Design-Based Safety

David MacCollum

Is System Safety a Public Misconception?

Outside our professional fraternity of system safety practitioners, I am amazed at the "hocus-pocus" image of what system safety is. In lay terms, system safety needs to be explained as a learning process to identify unrecognized hazards at time of design.

The creative abilities of engineers will develop complex facilities and machines to enhance progress. When a new, innovative design is conceived to achieve specific objectives, usually many components are incorporated without the consideration of possible internal failures. For the most part, the accidents which result from these "internal failures" are a surprise! Without a system safety analysis to identify and overcome the design's hazardous conditions, its use can be plagued by many surprises (accidents) with unknown consequences.

Some insurance underwriters have perpetrated a myth, which assumes that a speculated risk factor can be assigned to a new design without a system safety analysis. Those without system safety expertise are imposing an unreasonable burden on creative engineering by assuming that risk can be controlled in this way. As an example, automobile litigation highlights the countless component design failures that were not identified at the time of planning and design and therefore left untreated, only to be dealt with as a surprise. With a history of failures, monumental punitive damage awards became commonplace. For a miniscule cost for a system safety analysis with safe design modifications, the bankrupting cost of faulty risk assessment could have been avoided.

In order to overcome public misconceptions, a system safety specialist assigned to a project should maintain a record of his/her analysis, including the reliability calculations noting the length of time of failure-free performance. These records provide a method for publicizing the learning process used to examine new systems at the time of design. The factual failure-free performance analysis needs to be available to explain how the design was achieved. The misconception about system safety is the result of an absence of an explanation available to the layman.

Recently, a successful landing on Mars with a faultless design was attributed to a system safety analysis at the time of design — even though this automated mission to Mars gave no details of how the design was examined in order to find potential faults that could cause surprise failures. The automotive industry needs to adopt similar system safety analyses to prevent the ever-present plague of ongoing hazard litigation. This is also true for civil engineering projects.

"For a miniscule cost for a system safety analysis with safe design modifications, the bankrupting cost of faulty risk assessment could have been avoided."

Uninterrupted operating performance without surprise accidents increases the value of new complex machines and facilities. All transportation systems (aircraft, automotive, rail and water) rely on reliable failure-free performance with an increase of automated operating control and a declining reliance on human operating performance.

To promote public acceptance of system safety, there is a critical need to inform the public in lay terms of how system safety is a learning process to institute the necessary design improvements that prevent hazardous circumstances from occurring. As the scope of automated machinery and technology expand into other enterprises beyond aerospace, system safety's role expands. An uninformed public is a serious impediment to the public acceptance of all new technology.