UNIVERSITY OF CALIFORNIA, BERKELEY

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

TELEPHONE: (510) 643-8678
TELEFAX: (510) 643-8919
E-MAIL: bea@ce.berkeley.edu
HTTP://www.ce.berkeley.edu/

CENTER FOR CATASTROPHIC RISK MANAGEMENT
DEPARTMENT OF CIVIL & ENVIRONMENTAL ENGINEERING
212 McLAUGHLIN HALL
BERKELEY, CALIFORNIA 94720-1710

Learning from Failures:

Lessons from the Recent History of Failures of Engineered Systems

Center for Catastrophic Risk Management

Lessons from the past

The following is a summary of important observations that have resulted from a long-term study (1988-2005) of more than 600 well documented major failures and accidents involving engineered systems. Sufficient reliable documentation was available about these failures and accidents to understand the roles of the various components that comprised the systems during their life-cycle phases leading to the accident or failure; in many cases, personnel who had participated in the developments were interviewed to gain additional insights about how and why the accidents and failures had developed. Extensive care was exercised to neutralize biases in this work (e.g. triangulation of multiple reliable sources.

Defining failure

In this work, *failure* has been defined as realizing undesirable and unanticipated compromises in the *quality* of the engineered system. Quality is characterized as resulting from the integrated effects of four attributes: 1) *serviceability* (fitness for purpose), 2) *safety* (freedom from undue exposure to harm or injury), 3) *durability* (freedom from unanticipated degradation in the quality attributes), and 4) *compatibility* (meets business and social objectives – on, time, on budget, and happy customers, including the public and the environment).

Defining the system

The early phase of this work indicated that the *system* involved in development of failures needed to be carefully defined and evaluated. Seven primary interactive, inter-related, and highly adaptive components were defined to characterize engineered systems:

- structure (provides support for facilities and operations),
- hardware (facilities, control systems, life support),
- procedures (formal, informal, written, computer software),
- environments (external, internal, social),
- operators (those who interface directly with the system),
- organizations (institutional frameworks in which operations are conducted), and
- interfaces among the foregoing.

This is not a static mechanical system; it is dynamic and organic. The work clearly identified the importance of system interfaces in the development of failures; for example, breakdowns in communications frequently developed at the interface between the operators and the organizations that controlled resources, means, and methods; communication malfunctions at organization-to-organization interfaces were even more prevalent.

Understanding the life-cycle

The work indicated that it was essential to identify how the system had been developed throughout its life-cycle to the point of failure including development of the concept/s, design, construction, operation, maintenance, and for some systems, decommissioning. The history (heritage) of a system generally had much to do with development of failures. This work indicated that in a very large number of cases, the seeds for failure

were sown very early in the life of a particular system; during the concept development and design phases. These seeds were allowed to flourish during the operation and maintenance phases, and with the system in a weakened or severely challenged condition, it failed.

Uncertainties

Uncertainties that were major contributors to the accidents and failures were organized into four major categories: natural variability, analytical modeling uncertainties, human and organizational performance uncertainties, and knowledge related uncertainties. Often, it was not possible to develop unambiguous definitions and evaluations of these uncertainties. A fundamental purpose of this definition was to help direct efforts to understand and manage better the sources and effects of the different categories and sources of uncertainties. There is no deep philosophical basis for this definition; it is heuristic.

We have met the enemy

The studies of major failures clearly showed that the factors involved in causation of the failures (direct cost more than 1988 U.S. $ 1 millions) most often (80 % or more) involved human, organizational and knowledge uncertainties. These were identified as *Extrinsic factors (not belonging to the essential nature)*. In this work, human and organizational performance uncertainties and knowledge related uncertainties were grouped as extrinsic factors. The remaining 20% of the causation factors involved natural and model related uncertainties. These were identified as *Intrinsic factors (belonging to the essential nature)*. In this work, natural variability and analytical modeling uncertainties have been grouped as intrinsic factors.

Life-cycle failures

Of the extrinsic factors, about 80% of these developed and became evident during operations and maintenance activities; frequently, the maintenance activities interacted with the operations activities in an undesirable way. Of the failures that occurred during operations and maintenance, more than half of these failures could be traced to seriously flawed engineering concept development and design; the physical system may have been designed according to accepted standards and yet was seriously flawed due to limitations and imperfections that were embedded in the standards and/or how they were used. Frequently, engineered systems were designed that could not be built, operated, and maintained as originally intended. Changes (work-arounds) were made during the construction process to allow the construction to proceed; flaws were introduced by these changes or flaws were introduced by the construction process itself. After the structure was placed in operation, modifications were made in an attempt to make the structure workable or to facilitate the operations, and in the process additional flaws were introduced. Thus, during operations and maintenance phases, operations personnel were faced with a seriously deficient or defective system that could not be operated and maintained as intended.

Of the 20% of failures that did not occur during operations and maintenance of the systems, the percentages of failures developing during the design and construction phases were about equal. There are a large number of ‘quiet’ failures that develop during these phases that represent project failures and frequently these failures end up in legal proceedings.

How's of failures

The classifications of how engineered systems fail developed here are based on the study of failures and accidents cited earlier. This classification is heuristic and intended to identify the key modes (how’s) in which malfunctions or failures develop (why’s are not identified). This approach was taken so that when the activities or actions were identified they could be evaluated for mitigation.

Operator malfunctions

There are many different ways to define, classify and describe operator (those who have direct interfaces with the system) malfunctions. Operator malfunctions can be defined as actions taken by individuals that can lead an activity to realize a lower quality and reliability than intended. These are malfunctions of commission. Operator malfunctions also include actions not taken that can lead an activity to realize a lower quality than

intended. These are malfunctions of omission. Operator malfunctions might best be described as action and inaction that result in lower than acceptable quality to avoid implications of blame or shame. Operator malfunctions also have been described as mis-administrations and unsafe actions. Operator errors result from operator malfunctions.

Frequently, the causes of accidents are identified as the result of 'human errors.' This identification is seriously flawed because errors are results, not causes. This is an important distinction if one is really interested in understanding how malfunctions develop and how their development might be impeded or eliminated.

Operator malfunctions can be described by types of error mechanisms. These include slips or lapses, mistakes, and circumventions. Slips and lapses lead to low quality actions where the outcome of the action was not what was intended. Frequently, the significance of this type of malfunction is small because these actions not are easily recognized by the person involved and in most cases easily corrected.

Mistakes can develop where the action was intended, but the intention was wrong. Circumventions (violations, intentional short-cuts) are developed where a person decides to break some rule for what seems to be a good (or benign) reason to simplify or avoid a task. Mistakes are perhaps the most significant because the perpetrator has limited clues that there is a problem. Often, it takes an outsider to the situation to identify mistakes.

Based on studies of available accident databases on engineered systems, and studies of case histories in which the acceptable quality of these systems has been compromised, a taxonomy of human malfunctions is summarized as follows:

- Communications – ineffective transmission of information
- Slips – accidental lapses
- Violations – intentional infringements or transgressions
- Ignorance – unaware, unlearned
- Planning & Preparation – lack of sufficient program, procedures, readiness, and robustness
- Selection & Training – not suited, educated, or practiced for the activities
- Limitations & Impairment – excessively fatigued, stressed, and having diminished senses
- Mistakes – cognitive malfunctions of perception, interpretation, decision, discrimination, diagnosis, and action

The sources of mistakes or cognitive malfunctions (operators, organizations) are:

- Perception – unaware, not knowing
- Interpretation – improper evaluation and assessment of meaning
- Decision – incorrect choice between alternatives
- Discrimination – not perceiving the distinguishing features
- Diagnosis-incorrect attribution of causes and or effects
- Action- improper or incorrect carrying out activities

This study of accidents and failures clearly indicates that the single leading factor in operator malfunctions is communication breakdowns. Communications can be very easily flawed by 'transmission' problems and 'reception' problems. Feedback that is so important to validate communications frequently is not present nor encouraged. Language, culture, societal, physical problems, and environmental influences can make this a very malfunction prone process. In team settings, 'authority gradients' (lethal arrogance) are frequently responsible for breakdowns in communications ("do not bother me with the facts, I already have my mind made up").

Organization malfunctions

Analysis of the history of failures of engineered systems provides many examples in which organizational malfunctions have been primarily responsible for the failures. Organization malfunction is defined as a departure from acceptable or desirable practice on the part of a group of individuals that results in unacceptable or undesirable results. Based on the study of case histories of failures of engineered systems, studies of Higher Reliability Organizations (HRO), a classification of organization malfunctions is as follows:

- Communications – ineffective transmission of information
- Culture – inappropriate goals, incentives, values, and trust
- Violations – intentional infringements or transgressions

- Ignorance – unaware, unlearned
- Planning & Preparation – lack of sufficient program, procedures, readiness
- Structure & Organization – ineffective connectedness, interdependence, lateral and vertical integration, lack of sufficient robustness
- Monitoring & Controlling – inappropriate awareness of critical developments and utilization of ineffective corrective measures
- Mistakes – cognitive malfunctions of perception, interpretation, decision, discrimination, diagnosis, and action

Frequently, the organization develops high rewards for maintaining and increasing production; meanwhile the organization hopes for quality and reliability (rewarding 'A' while hoping for 'B'). The formal and informal rewards and incentives provided by an organization have a major influence on the performance of operators and on the quality and reliability of engineered systems. In a very major way, the performance of people is influenced by the incentives, rewards, resources, and disincentives provided by the organization. Many of these aspects are embodied in the 'culture' (shared beliefs, artifacts) of an organization. This culture largely results from the history (development and evolution) of the organization. Cultures are extremely resistant to change.

Several examples of organizational malfunctions recently have developed as a result of efforts to down-size and out-source as a part of re-engineering organizations. Loss of corporate memories (leading to repetition of errors), inadequate 'core competencies' in the organization, creation of more difficult and intricate communications and organization interfaces, degradation in morale, unwarranted reliance on the expertise of outside contractors, cut-backs in quality assurance and control, and provision of conflicting incentives (e.g. cut costs, yet maintain quality) are examples of activities that have lead to substantial compromises in the intended quality of systems. Much of the down-sizing ('right-sizing'), outsourcing ('hopeful thinking'), and repeated cost-cutting ('remove the fat until there is no muscle or bone') seems to have its source in modern 'business consulting.' While some of this thinking can help promote 'increased efficiency' and maybe even lower CapEx (Capital Expenditures), the robustness (damage and defect tolerance) of the organization and the systems its creates can be greatly reduced. Higher OpEX (Operating Expenditures), more 'accidents', and unexpected compromises in desired quality and reliability can be expected; particularly over the long-run.

Experience indicates that one of the major factors in organizational malfunctions is the culture of the organization. Organizational culture is reflected in how action, change, and innovation are viewed; the degree of external focus as contrasted with internal focus; incentives provided for risk taking; the degree of lateral and vertical integration of the organization; the effectiveness and honesty of communications; autonomy, responsibility, authority and decision making; rewards and incentives; and the orientation toward the quality of performance contrasted with the quantity of production. The culture of an organization is embedded in its history.

One of the major culture elements is how managers in the organization react to suggestions for change in management and the organization. Given the extreme importance of the organization and its managers on quality and reliability, it is essential that these managers see suggestions for change (criticism?) in a positive manner. This is extremely difficult for some managers because they do not want to relinquish or change the strategies and processes that help make them managers.

Structure / hardware / equipment malfunctions

Human malfunctions can be initiated by or exacerbated by poorly designed and engineered systems that invite errors. Such systems are difficult to construct, operate, and maintain. A classification system for hardware (equipment, structure) related malfunctions is as follows:

- Serviceability – inability to satisfy purposes for intended conditions
- Safety – excessive threat of harm to life and the environment, demands exceed capacities
- Durability – occurrence of unexpected maintenance and less than expected useful life
- Compatibility – unacceptable and undesirable economic, schedule, and aesthetic characteristics

New technologies compounds the problems of latent system flaws (structural pathogens). Excessively complex design, close coupling (failure of one component leads to failure of other components) and severe performance demands on systems increase the difficulty in controlling the impact of human malfunctions even

in well operated systems. The field of ergonomics (people-hardware interfacing) has much to offer in helping create ‘people friendly’ engineered systems. Such systems are designed for what people will and can do, not what they should do. Such systems facilitate construction (constructability), operations (operability), and maintenance (maintainability, repairability).

The issues of system robustness (defect or damage tolerance), design for constructablity, and design for IMR (Inspection, Maintenance, Repair) are critical aspects of engineering systems that will be able to deliver acceptable quality. Design of the system to assure robustness is intended to combine the beneficial aspects of configuration, ductility, excess capacity, and appropriate correlation (it takes all four!). The result is a defect and damage tolerant system that is able to maintain its quality characteristics in the face of HOF malfunctions. This has important ramifications with regard to engineering system design criteria and guidelines.

Design for constructability is design to facilitate construction, taking account of worker qualifications, capabilities, and safety, environmental conditions, and the interfaces between equipment and workers. Design for IMR has similar objectives. Reliability Centered Maintenance (RCM) has been developed to address some of these problems, and particularly the unknowable and HOF aspects.

It is becoming painfully clear that the majority of engineering design codes and guidelines do not provide sufficient direction for creation of robust – damage – defect tolerance systems. Thinking about sufficient damage tolerance and inherent stability needs rethinking. Thinking about designing for the ‘maximum incredible’ events needs more development. While two engineered systems can both be designed to ‘resist the 100-year conditions’ with exactly the same probabilities of failure, the two structures can have very different robustness or damage stability. The ‘minimum’ CapEx system will not have a configuration, excess capacity, ductility , or appropriate correlation to allow it to weather the inevitable defects and damage that should be expected to develop during its life. Sufficient damage tolerance almost invariably results in increases in CapEx; the expectation and the frequent reality is that OpEx will be lowered. But, one must have a ‘long-term’ view for this to be realized.

This work has clearly shown that the foregoing statements about structure and hardware robustness apply equally well to organizations and operating teams. Proper configuration, excess capacity, ductility, and appropriate correlation play out in organizations and teams in the same way that they do in a structure and hardware. It is when the organization or operating team encounters defects and damage – and is under serious stress, that the benefits of robustness become evident. A robust organization or operating team is not a repeatedly downsized (lean and mean), out-sourced, and financially strangled organization. A robust organization is a Higher Reliability Organization (HR0).

Procedure & software malfunctions

Based on the study of procedure and software related problems that have resulted in failures of engineered systems, A classification system for procedure or software malfunctions is as follows:

- Incorrect - faulty
- Inaccurate - untrue
- Incomplete - lacking the necessary parts
- Excessive Complexity - unnecessary intricacy
- Poor Organization - dysfunctional structure
- Poor Documentation - ineffective information transmission

These malfunctions can be embedded in engineering design guidelines and computer programs, construction specifications, and operations manuals. They can be embedded in contracts (formal and informal) and subcontracts. They can be embedded in how people are taught to do things. With the advent of computers and their integration into many aspects of the design, construction, and operation of oil and gas structures, software errors are of particular concern because the "computer is the ultimate fool".

Software errors in which incorrect and inaccurate algorithms were coded into computer programs have been at the root cause of several recent failures of engineered system. Guidelines have been developed to address the quality of computer software for the performance of finite element analyses. Extensive software testing is required to assure that the software performs as it should and that the documentation is sufficient. Of particular importance is the provision of independent checking procedures that can be used to validate the results from

analyses. High quality procedures need to be verifiable based on first principles, results from testing, and field experience.

Given the rapid pace at which significant industrial and technical developments have been taking place, there has been a tendency to make design guidelines, construction specifications, and operating manuals more and more complex Such a tendency can be seen in many current guidelines used for design of engineered systems. In many cases, poor organization and documentation of software and procedures has exacerbated the tendencies for humans to make errors. Simplicity, clarity, completeness, accuracy, and good organization are desirable attributes in procedures developed for the design, construction, maintenance, and operation of engineered systems.

Environmental influences that can promote malfunctions

Environmental influences can have important effects on the quality and reliability of engineered systems. Environmental influences that can promote malfunctions include: 1) external (e.g. wind, temperature, rain, fog, time of day), 2) internal (lighting, ventilation, noise, motions), and 3) sociological and cultural factors (e.g. values, beliefs, morays). Sociological factors proved to be of critical importance in many of the failures that were studied during this work. These environmental influences can have extremely important effects on human, operating team, and organizational malfunctions, the structures and hardware, and on the primary mediums that engineers must deal with.

Understanding failures

The failure development process was organized into three categories of events or stages: 1) *initiating*, 2) *contributing*, and 3) *propagating*. The dominant initiating events were developed by operators (e.g. design engineers, construction, maintenance personnel) performing erroneous acts of *commission;* what is carried out has unanticipated and undesirable outcomes. The other initiating events are acts or developments involving *omissions* (something important left out, often intentional short-cuts and violations). Communications breakdowns (withheld, incomplete, untrue, not timely) were a dominant category of the initiating events. Various categories of violations (intentional, unintentional) were also very prevalent and were highly correlated with organizational and social cultures.

The dominant contributing events were organizational malfunctions (about 80%); these contributors acted directly to encourage or trigger the initiating events. Communication malfunctions, interface failures (organization to operations), culture malfunctions (excessive cost cutting, down-sizing, outsourcing, and production pressures), unrealistic planning and preparations, and violations (intentional departures from acceptable practices) were dominant categories of these organizational malfunctions.

The dominant propagating events also were found to be organizational malfunctions (about 80%); these propagators were responsible for allowing the initiating events to unfold into a failure or accident. With some important additions, the dominant types of malfunctions were found to be the same as for the contributing events. The important additions concerned inappropriate selection and training of operating personnel, failures in quality assurance and quality control (QA/QC), brittle structures and hardware (damage and defect intolerant), and ineffective planning and preparations.

Impossible failures

Most failures involved never to be exactly repeated sequences of events and multiple breakdowns or malfunctions in the components that comprise a system. Failures resulted from breaching multiple defenses that were put in place to prevent the failures. These events are frequently dubbed incredible or impossible. After many of these failures, it was observed that if only one of the barriers had not been breached, then the accident or failure would not have occurred. Experience adequately showed that it was extremely difficult, if not impossible, to recreate accurately the time sequence of the event that actually took place during the period leading to the failure. Unknowable complexities generally pervade this process because detailed information on the failure development is not available, is withheld, or is distorted by memory. Hindsight and confirmational biases are common as are distorted recollections. Stories told from a variety of viewpoints involved in the development of a failure were the best way to capture the richness of the factors, elements, and processes that

unfold in the development of a failure.

Look out for software

Procedure and software (computer) related malfunctions frequently were found to be a primary player in failure causation. The procedures were found to be incorrect (faulty), inaccurate (untrue), incomplete (lacking important parts), excessively complex (unnecessary intricacy), obsolete (did not incorporate the best available technology), poorly organized (dysfunctional structure), and poorly documented (ineffective information transmission). These malfunctions often were embedded in engineering design guidelines and computer programs, construction specifications, and operations manuals. They were also embedded in contracts (formal and informal) and subcontracts. They were embedded in how people were taught to do things; "this is how we do things here."

With the advent of computers and their integration into many aspects of the design, construction, and operation of engineered systems, software errors are of particular concern because the "computer is the ultimate fool" and it is easy to become "trapped in the net". Software errors in which incorrect and inaccurate algorithms were coded into computer programs have been at the root cause of several recent failures of engineered system (computer aided failures). Guidelines have been developed to address the quality of computer software for the performance of engineering analyses and qualification of software users. Extensive software testing is required to assure that the software performs as it should and that the documentation is sufficient. Of particular importance is the provision of independent checking procedures that can be used to validate the results from analyses. High quality procedures need to be verifiably based on first principles, results from testing, and field experience.

Given the rapid pace at which significant industrial and technical developments have been taking place, there has been a tendency to make design guidelines, construction specifications, and operating manuals more and more complex. Such a tendency can be seen in many current guidelines used for design of engineered systems. In many cases, poor organization and documentation of software and procedures has exacerbated the tendencies for humans to make errors. Simplicity, clarity, completeness, accuracy, and good organization are desirable attributes in procedures developed for the design, construction, maintenance, and operation of engineered systems.

Knowledge

One of the very sobering observations concerning many accidents and failures is that their occurrence is directly related to knowledge (information) access and development. During this work, these challenges were organized into two general categories: *unknown knowables*, and *unknown unknowables*. The first category represents information access and understanding challenges. The information exists but is either ignored, not used, not accessed, or improperly used. This category has been identified as rejection - misuse of technology. Others have identified this category as "predictable surprises."

The second category - *unknown unknowables* - represents limitations in knowability or knowledge. There are significant limitations in our abilities to project system developments or characteristics very far in space or time. Our abilities to know all of the things that are potentially important to the systems that we engineer is limited. Often, there are major limitations in knowledge concerning new or innovative systems and the environments in which these systems will be developed and exist. There is ample history of accidents and failures due to both of these categories of challenges to knowledge. They appear to be most important during the early phases of constructing and operating engineered systems; 'burn-in' failures. Things develop that one did not know or could not know in advance of the activities. They also appear to be most important during the late life-cycle phases; 'wear-out' failures. In this case, the quality characteristics of the system have degraded due to the inevitable effects of time and operations (frequently exacerbated by improper or ignored maintenance) and the hazards posed by unknown knowables and unknown unknowables interact in undesirable ways. This recognition poses a particularly important limitation on proactive reliability and risk analyses that are conducted before systems are constructed and put in service; in a predictive sense, one can only analyze what one understands or knows.

High & low powered accidents

The studies indicated that there was an important discriminating difference between major and not-so-major failures that involved the *energy* or *power* released by or expended during the accidents and failures. Not-so-major failures generally involve only a few people, only a few malfunctions or breakdowns, and only small amounts of energy that frequently is reflected in the not-so-major direct and indirect, short-term and long-term costs associated with the failure. Major failures are characterized by the involvement of many people and their organizations, a multitude of malfunctions or breakdowns, and the release or expenditure of major amounts of energy; this seems to be because *it is only through the organization that so many individuals become involved and the access is provided to the major sources of this energy*. Frequently, the organization will construct barriers to prevent the failure causation to be traced in this direction. In addition, until recently, the legal process has focused on the proximate causes in failures; there have been some recent major exceptions to this focus, and the major roles of organizational malfunctions in accident causation have been recognized in court and in public. Not-so-major accidents, if repeated very frequently, can lead to major losses and it has become obvious that it is important for engineers to develop approaches and strategies to address both categories of accidents.

The engineering challenge

Two things are the bane of engineers: uncertainties and people. Uncertainties devil the engineer because his designs must be deterministic; certain. But, the world is uncertain and the engineer constantly struggles with how to cope with the uncertainties. People devil the engineer because fundamentally they are not predictable, and often not controllable. They do not fit easily into engineering equations and analytical models. In addition most engineers "want to believe that the planet is not inhabited". The history of failures of engineered systems clearly show that it is these two things that are at the heart of failures of most engineered systems.

This study also indicated that, to many engineers, the human and organizational factor part of the challenge of designing high quality and reliability systems is not an engineering problem; frequently, this is believed to be a management problem. Often, the discrimination has been posed as technical and non-technical. The case histories of recent major failures clearly indicate that engineers have a critical role to play if the splendid history of successes and achievements is to be maintained or improved. Through integration of technologies from the physical and social sciences, engineers can learn better how to reach such a goal. The challenge is to apply wisely what is known. To continue to ignore the human and organizational issues as an explicit part of engineering is to continue to experience things that engineers do not want to happen and whose occurrence can be reduced. This work has clearly indicated that engineers can exert important influences on the 'non-technical' parts of systems.

Bob Bea
Professor, Department of Civil & Environmental Engineering
University of California Berkeley
January 22, 2006