

Optimization of Second Fault Detection Thresholds to Maximize Mission POS

Evan Anzalone, Ph.D., NASA/MSFC

In order to support manned spaceflight safety requirements, the Space Launch System (SLS) has defined program-level requirements for key systems to ensure successful operation under single fault conditions. To accommodate this with regards to Navigation, the SLS utilizes an internally redundant Inertial Navigation System (INS) with built-in capability to detect, isolate, and recover from first failure conditions and still maintain adherence to performance requirements. The unit utilizes multiple hardware- and software-level techniques to enable detection, isolation, and recovery from these events in terms of its built-in Fault Detection, Isolation, and Recovery (FDIR) algorithms. Successful operation is defined in terms of sufficient navigation accuracy at insertion while operating under worst case single sensor outages (gyroscope and accelerometer faults at launch).

In addition to first fault detection and recovery, the SLS program has also levied requirements relating to the capability of the INS to detect a second fault, tracking any unacceptable uncertainty in knowledge of the vehicle's state. This detection functionality is required in order to feed abort analysis and ensure crew safety. Increases in navigation state error and sensor faults can drive the vehicle outside of its operational as-designed environments and outside of its performance envelope causing loss of mission, or worse, loss of crew. The criteria for operation under second faults allows for a larger set of achievable missions in terms of potential fault conditions, due to the INS operating at the edge of its capability. As this performance is defined and controlled at the vehicle level, it allows for the use of system level margins to increase probability of mission success on the operational edges of the design space.

Due to the implications of the vehicle response to abort conditions (such as a potentially failed INS), it is important to consider a wide range of failure scenarios in terms of both magnitude and time. As such, the Navigation team is taking advantage of the INS's capability to schedule and change fault detection thresholds in flight. These values are optimized along a nominal trajectory in order to maximize probability of mission success, and reducing the probability of false positives (defined as when the INS would report a second fault condition resulting in loss of mission, but the vehicle would still meet insertion requirements within system-level margins). This paper will describe an optimization approach using Genetic Algorithms to tune the threshold parameters to maximize vehicle resilience to second fault events as a function of potential fault magnitude and time of fault over an ascent mission profile. The analysis approach, and performance assessment of the results will be presented to demonstrate the applicability of this process to second fault detection to maximize mission probability of success.