Design-Based Safety

David MacCollum

Design is the "Holy Grail" of Safety

The prevention of unintended occurrences — usually identified as "accidents" that result in personal injury or damage — is usually considered as "*safety*." The most common approach to safety focuses on behavior that attempts to prevent accidents from occurring with the involvement of users and operators. In many circumstances, this has been the only option to prevent accidents.

Technology has provided us with many machines, and society relies more and more on complex equipment which now is entering an age of automation. Going forward, safe design will be the key to preventing accidents. The transition from behavior-based safety to design-based safety is not easy, as both the public and engineering professionals lack the wide scope and diversity of knowledge needed to ensure for safe design in complex systems. Traditionally, many designers and manufacturers have considered the cause of accidents to be the ineptness of users/operators. As more and more of the error-producing tasks become automated, the measuring of safe performance becomes an issue of reliability. The new concept of safety shifting from behavior-based to design-based safety now becomes a whole new ball game.

In the late 1920s, two legal precedents were established to ensure the equipment safety of component parts and enterprise adoption. The first case was *McPherson vs. Buick*, which required the auto manufacturers to examine all components that were assembled to make an automobile safe, and the important requirement to reject unsafe defective components. In this case, a wooden wheel spoke with a huge knot should have been rejected by Buick. The spoke failed when the car drove over a pothole, and caused the vehicle to crash. The second case was the *T.J. Hooper* case regarding the loss of expensive cargo carried aboard a barge being towed at sea in bad weather. The *T.J. Hooper* — a tug boat — was without a radio receiver that would have allowed the crew to receive a signal from a U.S. Coast Guard radio station that reported stormy weather at sea. The defense attorney argued that radios at the time were unreliable and the tug boat trade association rejected the need for these unreliable receivers. Learned Hand, the U.S. Circuit Court judge, ruled that even with unreliable radios, it was better to learn of bad weather part of the time than none of the time. He also ruled that rejection of radio receivers by the tugboat industry was an invalid excuse not to use available communication. Little by little, legal liability grew to become an effective advocate for safe design. Safe design is a moral issue and cannot be put aside. Because identifying of hazards and providing for safe design is a complex process, many design engineers avoided this priority for fear that they would err.

There have been two enterprising groups that created incentives for design-based safety. In the 1960s, first and foremost, was the Department of Defense. To ensure safe aerospace systems, it adopted MIL-STD-882, which fostered the systems safety profession. Unrecognized, and often subject to insurance intolerance, the second and most dramatic force to promote design-based safety is plaintiff attorneys, who have pursued liability claims against the unsafe design of countless products, machines, equipment and systems. Probably most notable was the Ford Pinto automobile's dangerously located gas tank; several passengers were incinerated during a rear-end collision as a result of this dangerous design.

Heroes of the 1970s, when auto and equipment personal injury liability litigation began to take off, were engineering experts who testified on how inherent hazards could be overcome with safer design. Many of these safety advocates were System Safety Society members.

The schools in various disciplines of engineering need to work together to provide common marketable skills in design-based safety. These designs will require software to store records, monitor performance for anomalies that are hazardous and quickly direct an appropriate interaction to report or fix the hazard. Change is on the way, as one only needs to look at automotive near-object detection television advertisements on collision prevention.

In the past, it was politically correct *not* to raise safety issues that involved design defects or needed improved procedures. As design replaces reliance on human performance, design-based safety has become the desired measure of performance. This priority has made design the "Holy Grail" of safety.