Design-Based Safety

David MacCollum

The Evolution of Safety

The word "safety" has a variety of meanings. It is a condition of being free from "accidents," or any device for preventing an accident. The word "accident" means "unintended event," and does not reveal that there is a cause created by a "hazard." In many people's minds, an "accident" is the result of someone's failure to avoid or prevent a dangerous condition or circumstance. It is often assumed that all one needs to do is just "be safe." Overlooked is that "hazards" are not obvious to everyone all of the time. It is a fact that as machines and systems become increasingly complex, many hazards are hidden. The evolution of safety is the transition of "behavior-based safety" to "design-based safety."

The roots of design-based safety go back to Biblical times. Deuteronomy 22:8 cautions, "When you build a new home, be sure to put a parapet around the edge of the roof. Then you will not be responsible if someone falls off and is killed." At that time, living space for most people was very limited, and the flat roof was a convenient, open space for people to gather. Today, there is often a design omission on commercial buildings with flat roofs with no parapets where mechanical systems are located and require maintenance. Design-based safety is not generally perceived as a necessary engineering requirement. The public often views safe design features as misplaced priorities that produce money for someone. A common management oversight is that development of a new product requires testing and evaluation to identify and eliminate all hazards before the product is released to the marketplace. Part of the problem is that conventional safety practitioners are only skilled in behavior-based safety and are unknowledgeable in design-based safety. The entrenched governmental regulatory processes focus on standards developed after a number of injury-producing failures occur. Usually, tack-on safety features are required and enforced by citations with fines. Sometimes, this practice is the basis of liability litigation. Conspicuously absent is the government's providing general enterprise with the tools or knowledge of how to achieve design-based safety. Our military and aerospace establishments understand the need for ensuring for design-based safety as they ensure reliability by having proving grounds that test and evaluate new aircraft and missiles. Perhaps the absence of governmental regulation of methods to ensure design-based safety is a good thing. This absence is a positive incentive for system safety specialists to become the authoritative profession, with a nationally recognized certification process. Most members of the public are skeptical of design-based safety, as they are not knowledgeable about how reliably safe products or systems are developed. Environmentalists oppose the Keystone Pipeline with the single thought that pipelines can leak. They do not relate that the Alaska Pipeline is in a harsh location and has done remarkably well. Further, they are unaware that pipeline design is now much more advanced and more reliable. They never consider that pipeline failures involve installations that are 50 to 60 years old. The objection environmentalists do not consider is that the use of railroad tank cars to transport oil is much more dangerous, as many hazards exist in their operation. There are countless examples of everyday experiences in which machine or systems design proves to be far more reliable than known levels of human performance that has a propensity to err.

One of the key issues for rejecting automation is the use of automation to monitor human performance. At present, new automobiles are not equipped with sensors that can detect and respond to traffic lights at intersections to prevent the running of red lights. Google's autonomous self-driving cars have sensors on their test vehicles, and these driverless cars have travelled for more than 100,000 miles on freeways and will reliably respond to traffic signals. Anti-safety agitators object to cameras that record red light runners and believe they are just a money-making process of fining red light runners. They say safety is a straw-man issue as the cameras are an unfair tax on drivers. Some of the anti-red-light-camera people believe these cameras are an invasion of their privacy. Their reasoning is wrong because they are endorsing the law-breaking of the ordinances requiring drivers to obey traffic lights.

A traffic signal is a hazard in "dormant" mode most of the time because most people stop at the red light. When someone runs the red light, the hazard is in the "armed" mode. When the driver collides with a car in the crossing, the hazard is in the "action" mode. No one can predict the outcome when a driver runs a red light. System safety engineers know that it is Bayes Theory of chance that another vehicle will be struck and no one knows how serious the consequences will be. Anti-safety, no-red-light-camera advocates assume no collision will occur, as they cannot reason the nature of hazards always being in one of the three modes discussed above. Having sensors in cars to reliably and automatically respond to traffic signals is the next step in automobile design-based safety. The National Transportation Safety Administration supports the development of autonomous safety features, as it is the next great leap for improving traffic safety. The driving public will be slow to accept these changes. In the past, a small vocal minority was against seat belts, cruise control, air bags and other car safety features. The transition from behavior-based safety to design-based safety will be slow because many people cannot accept that human performance is less reliable than design-based safety performance.

Most people have difficulty in projecting how a hazard produces different dangers in different locations. A puddle in a walkway is an inconvenient, shoe-wetting hazard. In the tropics, the puddle can be a host for breeding mosquitoes that spread malaria. In Northern winter climates, the puddle freezes and becomes a sheet of ice that can cause a fall resulting in a broken hip. As we begin to include more technology in our infrastructure, production facilities and consumer goods, hazards will fade from view. For this reason, many system safety engineers will be needed to aid all enterprise as it makes the transition from behavior-based safety to design-based safety. No longer can the general public be relied on to identify all hazards that new technology creates. Emerging technology in all professions and enterprise is becoming complex and far removed from the involvement of those who rely on its use or benefits. Medical doctors rely on symptoms to identify the ailment and conduct tests to ensure the diagnosis is valid. Medicines to treat ailments go through extensive tests before they are permitted to be used. Medical researchers who test new cures for disease are really involved in medical system safety, as they identify all side effects that need to be eliminated. Even with this research and testing of vaccines, there are still a few people who refuse their use and bad-mouth these reliable life-saving vaccines.

A hazard is often an unseen, defective part or component of a mechanical device and can be well hidden in a complex system. Electronics manage the system and are vulnerable to faulty software, sneak circuits and hackers. System safety relies on a wide diversity of expertise to identify these hazards. System safety is not confined to design, as it includes project construction, planning operational methods and maintenance. System safety engineering includes an examination of all the hazardous interfaces that will arise in construction, operation and maintenance. Hazards need to be removed by design and planning, as reliance on behavioral modification is unreliable.

Historically, the design of buildings, cathedrals and even ships was a well-kept secret. In 1627, *Vasa*, a Swedish warship, was the unwritten work-product of the builder. After it was launched, the King of Sweden, without consultation with the builder, added heavy guns to the top deck. In the fanfare of its 1628 maiden voyage in the Stockholm harbor, it capsized from a gross lack of stability. Less than a century later, design of the battleship *U.S.S. Constitution* (Old Ironsides) and a sister ship, *U.S.S. Constellation*, were the products of detailed design plans. One was built in Boston and the other in Baltimore. Today, both are U.S. Navy relics marking the beginning of carefully developed Navy warship design that included, at that time, state-of-the-art ship design by a team of experts.

The transfer of safety from behavioral-based safety to design-based safety has no limits. Agriculture, electric power transmission, auto freeways, construction equipment and homes are just a few that are experiencing this change in priorities. Those accustomed to ensuring uniform behavior do not always perceive that this transition involves the adoption of automated features that reduce human error that may arise during input or control, and they immediately object to such technological progress. This is why the evolution of safety is slow, as those outside the system safety profession lack the skills for this new age of safety. The acceptance of design safety features in construction equipment, such as rollover protective structures (ROPS) on mobile construction equipment and a number of safety devices on cranes, were bitterly opposed by manufacturers, sales organizations, rental companies and buyers. The lack of design safety features was often the source of personal injury litigation because OSHA did not include some form of cost relief for the employer or buyer of equipment, which delayed provision for life-saving features being included in regulations. An important consideration of system safety is to ensure that the buyer/user will enjoy a profit by adopting design-based safety.

Additionally, the system safety engineer must become a spokesperson and authority for the benefits of the safer design he or she has developed. To subdue public objections to any change that design-based safety brings, the benefits of how improved design works need to be explained in lay terms, in small bites of informa-

“The evolution of safety will forever be an ongoing process. Supervisor control of almost every function accomplished by manual labor will disappear as autonomous machines replace both human supervisory control and manual labor. Let’s face this issue head on.”

tion to gain public acceptance. There are two reasons it took so long for the final acceptance of design safety for construction equipment, such as rollover protective structures (ROPS) on mobile construction equipment and a number of safety devices on cranes. The absence of design safety features was often a source of personal injury litigation because OSHA did not include training of manufacturers, employers or buyers of equipment on how to ensure safe design. An important consideration of system safety is to advise manufacturers and employers that they will enjoy greater user productivity by adopting design-based safety and will have reduced exposure to litigation.

The evolution of safety will forever be an ongoing process. Supervisor control of almost every function accomplished by manual labor will disappear as autonomous machines replace both human supervisory control and manual labor. Let’s face this issue head on. In the future, there will be little human involvement in many production or service activities. What will become of the workforce? It will be replaced by highly skilled design engineers, specialized maintenance personnel and computer software program monitors. These people will be paid far higher salaries and make for a much more affluent middle class. Machine-made products will cost less and attract more purchasers because of the lower prices. Automation will increase our national wealth and provide a well-to-do middle-class that can afford to enjoy more leisure time as automation fuels and accelerates the transition from behavior-based safety to design-based safety.

Every system safety specialist is a learned, creative practitioner who is not receptive to being held to old ideology or dogma, which are myths that do not save lives. The very existence of our Society is based on our ability to exchange thoughts and theories about the development of reliably safe performance for a wide diversity of systems. Our annual Conference, *Journal of System Safety* and a one-on-one with members achieve this goal. Our members’ quest of hazard data and design options to eliminate hazards makes our International System Safety Society a valuable resource for all enterprise. There is no distraction, wasted time or effort in our Society’s governance of system safety experts. The last thing system safety experts want is a Society that attempts to dictate how they conduct their research and analysis. The issue of globalization of system safety does not exist as the focus of our work product relates to the world-wide enhancement of reliability of productivity and the often autonomous operation of equipment and services. Recent articles published in *Harvard Magazine* and the *Atlantic Monthly* portray how globalization does not raise the economic status of people in developing countries. A major role of our International System Safety Society is to publicize to both industrial leaders and the public our special skills and accomplishments in developing design-based safety. This is the evolution that true and real safety is all about.

System safety engineering in the future will most likely become the most dominant professional practice involved in safety. Public acceptance will occur because system safety skills are able to eliminate hazardous conditions and circumstances by design, assembly and construction planning. System safety expertise provides a hands-on interface with all disciplines of engineering and science. The system safety engineering practice of test and evaluation helps to ensure the reliability goal of preventing operational failures. The plague of ‘”accidents” is removed with a systematic identification and removal of hazards by design and planning. System safety provides a universal comfort of confidence to management, users and the public, with failure-free operations. The development of all these objectives is the “Evolution of Safety.”