DREAMS, DESIGN, AND DESTINY

Richard J. Hornick
Hughes Ground System Group

DREAMS

In 1985, an intrepid British sailor made his fourth attempt at a solo crossing of the Atlantic. According to a *Los Angeles Times* news item ("Sailor Is No Match," 1985), the 65-year-old man set out from Campbletown, Scotland, in a five-foot boat, the *Marmaduke Jinks IV*. Almost immediately, his outboard engine lost power. So he hoisted sail, but his boat drifted backward and he fell asleep. When he woke up, he didn't know where he was. He used an emergency hand flare and was rescued by the Coast Guard after having traveled four miles – the wrong way! As an aside, the article states that one of his previous attempts to cross the Atlantic was in 1984, when he set out from England in a barrel. When he boarded it, it capsized!

Who knows what the sailor's dreams consisted of. Does it matter, though whether he was motivated by a dream of innovation and accomplishment, or one of simple notoriety? In either event, he certainly did not surround himself with a high-technology system.

How universal it is for humans early in life to dream many marvelous things. Not only are our nocturnal dreams so often filled with hopes and happy times, but in those years our waking state is also replete with aspirations to be someone heroic, or courageous, inventive, artistic, of high stature and recognition, of great wealth, with great wisdom, or some combination thereof. Somewhere along the way, we also learn to strive for competitive goals – to be the fastest, the first, the most, the greatest, etc. And, generally, we wish our destinies to be fulfilled within the context of ever more sophisticated and comfortable support systems.

With humankind's gift for creativeness, many impressive dreams have been realized. Certainly these include rapid travel by jet aircraft; food processing and preparation; environmental control, such as air conditioning; medical advances; television; satellite communications; and so many others that we now take for granted. Could Columbus, on setting sail for the New World in three small vessels, ever have conceived of hydroplanes or surface-effect ships? Could the settlers of the western United States, who wagon-traveled at an average of four miles per day, picture a jet aircraft, carrying hundreds of persons above them, capable of flying those four miles in only 24 seconds? More wondrous, perhaps, has been our ability to harness the energy of the atom for power generation and to explore the universe in manned spacecraft. Our dreams, then, do result in marvelous destinies.

I was privileged to have two grandfathers who shared their dreams of technology with me. As we'd listen to a football game or boxing match on the radio, both stated with certainty that someday people would watch the images of such events in their homes. One of them even predicted that the units would not require an antenna or a power cord – that we'd be able to carry around portable units "without wires of any kind." You can imagine the incredulous looks they received from my "wiser" relatives!

Each also spoke of manned space flight as something they knew that my generation would see. Perhaps they had read the Apollo-predictive novel of Jules Verne. No matter, because those dreams were such that each believed that eventual design would offer a destiny that they might not witness, but that we would.

DREAMS TO NIGHTMARES

Unfortunately, it is true that our dreams contain elements of fear or predicted disaster. In the ancient myth of Icarus, did not his father, Daedalus, while desiring a successful flight for Icarus,

fear the potential disaster of flying either too close to the sea or the sun? In dreaming of the potential benefits of a nuclear power technology, did we not have some misgivings about the strangely intriguing atom? In wishing to explore the universe, have we not, in our movies, expressed fears of the unknown and the hazards of technological limits? While crossing a high suspension bridge, have we had a momentary thought of collapse reminiscent of other bridge disasters?

It is my belief that when we learn of failures and disasters, we wonder about the causes and also think that if somehow we had been involved in the design or decision-making process, the tragedy would not have occurred. Why else would we express such indignation at an illogical management process, the faultiness of a design, the basis for a decision, or the paucity of protective measures or safety margins?

I submit that there are currently two prime causes for the events that turn design dreams into nightmares. One is attitudinal; the other is organizational.

Analyses of our failures often reveal an *attitude of complacency or indifference* that almost guarantees that human error will be introduced during concept definition, in analysis, in design, during production, in maintenance, in training, in operational manuals, during tests, and/or, ultimately, during operation. Probably most significantly damaging and dangerous is when such an attitude exists within high levels of management that presides over those processes prior to consumer use.

The second cause for design disasters, I believe, is that of *organization diffusion of responsibility*. Even where management has a positive attitude toward design excellence, the ultimate user or operator may suffer because each element of an organization assumed that proper procedures were being performed by some other organizational entity. I bow to the organization development and management experts among us, but I would guess that such diffusion of responsibility comes from the following factors.

1. *Size* where the sheer numbers of people would suggest to any one individual that "somebody must be doing it."

2. *Top-heavy management structure* in which there are "too many chiefs and not enough Indians," so that the job is not done in sufficient technical or scientific depth.

3. *Bureaucratic environment* wherein paperwork is pushed in order to meet milestones or other on-paper requirements, irrespective of quality.

Nightmares of recent vintage include, among so many others, the Three Mile Island accident, the Chernobyl disaster, the collapse of the Kansas City Hyatt-Regency Hotel walkways, the gas poisoning of thousands in Bhopal, the mid-air collision over Los Angeles, and the explosion of the Space Shuttle *Challenger*. Let's review only a few of these to examine the attitudinal and organizational factors involved.

Hyatt-Regency Hotel

Table 1 summarizes the collapse of the Kansas City Hyatt-Regency walkways, the significant factors, and some of the known effects. Initially, the collapse was suspected to have been caused by too many people moving on the walkways in rhythm while listening to an orchestra below. In fact, however, there was a design mistake and a failure to analyze what seemed to be a minor change in a detail of the support design.

Table 1: Kansas City Hyatt-Regency Hotel Walkway Collapse, July 17, 1981

Event

Collapse of crowded walkways in lobby

Factors	*Effects*
Heavy walkway load	114 killed, 200 injured[placement of entries unclear]
Rhythmic motions of people	Emotional impact on survivors
Initial marginal design	Negative publicity/reputation
Failure to perform calculations	Cost of reconstruction
Failure to analyze design	Litigation for gross negligence in design and analyses
Failure to perform analyses	Over $3 billion in lawsuits filed
Requested by owner	Potential loss of engineering licenses

It was necessary to connect second-, third-, and fourth-floor levels across the lobby to enhance pedestrian flow. Plans called for suspending the walkways (like bridges, but from the ceiling), with the third level hanging independently and the second- and fourth-floor levels being suspended together. Suspension rods were to pass directly through I-beam supports with washers/bolts holding the second- and fourth-level beams (the rods presumably being strong enough to support the total load – but just barely, as later analysis revealed). Recognizing the challenge of threading the upper bolt to the fourth-level support, the design was changed to offset a lower support rod as shown in Figure 1[?]. The resulting change in load-bearing points went undetected. This was human error in design, and human failure to perform appropriate[?] was exacerbated by the fact that such analyses were not performed even when, after partial roof collapse during construction, the owner had asked for them.

Three Mile Island

Given the immense amount of data published in every kind of news and information medium, Table 2 is only a brief summary of that nuclear accident, which approached core meltdown. Both the President's Commission (Kemeny et al., 1979) and the Nuclear Regulatory Commission (NRC) Special Inquiry Group (Rogovin and Frampton, 1980) cited neglect of human factors engineering in most of the key technical problems contributing to the accident. Reading those accounts clearly reveals the technical flaws and the organizational diffusion of responsibility, and suggests an almost cavalier system-design attitude on the part of major elements in the nuclear power industry.

Table 2: Three Mile Island Accident, March 28, 1979

Event

Loss of coolant, turbine and reactor trip, radioactive coolant spill, serious core damage

Factors	*Effects*
Inadequate training	Partial core meltdown[placement of entries unclear]
Incorrect operator decisions	Loss of revenue
Confusing operator procedures	Public distrust
Poor information presentation	Generation of new regulations
Bad control-room design	Requirements for evacuation plans
Confusing alarm system	Recognition of regional dangers
Incorrect maintenance	Pressure for major reorganization
Mismanagement	Loss of orders for new reactors
Emphasis on continued power generation	Impact on closures of other plants
Bureaucratic functioning	
Diffusion of responsibility	
Minimal human factors at NRC	

A common attitude that existed was disregard for human factors through ignorance or intent. When seven members of the Human Factors Society (Charles Hopkins, Robert Makcie, Harold

Price, Robert Simillie, Harry Snyder, Robert Sugarman, and I) served on the Society's contract to develop a long-range, comprehensive human factors plan for the NRC in 1981, too often did we hear the expression so indicative of that attitude – "it's just common sense." As you might well imagine, we had our favorite rejoinder of that vacuous expression. Some examples of design deficiencies that we found appear in Figures 2 through 6[?]. Indeed, if human factors design is merely "common sense" then these photographs would not exist. To most of us, such a travesty of quality design, is perhaps, not unfamiliar. But those are only a few examples. I have seen the word *pump* designated four different ways on the same control panel – PUMP, PP, PMP, and PU – even where there was adequate space available so as not to require abbreviation at all. Another panel contained the color red to signify three different states – emergency, warning/marginal, and normal/go!

Unfortunately, there is not much to suggest that this attitude has changed significantly, or that human factors within the NRC has a potent role, or that the nuclear industry is hungry for our participation. Some believe that the status of human factors is nearly as bad as it was before TMI. Perhaps so, or perhaps it is a bit better. However, one can conclude that the general nuclear power community is couching a cavalier attitude in the (false?) comfort of risk-assessment statistics.

Chernobyl, USSR

By any standard, the most catastrophic nuclear power plant accident is that summarized in Table 3. Less has been published formally in the United States about the intimate causes of the disaster, though much has been presented in newspaper accounts as well as at the International Atomic Energy Agency meeting held in Vienna in August 1986 (American Nuclear Society, 1986).

Table 3: Chernobyl Disaster, April 26, 1986

Events	
Fire, rupture of containment, explosion, massive release of radioactive elements, massive evacuation, serious core meltdown	
Factors	*Effects*
Breaches of discipline	Approximately 30 near-term deaths[placement of entries OK?]
Violation of operational procedures	Estimates of 5,000 to 45,000 deaths over the next 70 years
Unauthorized experiments	
Inadequate management/supervision	Direct economic loss of $2.7 billion
Improper safety measures	Water table and farmland contamination
Operator errors	Installation of new automatic shutdown systems in all plants
Control difficulty	
Design errors and lack of foreseeable use	Recognition of worldwide effects
Bureaucratic environment	International notification agreements
Diffusion of responsibility (?)	Firings/criminal charges against bureau officials

It is rather interesting that a *Los Angeles Times* review of Soviet newspapers and periodicals published in the last several years *prior* to Chernobyl identified many instances that resulted in criticism of the lack of quality control, shortcomings in reactor construction, routine violations of safety regulations, and " . . . crude violations committed by leaders of certain ministries, departments and their subordinate organizations in planning, building, and operation production" (Stein, 1986). Apparently, a less than fully responsible attitude existed in some parts of the Soviet nuclear power community. Perhaps Kremlin pressure to hasten reactor construction as a response to the oil shortages in the early 1980's led to such attitudes. Certainly, there was diffusion of organizational responsibility and communication at the time of the Chernobyl accident.

Space Shuttle Challenger

I believe that no report has been as critical of management carelessness, bureaucratic interactions, disregard for safety, and flaws in the decision-making process as that of the Presidential Commission on the *Challenger* explosion (U.S. Government, 1986). Table 4 presents the commission's major points.

Table 4: Space Shuttle *Challenger* Disaster, January 23, 1986

Event

Launch of vehicle in cold weather with reused booster elements, leak in solid booster, sudden explosion 73 seconds into flight, loss of life

Factors	*Effects*
Serious flaws in decision-making process	Loss of life to seven astronauts[placement of entries unclear]
Loss of credibility in space program	Emotional trauma to key personnel
Waving launch constraints at expense of flight safety	
Lack of external communication of problems	Major NASA policy shifts at Marshall Space Flight Center
	Delay in further launches
Pressure on Thiokol to reverse "hold" recommendation	Redesign of booster seals
	Litigation
Response of Thiokol to please NASA	
Ignoring design problems in "O" ring	
Poor maintenance procedures	
Disdain of technical inputs	
Complacent attitude	
"Silent Safety Program"	
Distilled safety responsibility	

One item bears elaboration – the "Silent Safety Program" – a chapter so titled in the report. It was determined that the chief engineer at NASA headquarters had overall responsibility for safety, reliability, and quality assurance and had a staff of 20 people, only two of whom spent 10% and 25%, respectively, of their time in these areas. Further, the safety programs at the Johnson, Marshall, and Kennedy Space Flight Centers were judged to be in ineffective authority/responsibility organizational positions, with lack of independence in the management structure. Lastly, the critical teleconference calls between Marshall and Thiokol did not include a single safety, reliability, or quality-assurance engineer.

Obviously, upper management has pointed lessons to learn with respect to the nightmares that can result from complacency about human safety, design limits, and organizational location of responsibility.

DREAMS AND MIND-SETS

Henry Petroski's book, *To Engineer Is Human* (1985), should be required reading for any of us. Beyond giving examples of specific design failures and disasters, he presents a mind-set possessed by too many in the engineering community. Table 5 is a list of thematic statements from his book.

Does this list properly portray Pertorski's innermost philosophy? It is hard to tell, for he does not *advocate* overly extravagant design departures in lieu of departures based on some combination of (bad) experiences and established successes. Indeed, he acknowledges the tragic cost of mistakes, the value of (post facto) failure analyses, the need for including many elements in trade-off studies, and the consequences of over-reliance on computer-based design decisions and the accuracy of their databases.

Nonetheless, I can't help but believe that subscribing to that body of tenets can only lead to an attitude that is cavalier and/or an organizational philosophy leading to diffusion of the responsibility for human factors and system safety. While it is true that they often disregard, treat with disdain, underfund, or otherwise denigrate certain design-support disciplines (such as our own) in favor of flair, style, competitive schedule, political expediency, and other driving factors – real or imagined.

Each of Petroski's statements may seem innocuous by itself. They seem almost to be truisms. Even so, each statement can and should be countered.

In childhood, falling down may be part of growing up. But do we need the falls of hundreds of "London Bridges," Tacoma Narrows bridges, and Hyatt walkways? Do we need DC-10's to plummet, commercial and private aircraft to collide and devastate a neighborhood, nuclear plants to release radioactive fallout, and other such falls to wake us to the critical importance of human factors in design, analysis, production, installation, maintenance, training, and operation of our products?

If failure teaches us more than does success, should not the failures be anticipated in *preliminary* (rather than post facto) hazard analyses, and then more safely assessed during test and evaluation *before* release to the market?

Is it really true that design engineers are unable to take into account the human equation for their system calculations? Much of our human factors data is soundly empirical and quantifiable. How often are those data used? Are not design engineers often urged and rewarded by program managers to get on with the design and to minimize costs?

However, isn't it also true that some human factors practitioners are not persistent enough to change that course? When we have a supportive management, it is our even greater obligation to identify, document, and recommend effective changes based on established criteria. I believe that we have sometimes failed to do that . . . and that is *our* fault.

WAKING UP

What happens when our design dreams take on the destiny of tragedy? Our courts of law are filled with liability litigation for faulty product and workplace designs that have injured or killed users or bystanders. Some have argued that the number of cases is distorted; that causes are too minor for such pursuit; that awards, especially punitive ones, are excessive. Though we may be aware of some cases that seem to be without much foundation, I disagree strongly that such cases are rampant.

TABLE 5

Theses from Petroski's *To Engineer Is Human*

- Human desire for innovation leads to greater likelihood of failure.
- Humans are fallible and so must be their creations.
- Falling down is part of growing up.
- Failure often teaches us more than does success.
- Each new design should be considered as a structural hypothesis.
- We must accept risk as the cost of life's pleasures—and we have no choice in that.
- Absolute certainty about fail-proof can never be achieved.
- We cannot learn enough from successes to go beyond the state of the art.
- Design engineers cannot factor the unknown human element into calculations.
- People are not expected to "push" themselves, so machines or structures should not be expected to be "pushed" or overloaded.
- Failure leads to conservatism and new successes.
- While there is no excuse for faulty design, there should be room for understanding.
- Endangering life "is bad for business."

If there is more such litigation than previously, I believe that to be a result of several factors – a heightened sense of social consciousness about personal safety, a more complex technology rapidly evolving with uneven regard for standards, a more sophisticated legal system for seeking redress, and a more informed populace that is angered by stupidity or carelessness in design or by authority not exercised with responsibility.

The resurgence of penalty litigation may well be only a reawakening of our collective social sense of justice. Several thousand years ago, the concern of the Babylonians for safety was reflected in legal prescriptions in what became known as the Code of Hummurabi. In the code are provisions for such penalties as paraphrased in Table 6. So humankind has long desired proper design and imposed rather severe penalties on those judged to be at fault in not meeting requirements.

It is not surprising, then, that the human factors specialist is increasingly involved in forensic matters. The legal profession has only relatively recently become aware of the value of expert-witness testimony by human factors practitioners. If we accept the premise, as I think we do, that there is a human involved in almost every accident, then it is clear that we have much to contribute. The matters to which we can testify rest heavily on such familiar areas of human behavior as perception, reaction during stress, influence of environmental factors, job aids, procedures, skills, anthropometrics, and all of the other topics that compose typical human factors texts.

REVERIE

I don't know completely how many parallels there were between Three Mile Island and Chernobyl (as well as with the *Challenger*), though there seem to be plenty suggested by such terms as *human error, poor workmanship, faulty design, poor decision making,* and *mismanagement*. In looking over my notes, reports, and articles regarding TMI, I was struck by the remarkable similarity of the immediate lack of accurate information surrounding the two nuclear accidents. After Chernobyl, there was a popular outcry of indignation that the Soviets withheld information for 2 or 3 days following the accident. Reading accounts of Chernobyl may make that somewhat understandable in light of TMI if one considers the remoteness of the site, lack of direct communication with the Kremlin, and the self-serving actions of plant management in providing little information to the bureaucratic authorities.

TABLE 6

Babylonian Code of Hammurabi (Paraphrased)

- Build a wall, and if it collapses, you will rebuild the wall at your own expense and materials
- Build a structure, and if it collapses, you will rebuild the structure at your own expense and materials
- Build a structure, and if it collapses and kills its owner's son or slave, your son or slave shall die
- Build a structure, and if it collapses and kills its owner, you shall die

The Presidential Commission Report on TMI also cites lack of knowledge, inaccuracy of utility representatives, discord and disagreement within the NRC, and lack of information for a similar amount of time to that in the Soviet Union – *four* days. In its preface, the Commission Report states, "During the next 4 days, the extent and gravity of the accident was unclear to the managers of the plant, to federal and state officials, and to the general public." How soon we forget our own faults when we see egg on the other fellow's face.

There really should be no satisfaction in gloating about the other party's misfortune. When TMI occurred, regional concern for nuclear safety became elevated to a national concern. Chernobyl had forced nationalistic concerns to become international ones. Indeed, we are a world community, and the responsibility for public safety, for astronaut safety, for excellence in product design, is every individual designer's or the government's.

Penalties for agency mismanagement are increasingly severe, as seen in NASA's organizational shake-up and in the management of nuclear energy in the Soviet Union; penalties for companies that produce faulty products are being exacted in the courts; and individual professionals who are party to unsafe products, procedures, inspections, and maintenance are increasingly open to judgments and loss of licenses.

As a profession assisting the design process through analysis, research, application, and evaluation, we have not only an opportunity but also an obligation to be involved early in design, to refuse to sign off on specifications that do not meet criteria, to stay entrenched in the decision-making process, to conduct research to exacting standards, to teach and inspire students not only with knowledge but also with ethical principles, and to be willing to testify with integrity in litigation where our expertise matters.

Fortunately, the Human Factors Society has many infrastructures for providing mechanisms and support to individual members in accomplishing these objectives. Our many committees and technical groups can provide a platform and resources that include, among many others, organizational design and management, environmental design, industrial ergonomics, safety, training, system development, consumer products, forensics, professional standards, education, certification, ethics, and technical standards. Each of us has an avenue in this Society to reaffirm and to recommit to these ideals.

I urge that we in the human factors profession maintain such behavior. If we do so, then we can be confident that we have rejected a resigned attitude about risk and failure and moved instead to the positive position of making humankind's dreams become realized in exciting destiny.

ACKNOWLEDGMENTS

I express sincere gratitude to O. Keith Hansen and Michael Lyon for their constructive comments during the writing of this address. My thanks are also extended to my many colleagues who have stimulated conversations about these matters.

REFERENCES

American Nuclear Society. (1986, September 11). Chernobyl; The Soviet report. *Nuclear News,* pp. 1–8.

Kemeny, J. C., Babbitt, B., Haggerty, P. E., Lewis, C., Marks, P. A., Marrett, C. B., McBride, L., McPherson, H. C., Peterson, R. W., Pigford, T. H., Taylor, T. B., and Trunk, A. D. (1979). *The President's commission of the accident at Three Mile Island.* Washington, DC: U.S. Government Printing Office.

Petroski, H. (1985). *To engineer is human*. New York: St. Martin's Press.

Rogovin, M., and Rampton, G. T. (1980). *Three Mile Island: A report to the commissioners and the public.* Washington, DC: U.S. Nuclear Regulatory Commission, Special Inquiry Group.

Sailor is no match for the Atlantic. (1985, June 22). *Los Angeles Times*, Part III, p.2.

Stein, G. (1986, May 16). Soviet nuclear industry riddled with problems. *Los Angeles Times*, Part I, p. 1.

U.S. Government. (1986). *Report of the Presidential commission on the Space Shuttle Challenger accident*. Washington, DC: Author.