The Illusion of Safety

By Jason A. Campagna, M.D., Ph.D.

The Meaning of Safety

Medicine is an enterprise like few others in human affairs. It seeks, in essence, to put itself out of business. By helping to care for those who are ill and prevent others from becoming ill, medicine strives to alleviate the burden that gives it purpose. But, because medicine is fundamentally a human endeavor, it is, and forever will be, troubled by human failings.

Humans, despite their best efforts on their best days under the best of circumstances, will fail. To fail is to remind oneself that striving to be better is a moving target. With this specter of "effortless failure" looming over us, how does one think about safety? We hear the word so often and see the accompanying yellow safety ribbons that adorn every lapel and scrub top. But words and ribbons are not safety. We face a conundrum in medicine: How can we reduce errors in a system so dependent on human infallibility?

I have come to understand a few simple truths about this elusive concept. First, safety is not organizational: it is cultural. Second, safety is not in any way "bankable." Three safe days or months cannot be stored someplace and used later during a relative paucity of safety or reliability. Like so many other things in life, it must constantly be created. Beyond these basics any attempt to define safety is largely, in my opinion, wasted effort. This column aims to explore in detail the question of what is safety. We will draw on stories from the world around us: the military, the space program, the petrochemical and nuclear industries, from mountain climbers and underwater explorers, and even from the ranks of medicine itself. We will extract lessons from these stories, and we will apply these lessons to our world of medicine in the hopes of trying to better understand what safety is.

The Concept of "Normal" Accidents

It has become fashionable to make a distinction between "systems" accidents and "operator" accidents. The former is said to be the result of some mystical interaction among opaque processes, while the latter is clearly and effortlessly attributable to some error committed by an identifiable human. This distinction is arbitrary and wrong.

In 1984, a Yale sociologist named Charles Perrow introduced the concept of a "normal" accident. Simply put, given the presence of sufficient complexity and very tight coupling of events in any system, multiple and unexpected interactions or failures are inevitable. This concept of normal is not a reflection of frequency, rather it is a reflection of the innate characteristics of such systems. His analogy that it is normal for us to die, but we do so only once, captures well this distinction. Humans and their actions are just one feature of the complexity of a system. They are not outside of it, and thus their actions, although possibly identifiable, are highly unlikely to be causally related to anything.

The definition of complex interactions is one that acknowledges their "outside of the design of the system" origin. Things happen that were never anticipated or planned for. This is disconcerting, no doubt, though nonetheless true. System accidents, Perrow argued, are uncommon, but they matter because of their potential to produce catastrophe. For this reason, better understanding of systems and accidents may help the complex system of medicine "be safer."

There have been some valuable lessons derived from Perrow's work. First is that the most banal and trivial things underlie some of the most serious accidents. Secondly, that the cause of almost any systems accident is found in the sheer complexity of the system: each small failure—design, equipment, people, procedures, environment—all are trivial by themselves. We take little notice of them. Yet, together, they often sum in non-linear ways to produce catastrophe.

A third lesson learned from Perrow is that organizations play a key role in facilitating error and failure. "Time and time again, warnings are ignored, unnecessary risks taken, sloppy work done …," writes Perrow. The problem, as he so deftly noted, is that such routine sins of organizations have very non-routine consequences. Our ability to organize matches up very poorly with the hazards of some organized activity. Medicine is such an organization.

The last lesson, but by no means the least important, is that "safety devices" can, and do, create new accidents. In 1961, Gus Grissom lost his Liberty Bell space capsule in the Pacific Ocean because a hatch with explosive bolts that had been installed for added pilot safety had blown prematurely. Although debate surrounds the cause of the failure, one thing is abundantly clear: without the safety hatch the ship would not have sunk. Fixes to system in the form of safety devices often allow those in charge to run the system faster, or in worse weather, or with bigger explosives, or with less margin of error.

Another derivation of Perrow's work is that investment in efforts at accident prevention are not nearly as productive as investments in mitigation of an accident's consequences. Given that much effort in medicine is expended on prevention, this topic needs further discussion at a later date.

Complexity

In 1947, Texas City, Texas, experienced what is widely recognized to be the worst series of fires and explosions in United States history prior to September 11, 2001. The major explosion involved a land-based oil refinery, which started as a fire on the *S.S. Grandcamp*, a ship in the Gulf of Mexico loaded with chemical fertilizer. Despite the efforts of the crew and the Texas City Fire Department, the fire could not be contained and the ship exploded. Fragments for this explosion were blown over three miles into the air, striking two airplanes which in turn exploded and fell to earth, igniting nearby oil tanks. The fires spread to a nearby chemical plant. Meanwhile, the sister fertilizer ship, not yet on fire, tried to escape. In the smoke, she rammed a second ship. Neither could then be moved. Within hours, the heat from the fire on the *Grandcamp* ignited the pair of "stuck" ships. This explosion ignited a sulfur refinery, causing another enormous explosion. At the time of the disaster, phone services in Texas City were not working because of a telephone operators' strike. When the operators learned of the accident, they quickly went back to work, but the strike caused an initial delay in coordinating rescue efforts. Over 50 percent of Texas City was on fire and more than 500 people had died.

There are many lessons here, but for our purposes there is only one: failures that were not anticipated (airplanes falling from skies, ships ramming one another in smoke-filled air) interacted with an expected failure (fire on a fertilizer ship) to produce catastrophic outcomes. The complexity of this system emerged as the events unfolded. How could one possibly make this system safer? What would a root cause analysis show when this accident was examined? Perrow is instructive here. He tells us that "Both our predictions about the possibilities of accidents and our explanations of them after are profoundly colored by social construction. We do not know what to look for in the first place and we jump to the most convenient explanation (culture, production pressure, human error) in the second place. When an accident occurs, we will find the most convenient explanation."

We do not look at other chemical plants or ships that have run for decades without any such horrid event. The explanation we have conjured may be present in other facilities but not ever resulted in any accident. Similarly, other places may have similar accidents but not because of the same "explanation" we have created, even though the exact conditions and the exact accident were present. Perrow continues: "If we were to perform a thought experiment, in which we could go into a plant or a ship that was not having an accident, but assume there had just been one, we would almost certainly find an accident waiting to happen. The results we investigate contaminate our investigation."

What then, is safety? Clearly the above demonstrates that it is not retrospective. The ability to learn from mistakes is clearly necessary, but by no means sufficient, to produce "safe" things or places. Safety is also not something that can be engineered. People and systems already get in the way, safety devices have a way of becoming unsafe. Antilock brakes let drivers go faster because they have better brakes. And so it goes. Yet we must continue to try to better understand this mystical thing that is the focus of so much attention in medicine right now.