The 2015 Annual Reliability and Maintainability Symposium

Reliability and Probabilistic Risk Assessment - How They Play Together

Fayssal Safie Ph. D. [1]**, Richard Stutts** [2]**, & Zhaofeng Huang, Ph. D.** [3]

(1) NASA/MSFC, Huntsville, AL, USA, fayssal.m.safie@nasa.gov
(2) NASA/MSFC, Huntsville, AL, USA, richard.g.stutts@nasa.gov
(3) Aerojet Rocketdyne, Los Angeles, CA, USA, Zhaofeng.Huang@rocket.com

ABSTRACT

Since the Space Shuttle Challenger accident in 1986, NASA has extensively used probabilistic analysis methods to assess, understand, and communicate the risk of space launch vehicles. Probabilistic Risk Assessment (PRA), used in the nuclear industry, is one of the probabilistic analysis methods NASA utilizes to assess Loss of Mission (LOM) and Loss of Crew (LOC) risk for launch vehicles. PRA is a system scenario based risk assessment that uses a combination of fault trees, event trees, event sequence diagrams, and probability distributions to analyze the risk of a system, a process, or an activity. It is a process designed to answer three basic questions: 1) what can go wrong that would lead to loss or degraded performance (i.e., scenarios involving undesired consequences of interest), 2) how likely is it (probabilities), and 3) what is the severity of the degradation (consequences). Since the Challenger accident, PRA has been used in supporting decisions regarding safety upgrades for launch vehicles.

Another area that was given a lot of emphasis at NASA after the Challenger accident is reliability engineering. Reliability engineering has been a critical design function at NASA since the early Apollo days. However, after the Challenger accident, quantitative reliability analysis and reliability predictions were given more scrutiny because of their importance in understanding failure mechanism and quantifying the probability of failure, which are key elements in resolving technical issues, performing design trades, and implementing design improvements.

Although PRA and reliability are both probabilistic in nature and, in some cases, use the same tools, they are two different activities. Specifically, reliability engineering is a broad design discipline that deals with loss of function and helps understand failure mechanism and improve component and system design. PRA is a system scenario based risk assessment process intended to assess the risk scenarios that could lead to a major/top undesirable system event, and to identify those scenarios that are high-risk drivers. PRA output is critical to support risk informed decisions concerning system design.

This paper describes the PRA process and the reliability engineering discipline in detail. It discusses their differences and similarities and how they work together as complementary analyses to support the design and risk assessment processes. Lessons learned, applications, and case studies in both areas are also discussed in the paper to demonstrate and explain these differences and similarities.