

Learning from Failure: The Teachings of Petroski

Richard Schrenker

You need not have any familiarity with clinical engineering to page through an issue of *BI&T* and conclude that medical device and system failures and patient safety are high on the profession's list of concerns. However, open public discussion of specific device or system failures that compromise safety or lead to patient injury are rare. Even in light of *To Err is Human*, the highly visible Institute of Medicine's 1999 recommendations to improve error-reporting systems that inform patient safety activities, information is still not disseminated as much as it perhaps should be.¹⁻³

Efforts to reverse this state of affairs are becoming more visible, though. For example, in 2005 the Joint Commission released a publication that leans heavily on case studies derived from real problems experienced in the delivery of care to illustrate the role of human factors engineering in addressing them.⁴

Experience, some joke, enables you to recognize a mistake when you make it again. It will take time before we gain experience with these new error-driven improvement systems, and certainly there are mistakes we would rather not repeat. That *To Err is Human* begins with a mention of *Boston Globe* health reporter Betsy Lehman's death from a chemotherapy overdose in 1994 should give us pause, as the technological systems to address that one type of failure started moving into widespread use

only in the last few years.⁵ Failure is indeed a powerful teacher, but are there ways to learn from it besides waiting for the *next* catastrophic error?

Henry Petroski, a professor of civil engineering at Duke University, has written many books on the history of engineering that focus on failure analysis and design theory:

*I believe that the concept of failure... is central to understanding engineering, for engineering design has as its first and foremost objective the obviation of failure. Thus the colossal failures that do occur are ultimately failures of design, but the lessons learned from these disasters can do more to advance engineering knowledge than all the successful machines and structures in the world.*⁶

Taken from the preface to Petroski's *To Engineer is Human: The Role of Failure in Successful Design*, the above pretty much sums up the advice delivered in many of his writings. He goes on to end that book with:

*... every case study—no matter how obsolete its technology or how fresh its trauma, whether in a book or in tomorrow's news—is potentially a paradigm for understanding how human error and false reasoning can thwart the best laid plans.*⁷

Petroski often uses the history of bridge failures to illustrate how we have learned, or neglected to learn, from failures of engineering practice. Probably every practicing engineer in the United States has seen the film of the 1940 collapse of the Tacoma

Narrows Bridge in Washington in an introductory engineering course. Petroski lays out the history of successes and failures that preceded the oft-viewed collapse.⁸ He uses it and other stories to influence current and future generations of engineers; he wants us—his students and his readers—to be informed by the case studies taken from the history of engineering.⁹ The messages are universal and reach well beyond engineering. After all, not all design is done by engineers:

*Given the faults of human nature, coupled with the complexity of the design of everything, from lectures to bridges, it behooves us to beware of the lure of success and listen to the lessons of failure.*¹⁰

Underestimating Risk

Returning to healthcare in general and medical technology in particular, what can we in the related engineering and service professions take from Petroski's writings? For me, his insights resonate most clearly with what we tend to call the "convergence of biomedical and information technologies." Speaking to the impact of computers on the practice of civil engineering, Petroski quotes a colleague:

*...changes have occurred so rapidly that the profession has yet to assess and allow for the implications of these changes.*¹¹

Arguably clinical engineering's first and foundational story centers

on electrical safety. The story is grounded (pun intended) in Ralph Nader’s 1971 *Ladies Home Journal* article, which claimed that 1,200 people were dying annually as a result of exposure to microshock. The story was recently cited in *BI&T*, emphasizing that “history would later show that Nader’s characterization of the problem was a bit overstated.”¹² I agree, although having visited a hospital in the early 1980s where electrical safety wasn’t receiving adequate attention, I can say there was at least some justification for the overreaction. But in light of the remarkable lack of microshock-related deaths and injuries after all these years, is there a risk that we may *underestimate* the risk, and not only for electrical safety?

Petroski returns time and again to that theme, describing it as “... the myopia that can occur in the wake of prolonged and remarkable success...”¹³ Intellectually we know that a safe past does not guarantee a safe future, but Petroski drives the point home by describing how success-fueled hubris took the National Aeronautics and Space Administration (NASA) from the glory years of the Apollo program to and through the failures of Mars satellites and two space shuttle disasters.¹⁴ And it is worth remembering that many of the space program failures were not associated so much with design as with program management.

In discussing the failure of England’s Dee Bridge in 1847, which resulted in five deaths, Petroski differentiates between what he calls “normal” and “extrapolatory” design. It is implementations of the latter that most commonly contain consequential flaws.¹⁵ Consider how rapidly medical device design is extrapolated these days, i.e., how frequently software is upgraded and patched. Certainly there are design and other regulatory controls in place to guide development, but what happens if and when the technology under control evolves to design or applications boundaries not considered when the controls were put in place? Much like the Dee Bridge, which took a previously successful design to the next level without appropriate safeguards, systems can collapse.

The Challenge of Learning from Failure

Another oft-cited error in medical technology literature is the story of Therac-25, where a combination of engineering and other technology-related errors contributed to the deaths of six patients undergoing radiation therapy in the mid-1980s. A 1993 *IEEE Computer* article on the tragedy offered the following lessons:

We have assumed...manufacturers have all kinds of safety design experience since they’ve been in the business a long time. We know that there are many safety codes, guides, and regulations to guide them and we have been reassured by the hitherto excellent record of these machines...Perhaps, though, we have been spoiled by this success...

It is clear that users need to be involved. It was users who found the problems with the Therac-25 and forced [Atomic Energy of Canada Limited] to respond. The process of fixing the Therac-25 was user driven—the manufacturer was slow to respond. The Therac-25 user group meetings were, according to participants, important to the resolution of the problems. But if users are to be involved, then they must be provided with information and the ability to perform this function...

*...previous accounts of the Therac-25 accidents blamed them on a software error and stopped there. This is not very useful and, in fact, can be misleading and dangerous: If we are to prevent such accidents in the future, we must dig deeper. Most accidents involving complex technology are caused by a combination of organizational, managerial, technical, and, sometimes, sociological or political factors.*¹⁶

.....

How can we break the cycle and use failure to prevent failure?

.....

Were the lessons heeded? A year after this was published Betsy Lehman died of an overdose. Five years later *To Err is Human* was released with its recommendations for improving patient safety. How can we break the cycle and use failure to prevent failure? According to Petroski:

*Things work because they work in a particular configuration, at a particular scale, and in a particular context and culture.*¹⁷

*Any design change...can introduce new failure modes or bring into play latent failure modes. Thus it follows that any design change, no matter how seemingly benign or beneficial, must be analyzed with the objectives of the original design in mind.*¹⁸

In 2002, Boston’s Beth Israel Deaconess Medical Center experienced a four-day network outage that virtually crippled the institution. As one physician noted, “we depend on the network, but we also take it for granted [and] operate with a mindset that the computers never go down [and] put more and more critical demands on the systems. Then there’s a disaster.” Among the consequences was reverting to paper forms that had not been used in years, which of course made them new to young

physicians used to the support of background systems (checking for drug allergies, for example). That we know this and a lot more about the event is a tribute to the hospital's chief information officer, John Halamka, MD, who went public with the story because, he said, "I made a mistake... And the way I can fix that is to tell everybody what happened so they can avoid this." A consultant had told him not long before the crash, "You have a state-of-the-art network—for 1996."¹⁹

An article in the *New England Journal of Medicine* on lessons learned from the failure said that Beth Israel Deaconess "was operating an extended computer network designed to meet the requirements of a much simpler environment... The principal point of failure was a software program for directing traffic [that] was overwhelmed by a combination of data volume and network complexity that exceeded the software's specifications."²⁰ In other words, changes were being made to their network without adequate analysis as to whether the network infrastructure could support them and what the consequences might be if it could not—the very thing Petroski cautions against in his writings.

Imagine the implications as medical devices increase their use of and dependence on networked resources, particularly in light of the rate of change and heterogeneity of clinical applications and systems implementations. This begs the question of whether anyone has examined, let alone established, the validity of extrapolating 20th-century medical technology development, assessment, and regulatory practices for the 21st-century healthcare system.

The Good Old Days: Lessons of Experience

...Thirty years is about the time it takes one "generation" of engineers to supplant another within a technological culture... Though a new or evolving bridge type might be novel for its engineers to design, an older one that has become commonplace does not hold the same interest or command the same respect of a younger generation, who treat it as normal technology... Thus, in the absence of oversight and guidance from those who knew the underlying ignorance, assumptions, and cautions best, the technology was pushed further and further without a full appreciation of its or its engineers' limitations.²¹

Petroski and others have observed that major bridge failures have occurred at 30-year intervals since the mid-19th century.²² This is, arguably, close to the span of an average engineering career. It has been almost 30 years since I entered the field. What stories can I tell, and who will listen?

Among my stories are two that I shared a few years ago with a columnist for *Embedded Systems Magazine* describing what I perceive to be differences between now and the "good old days." In the first, I wondered whether today's service manuals are as informative or complete as those of the past (I often hear that is not the case, and my experiences concur):

.....

How effective can support systems be at ensuring safety if every technical document or medical device user interface represents an unexamined opportunity for extrapolatory design?

.....

Twenty years ago, I could go to the service manual of any device in our inventory and determine what it was supposed to do and how it did it. The key, of course, was the schematic diagram. What made it so useful was its use of standard symbols to represent components. The abstractions were consistent across the industry... Based on the schematic and related information, I could train technicians how to provide service to the device, or clinicians how to use it. I could develop tests to verify operation, and I could validate that the device could do what it was supposed to do...

The second story describes my experience on examining three PCA pumps during a pre-purchase evaluation:

Not only did each have a different user interface, but I couldn't intuit any of them. Back when I practiced on the floor that was a key criterion for me. There was only so much time for training, and if a device didn't provide at least some guiding context of itself, I found it relatively more difficult to teach... What strikes me as least defensible in all of this is that throughout my life I have been able to go into any auto showroom and test drive a car within minutes, but licensed practicing clinicians almost always require fundamental user training every time they encounter a new model or type of devices that have been around for 25 years. I'm not talking about training for new features. I'm talking about just learning the user interface.²³

How effective can support systems be at ensuring safety if every technical document or medical device user interface represents an unexamined opportunity for extrapolatory design? As *To Err is Human* reminds us, "Safety is a characteristic of systems and not of their components. Safety is an emergent property of systems."²⁴ Of course it is not news that adherence to good manufacturing practices and FDA approval only represent one facet of what

it takes to make devices safe. But it may very well be that standards are as needed for service manuals, user training, and other resources needed to support the application of medical technology as they are for the technology itself.

Before leaving you with one final story, it bears repeating that Petroski is a professor of engineering, which is to say a champion of innovation. As he puts it,

*Yet were we not willing to try the untried, we would have no exciting new uses of architectural space, we would be forced to take ferries across many a river, and we would have no trans-Atlantic jet service. While the course of human nature appears to be to make mistakes, its determination appears to be to succeed.*²⁵

About 15 years ago, I worked with a cardiologist to put together a system to measure left ventricular pressure using a transducer-catheter system, which was significantly less expensive than the transducer-tipped catheters often used to study certain ventricular dynamics. I neglected to ensure we were sampling the acquired signal at the rate called for by sampling theory. The journal review caught the omission, and our funded study's output was for naught. No one was hurt, and the research data would not have been used clinically anyway. Besides being embarrassed, I was burdened by wondering what I could have done differently. After all, I had taken sampling theory into account in prior work. I finally came to the conclusion there was only one thing I could have done that I did not: I had not asked others to review my work. They might have missed it, too, but maybe not. So now I try very hard to remember to call for requirements and design reviews no matter what kind of system I'm developing or changing, whether technical or management. And because the next time the consequence could be worse than simple embarrassment, I share this story.

I suggest that we engineers capture more stories like this, here in *BI&T* and elsewhere in the healthcare literature. We need to help our clinical colleagues understand the nature of systems change and the lessons that Petroski has tried to teach us. We should keep telling stories for as long as they happen. We need to listen, learn, and change our actions based on these stories. Yet, no matter how much we do that, and how many other potential stories we will have stopped in their tracks, we'll still have more to tell. ■

Richard Schrenker is the systems engineering manager in the Department of Biomedical Engineering at Massachusetts General Hospital, Boston, MA.

Author's Note: As this issue of BI&T was being finalized, another bridge collapse happened in Minneapolis. As we ponder what lessons can be learned from the tragedy, our thoughts go out to the victims and their families.

References

1. Kohn L, et al., eds. *To Err is Human*. National Academies Press (1999):9–12.
2. Brennan T, Mello M. Patient safety and medical malpractice: a case study. *Ann Intern Med*. 139(4):270–271.
3. Mello M, et al. Health courts and accountability for patient safety. *The Milbank Quarterly*. 2006;84(3). Available at <http://www.milbank.org/quarterly/8403feat.html>. Accessed July 17, 2007.
4. Gosbee J, Gosbee L, eds. *Using Human Factors Engineering to Improve Patient Safety*. Joint Commission Resources, 2005.
5. Kohn L, et al., eds. *To Err is Human*. National Academies Press (1999):1.
6. Petroski H. *To Engineer is Human*. Vintage Books(1992):viii.
7. Petroski H. *To Engineer is Human*. Vintage Books(1992):232.
8. Petroski H. *Design Paradigms—Case Histories of Error and Judgment in Engineering*. Cambridge University Press(1994):144–165.
9. Petroski H. *Design Paradigms—Case Histories of Error and Judgment in Engineering*. Cambridge University Press(1994):180–186.
10. Petroski H. *Success through Failure—The Paradox of Design*. Princeton University Press(2006;1994).
11. Petroski H. *To Engineer is Human*. Vintage Books(1992):201.
12. Larrick K. *Connecting past and present*. *Biomed Instrum Technol*. 2007;41(1)73–74.
13. Petroski H. *Design Paradigms—Case Histories of Error and Judgment in Engineering*. Cambridge University Press(1994):162.
14. Petroski H. *Success through Failure—The Paradox of Design*. Princeton University Press(2006;1994):163–167.
15. Petroski H. *Design Paradigms—Case Histories of Error and Judgment in Engineering*. Cambridge University Press(1994):94–97.
16. Leveson N, Turner C. An investigation of the Therac-25 accidents. *Computer*. 1993; 18–41.
17. Petroski H. *Success through Failure—The Paradox of Design*. Princeton University Press(2006;1994):167.
18. Petroski H. *Design Paradigms—Case Histories of Error and Judgment in Engineering*. Cambridge University Press(1994):57.
19. Berinato S. Halamka on Beth Israel's health-care IT disaster. *CIO*. Feb 15, 2003. Available at http://www.cio.com/article/31701/Halamka_on_Beth_Israel_s_Health_Care_IT_Disaster/1. Accessed July 17, 2007.
20. Kilbridge P. Computer crash—lessons learned from a system failure. *N Engl J Med*. 2003;348(10):881–882.
21. Petroski H. *Success through Failure—The Paradox of Design*. Princeton University Press(2006;1994):175.
22. Petroski H. *Success through Failure—The Paradox of Design*. Princeton University Press(2006;1994):169.
23. Ganssle J. First do no harm. *Embedded.com*. Mar 10, 2003. Available at. <http://www.embedded.com/showArticle.jhtml?articleID=159400817>. Accessed July 17, 2007.
24. Kohn L, et al., eds. *To Err is Human*. National Academies Press (1999):157.
25. Petroski H. *To Engineer is Human*. Vintage Books(1992):105.