Application of Fault Management Theory to the Quantitative Selection of a Launch Vehicle Abort Trigger Suite

Yunnhon Lo, Ph.D.[i], Dr. Stephen B. Johnson[ii], Jonathan T. Breckenridge[iii]

The theory of System Health Management (SHM) and of its operational subset Fault Management (FM) states that FM is implemented as a "meta" control loop, known as an FM Control Loop (FMCL). The FMCL detects that all or part of a system is now failed, or in the future will fail (that is, cannot be controlled within acceptable limits to achieve its objectives), and takes a control action (a response) to return the system to a controllable state. In terms of control theory, the effectiveness of each FMCL is estimated based on its ability to correctly estimate the system state, and on the speed of its response to the current or impending failure effects. This paper describes how this theory has been successfully applied on the National Aeronautics and Space Administration's (NASA) Space Launch System (SLS) Program to quantitatively estimate the effectiveness of proposed abort triggers so as to select the most effective suite to protect the astronauts from catastrophic failure of the SLS. The premise behind this process is to be able to quantitatively provide the value versus risk trade-off for any given abort trigger, allowing decision makers to make more informed decisions.

All current and planned crewed launch vehicles have some form of vehicle health management system integrated with an emergency launch abort system to ensure crew safety. While the design can vary, the underlying principle is the same: detect imminent catastrophic vehicle failure, initiate launch abort, and extract the crew to safety. Abort triggers are the detection mechanisms that identify that a catastrophic launch vehicle failure is occurring or is imminent and cause the initiation of a notification to the crew vehicle that the escape system must be activated. While ensuring that the abort triggers provide this function, designers must also ensure that the abort triggers do not signal that a catastrophic failure is imminent when in fact the launch vehicle can successfully achieve orbit. That is, the abort triggers must have low false negative rates to be sure that real crew-threatening failures are detected, and also low false positive rates to ensure that the crew does not abort from non-crew-threatening launch vehicle behaviors.

The analysis process described in this paper is a compilation of over six years of lessons learned and refinements from experiences developing abort triggers for NASA's Constellation Program (Ares I Project) and the SLS Program, as well as the simultaneous development of SHM/FM theory. The paper will describe the abort analysis concepts and process, developed in conjunction with SLS Safety and Mission Assurance (S&MA) to define a common set of mission phase, failure scenario, and Loss of Mission Environment (LOME) combinations upon which the SLS Loss of Mission (LOM) Probabilistic Risk Assessment (PRA) models are built. This abort analysis also requires strong coordination with the Multi-Purpose Crew Vehicle (MPCV) and SLS Structures and Environments (STE) to formulate a series of abortability tables that encapsulate explosion dynamics over the ascent mission phase. The design and assessment of abort conditions and triggers to estimate their Loss of Crew (LOC) Benefits also requires in-depth integration with other groups, including Avionics, Guidance, Navigation and Control(GN&C), the Crew Office, Mission Operations, and Ground Systems. The outputs of this analysis are a critical input to SLS S&MA's LOC PRA models.

The process described here may well be the first full quantitative application of SHM/FM theory to the selection of a sensor suite for any aerospace system.

---

[i] Jacobs ESSSA Group, Ducommun Miltec, Huntsville, AL 35806, U.S.A.
[ii] Jacobs ESSSA Group, Dependable System Technologies, LLC, Larkspur, CO 80118, U.S.A
[iii] Jacobs ESSSA Group, Ducommun Miltec, Huntsville, AL 35806, U.S.A.