Design-Based Safety

David MacCollum

There Is No Such Thing as an "Acceptable" Risk

The amount of harm a hazard can cause is unknown, as many hazards remain dormant most of the time and become armed infrequently. Once armed, of course, they are able to cause harm or injury; however, in most circumstances, it is rare that the hazard actually causes injury or damage. But, because the natural seriousness of harm cannot be quantified, there is no such thing as an "acceptable" risk.

In 1912, the newly launched *Titanic* did not sink as the result of its steel hull plates being pierced and torn open after colliding with an iceberg. This was the belief until the broken hull was found on the bottom of the sea floor and inspected. At the time *Titanic* was constructed, the shipbuilders were unable to assure for slag-free rivets and therefore assumed that rivets contaminated by slag were an acceptable risk. During the ship's construction, it was known that the rivets holding the sheets of the hull steel together were contaminated with slag, which weakened their strength. At the time, the only way to identify completely defective rivets was to tap the rivet with a hammer to determine if it was loose. When the wreckage of *Titanic* was found and inspected, it was proven that rivet failures caused the hull sheets of steel to part. As a result, the previous theory that the iceberg pierced the steel hull was determined to be false. Some of the broken rivets were retrieved and found to have failed under stress due to contamination with slag.

In today's world of complex design of missiles and machines, reliability of every component leaves no option for an "acceptable" risk of failure simply because it may be a rare event. In comparing risk management with system safety analysis, the key to safety is to ensure reliable performance of each safety-critical component before the machine enters the marketplace.

Some 50 years ago, fault-tree analysis brought system safety to the forefront of hazard prevention

"During (*Titanic's*) construction, it was known that the rivets holding the sheets of the hull steel together were contaminated with slag, which weakened their strength. At the time, the only way to identify completely defective rivets was to tap the rivet with a hammer to determine if it was loose When Titanic was found and inspected, it was proven that rivet failures caused the hull sheets of steel to part. As a result, the previous theory that the iceberg pierced the steel hull was determined to be false. Some of the broken rivets were retrieved and found to have failed under stress due to contamination with slag."

at the time of design. Counting accidents to measure safety performance is ridiculous when a system safety analysis can eliminate designed and planned hazards before a new product or operation is introduced.

The introduction of MIL-STD-882 required a system safety analysis at the time of design. This resulted

in "miracles" of failure-free design that ensured for reliable accident-free performance in the U.S. military's aerospace activities.

The term "risk" is not about prevention. It is about establishing a mechanism to compensate for a loss that may occur. The term "reliability" is about hazard prevention. It is about identifying and preventing design and operational hazards to achieve failure (accident)-free performance. Risk management is an oxymoron, as the magnitude of damage and/or loss of life is an unknown, as was the failure of the slag-contaminated rivets on *Titanic*. NASA does not hold management accountable with MIL-STD-882. The three major catastrophic aerospace disasters (the incinerating fire of a nitrogen-free rocket capsule on *Apollo 1*, the faulty gasket that could not resist freezing weather on the space shuttle C*hallenger* and the loss of the space shuttle C*olumbia* after being damaged with a large piece of separated Styrofoam during launch) had no previous record of occurrence and were therefore not considered risks. A management analysis ignored the voluminous warning of system safety specialists on the basis that no previous occurrence of the hazard existed and, therefore, management believed no risk existed. Acceptable risk management is a "killer" fraud. The system safety ideology dogma needs to become a part of all industry, and of the automotive engineering profession in particular. This will ensure the reliable, safe design of our cars, trucks and industrial machines used in agriculture, construction, forestry and mining and will help prevent hazard occurrence failures. Unfortunately, the concept of acceptable risk is a golden excuse for management to avoid the need for system safety analysis at the time of design and operational planning.

The opening paragraph of the Constitution of the United States of America established justice and promotes the general welfare of the public. Nowhere does the Constitution establish what risks the public shall endure as "acceptable." No anonymous management party has the right to establish an "acceptable" risk through either ignorance or direction. Management has the duty to protect life and property from hazards and has no authority to compromise safety by design or operational procedures under the guise of "acceptable" risk.