Design-Based Safety

David MacCollum

Reliability

As both business enterprise and governmental activities become automated, reliability will be the measure of performance. The term "reliability" establishes an actual value of absolute dependable failure-free performance from all hazardous conditions or circumstances during a specific time period or cycles of operation. Reliability ensures for the reliable and safe design of products, facilities and systems of operation, production, construction, resource extraction, transportation and storage. To achieve reliability, design becomes the "Holy Grail of Safety." The primary hindrance to achieving reliable safe performance is the intervention of human input. A choice of developing a reliable machine or system depends on either eliminating hazards that are activated by people or eliminating people with a completely autonomous system.

Many common examples exist in which design eliminates a hazard that becomes active by human involvement. A classic example is the evolution of the home washing machine. Originally, washing machines came with powered rollers to squeeze water out of the wet laundry. The hazard became active when a hand of the user was caught and crushed between the rollers before the pressure could be released. Then came the spin-dry cycle that eliminated the hazardous wringer. The spin-dry cycle eliminated the need for hand labor while increasing safety. Another example is the archaic horse-and-buggy roadway with opposing travel directions. These roadways are ill-suited for high-speed vehicular traffic, as the slightest lapse in driver attention can cause a head-on collision. Divided highways help eliminate this hazard. In addition, new hospital design usually includes separate rooms for all patients to reduce the transmission of infections.

The driverless car is an autonomous system that eliminates a human operator. The removal of human involvement creates a requirement for a much higher level of safe design, as the public will not tolerate a hazardous design defect. Reliability does not include any acceptable degree of machine failure. Often, human failure was excusable since lapses in people's performance were known.

Mechanical contrivances with unsafe design are unable to achieve reliable failure-free performance. The General Motors' (GM) ignition switch failure triggered a multi-million car recall — blindsiding the president of GM — and is a classic example of the absence of a basic system safety hazard analysis program within the company. The unsafe faulty design required key insertion in a vertical position, with the serrated edge pointing downward. With a quarter turn, the key became horizontal, and if there was too much weight from other keys hanging on the key ring, the key could rotate downward into the "off" position. Design should have provided for horizontal key insertion so the key would have to be in a *vertical* position for starting, thus eliminating key ring weight from rotating the key downward due to the force of gravity. It appears that reliance on faulty risk assessment, rather than a simple logic test, led to numerous driver deaths when the car unexpectedly stopped running, causing the loss of the air bag system that became inert because of a loss of power steering.

The biggest threat to reliability is when cybersecurity is hacked, as many remote-controlled systems and sensors rely on the Internet or other wireless systems that can be easily hacked. The July 12, 2014 issue of *The Economist*, in an article entitled "The Internet of Things (to be hacked)," tells how former Vice President Dick Cheney's wireless heart monitor was modified to prevent a remote assassination attempt. The same article quoted an estimate by a think tank, the Centre for Strategic and International Studies, that the cost to the global economy of cyber-crime and online industrial espionage is about $45 billion each year. This is a new phase of reliability vulnerability. When

"Most people are concerned with the probability of any failure from all causes. Some managers, executives and corporate leaders have a lack of understanding of reliability and only want to know what the overall chance of failure is. The task of system safety engineers is difficult, as their function is to identify each hazard that presents a compromise to reliable performance and provide a concept of a design feature that will control or eliminate the hazard. In most circumstances, the cure is remarkably simple — as with the GM faulty ignition key."

miniature computers are implanted in machines so they can be remotely controlled by wireless technology, they become vulnerable to hacking and destruction. Using "guinea pig" identification of failure modes and issuing patches to fix the flaws are management practices that destroy reliability. The system safety specialist needs to review and test software before it reaches the consumer. These issues should not be neglected. We should not wait for governmental intervention that would develop too much restrictive regulation. High-tech firms need system safety specialists to find ways to make these wireless-controlled systems reliably dependable.

The scientific development of reliability is often overshadowed by traditional thinking that goes back to the blindfolded Greek goddess Tyche, who spun the wheel of fortune to signify the uncertainties of risk. Most people are concerned with the probability of any failure from all causes. Some managers, executives and corporate leaders have a lack of understanding of reliability and only want to know what the overall chance of failure is. The task of system safety engineers is difficult, as their function is to identify each hazard that presents a compromise to reliable performance and provide a concept of a design feature that will control or eliminate the hazard. In most circumstances, the cure is remarkably simple — as with the GM faulty ignition key. The good news is, as automation becomes a dominant part of industrial enterprise, reliance on complex employee safety programs is no longer needed. Exercises in developing a safety culture, risk management concepts and unreliable personal value adjustment programs only offer a way of living with hazardous conditions and circumstances. Our entire social attitude changes when a person's survival is no longer limited by the ravages of disease or exposure to dangerous environments. In its place, people-generated violence can occur with an absence of social responsibility and is in direct opposition to reliable safety performance. To overcome the thrill of excitement experienced in dangerous conduct, our educational institutions need to define clearly the actual consequences of not adopting safety features. In some states legislators have repealed the need for motorcyclists to wear safety helmets in the belief that this regulation limits personal freedom of choice. The system safety specialist can perform an invaluable service to the public and our educational institutions by making a comparison, in lay terms, between having no safety feature and the actual magnitude of consequences in terms of injury and damage without such a safety feature. In the halls of the legislature, the need for motorcycle safety helmets was dismissed because the factual increased social burden of such incidents was not introduced. Perhaps our media has overly glorified sports that promote dangerous conduct. However, a topic in personal liability that is arising is the use of painkillers so football, basketball and other high-hazard sports players can continue to play by deadening the pain produced by a severe injury.

The pursuit of reliably safe performance should not be a "killjoy," but a recipe for a longer productive advancement of civilization and personal well-being.

To me, the recent excellent article in the Spring/Summer 2014 of our *Journal of System Safety*, entitled

"*Exxon Valdez*: Human Error Plain and Simple," exemplifies 10 human failures. Applied cybernetics technology can do a lot to monitor human performance to achieve reliably safe navigation. Many examples exist about cybernetic design that can totally overcome foreseeable lapses in human performance when operating ships, aircraft, cranes and other equipment. This is how reliability is developed.

With great speculation, I wonder where the quest for applied concepts of reliability will lead. Will it be to the use of cybernetics to ensure safe performance of many activities?

The recent, much-publicized loss of Malaysia Airlines Flight 370 from Kuala Lumpur, Malaysia to Beijing, China, on March 8, 2014, with the loss of everyone on board could have been prevented by greater application of cybernetics.

First and foremost, long before the aircraft reached the area where severe weather storms existed, a revised flight plan should have been issued based on a computer analysis, rather than by decisions of ground-based remote flight controllers.

To avoid unfounded speculation as to the location of aircraft in flight, a running Internet log of the GPS should be maintained by the originating airport or controllers. It also appears the less-experienced copilot had, for unknown reasons, failed or was unable to use the onboard automatic pilot computer.

Ensuring flight safety involving any change of circumstances is an issue of reliability. Tools are available to anticipate and sense any change of circumstances that endangers the flight of aircraft, and with automation, cybernetics overcomes errors in judgment by both pilots and ground-based flight controllers. The Malaysia incident is a classic example of how rampant speculation as to what occurred was revealed when the black-box recorder was retrieved. Reliability to ensure for flight safety provides a strong incentive to develop and install automated cybernetic systems to avoid the hazards that can arise from a change of circumstances and even terrorism.

The transition to reliability from conventional assessment of unintended hazards with so-called judgment of risk is difficult for those in the top leadership hierarchy, as they often lack a diversity of knowledge and experience. Everyone in management with the same mindset and similar background can become easily misguided by peers and become prepositioned to make, individually, the same errors or mistakes of judgment. Some managers cannot believe that with available technology incorporated in design, even acts of terrorism such as aircraft hijacking can be reliably overcome. As with many other unwanted human intrusions, the implanting of small computer chips in equipment can alert people to the presence of an unwanted change of circumstances. The simple implant of an identity chip in house pets has afforded reliable return of lost pets to their owners. Reliability is the backbone that makes *design* the "Holy Grail" of safe performance.

"The transition to reliability from conventional assessment of unintended hazards with so-called judgment of risk is difficult for those in the top leadership hierarchy, as they often lack a diversity of knowledge and experience. Everyone in management with the same mindset and similar background can become easily misguided by peers and become prepositioned to make, individually, the same errors or mistakes of judgment."

Adoption of reliable equipment design performance goals minimizes blame — no failure, no blame! A reliable design prevents stress to operational personnel, as it ensures for failure-free performance within specific time periods of operation. A pilot of a jet passenger aircraft has confidence that the jet engines will function without failure for a given number of hours. The New York airport had failed to make a reliability assessment of the hazard of large flocks of big birds flying into the airport's environment, which rendered the jet engines inoperable. Reliability includes how to avoid such a hazard during take-offs and landings. Reliability goes beyond the expectation that both jet engines could be simultaneously stopped. Records did not show that any such event had happened in the past, but this does not make it an acceptable risk. The key to airport reliability is to stop flights in and out when large bird flocks are in the vicinity of the airport. Further, this reliability criterion also allows for development of features that the birds dislike, so the airport will become an undesirable location into which birds wants to fly. There is an old adage that a missile system is so reliable that there is only one chance in a million of failure. This does not mean that if the first missile to be launched fails when launched that the next 999,999 missiles will be failure-free.

The tool kit for system safety specialists includes knowledge of how reliability is developed. As specialists, they have the ability to identify hazards and eliminate them by design.