

Cambridge University Press

978-0-521-46649-3 - Design Paradigms: Case Histories of Error and Judgment in Engineering

Henry Petroski

Excerpt

[More information](#)

I

Introduction

The concept of failure is central to the design process, and it is by thinking in terms of obviating failure that successful designs are achieved. It has long been practically a truism among practicing engineers and designers that we learn much more from failures than from successes. Indeed, the history of engineering is full of examples of dramatic failures that were once considered confident extrapolations of successful designs; it was the failures that ultimately revealed the latent flaws in design logic that were initially masked by large factors of safety and a design conservatism that became relaxed with time.

Design studies that concentrate only on how successful designs are produced can thus miss some fundamental aspects of the design process, which is difficult enough to articulate as it is. Yet while practicing designers especially are notorious for saying little, if not for consciously avoiding any discussion at all of their own methodology, there have been some notable exceptions (especially, e.g., Glegg, 1973, 1981; Leonhardt, 1984), and when these engineers have reflected on the design process, they have acknowledged the important role that failure plays in it. Although often an implicit and tacit part of the methodology of design, failure considerations and proac-

Cambridge University Press

978-0-521-46649-3 - Design Paradigms: Case Histories of Error and Judgment in Engineering

Henry Petroski

Excerpt

[More information](#)

tive failure analysis are essential for achieving success. And it is precisely when such considerations and analyses are incorrect or incomplete that design errors are introduced and actual failures occur. Understanding how errors are made and can be avoided in the design process can help eliminate them and can illuminate the very process of design.

The role of failure in successful design has been argued explicitly in the context of structural engineering (cf. Petroski, 1985), but the argument applies by analogy in fields as seemingly divergent as aerospace, chemical, computer, electrical, and mechanical engineering. Alexander (1964) has reasoned that whenever any designer does not merely copy exactly what has already been made and pronounced successful – that is, acceptable – then it is difficult to say whether a new or modified design will be or will continue to be successful. A building or a bridge may be declared successful during decades of problem-free service, but if it suddenly collapses we may find that a serious design flaw was present all along. Thus, the elevated walkways in the Kansas City Hyatt Regency Hotel were considered safe enough to hold the crowds that they did until they collapsed on the afternoon of Friday July 17, 1981; and the Mianus River Bridge near Greenwich, Connecticut, daily carried the heavy traffic of Interstate 95 until it suddenly collapsed early in the morning of June 28, 1983.

Recognizing failure is something “even the simplest” person can do, and Alexander has noted that even if only a few of us have “sufficient interpretative ability to invent form of any clarity, we are all able to criticize existing forms.” He considers this an “obvious point,” acknowledging that it is at least as old as Pericles, who is quoted as saying, “Although only a few may originate a policy, we are all able to judge it.” So when a structure collapses or a design fails to live up to its promise, the lesson should be accessible to all, and even a jury of laypersons is presumed capable of ruling on culpability.

While it may be easy to recognize failure after the fact, engineers

are expected to anticipate and obviate it in their designs. The idea of proactive failure analysis has been elaborated upon by Alexander: he gives some forceful examples of how much more natural it is for us to recognize failure or “misfit” between context and form than to recognize the success or fitness of a design in meeting stated requirements. Indeed, Alexander goes so far as to say:

We are never capable of stating a design problem except in terms of the errors we have observed in past solutions to past problems. Even if we try to design something for an entirely new purpose that has never been conceived before, the best we can do in stating the problem is to anticipate how it might possibly go wrong by scanning mentally all the ways in which other things have gone wrong in the past.

According to Lev Zetlin (1988), whose career as a prominent structural design engineer included many major projects:

Engineers should be slightly paranoid during the design stage. They should consider and imagine that the *impossible could* happen. They should not be complacent and secure in the mere realization that if all the requirements of the design handbooks and manuals have been satisfied, the structure will be safe and sound.

Furthermore, according to Zetlin (as quoted in Browne, 1983), what is needed to improve designs and the reliability of structures is “preventative and curative engineering.” He elaborated on what he meant by explaining his own design and review technique: “I look at everything and try to imagine disaster. I am always scared. Imagination and fear are among the best engineering tools for preventing tragedy.” No one is advocating that today’s engineers become immobilized by the design process, but Zetlin merely echoed what great engineers like Robert Stephenson and Herbert Hoover also reported: they lost sleep over the design problems they took to bed with them. Rather than being the curse of engineering, this manifestation of concern should be worn by the profession as a badge of honor.

Other reflective engineers have made similar observations, and in order to imagine what can go wrong with one's current design, it is clearly advantageous to know what has gone wrong with others in the past. The dictum of Santayana that those who do not remember the past are condemned to repeat it should always weigh heavily on the minds of engineers. And it would seem to be especially important that we think more about past design failures in light of the report of a recent National Science Foundation workshop group on occurrence of errors that "in many cases the same errors are repeated again and again" (Nowak, 1986).

Because of their long history and their scale, large civil engineering structures and mechanical engineering systems have had their designs and failures most thoroughly documented, and thus there are archives of information about them that are unequalled. Furthermore, because they are so visible and public, the record of failures of civil structures and large public systems can be expected to be more complete and wide-ranging than those of other failures, with technical reports often being supplemented by contemporary non-technical reports that place the failures in the broader social and human context in which designers must necessarily operate and in which errors occur.

Although structural engineering examples are often the most common in arguing for the role of failure in the design process, this concentration by field in no way restricts the applicability of the general concepts involved. Publications in computer, electrical, manufacturing, mechanical, and other fields of engineering frequently contain reports and analyses of failures that at first might seem far afield.

The relevance of lessons learned in structural engineering for other engineering applications was emphasized by the publication of a long interview with a bridge engineer in a journal of the Association for Computing Machinery (Spector and Gifford, 1986), an introduction to which declared: "Though some computer systems are more complex than even the largest bridges, there is a wealth of

Cambridge University Press

978-0-521-46649-3 - Design Paradigms: Case Histories of Error and Judgment in Engineering

Henry Petroski

Excerpt

[More information](#)

Introduction

5

experience and insight in the older discipline that can be of use to computer systems designers, particularly in such areas as specification, standardization, and reliability.” The editors clearly felt that there was much to be learned by analogy from a field with a long history by one with a very short one. Interestingly, bridge failures played a prominent role in the interview.

This view of the generality of lessons to be learned from failures was reiterated in a special report on managing risk in large complex systems published even more recently in *Spectrum*, the magazine of the Institute of Electrical and Electronics Engineers (Bell, 1989). According to the report’s introduction:

Although some of these case studies examine systems that are neither electrical nor electronic, they highlight crucial design or management practices pertinent to any large system and teach all engineers important lessons. What large systems have in common counts for more than how they differ in design and intention.

Aeronautical and aerospace engineering failures have also been the subject of much professional attention, not to mention extensive coverage in the mass media. Nuclear engineering incidents like the 1979 loss of coolant at the Three Mile Island plant near Harrisburg, Pennsylvania, and the 1986 explosion and fire at the Chernobyl plant near Kiev, which released radioactive material that spread well beyond its origin in the Soviet Union, have become shibboleths for discussions of the risks of modern high technology. Chemical engineering shortcomings have been the focus in discussions of industrial accidents such as the 1984 release of toxic gas from a Union Carbide insecticide plant at Bhopal, India, which killed more than 2,000 people and harmed about 150,000 more. Mechanical engineering failures can result in death due to exploding gasoline tanks in automobiles and trucks, not to mention less life-threatening but wide-reaching effects such as massive recall campaigns and product liability suits. And electrical and software engineering have had to deal with questions of reliability and assurance in the wake of massive power black-

outs and telephone system breakdowns that have inconvenienced tens of millions of people at a time. In short, no field of modern engineering is untouched by the effects of failures and their invaluable lessons.

It appears incontrovertible that understanding failure plays a key role in error-free design of all kinds, and that indeed all successful design is the proper and complete anticipation of what can go wrong. It follows, therefore, that having as wide and deep an acquaintance as possible with past failures should be at least desirable, if not required, of all engineers engaged in design. Understanding from case histories how and why errors were made in the past cannot but help eliminate errors in future designs. And the more case histories a designer is familiar with or the more general the lessons he or she can draw from the cases, the more likely are patterns of erroneous thinking to be recognized and generalizations reached about what to avoid.

Human Error

Many thoughtful researchers have reflected on the sources of error in design, including Blockley (1980), who has stated flatly that in the final analysis “all error is human error, because it is people who have to decide what to do; it is people who have to decide how it should be done; and it is people who have to do it” (cf. FitzSimons, 1988). Some might argue with Blockley’s singular classification of error, but the human element clearly increases failure rates and thus reduces the reliability of our designed artifacts and systems compared to analytical predictions that obviously ignore or underestimate the human element in design.

According to Ingles (1979), statistical methods for quantifying variability in design are insufficient if the human sources and nature of variability are not more closely examined. Writing more recently, Santamarina and Chameau (1989) have reiterated the problem, and

have reemphasized the need to look to the human element in design methods and practices. Nowak and Tabsh (1988) have stated that the “major challenge to reliability theory was recognized when the theoretical probabilities of failure were compared with actual rates of failure [and] actual rates exceed the theoretical values by a factor of 10 or 100 or even more.” They identified the main reason for the discrepancy to be that the theory of reliability employed did not consider the effect of human error. A host of further studies, such as referenced in the work of Blockley (1980), Ingles (1979), and others, make it clear that there is a strong sense that improved reliability in design will come only when our already highly developed analytical, numerical, and computational design tools are supplemented with improved design-thinking skills. While artificial intelligence and expert systems have been promised as solutions to the problem of human error, the design of computer-based methods will itself benefit from an understanding of human error and how to reduce it.

We should expect to learn more about human error in design from case studies of actual design errors and failures. However, as Blockley (1980) has noted in the context of structural design, the commercial nature of engineering works against the wide dissemination of accounts of human error, except in cases of failures that lead to some form of public inquiry. According to Blockley, although we have accounts of successful projects, “from these there is the least to learn.” The gravity of the situation was further emphasized during hearings before the U.S. House of Representatives Committee on Science and Technology (1984) in which the practice of sealing the testimony of legal proceedings dealing with liability over design failures was deplored. Such a practice deprives the larger design community of invaluable lessons learned.

Human error in anticipating failure continues to be the single most important factor in keeping the reliability of engineering designs from achieving the theoretically high levels made possible by modern methods of analysis and materials. This is due in part to a

Cambridge University Press

978-0-521-46649-3 - Design Paradigms: Case Histories of Error and Judgment in Engineering

Henry Petroski

Excerpt

[More information](#)

de-emphasis on engineering experience and judgment in the light of increasingly sophisticated numerical and analytical techniques. According to the report of a working group on the occurrence of errors (Nowak, 1986), some observers hold that society has found the current average level of risk acceptable, while others note that increased legal liability costs show that society has not. Whatever society's perception, since human beings are the only feature common to the diverse systems surveyed in a variety of historical, geographical, and economic contexts, the discrepancies between predictions and reality have been attributed primarily to the human element in the design, construction, and maintenance processes. Education, motivation, and quality control provide clear, if not necessarily easily implemented, ways of reducing human error in manufacturing, construction, and maintenance, but ways to eliminate human error from the design process are much less obvious.

We now have very sophisticated theories of structures and elaborate multipurpose computer programs that are capable of quite refined analysis, but these have not led to an improvement in the reliability of engineering design. Indeed, more than one survey of engineering failures have concluded that refined methods of analysis would not prevent future failures. The foundation engineer Peck (1981), speaking of dams, concluded that "nine out of ten recent failures occurred not because of inadequacies in the state of the art, but because of oversights that could and should have been avoided." He pointed out that the "problems are essentially nonquantitative" and the "solutions are essentially non-numerical." Peck acknowledged that improvements in analysis and testing might be profitable, but felt it was also likely that "the concentration of effort along these lines may dilute the effort that could be expended in investigating the factors entering into the causes of failure." Hauser (1979), after reviewing a survey of about 800 European failures, concluded that "the most efficient way to improve structural safety or to reduce the overall effort to maintain a certain level of structural safety is to refine the methods of data checking [to catch design errors] and not

Cambridge University Press

978-0-521-46649-3 - Design Paradigms: Case Histories of Error and Judgment in Engineering

Henry Petroski

Excerpt

[More information](#)

to refine the models of analysis.” There has been little change of concern in the ensuing decade (cf. Santamarina and Chameau, 1989), principally because failures continue to occur at unexpectedly high rates. Indeed, such a state of affairs and the accompanying questions of liability led the American Society of Civil Engineers in 1988 to draft a manual of professional practice, *Quality in the Constructed Project*.

It is inevitable that errors are going to be made in design. Some conceptual designs are just bad ideas from the start, and it is the self-critical faculty of the designer that must be called into play to check him- or herself and to abandon bad ideas on the drawing board (cf. Petroski, 1985). Other designs are fundamentally sound conceptually, but they can be weakened by poor choices of components or inferior detailing or by seemingly simple but poorly considered design changes. It is the function of checking, whether by the original designer or by peers, to catch the omission of a critical calculation, the lapse in logic, the error in analysis, or the mistake in mathematics. But all too often the process of checking – an integral component of the design process itself – is myopic. The original designer can continue to overlook the same errors of commission or omission, and the peer can nod at the faulty logic (cf. Stewart and Melchers, 1989).

Alexander (1964) has reminded us of the fundamental fact that the main objective of design and the study of its methodology is to make better designs – that is, to improve reliability. Looking for rules of success in the design process as it is currently practiced will not necessarily accomplish this goal, for it is design as practiced that is failing to live up to its desired or theoretical potential. Rather, we must look anew at the design process and learn how better to identify the causes of error in it. Since the ideally successful design properly anticipates all relevant and possible ways in which failure can occur, it is imperative to understand how failure is introduced by human designers into the design process.

Cambridge University Press

978-0-521-46649-3 - Design Paradigms: Case Histories of Error and Judgment in Engineering

Henry Petroski

Excerpt

[More information](#)*The Case for Historic Case Studies*

Even when information about contemporary failures is available, there can be honest disagreement among experts over the ultimate cause of a failure, in part because of human nature and our reluctance to be perfectly candid about our own errors. Thus, even when modern case studies are available, they may provide a skewed perspective on the actual design process because of pending law suits, because of professional reputations that are at stake, or because of commitments to current theories. Such difficulties and complications argue for looking to historical case studies for examples of human error and how to deal with it. Although new theoretical and computational design tools have made the old obsolete, the nature of the design problem and the design logic and thought processes used to solve it have remained essentially unchanged from ancient times.

Design today is commonly done in collaboration, and thus all the elements of the process are not necessarily embodied in a single individual. Mainstone (in Pugsley, Mainstone, and Sutherland, 1974) has recognized this difficulty and has written that he has “found it easier in some ways to get under the skin of earlier designers . . . than to do the same in the case of the more typical design teams of today.” Studying earlier designers can thus complement studies of design groups.

Whenever the most gifted thinkers and designers, whether classical or modern, have without external prompting reflected on their art and its failings, they have given us potentially very valuable data on the nature of engineering design that applies beyond the specific case study. Since all design necessarily must conform to both technical and nontechnical constraints, the most meaningful data on the design process tend to be those which place a given design in a contemporary context. And since failures contain more unambiguous information than successes, the most fruitful data that any designer can be provided are case studies of failure or the explicit avoidance of failure.