they engineer. Historically, FoS have been developed primarily based on experience. Typically FoS are focused on the elements that comprise systems, not on the performance of the entire system. If an element or system worked well when it was put into place and operated, then it was replicated. If there were failures, then the FoS would be increased. If there deficiencies in QA/QC or management, then improvements to correct the deficiencies would be made. This 'try, try again' experience based process characterized much of engineering until late in the 20th Century.

It was not until potentially very hazardous or potentially 'high risk' systems (e.g. commercial nuclear power generation, commercial aviation) were engineered that the experience based process was modified so the performance characteristics of such systems could be assessed before new systems were put into operation. A variety of experimental and analytical processes were developed to help address the performance characteristics of these high risk systems before they were put into operation. An example of this progress is commercial aviation, particularly associated with commercial jet-powered aviation transportation. Formal ways were developed to quantitatively evaluate safety, reliability, and potential risks associated with these complex systems - including both hardware and human parts. These quantitative processes were used to help define systems that had desirable performance characteristics before the systems were put into operation. Prototype experimental testing methods were used to validate these proposed systems could produce desirable performance characteristics - including potential risks and safety characteristics.

A special challenge develops when it is realized that safety is not an absolute term; safety is relative. Formally, safety can be defined as "freedom from undue exposure to injury and harm". This definition is premised on an important concept: high potential consequence of failure systems require maintenance of low likelihoods of major failures (Figure 1).

Experience with determining the 'acceptable' or 'tolerable' risks associated with engineered systems has demonstrated that such determinations should develop from structured collaborations of concerned and knowledgeable representatives from four groups:[10] 1) the affected publics, 2) commerce and industry, 3) the responsible government agencies, and 4) representatives of the affected environments. There are 'first principles' methods and 'practical considerations' that should be used to develop definitions of the desirable safety of systems. Examples of first principle approaches include cost-benefit analyses, historic experience with comparable systems, and current 'standards-of-practice'. Insurance and legal requirements - precedents are examples of practical considerations. These approaches have been used to determine the locations of the two diagonal lines in the example shown in Figure 1 that identify risks that are "As Low As Reasonably Practicable".[11]

Engineers can provide important insights and information for the collaborative analyses. Engineers should not by themselves be expected to provide adequate definitions or characterizations of the acceptable or desirable safety of systems. Most engineers are taught to keep the safety of the public paramount in their work, but most engineers are not taught about how to realistically determine what constitutes system safety; they need information and direction provided by the four groups and support from the management of organizations for which they work. They need special training and experience in how to quantitatively assess safety, reliability, and risk using valid and validated analytical models that address both Intrinsic and Extrinsic uncertainties.

Because of the uncertainties associated with systems that operate in hazardous environments, the concept of the likelihood or probability or failure has been introduced. The uncertainties associated with performance of complex systems can be analytically determined to define the likelihood of failure, and the uncertainties associated with this likelihood. If only intrinsic uncertainties are included in analyses to determine the probabilities of failure of a given system, then it is easy to understand why these analyses typically result in significant underestimates of the actual probabilities of failure.

Given that the risk assessment processes explicitly address extrinsic uncertainties, then there are two major additions to the determination of the probability of failure. Both additions require characterizations of the Type 3 and Type 4 uncertainties. The additions also require characterizations of the Robustness or damage and defect tolerance of the system to Type 3 and Type 4 uncertainties.[12]

Comparisons of analyses of system failures that have included only Type 1 and Type 2 uncertainties with historic data on comparable system failures has shown that such analyses underestimate the likelihood of failure by factors of 10 or more. Extrinsic uncertainties

Copyright: ©2016 Bea et al.

dominate causation of most major system failures and disasters. It is only when the Type 3 and Type 4 uncertainties are included that the likelihoods of system failures agree reasonably well with those from 'history'- actuarial statistics.

Assessments of the potential consequences associated with failures of systems are another very important part of risk assessment. Experience with risk assessments has clearly shown one consistent trend when the consequences assessed for a given system's failure are compared with the actual consequences associated with failure of the system; they are consistently significantly underestimated. While immediate 'on site' consequences might be reasonably estimated, the long-term 'on-site' and 'off-site' consequences are dramatically underestimated. The long-term 'off-site' consequences frequently are underestimated by factors exceeding 100. Persistent and pervasive failures to accurately estimate long-term environmental, property, quality of life, and productivity impacts are generally responsible for these important underestimates.

When it is recognized that Extrinsic uncertainties are omitted frequently in development of assessments of the likelihood of system failures combined with a general tendency to dramatically underestimate the consequences of system failures it is easy to understand why we are so frequently 'surprised' in the aftermath of large disasters. Many such failures often are attributed to 'organizational' disasters.[13]

Further, it is easy to understand why we frequently make the wrong corrections to systems following disasters. Deficiencies in the assessments of Type 1 and Type 2 uncertainties are 'blamed' for the failures when the Type 3 and Type 4 uncertainties have dominated causation of the system failures. The organizations responsible for causation of the disasters often prevent or inhibit identification of the Type 3 and Type 4 uncertainties. They encourage blame for the system failure be placed on the people at the 'pointed end' of the disaster causation spear. As a result, frequently we end up fixing the wrong problems in the wrong ways.

Reducing ambiguity and its effects

In cases involving complex systems that operate in hazardous environments, ambiguity cannot be reduced to zero-certainty. There will always be ambiguity and there will always be the risks associated with ambiguity. However, thanks to several thousand years of experience and knowledge gained from attempts by humans to assess and manage ambiguity, we have learned there are ways that ambiguity can be effectively managed. The adage is "manage or be managed". There is an important corollary to this adage: "you can only properly manage what you can properly measure".

We have learned the different types of ambiguity must be properly recognized and quantified (measured) so they can be properly managed. This management includes planning, organizing, leading, and controlling to assure that desirable performance is realized from the systems we create. This management must be initiated when a system is conceived and designed, continued when it is constructed-manufactured and put into operation, extended when it is maintained and adapted to changing conditions, and finally concluded when the system is decommissioned. The management of ambiguity is a continuous process- never ending and should be always improving and vigilant. It is a constant struggle to 'make sense' of what is happening to a complex system and then to take effective steps to react and properly adapt to the constantly changing environments in which real systems exist.

As a part of the research and practice experience upon which this paper is based, there was a phase of the work in which seven organizations participated in efforts to improve their capabilities to properly access and manage ambiguity. This work continued for more than 10 years.[13]

At the end of the study period, 2 of the 7 organizations 'succeeded' in their efforts to develop and operate systems that developed acceptable and desirable performance characteristics. As evidenced by the outcomes from this experience, failure of organization efforts to develop HROs with High Reliability Systems (HRSs) was more frequent than success.

The characteristics that defined 'success' were defined by the organizations. These characteristics included the following attributes - the HRSs had: 1) acceptable and desirable serviceability (fitness for purpose), 2) safety (freedom from undue exposure to injury and harm), 3) compatibility (met commercial, regulatory, and environmental requirements), and 4) durability (freedom from unexpected and undesirable degradation in the system performance capabilities). These systems possessed desirable resilience (ability to rapidly recover functionality following disruptions) and sustainability (ability to maintain functionality without undue impacts on future resources). The combination of these characteristics was termed 'System Quality'.

It is important to note that safety is a system attribute that is included as one of the attributes that a system should possess. Safety is not a separate or stand-alone attribute. A basic goal is to preserve acceptable balances between the Production developed by a system and the Protections required to properly sustain the Production. What frequently are conflicting goals in the quest for system Quality (e.g. between commercial compatibility-profitability and safety) are made explicit so the people responsible for the creation, management and operations of the system can rationally address these conflicting goals to preserve acceptable system Quality. When properly developed and maintained, such systems have proven that development and maintenance of acceptable safety is good business.

A 'case based' study of the seven organizations identified 5 C's that were required for the organization to realize success: 1) Cognizance, 2) Capabilities, 3) Culture, 4) Commitment, and 5) Counting. All of the 5 C's had to be operationally effective to realize success. If one or more was deficient, then failure to achieve the desired results was the result.

Cognizance was a realistic, clear recognition of the hazards and threats that their systems faced and posed; valid assessments of the likelihoods and consequences associated with major system failures. Capabilities were the human, organizational, leadership and monetary resources required to develop and maintain HROs that created and maintained HRSs. Most important were the knowledgeable, experienced, and properly motivated and supported human resources. Culture was organizational and operating group cultures (shared beliefs, values, feelings, artifacts) fostering HROs with HRSs possessing balanced Production and Protection - Quality performance characteristics. Commitment was 'top down' and 'bottom up' continuous effective sustained support provided by the organization management and leadership (including regulators) and operating

Copyright: ©2016 Bea et al.

groups to develop and maintain HROs with HRSs.

Counting-was a surprise result from this study. Counting included development of quantitative measurement methods and metrics that could be used to monetarily value and measure the results from corporate financial and human resource investments required to develop and maintain HROs with HRSs. Monetary cost-benefit analysis processes were developed that enabled recognition of the long-term benefits of short-term investments required achieving acceptable HROs with HRSs. The monetary benefits from major failures that did not occur were recognized and measured. The processes demonstrated that development and maintenance of HROs with HRSs was good business. Corporate internal and public external 'report cards' were developed to communicate what had been achieved by these efforts. This Counting provided key ways to help maintain the means and methods required to achieve and sustain balanced system Production and Protection.

After the study was completed, several years later the two organizations that had succeeded in developing and maintaining the 5 Cs reverted back to their previous 'states' - the corporate leadership that established the HROs and HRSs retired. As one employee put it: "the pipes started leaking again." Then there was a rash of major system failures. Following these failures, the organizations went back to work to re-establish the 5 Cs.

Reflections

During the past 25 years, the writer has served as a principal investigator charged with helping determine the 'root causes' of several major system failures and disasters. These failures include the Piper Alpha oil and gas production platform in the North Sea, the grounding of the Exxon Valdez tankship, the crash of the NASA Columbia shuttle, the flooding of the Greater New Orleans area following Hurricanes Katrina and Rita, the San Bruno, California gas pipeline explosion, and the BP Deepwater Horizon Macondo well blowout offshore the coast of Louisiana.

The writer makes an important distinction between the work as a primary investigator of major failures (total of more than 30) and the work to study - perform research on such failures (total of more than 600). Work as a primary investigator has involved extensive 'boots on the ground' long-term exposure to the complex systems that were involved in major failures-disasters. These investigations consumed thousands of hours and involved personal discussions with many of the people directly involved in development of the failures. This 'boots on the ground' investigation experience consistently has provided 'deeper' insights into how and why these disasters happen.

The primary motivation for my work as an investigator has been to learn why the extensive body of knowledge - experience and knowledge about how to prevent major failures was not utilized or if it was utilized, why the technology was not effective at preventing the major failure - disaster.

The writer summarized what he learned as a simple mathematical expression: A+B=C. 'A'are the important hazard and threat environments in which complex systems exist. 'B' are human and organizational deficiencies and defects including hubris, arrogance, greed, complacency, ignorance, and indolence that can degrade the acceptable performance of complex systems. 'C' are major system failures and disasters that happen sooner or later.

The A+B=C equation makes it clear the primary obstacles to develop and maintain HROs and HRSs are human and organizational defects and deficiencies. If these defects and deficiencies can be effectively ameliorated, then there is a high likelihood of developing and maintaining systems that are able to operate successfully in a world that is ambiguous and risky. These are systems whose responsible organizations understand and effectively manage the inevitable ambiguities that systems experience.

Another, and perhaps more helpful way to summarize what has been learned from investigations of major system failures and disasters is recognition that all of these failures and disasters resulted when there were important defects and deficiencies in one or more of the 5Cs. Most of the time, there were important defects and deficiencies in ALL 5 of the Cs. This helps explain why recoveries from major system disasters are so difficult. It takes a lot of time and other resources (human, monetary, technology) to be able to achieve and maintain success in effectively dealing with ambiguity to prevent major system disasters.

Acknowledgements

None.

Conflict of interest

The author declares no conflict of interest.

References

1. Reason J. *Human Error*. UK: Cambridge University Press; 1990. p. 1–302.
2. Woods D. Risk and Human Performance: Measuring the Potential for Disaster. *Reliability Engineering and System Safety*. 1990;29(3):387–405.
3. Dekker S. *The Field Guide to Understanding Human Error*. USA: Ashgate Publishing Co; 2006.
4. Bazerman, Watkins. *Predictable Surprises*. Boston: Harvard Business School Press; 2004.
5. Taleb NN. *The Black Swan*. USA: Random House Publishing Group; 2007.
6. Bea RG. *Human and Organizational Factors in Design and Operation of Deepwater Structures*. Proceedings Offshore Technology Conference. Society of Petroleum Engineers, OTC 14293, Richardson, TX. USA; 2002.
7. Weick KE, Sutcliffe KM. *Managing the Unexpected*. USA: John Wiley & Sons, Inc Josey Bass Publishers; 2007.
8. Roe E, Schulman PR. *High Reliability Management*. USA: Stanford Business Books; 2008.
9. Wenk E. *Making Waves*. USA: University of Illinois Press; 1995.
10. International Standards Organization. *International Standard, Risk assessment–Risk management techniques*. IEC ISO 31010. Paris, France; 2009.
11. Bea RG, Mitroff I, Farber D, et al. A New Approach to Risk: The Implications of E3. *Risk Management*. 2009;11(1):30–43.
12. Bea RG. *Managing the Unpredictable*. USA: Engineering Management, American Society of Mechanical Engineers; 2008.
13. Reason J. *Managing the Risks of Organizational Accidents*. USA: Ashgate Publishing Co; 1997.