Unintended Consequences

TWA Flight 800 Accident

by Terry Hardy

On July 17, 1996, Trans World Airlines (TWA) Flight 800, a Boeing 747, crashed into the Atlantic Ocean just after take-off from John F. Kennedy International Airport in New York. All 230 people onboard were killed. The National Transportation Safety Board (NTSB) determined that the probable cause of the accident was an explosion of the center wing tank. The tank likely exploded from a flammable fuel/air mixture ratio in the tank, probably ignited by a short circuit outside the tank, resulting in excessive voltage surging through the wiring of the fuel quantity indicator system inside the tank. The NTSB faulted the certification of the Boeing 747. This certification process allowed heat sources to be located beneath the tank, with no means to reduce the heat transferred into the tank or render the fuel tank vapor nonflammable. The NTSB also faulted the design and certification concept that assumed that tank explosions could be precluded solely by eliminating ignition sources.

The NTSB stated that experience has shown that all possible ignition sources cannot be predicted and reliably eliminated. In this case, the NTSB found that qualification testing had been performed on fuel quantity indicator system probes, and that testing showed that the probes were free of arcing up to 2000 volts. Therefore, the system was assumed to be "explosion proof." However, that testing had been performed in the 1960s, and the probes had been in use for more than 30 years, leading to deterioration and potential for arcing that invalidated this assumption. While conducting its investigation, Boeing provided the NTSB with a fault tree analysis of possible ignition mechanisms. The Boeing analysis concluded that the probability of wiring producing an ignition source in the tank as being 1x10-6 events per hour. An independent review of that analysis by NASA showed that the Boeing analysis had relied on unrealistic inputs, and — had realistic numbers been used — a much higher probability of ignition would have been obtained for the fuel quantity indicator system wiring. In its evaluation, NASA stated that, "Many of the probabilities, failure rates, and/or exposure times were much lower than would reasonably be expected." As a result, NTSB stated that, "Failure modes and effects analyses and fault tree analyses should not be relied upon as the sole means of demonstrating that an airplane's fuel tank system is not likely to experience a catastrophic failure."

Lessons Learned: Risk assessment helps to understand significant problems, and to focus and prioritize resources to fix those problems. When risk assessment is not rigorous or is performed improperly, decision makers may not fully understand the potential for harm or the likelihood of a catastrophic event. Therefore, every attempt should be made to validate analysis inputs, and to allow for independent review of the results of any risk assessment. In addition, the assumptions we make in our analyses should be questioned, including both assumptions in our safety approach and assumptions in our quantitative analyses. Also, analyses alone should not be used for safety decisions. Analyses should be supported by testing, accepted industry standards, validated processes and sufficient design margin to ensure that the risk has been reduced.

Readers are encouraged to review the full accident and mishap investigation reports [Ref. 1] to understand the often complex conditions and chain of events that led to each accident discussed here. Additional lessons learned are available at www.systemsafety skeptic.com.

References