TBD

by Charles Hoes

This installment of my TBD column involves three safety fairy tales. As is common with fairy tales, they are based on factual events, but with muddled and incomplete descriptions of what happened and why. The purpose of fairy tales is not to frighten, but to point to universal safety messages that will hopefully keep us from future dangers. I doubt my thoughts will have the impact of a great Grimm's fairy tale, but maybe they can serve as stones on the path to improvement.

As I sit to write this, there are three big safety events sharing the front pages of current newspapers. While they are all different, I see important similarities. Because each of my fairy tales is based on current news, the descriptions and my guesses about the events are incomplete and almost certainly incorrect in many details — hence, the "fairy tale" nature of my stories. Still, even if it turns out that I am totally incorrect in all of the details, there may be some useful insights to be gleaned.

The first story is about a train, pulling many oil tankers, that ran away and crashed in a huge ball of flame in a small town in Canada. Apparently, the engineer had stopped for the night and gone to sleep in a nearby hotel. The train slowly started to roll back downhill, picking up speed until it derailed in the middle of a small town, bursting into flames, destroying a large part of the town and killing dozens of people. My first reaction when I saw the footage on the evening news was to turn to my wife and — half in jest — say that the engineer failed to set the parking brake before leaving the train for the night. After a couple of weeks, I am hearing stories in the news that, apparently, the engineer failed to set the parking brake. The reason given is that there was an earlier fire on the train, the fire department had messed with the brakes and the engineer failed to notice. Somehow, this led to his failure to properly set the brakes. This seems odd, but not knowing the details of the braking system, all I can do is wonder how that could occur.

The second story that has been given front-page coverage in California has to do with the broken bolts on the new section of the Bay Bridge designed to reduce earthquake risks. This is a slowly evolving story having to do with very large, very strong bolts snapping when tensioned. Of course, hydrogen embrittlement was the first thing that popped into my mind when I first heard about the snapping bolts. This seemed highly unlikely because of the well-known nature of the problem and the equally well-known solutions. Over the past couple of months since the initial event, much has been said about poor Chinese quality control, failure to perform proper testing/inspections on the bolts, etc. None of this made much sense to me, but lately the news has been getting a little more specific and it is starting to make more sense. The current story is that high-strength bolts were selected and that the bolts were galvanized to prevent corrosion. As we all know, galvanizing high-strength steel is a recipe for causing hydrogen embrittlement, which has now been identified as the cause of the bolt failures. A little bird whispered into my ear that once upon a time, a long time ago, an engineering study was performed on this aspect of the design with the recommendations that:

- High-strength bolts not be used in this application because of the propensity for hydrogen embrittlement failures
- Galvanizing not be used on high-strength steel (if used) because of the potential for hydrogen embrittlement
- Every item be individually tested and inspected if high-strength steel is used
- Bolts be protected with a specific type of epoxy material

Apparently, none of these recommendations was followed. By the way, that same little bird indicated that the current behind-closed-doors engineering meetings on the subject are deciding whether to open the bridge or tear it down because the same problem exists elsewhere in the structure in locations that cannot be fixed. As with

any good fairy tale, I have no validation of that last point — it is just a quiet rumor in the hallways. I assume the engineering review team will make the correct decisions.

The third story has to do with an airliner crashing upon approach at the San Francisco airport. Apparently, the plane came in a bit too low and slow, hitting the tail section on a breakwall and coming to a spectacular crash on the runway. "Luckily," only three people were killed (not so lucky, of course, for those three and their families and friends). The story in the news is that the plane was coming in above the glide slope, then it was below the glide slope. There was also a "stick shaker" event, warning the pilot of an impending stall. It appears that once it became clear that the plane was too low, the pilot "pulled" up, most likely right into a stall condition. It is my imagination that the maneuver not only caused the plane to stall and therefore lose more altitude, but it also changed the attitude of the plane, causing the tail section to drop even lower and allowing it to hit the wall. Of course, there is much more to be learned — such as what was going on to allow the plane to get into the incorrect orientation and speed in the first place.

"A common element of all three stories as I have related here is a failure of human judgment and/or actions. However, I doubt if any of the parties in these stories did anything 'wrong' or in 'error' in the sense that they *intended* to do one thing and did something else."

A common element of all three stories as I have related here is a failure of human judgment and/or actions. However, I doubt if any of the parties in these stories did anything "wrong" or in "error" in the sense that they *intended* to do one thing and did something else. My guess is that they were all highly qualified and experienced professionals who did exactly what they thought was the correct thing, and did it perfectly — with the intention of doing it safely. There were no "errors" in the sense of intending to do something but failing to pull it off, such as slipping on a rock when crossing a stream, and no errors from inattention, such as failing to notice the car next to you when changing lanes because of texting while driving. Rather, these all seem to be errors that were purposeful, thought out and intentional. In the first case, it may have been based on a mental model of the status of the train controls. The engineer almost certainly didn't "forget" to set the parking brake; he probably thought about it and was certain that it was set. In the second case, it wasn't that the management didn't notice the memos warning of the dangers of hydrogen embrittlement; it involved a reasoned decision that the memos were incorrect and that the danger did not exist. The third event seems to have involved a problem with the pilot's "mental model" of what would happen if he were to "pull up" at that particular moment. He undoubtedly thought that the plane would gain elevation so he could go around for a second try, rather than drop and rotate enough to cause the landing gear and tail to hit the wall.

It seems that we are faced with three more instances where the events immediately proximate to the accident point to "human error" of one kind or another, rather than to equipment design. With the possible exception of the bridge, the designs were "good" — the brakes would have held the train, the steel bolts had adequate strength, the flight control system did everything it was intended to do. Yet we still had huge economic and personal losses because of the failure of a person (or persons) to do the "right" thing. I contend that the design, the design process and the social pressures in existence during the design process led to these errors. They were not errors of judgment; they were errors evolving from the failure of the design team to fully anticipate the mental models of the people who make the ultimate decisions about which action to take.

As I sit and watch the news unfold on these events and "armchair quarterback" what could have been done to prevent these situations, it appears that we might be focusing too much on how things work (the mechanical and software side of safety) and too little on the mental models that we all use to successfully get through our days. A personal example might help clarify the point. When I was first learning to drive, I had one heck of a difficult time learning to shift smoothly. Finally, one day I saw a clutch assembly in my brother's shop and saw how it worked. It then was totally natural to shift smoothly — once I had the correct mental model, it was a piece of cake to do it right. Without that model, I was learning motions, but there were just too many variations for me to learn them all. It went from thousands of learned micro-actions to one consistent set of actions based on a complete mental model.

I think we need to spend more time considering and learning about the *psychology* of engineering. This includes the engineering processes themselves so that we avoid integrating bad ideas into designs because of group pressure or outdated understanding, as well as how people learn to acquire the correct mental models of how complex equipment works so that the "instinctual" reaction is the correct reaction.