

An Example of Risk-Informed Design

Rick Banke – SAIC

Warren Grant – NASA

Paul Wilson - SAIC

NASA Engineering requested a Probabilistic Risk Assessment (PRA) to compare the difference in the risk of Loss of Crew (LOC) and Loss of Mission (LOM) between different designs of a fluid assembly. They were concerned that the configuration favored by the design team was more susceptible to leakage than a second proposed design, but realized that a quantitative analysis to compare the risks between the two designs might strengthen their argument. The analysis showed that while the second design did help improve the probability of LOC, it did not help from a probability of LOM perspective. This drove the analysis team to propose a minor design change that would drive the probability of LOM down considerably.

The analysis also demonstrated that there was another major risk driver that was not immediately obvious from a typical engineering study of the design and was therefore unexpected. None of the proposed alternatives were addressing this risk.

This type of trade study demonstrates the importance of performing a PRA in order to completely understand a system's design. It allows managers to use risk as another one of the commodities (e.g., mass, cost, schedule, fault tolerance) that can be traded early in the design of a new system.