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

Yunnhon Lo
Jacobs ESSSA Group
Ducommun Miltec
Huntsville, Alabama

Stephen B. Johnson
Jacobs ESSSA Group
and University of Colorado, Colorado Springs
Colorado Springs, Colorado

Jonanthan T. Breckenridge
Jacobs ESSSA Group
Ducommun Miltec
Huntsville, Alabama

***Abstract*—This paper describes the quantitative application of the theory of System Health Management and its operational subset, Fault Management, to the selection of abort triggers for a human-rated launch vehicle, the United States' National Aeronautics and Space Administration's (NASA) Space Launch System (SLS). The results demonstrate the efficacy of the theory to assess the effectiveness of candidate failure detection and response mechanisms to protect humans from time-critical and severe hazards. The quantitative method was successfully used on the SLS to aid selection of its suite of abort triggers.**

***Keywords-Fault Management; abort trigger; probabilistic risk assessment; state estimation; failure response; human rating; launch vehicle***

## I. Introduction

The purpose of System Health Management (SHM) is to "preserve the system's ability to function as intended." SHM provides the capabilities that preserve functionality, and can be divided into passive capabilities such as design margins and operational capabilities such as failure detection, isolation, and response (FDIR). These latter operational capabilities are termed Fault Management (FM), and are implemented as control loops, known as FM Control Loops (FMCLs). 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 [1].

As a type of control loop, aspects of control theory can be applied to understanding FMCLs. Control theory divides control loops into two major portions: state estimation and state control. Performance of control loops is also divided into two pieces, with separate metrics to determine the performance of state estimation and state control. For FMCLs, state estimation can be measured and assessed using "confusion matrix" parameters: false positive, false negative, true positive and true negative. State control assessments are based on the speed of the FM response compared to the current or impending failure effects that it mitigates.

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 assess the effectiveness of proposed abort triggers so as to select the most effective suite to protect the astronauts from catastrophic failure of the SLS vehicle. An abort trigger, in context of SLS, is the means by which the SLS detects a crew-threatening failure and sends a recommendation to the Multi-Purpose Crew Vehicle (MPCV) to initiate an abort response. An abort response during ascent enables the MPCV with its astronaut crew to escape from a failing SLS and safely return to Earth. The success or failure of the abort is ultimately measured by the probability that the crew returns safely to Earth in situations when failure threatens their safety. The value of an abort trigger is assessed by its contribution to enabling the MPCV and crew to escape the SLS-caused threat and hence minimizing the likelihood of Loss of Crew (LOC). The effectiveness of abort triggers is one important factor in the calculation of LOC, and hence to verify the program LOC requirements.

The methods described in the remainder of this paper provide one crucial set of information to risk-informed design and to the Probabilistic Risk Assessment (PRA) methods that support it: the effectiveness of FMCLs to mitigate the effect of failures. This paper describes one particular example of this general problem: the calculation of the improvement to crew safety gained (measured as LOC Benefit) by adding abort

The work described here was performed on the NASA SLS Program under contract NNM12AA41C.

triggers to the design, compared to the cost of adding such abort triggers (measured as Loss of Mission (LOM) Cost and the small additional LOC Cost). For FM, to date there have been few instances of quantitative assessment of the value or performance of FMCLs. Or, at least these authors are unaware of any full application of these ideas for entire FMCLs for a system, though there have been numerous assessments of parts of FMCLs in many systems. We believe that the assessments and metrics applied here may be the first such application for entire suites of FMCLs for a large complex system such as a launch vehicle and crew capsule.

Even though this paper describes the application of FM theory to the assessment and selection of a launch vehicle abort trigger suite, much of the methodology described here applies to any system in which FM is applied to predict, detect, and respond to failures. This paper describes the kinds of quantitative metrics by which FM is assessed for state estimation and state control, and demonstrates typical issues involved in applying those metrics to FM design and operations. It therefore provides insights that can be applied to any complex system in which prospective or current failures must be mitigated.

## II. Fault Management Metrics and Application to Human-Rated Launch Vehicle Abort Triggers

### A. *Abort Conditions and Triggers*

NASA's SLS, managed and integrated by Marshall Space Flight Center (MSFC), is intended to fly both humans and cargo, though unlike the Space Shuttle, only on separate SLS missions. For its crewed, human-rated configuration, an abort trigger is a specific type of failure detection that detects the existence of an "abort condition," which is a state or behavior whose existence implies a current or impending threat to crew safety. Most crew threatening failures ultimately result in one of three major situations: explosions of the launch vehicle, loss of control of the launch vehicle, or inability to achieve orbit even though the vehicle is otherwise able to fly normally. The need to escape from an exploding launch vehicle is obvious. Loss of control usually leads to an explosion as well, but the immediate threat is that the crew will be unable to safely abort off the launch vehicle that is oriented in the wrong direction. Finally, an abort is ultimately needed if the MPCV will be unable to achieve orbit. However, in these relatively benign scenarios, the MPCV generally has anywhere from a few seconds to a few minutes to abort from the stable launch vehicle.

While some abort triggers directly detect these three ultimate situations, some abort triggers detect precursors to these situations. Ideally, the latter is preferred due to warning time provided, however, except for limited failure scenarios, detecting all precursors with certainty is not currently technologically feasible. Triggers that pick up loss of control include decisions based on the vehicle attitude error that has exceeded its controllability threshold. Other abort triggers detect loss of communication with key components, which then cannot be controlled, which will eventually cause loss of vehicle control. These same triggers can also be indirect indicators of a structural collapse or explosion that has destroyed the components or communication to those components. Other abort triggers detect conditions relating to high or low solid rocket booster pressures or liquid propellant rocket engine temperatures. These indicate impending rupture of the solid rocket boosters or combustion chamber explosions.

When an abort trigger detects an abort condition, there are two possible situations. The first is that an abort is needed immediately. In this situation, it sends a message, called an "abort recommendation," to the MPCV. The second situation is when an abort is not required immediately, but will be required eventually. This happens in cases of slow-developing failures, or in cases in which the SLS will not achieve the desired orbit. In these cases, the SLS sends a warning message, not an abort recommendation.

In either case, only the MPCV or the crew inside the MPCV can initiate an abort action. The Flight Director in the Mission Control Center can also command the crew to initiate an abort based on telemetry data received from the SLS and MPCV. For situations that require an immediate abort, as designated by the SLS abort recommendation message, a set of MPCV computer algorithms known as the abort decision logic, will immediately and automatically initiate an abort. In cases in which the abort response is not required immediately, the crew has time to select the best time to abort.

The process used to identify abort conditions and potential abort triggers includes a variety of methods. Since SLS is composed of both new and existing hardware and software, some abort conditions and potential triggers are readily identified since they were defined or used in this fashion on prior programs. For example, the RS-25 Core Stage Engines (CSE) used on SLS are the same as were used on the Space Shuttle, but with upgraded controller electronics. These Space Shuttle Main Engines (SSME) have the capability to detect impending engine failures and shut themselves down through its failure detection and response capabilities, and these demonstrated capabilities are maintained for the SLS. Similarly the Space Shuttle and Constellation Ares I programs both used Solid Rocket Boosters and provided sensors and other hardware that can be used to detect booster pressures. This is an obvious candidate for use on the SLS as well.

Other abort conditions and potential abort triggers must be identified by assessment of new or evolving SLS designs. This is particularly true for the SLS Core Stage, which houses most of the avionics that controls the entire launch vehicle, with the exception of the Interim Cryogenic Propulsion Stage (ICPS), which acts as the upper stage for the first two SLS flights. For example, if the Core Stage Flight Computers have internal software failures, or fail too many strings of its redundant hardware, then they will be unable to control the vehicle and hence the MPCV must abort. Other potential triggers include detection of loss of control from the Guidance, Navigation, and Control System, of thrust vector control system gimbal angles, liquid oxygen tank and liquid hydrogen tank pressures, etc. These potential triggers are identified by considering the consequences of failure of the various boxes, with respect to ultimate crew safety on the MPCV.

One tool used to identify candidate abort triggers and to determine their coverage against mission and crew safety goals is the Goal-Function Tree (GFT). This representation provides a hierarchical representation of system goals and functions rigorously modeled using state variables. It enables a top-down assessment of the coverage of FM mechanisms to detect failures that can compromise system goals. For every goal that must be achieved, there is the possibility that it is not achieved. If it is critical to take action if the goal is not achieved, then the system designer can place a failure detection at that point. In turn, this detection can activate a failure response. By reviewing the impact of failure along all paths up the GFT, the FM engineer can design a suite of failure detections that ensure that all paths up the GFT are covered, and can provide preliminary information regarding how much warning time they provide for a response to be activated compared to the failure effects they are attempting to mitigate. For SLS, the GFT was used to assess the coverage and physical relationships of abort triggers. These relationships include understanding of whether two or more triggers existed along any given GFT path, which means that more than one trigger can detect failure effects for a given Loss of Mission scenario [2].

Once identified and described, these candidate abort triggers must be evaluated to determine if they provide sufficient benefit to crew safety to warrant inclusion in the SLS design. The evaluation process is based on the understanding of the launch vehicle risks through past failures, various design and safety analyses, such as GN&C controllability, Failure Mode and Effects Analysis (FMEA) and Hazard Analysis, Probabilistic Risk Assessment (PRA) and/or engineering judgment, and trades between technical capability, schedule, cost, benefit and risks. Because it is not technically and financially feasible to monitor all possible failure modes and to implement all abort triggers, a Risk-Informed Decision Making (RIDM) process, which is part of NASA's System Engineering Process, is implemented to emphasize the proper use of risk analysis in its broadest sense to make risk-informed decisions [3]. This is not new for NASA, or for engineering more generally. However, the quantitative analysis described in this paper to perform risk-informed decision-making involves several more engineering organizations in a comprehensive, in-depth quantitative analysis of Fault Management than has been performed to date.

### B. *Abort Trigger Relationships to Redundancy Management, Safing, and Caution & Warning*

In abort scenarios, frequently several other FM actions also occur. These include safing actions, Redundancy Management actions, and Caution & Warning notifications.

For any launch vehicle, history shows that the highest probability failures are those related to its propulsion system. For SLS, this includes the liquid oxygen and liquid hydrogen tanks, the plumbing to move the propellants to the liquid propellant engines, and the turbopumps, propellant injection, and combustion. However, liquid propellant engines have a major safety advantage compared to solid rocket motors insofar as they can be shut down. As previously stated, the SLS CSE, have the capability to detect failures and respond by shutting them down, i.e. engine redlines protections.

The CSE shutdown response is a so-called "safing" response. In general, safing is defined as an action to change system configuration, state, or goals to protect humans or assets. A CSE shutdown clearly fits the definition, as it changes the system configuration by removing failed CSEs from use, and in doing so it prevents an uncontained engine failure that protects the rest of the launch vehicle and the MPCV. In short, a shutdown, if successful, potentially prevents a catastrophic explosion.

For the SLS, if two or more CSEs shut down, the launch vehicle will either be unable to perform attitude control, or the launch vehicle will be unable to boost the MPCV to the desired orbit. In either event, an abort will be necessary. If only one CSE is shut down, then except for scenarios in which the shutdown occurs near the start of ascent, the launch vehicle can generally maintain control and the MPCV can reach orbit. From an analysis viewpoint, single engine shutdowns early in the mission, and multiple engine shutdowns are abort conditions. Single engine shutdowns, if they occur in the middle or end of the ascent, are not abort conditions because the MPCV remains safe and the MPCV can achieve nominal orbit. When a single engine shutdown is early in the mission and orbit cannot be achieved, the SLS sends a warning message to the MPCV, which signifies that an abort will be needed, but not immediately. If two or more engines shut down, then abort will be needed immediately and an abort recommendation is sent. For the purposes of analysis, the probability of successful CSE detection and shutdown is an important factor in the overall assessment of SLS aborts triggers.

CSE shutdowns are not the only potential safing actions for the SLS. During ascent, there are failure modes that result in the inability for one of the boosters to separate. If this occurs, it may be desirable to prevent both boosters from separating, as the launch vehicle is far more stable with two boosters remaining on the vehicle than only one. Prior to launch, there are a variety of safing actions that can occur, to prevent hazardous events from occurring. These will not be discussed in this paper, as these do not result in aborts.

Redundancy Management (RM) also plays a significant role in the analysis of abort triggers. This is because successful RM actions enable the mission to continue to successful completion. For example, if one of the three Core Stage (CS) Flight Computers (FC) fails, the RM action will remove the failed FC from the redundant suite, enabling the remaining two FCs to continue the mission. If one of the remaining two FCs fail, then the SLS will send an abort recommendation, because the ascent can no longer be continued safely.

Analytically, the successful RM response to a failure of one of three CS FCs is accounted for through a probabilistic estimate of the reliability of the redundant FC suite. If two of three FCs fail, this results in a LOM and consequent abort. If only one of the three fails, then the mission continues and no LOM results. Abort triggers come into play only if a LOM occurs, including False Positives of the abort triggers in a mission that otherwise would have succeeded and never when the mission continues successfully.

Finally, Caution & Warning (C&W) notifications are another aspect of the design worthy of mention. As described above, abort conditions that do not require an immediate abort are implemented as warning messages. Caution messages are sent from the SLS to the MPCV when a failure occurs that degrades SLS safety margins. Examples of this include the failure of a single CS FC of the suite of three FCs described above, or a propellant tank pressure that is higher or lower than expected, but not yet reaching safety margins that necessitate an abort. Warning messages and resultant non-immediate aborts must be accounted for in the analysis of abort triggers. Caution messages are only indirectly assessed insofar as they are related to the RM actions described above, which affect reliability of redundant component suites, and hence the calculation of LOM probabilities.

### *C. Abort Trigger Quantitative Metrics: LOC Benefit*

As described in the Introduction, FM is implemented as a suite of control loops that monitor state variables, determine if the states of these state variables indicate current or future failure, determine the location of the failure cause (isolation), decide on appropriate responses, and then execute these responses. Quantitative metrics that enable assessment of FM performance relate to these functions. While in general we can divide FM metrics into state estimation and state control metrics, the specifics of the metrics must be tailored to the application.

Since FM exists to preserve system functionality that achieve system goals, the designer must determine the goals and functions of the system that any given FM design is intended to protect. A given FM control loop might protect all of the top-level system goals, or it might protect some subset of the top-level goals or lower level goals. For example, for a real-time triplex voting computer system, the triplex voting (which detects a computer that is providing incorrect data and removes that data and/or the failed computer from use) preserves the system’s computing functions, which usually exist to support higher-level system goals.

Since abort triggers exist to protect the crew, for a human-rated launch vehicle such as SLS, the highest-level metric or measure of value of an abort trigger is the probability that the abort trigger and the resulting abort response enable the crew to escape the hazard and return to Earth. If no abort trigger exists to detect an abort condition, then the MPCV and crew will not escape the hazard or return to Earth. The abort triggers could be on the SLS, on the MPCV, with launch or mission operations on the ground, or could even be the crew itself. If an abort condition exists, an abort response must be taken, and this cannot occur unless the abort condition is detected, which is the purpose of an abort trigger. The value of the abort trigger in the analysis methodology described in this paper is measured as a Loss of Crew (LOC) probability per mission. To be precise, the measure of an abort trigger value is called “Loss of Crew Benefit”, or LOC Benefit, which is the per-mission probability that a given abort trigger saves the crew. In the NASA SLS Probabilistic Risk Assessment (PRA), LOC Benefit is sometimes called “Abortable LOM,” the per-mission probability that a LOM can be successfully ‘aborted.’

For LOC Benefit to be estimated, the abort trigger must detect the failure, which estimates the state (i.e. does an abort condition exist), and the abort response must succeed in removing the MPCV and crew from the hazard. Metrics are required for both, which follows the general rule that FM metrics are necessary for state estimation and state control. State estimation determines the current or future existence of the failure, and isolates (determines) the location of the failure to the necessary level of granularity. State control consists of deciding what response to take, and the effectiveness of the response. Between them, the state estimation and state control metrics must combine to calculate the LOC Benefit number.

State estimation metrics are based on the quad of True Positive, True Negative, False Positive, and False Negative. These are defined here.

- **False Negative:** An incorrect decision that a condition does not exist, when it actually does exist.
- **False Positive**: An incorrect decision that a condition exists, when it actually does not exist.
- **True Negative:** A correct decision that a condition does not exist, when it actually does not exist.
- **True Positive:** A correct decision that a condition exists, when it actually does exist.

For detection of abort conditions, the condition to which these definitions refer is not merely a failure, but a failure whose current or later effects will threaten the crew and require an abort response. Each of these metrics is specified as a probability. For False Positives, it is specified as a false positive probability per mission. For False Negatives, it is specified as a false negative probability per failure occurrence. True Positives and Negatives work similarly: a True Positive is specified per failure occurrence, and True Negative is specified per mission.

The next part of state estimation is fault diagnosis, which includes both fault isolation and fault identification. The former refers to determining the location of the cause of the detected failure effects, with a specified level of granularity. The latter refers to the specific failure mode or cause of the detected failure effects. For the on-board and immediate purpose of enabling the crew to escape from safety-critical hazards, identifying the cause of the crew-threatening hazard is unimportant, though it will matter for the post-flight failure investigation. Determining the location of the failure cause is also unimportant, as it only matters that the failure effects are somewhere on the launch vehicle. Once again, for post-flight analysis, it will be important to determining the location of the failure causes. Though fault diagnosis is a critical part of FM in general, for the purposes of abort trigger analysis it is not a significant issue and thus will not be discussed any further in this paper.

The next metric of potential relevance is the correctness of the selection of which response to take. In the case of abort conditions and triggers, during launch vehicle ascent there are only two possible responses: to abort immediately, or to abort eventually. From an implementation standpoint, the SLS distinguishes these two possibilities. For situations that require an immediate abort, the SLS sends an abort recommendation. For situations in which the abort does not need to be taken immediately, the SLS sends a warning message to the MPCV. Both of these cases are pre-determined before flight, and if the selection decision between these two responses is incorrect, it is incorrect in the design and analysis of the abort triggers.

The final metric of importance is the effectiveness of the abort response. In these cases, there are several factors involved. The first is the speed of failure effect propagations, which include failure effect propagations internal to the vehicle, and the propagations external to the vehicle, such as explosion overpressure, fireball, and debris. The second is the amount of warning time that the abort triggers provide. If more warning time is provided, then the MPCV has more time to escape the hazardous environment. The third is the criticality of these effects.

For explosion dynamics that consist of the three major factors of overpressure, fireball, and debris, the criticality of the impact to the crew can vary significantly over the course of ascent. During ascent, ambient air pressure, velocity through the atmosphere, and dynamic pressure vary greatly, as does the amount of propellant remaining in the launch vehicle. One of the most significant factors is the amount of debris generated in an explosion. In general, larger explosions resulting in more debris occur lower in the atmosphere. In turn, more debris means a larger probability of this debris striking the MPCV and causing LOC. Conversely, as the launch vehicle reaches very high altitude, much less debris is generated, and the MPCV can frequently survive the blast even if it has not escaped the hazardous environment, simply because no debris hits it.

All of these metrics are combined to generate the LOC Benefit for an abort trigger. The LOC Benefit is the measure of the value of the entire FM Control Loop in which the abort trigger resides. However, for every abort trigger added to the system, there is the possibility of a False Positive, in which the abort trigger erroneously determines that an abort condition exists and sends an abort recommendation leading to an abort. This produces an added probability of LOM, and is an inherent cost of an abort trigger. In addition, since every abort response can fail causing LOC, there is also a small added probability of LOC for every abort caused by a False Positive abort recommendation. This too must be accounted for in the overall calculation of the LOC Benefit, in which the False Positive LOC probability must be subtracted from the LOC Benefit of successful crew survival based on the existence of the abort trigger.

### D. *The Value of the LOC Benefit Calculation*

The calculation of LOC Benefit, compared to the LOM and LOC costs is a means of performing quantitative analysis of the value of abort triggers, or more generally, of the value of Fault Management and of System Health Management for a given system. The theory of SHM clearly indicates that as an extension of classical and robust control theory, the performance of FM Control Loops can be assessed in ways similar to classical control loops, and using similar metrics of state estimation and control. However, because the purpose of SHM and of FM is to mitigate potential, impending, and actual failure, the benefits of SHM/FM must account for the probability of failure. If a system were perfectly reliable at acceptable cost with a single-string design, no redundancy and no FM would be necessary. However, in practice few if any large-scale, complex systems are sufficiently reliable in this way, which makes FM necessary. Thus assessing the value and performance of FM requires estimation of the probability that failures will impact the system’s goals [1].

Estimating the probability of failure requires methods of reliability theory, PRA, and more generally, of risk-informed design. In addition to classical methods of estimating reliability of components, other sources of faults, such as common cause failure, human reliability or human error, and software faults are all needed to estimate the probability of failure of hardware, software, and humans. Since FM is implemented through FM Control Loops (FMCL) that mitigate the effects of failure, the value of these FMCLs inherently depends on the probability of the failures that they mitigate. Abort triggers necessarily exist to mitigate risks to the safety of the crew, which is only a subset of the failures that can occur in a human-rated launch vehicle. The different kinds of hazards to the crew (whether on the ground or on-board the MPCV) that can occur, and the probability with which these occur, must therefore be estimated.

The LOC Benefit value for an abort trigger in a launch vehicle, and also similar “benefit” calculations that can be performed for other systems for reliability, availability, or safety, is only useful in a comparative sense. For human-rated launch vehicles, abort triggers are useful only in situations in which the required orbit or mission success cannot be achieved and an abort will be required now or in the future. For the sake of argument, assume that the probability of achieving orbit is 90%, which equates to a LOM probability of 10%. If no abort action occurs, these LOM cases will result in Loss of Crew. Further, assume that the LOC requirement is set at 1% per mission. This means that the abort triggers and abort responses must reduce the LOC from 10% down to 1% or below. The difference between these values is the required amount of LOC Benefit that must be provided. Abort triggers are worthwhile only if they provide “significant” value in driving LOC down to the required level.

To these dependability-centered metrics one can also estimate other costs, such as the actual monetary and schedule costs. These non-dependability costs are not addressed in this paper, but of course are important for this and all other applications. However, these can be estimated in standard ways that do not require further elaboration here.

## III. SLS Abort Trigger Analysis Methodology

This section describes the analysis process used to assess the value of abort triggers on SLS for the program’s Preliminary Design Review (PDR) and one post-PDR cycle of analysis.

### A. *Abort Trigger Analysis Overview*

The SLS Abort Trigger Analysis can be generalized into the following seven major steps.

- Step One. Identify abort triggers to be assessed and insert into the Abort Analysis Matrix (AAM) spreadsheet.
- Step Two. Obtain the list of LOM scenarios, which is a combination of the mission phase, failure scenario, and LOM Environment (LOME), modeled by the PRA group.

- Step Three. For each LOM scenario, examine the associated PRA minimum cut sets to determine which abort triggers can detect the failure effects modeled in this LOM scenario as primary or secondary detections.
- Step Four. For each LOM scenario and trigger identified in Step Three, estimate the percent coverage of the LOM risk for each abort trigger based on associated minimum cut sets, and the corresponding minimum, mode and maximum Abortability Table Warning Time (ATWT) estimates.
- Step Five. Based on the LOM scenario's contributing failure scenario and LOME, identify which abortability table or tables to be used for the abort effectiveness (AE) value lookup, or specify manual AE inputs.
- Step Six. Execute AE lookup Front End Excel Visual Basic for Application (VBA) Macro to populate AE into the AAM.
- Step Seven. Format output results for PRA use.

### B. *Loss of Mission Scenario Identification*

For abort trigger analysis, the only failures that are relevant are those that threaten the MPCV and crew. As described above, whether these are immediate threats due to a vehicle that is breaking up or losing control, or whether the vehicle is stable but cannot boost the MPCV into the required orbit, the mission is lost. Therefore the failure scenarios that require aborts are always Loss of Mission scenarios. Determining the effectiveness and value of abort triggers requires estimation of the effectiveness of these triggers in all LOM scenarios. This in turn implies that all LOM scenarios must be identified.

In general, failure scenarios describe unique failure behaviors, with a unique set of failure responses, with a specific system configuration over a specified time period. In the SLS abort trigger analysis, LOM scenarios specify a unique set of failure behaviors with a specific system configuration over a specified time period. However, in these LOM scenarios, more than one abort trigger could be activated first. Since only one abort trigger can send an abort recommendation for an abort response to occur, it only matters which abort trigger detects the abort condition first and issues the abort recommendation (or for non-immediate aborts, the warning message). If the first abort trigger that could potentially detect the abort condition fails to do so, it is usually true that another abort trigger will detect a later, "downstream" failure effect, which is also necessarily an abort condition. The analysis methodology maps all abort triggers that can potentially detect the failure behaviors in a LOM scenario, so LOM scenarios themselves don't need to define all possible abort triggers that can be activated. It only needs to define the behaviors themselves, and then the abort triggers are mapped into the LOM scenario. In an actual operational event, only one of these abort triggers will be the one that activates first, and this defines an "abort scenario." Thus within a LOM scenario there are several possible abort scenarios, depending on which abort trigger detects the abort condition first.

As described in the previous major section, the Goal-Function Tree provides a method to identify potential abort triggers and understand their relationships to each other. The reason that the GFT aids this understanding is that every path in the GFT represents not only a set of needed goals and functions, but also the failure behaviors that will occur in a specific failure scenario when a goal cannot be achieved. Therefore the GFT can be used as a starting point to define failure scenarios for a given system [2]. Those failure scenarios that lead to direct threats to the crew or to inability to achieve orbit are the ones that must be identified.

For SLS, LOM scenarios were defined in an iterative process that started on the NASA Constellation program and Ares I project going back to 2005. This process involved several groups, including Mission and Fault Management (M&FM), Safety and Mission Assurance (S&MA) PRA, Guidance, Navigation and Control (GN&C), and Structures and Environments (STE). It took several years to work through several iterations of understanding about how to define failure scenarios, what level of detail is needed, and what the criteria were. When the Ares I Project and Constellation Program were cancelled in 2010, the transition to what became the SLS program enabled another reassessment of the criteria and modeling of failure scenarios needed to perform abort trigger analysis, leading to the criteria defined here. In sum, this was a multi-year, multi-organization iterative process, leading ultimately to the proper set of criteria that enabled the quantitative analysis described here.

We now know that we can use the GFT representation and analyses, as well as the PRA and Hazard cause tree models to help define the needed LOM scenarios, and with the experience of having done the abort trigger analyses, the proper level is now understood. Preferably, the LOM scenarios must be defined to the level necessary to map the abort triggers into the unique set of failure effects over relevant ascent time periods. These time periods include not just unique vehicle configurations, but also differing external environments at different altitudes, velocities, and pressures.

### C. *Loss of Mission Scenario Probability Estimation*

Once a set of LOM scenarios are identified and agreed to by the SLS abort analysis team, the S&MA PRA group quantifies the model based upon NASA PRA Procedures Guide for NASA Managers and Practitioners [4] and NASA Cross-Program PRA and SLS PRA Plans, and best industry practices. A PRA model is a logic model that represents a failure scenario or failure outcome for a system. For SLS, fault trees are being developed by the SLS S&MA PRA group to assess SLS LOM scenarios. The PRA fault tree is an integrated risk model representing the SLS LOM probability during flight by modeling system and component failure modes and dependencies from a LOM failure scenario's point of view. Once the fault tree models are completed, the models are populated with failure data in order to quantify the risks.

PRA uses various fault tree basic events quantification techniques depending on the failure mode, design maturity, and availability of data. Without going into specifics, typical SLS PRA data are grouped into the following general cases: functional failure, common cause failure, phenomenological failure, external causes, and process or manufacturing errors. Detailed descriptions for the various NASA PRA data classes can be found in NASA Procedures Guide for NASA Managers and Practitioners [4]. Although SLS is still in the design phase, the majority of the hardware used is Shuttle heritage or derived, or commercial off the shelf, where significant amount of reliability data exists. In situations where flight and test data is not available, reliability prediction values from similarity analysis, similar components, handbook data, and/or domain expert judgments are used to initially estimate the risks. The results from the SLS PRA model are in the form of fault tree minimum cut sets.

A cut set can be interpreted as a "failure scenario" that consists of a single failure or combination of failures that are assumed to result in a LOM. A cut set is said to be minimum if it cannot be Boolean-reduced further. Automatically generated by the PRA software, each minimum cut set includes a description of the event or events involved with the corresponding probabilities for a specific mission time. By default, the probability estimates represent the mean failure probability for each minimum cut set.

The LOM minimum cut sets and their associated probabilities are used in the AAM to understand the specific failure causations for a given LOM scenario, which is composed of the combination of mission phase, failure scenario and LOME. If the basic events' probability estimates contain uncertainty, then a Monte Carlo simulation can be used to estimate uncertainty around the mean likelihood estimates. The uncertainty analysis provides another crucial piece of information to allow for risk-informed decision making by understanding the probability intervals or "probabilistic estimate variability" for each failure scenario or effectiveness of specific design changes, such as hardware redundancy, FM protocols and abort triggers [3]. Further, because uncertainty analysis is required for NASA Cross-Program PRA (the PRA organization and model including SLS, MPCV, Ground Systems, and Mission Operations) [6], the SLS AE estimates generated by SLS M&FM group contain uncertainties, which will be described later. Currently, the AE uncertainty is only applied to the mean estimates of the LOM scenarios provided by the PRA group. For SLS Critical Design Review, integration of the AE and LOM scenario uncertainties will be implemented to better understand and communicate the uncertainty for the AE and LOC benefit estimates.

### *D. Failure Detection and Confirmation – False Positives and False Negatives*

Abort triggers are failure detection mechanisms, and as described in section II.C above, they are assessed using False Positive (FP) / False Negative (FN) / True Positive (TP) / True Negative (TN) metrics. A desirable abort trigger has low FP and low FN rates, and conversely high TP and high TN rates. FP and FN are logical complements to TP and TN, and on SLS the calculations are performed for FP/FN.

For SLS, abort triggers are generally designed to use redundant measurements so as to minimize the possibility that a failure in the measurements from one string of hardware will not lead to an abort based on a sensor or measurement failure. That is, redundant measurements are used to reduce the false positive rate. The way this is phrased on SLS is that there is a "detection" and a "confirmation". This means that an abort trigger requires two measurements that indicate an abort condition exists.

Calculation of FP/FN for a given abort trigger requires the application of reliability theory for redundant suites of hardware components and for common mode failures, and the physics-based assessment of threshold values for triggers that monitor continuous state variables. Failure of components that are involved with a given abort trigger, which include sensors, data buses, computers, and software algorithms are assessed in the usual way according to classical reliability theory, with two significant additions. First, the calculation needs to estimate the probability that component failures lead to an FP or FN, and incorporate them into the modified traditional reliability equations. Second, which is an issue of particular relevance for abort triggers, is the need to model and assess the effectiveness of "sensor data qualification" (SDQ). SDQ determines whether the information being used by the decision algorithm is valid, and hence it inherently reduces the possibility of false positives and false negatives. Because SDQ exists to reduce FPs and FNs, the effectiveness of the SDQ must itself be modeled. In other words, it is insufficient to build a typical, simple reliability block diagram. The models used to estimate the effectiveness of abort triggers must include detailed models of SDQ, to determine if the SDQ routines are providing sufficient value to be worthwhile to develop. Finally, the FP/FN calculation must also assess the common cause failure rates, as it typically happens that when the reliability of redundant strings of components is assessed, the dominant factor will be the common cause failure rates of hardware and software (or of humans, if part of the trigger design).

The other major factor in the calculation of the FP/FN of abort triggers is the assessment and determination of where to set the threshold values that distinguish the difference between nominal and failed behavior. For measurements of binary state variables, such as whether a bit is set to a 1 or 0, threshold values do not matter. However, for continuous variables such as pressure, temperature, position, or attitude (angular direction), it is essential to specify a threshold that differentiates between nominal and failed behavior. In general, there is no single threshold value that inherently distinguishes nominal from failed behavior. Rather, there is often a range of values that can occur when the system is in a nominal or failed state. Within this range, setting the threshold to guarantee detection of the failure (having a near 0% false negative rate) will be susceptible to a high false positive rate, in which the detection indicates that a failure exists, when in fact there is no failure. Conversely, trying to minimize the false positive rate will generally increase the false negative rate.

In cases where the overlap between nominal and failure behaviors overlaps a great deal, that is, when small changes to FP create large changes to FN or vice versa, then it may be advisable to not use that state variable for failure detection purposes, and conversely to monitor some other state variable instead. In this case, the other state variable to be monitored may have larger separation between nominal and failed behaviors. Or it may be that the original state variable can be monitored, but additional state variables must also be monitored to provide more information to distinguish nominal from failed behaviors.

In any event, determining where to set the threshold is a system-specific decision. Where failure cannot be tolerated, but false positive rates are acceptable, then the threshold can be set to provide a near guarantee that the failure will be detected, but at the cost of potentially higher false positive rates. Or the system may be biased to minimize false positives, in which case there will be a greater chance that a failure will occur that will not be detected.

It should also be noted that changing the threshold values does not determine simply whether failure is detected or not, but rather is often a case of when the failure is detected. It is often true that a failure causes an ever-increasing or decreasing value of the state variable, which will diverge further from nominal behavior over time. Thus biasing the threshold to reduce false positive rates often has the effect of delaying when the detection occurs, as opposed to reducing the probability of detection as a whole. If there is sufficient time for the system to recover from the failure, or in the case of the SLS, for the crew to escape the threat, then it may be possible to set the threshold to reduce false positives, yet still provide a reasonable amount of time for the crew to escape.

For the case of a human-rated launch vehicle, it is not inherently obvious which bias should be used. On one hand, setting the threshold to protect human life is crucial to provide astronauts a means to escape a current or impending threat to their safety. On the other hand, for a heavy-lift, deep space-capable vehicle such as SLS that will cost perhaps up to a billion dollars per flight, aborting a mission that could have succeeded is a tremendously expensive decision that could even jeopardize the program. To date, astronauts have accepted the high risks of space flight, and so the philosophy for setting abort trigger thresholds is not biased towards crew safety so as to create a large risk of false positives and unnecessary aborts. The discussion about the appropriate balance remains an ongoing debate, but it is clear that having a high false positive rate is not acceptable, just as having high risks to the crew is also unacceptable. The relative impact of changing threshold values on crew escape times is a large factor in the threshold design.

### *E. Crew Survivability - Explosion Dynamics*

When a launch vehicle's energetic system, such as solid rocket motors or liquid propellant engines experience an uncontained failure, the failure effects can propagate to the surrounding system and lead to potential detonation of the core stage. This explosion is the primary source of hazards to crew survivability during an abort by generating blast overpressure wave, fireball, and debris/fragmentation field toward the escaping crew module [5].

The severity of these hazards on the crew module depends on several variables that must be accounted for in the abort analysis. These variables are: nature and severity of the launch vehicle failure; failure propagation from element failure to vehicle explosion; vehicle and launch abort vehicle trajectories; design of the crew capsule and launch escape system (such as structural strength); propagation of the explosion dynamics to the crew capsule; abort warning time provided by the launch vehicle abort trigger; and attitude of the crew capsule when the hazards reach it [5]. To ensure consistency and traceability in the SLS and MPCV abort analyses, the design capability of the crew module to withstand aforementioned crew threatening explosion hazards are described in a set of MPCV abort environments table limits that are also being used as design requirements for SLS to meet either by design or analysis.

SLS STE group is responsible for modeling interactions of SLS element explosion dynamics, starting from characterizing the potential impact of the initial failure manifestation or LOME, and their abort environments against MPCV launch abort vehicle and its vulnerabilities. This entails the analysis of the likelihood that a failure producing a given LOME will propagate to other elements and ultimately to vehicle explosion, and the impact on the MPCV structure. The list of LOMEs is generated through discussions with SLS PRA and M&FM personnel with the objective of providing complete coverage of possible failure outcomes at a level of refinement sufficient to enable the identification of leading crew risks and effective mitigation strategies. The LOMEs include Core Stage (CS) engine explosion, booster burst, pad explosion, CS external explosion, and CS intertank internal explosion.

STE develops abortability tables as functions of mission phase and available warning time by integrating the effects of failure propagation with characterizations of the environment severity. The environment severity is developed by integrating characterizations of the failure environment initiation and propagation with MPCV abort trajectories and vulnerabilities. Results are time-averaged across mission phases, with results for each phase provided as functions of warning time in rows that are identified by the Mission Event Time at the midpoint of the associated mission phase. For SLS PDR, twelve abortability tables were generated. Each abortability table is contained within a separate Excel workbook, and each workbook contains three worksheets labeled Best, Worst, and Base representing the three types of modeling and failure propagation assumptions. Best case assumptions typically show higher levels of abortability resulting from the use of more optimistic assumptions regarding propagation and the application of more benign explosion environments. The lowest levels of abortability, typically shown in the Worst sheet, result from pessimistic assumptions regarding both propagation and environment severity. The abortability values in the Base sheet result from most likely estimates of propagation and environments, with some remaining conservative bias.

For use with SLS PRA, each AE "estimate" is composed of three values: worst, base and best assumptions, and for explosion cases these are extracted from the STE abortability tables based on the ATWT estimated by M&FM for each LOM scenario based on a worst-on-worst, base-on-base and best-on-best type of bounding analysis. That is, the worst AE is based on the shortest abort warning time with the worst case abortability table. Best AE corresponds to longest abort warning time with best case abortability table, and Base AE corresponds to median abort warning time.

### F. *Crew Survivability - Loss of Control*

Another typical kind of threat to the crew is when the SLS vehicle is unable to maintain control. In general this means that its attitudes (the direction that it is pointed) and attitude rates (the rate of change of pointing direction) diverge from nominal such that the vehicle will not achieve orbit, or threaten SLS or MPCV structural load limits, hence causing a "structural demise." Assessing the SLS vehicle's ability to control the vehicle's attitudes and rates, and the guidance to achieve orbit is the job of the SLS Guidance, Navigation, and Control (GN&C) group. This group performs typical launch vehicle GN&C analyses using physics-based Monte Carlo simulations and stability analyses. For the SLS, it also performs analyses of the GN&C subsystem's ability to detect failures to control through detecting diverging attitude errors and rate errors.

For SLS abort trigger analysis, GN&C uses the same kinds of physics-based, Monte Carlo methods as it uses for typical "nominal" guidance and control analyses. These methods are supplemented by modeling hypothetical abort triggers that monitor attitude and rate errors and other GN&C state variables as appropriate, with corresponding hypothetical thresholds. As described in Section D above, the threshold values are set based on assumed requirements for False Positive and False Negative rates, and analyzed against a variety of failures whose effects manifest themselves in GN&C state variables. Since these thresholds are set based on the needed FP and FN rates, and against SLS and MPCV structural limits and orbital performance metrics, the GN&C abort triggers are generally effective in detecting failures that manifest themselves through attitude and rate errors before a structural demise and explosion occurs. Abort responses are usually able to enable the MPCV to escape the resulting explosion, at least when the Launch Abort System is available.

Additionally, GN&C abort triggers provide a secondary benefit of detecting some situations in which the vehicle structure has collapsed or when an explosion has occurred. While not designed specifically to address these cases, if the SLS CS Flight Computers remain active and are not yet destroyed by an explosion, the GN&C abort triggers can detect that an explosion has occurred, causing the vehicle to lose control. In these cases the GN&C abort triggers do not provide much warning time, because the explosion is already occurring before the crew will be able to activate an abort response.

### G. *Crew Survivability – Benign Scenarios*

When a failure occurs that does not result in an immediate launch vehicle explosion or loss control, and the launch vehicle continues a stable, controllable flight, the LOM scenario is said to be benign. One example of a benign LOM scenario is an abort resulting from a false positive detection from an abort trigger. In this case, the MPCV aborts off a perfectly fine launch vehicle that is flying in a nominal trajectory. Another benign LOM scenario is the shutdown of a single CS engine , or "single engine out" that requires an abort at some point later in the flight. For SLS PDR, it was assumed that for benign LOM scenarios, the AE value, as confirmed by SLS STE group's abort dynamics analysis, is assumed to be 100% off the SLS vehicle. That is, there are no threats from SLS that will impede crew capsule abort.

Even if the SLS poses no threat in benign scenarios, this does not mean that the abort has no risks at all. There are always risks due to MPCV/crew capsule failures such as the Launch Abort System (LAS) not firing or a failure to deploy parachutes. These risks are captured in the Cross-Program PRA where successful crew capsule abort off SLS are linked to appropriate MPCV abort models that include both failure of the MPCV abort system and physical abort environment.

### H. *Abort Analysis Matrix*

The Abort Analysis Matrix (AAM) is an Excel spreadsheet that implements the M&FM group's model of SLS abort trigger effectiveness. It uses the LOM scenarios provided by PRA group and their associated probabilities, delineated by vehicle mission phase. In the AAM's M&FM Input sheet/tab, each row represents a LOM scenario, that is, a specific combination of the FS, LOME and mission phase. AAM columns represent candidate abort triggers to be assessed. This format allows for all candidate abort triggers to be assessed for their value in each LOM scenario.

Each abort trigger entry in the AAM consists of five sub headers. The first sub header consists of four columns that define the performance characteristics of the trigger when activated in a given LOM scenario. They are:

- Trigger Detection Class: Indicates if the trigger will be the first one to detect the failure behaviors in the LOM scenario (i.e. Primary) or if the trigger will detect the failure behaviors only after a primary trigger fails to detect the scenario failure behaviors (i.e. Secondary)
- False Negative: A percentage of the time that the trigger will not detect the failure behavior in the LOM scenario.
    - For Primary triggers, any FN probability will be potentially detected by a Secondary trigger, or if there is no Secondary trigger, it is assumed that the remaining probability will lead to LOC.
    - For Secondary triggers, it is assumed that any FN probability will lead to LOC. Any possible Tertiary triggers are ignored as having extremely low probability.
- Trigger Probabilistic Split: A percentage that indicates the portion of the LOM scenario probability that can be picked up or monitored by this specific trigger relative to other abort triggers in its trigger detection class. That is, the trigger probability splits for a primary trigger are associated only with other primary triggers, and secondary triggers only with other secondary triggers. As an example, if two triggers A and B are primary, and C is secondary, then a 60/40 split of A to B means that 60% of the given LOM scenario probability will be detected first by A, and 40% by B. Only false negative probabilities of A and B are potentially detected by C, which captures 100% of the FN probabilities of A and B.

- ATWT Uncertainty Distribution Type: Uncertainty distribution associated with estimated ATWT inputted. This is used to determine the mean of ATWT from the inputted Min, Mode and Max values, and for future Monte Carlo simulation.

The remaining four sub headers delineate probabilistic distribution attributes associated with the trigger. Each sub header, titled Minimum (Worst Case), Mode (Most Probable Case), Maximum (Best Case), and Mean (Average Case), have two columns, ATWT and AE.

With the format of the matrix defined, with the LOM scenario data as rows in the matrix and the abort triggers and their associated parameters as columns, the process of filling in the matrix can begin. The first step is to analyze each LOM scenario to determine which of the triggers will detect it first. If a trigger can directly detect the results of a LOM scenario then it is set as a Primary trigger by placing an “X” in the field that matches up with that trigger’s *Trigger Detection Class* field and the LOM scenario that is being analyzed. If multiple triggers can act as Primaries, then it is necessary to allocate a certain percentage of the specific LOM scenario probability to each of them. This allocation is based on an M&FM assessment of the failure causes modeled in the specific LOM scenario to determine what fraction of the resulting effects could be picked up by the trigger. In the current structure of the AAM, it is not possible for a primary trigger to act as secondary. It was discovered later in the analysis that there are some cases where a trigger could potentially be a primary or a secondary. This issue is dealt with through approximations now, but may be fixed in future versions of the AAM. The sum of the primary and secondary trigger split fractions for each LOM scenario will be 100%.

The AAM calculation sheet is set up in similar manner as the M&FM Input sheet. It consists of a matrix that has the LOM scenarios and associated data as rows and the abort triggers and associated data as columns. The calculation sheet reads in data from the M&FM Input sheet. Each trigger has a set of calculations that it performs for each LOME scenario; they are as follows:

- True Positive LOM: Portion of LOM scenario probability that is successfully detected by a given trigger.
- False Negative LOC: Portion of LOM scenario probability that is not detected by either primary or secondary triggers, resulting in LOC.
- AE LOC Residual: Probability associated with failure to abort successfully even if a trigger properly detects the failure behavior in the LOM scenario.
- LOC Benefit: Probability that a given abort trigger saves the crew from immediate launch vehicle failure given that it detected the failure behavior

From the definitions above, True Positive LOM (TP LOM) probability of primary trigger ($LOM_{TP_x}$) is related to the primary triggers’ probabilistic splits ($Split_{\%_x}$) of the remaining LOM scenario probability that are not subject to primary trigger FN ($FN_{\%_x}$), see (1).

$$LOM_{TP_x} = Split_{\%_x} \times LOM_{T_x} \times \left(1 - FN_{\%_x}\right) \qquad (1)$$

Accounting for AE associated with the specific LOM scenario and primary trigger, the LOC Benefit of the primary trigger is simply the product of the AE and TP LOM primary trigger calculated from (1), see (2),

$$LOC_{B_x} = AE_{\%_x} \times LOM_{TP_x} \qquad (2)$$

Because secondary triggers only operate on FN of primary triggers, the calculation of TP LOM of secondary triggers ($LOM_{TP_y}$) is similar from that of ($LOM_{TP_x}$) but with total FN LOC from primary triggers and against the remaining LOM scenario probability that are not subject to secondary trigger FN ($FN_{\%_y}$), see (3).

$$LOM_{TP_y} = Split_{\%_y} \times \left(1 - FN_{\%_y}\right) \times FN_{LOC_{x-Total}} \qquad (3)$$

where

$$FN_{LOC_{x_i}} = LOM_{TP_{x_i}} \times \frac{FN_{\%_{x_i}}}{\left(1 - FN_{\%_{x_i}}\right)}$$

$$FN_{LOC_{x-Total}} = \sum_{i=1}^{N} FN_{LOC_{x_i}}$$

$$FN_{LOC_{x-Total}} = \sum_{i=1}^{N} LOM_{TP_{x_i}} \times \frac{FN_{\%_{x_i}}}{\left(1 - FN_{\%_{x_i}}\right)} \qquad (5)$$

The LOC Benefit of secondary trigger ($LOM_{TP_y}$) is calculated similarly to that of the LOC Benefit of a primary trigger; it is based on the AE associated with the specific LOM scenario and secondary trigger, and TP LOM of the secondary trigger, see (6).

$$LOC_{B_y} = AE_{\%_y} \times LOM_{TP_y} \qquad (6)$$

With all of the calculations completed, the sum of the TP LOM and LOC Benefit for each of the triggers are taken and compared in a separate worksheet. Because a distribution of ATWT in turn determines the uncertainty distribution of AE, the overall trigger LOC Benefit can be assessed as a distribution or a “range of values”. This allows for initial estimates of the uncertainty spread of the variability without performing detailed Monte Carlo simulations to gauge the worst-on-worst vs. best-on-best vs. “Most Probable” vs. average benefit that each of the triggers provides within the analyzed trigger suite.

The process described above is used for any particular trigger sets of interest. If one desires to assess the benefit of adding or removing additional trigger or triggers, one would simply modify the trigger set’s columns, and repeat the process. This is necessary because of the intricacies of assigning primary and secondary triggers and trigger splits to each of the Trigger vs. LOM scenario locations on the spreadsheet. The addition or removal of triggers often alters the trigger split fractions. By repeating the analysis with a single additional candidate trigger a comparison can be made between sets of triggers. This gives a Delta LOC Benefit between one set of triggers and another set of triggers.

### I. *Abortabilty Tables Lookup Script*

To automate the AE lookup from the abortability tables, a set of Excel VBA macros were written. There have been several enhancements made to the AE lookup macros since its first revision to increase its speed, capability and simplicity. Housed within a separate Excel file called the Front End, the Front End file contains key information regarding the file names of the AAM and STE abortability tables, and user friendly features. The use of custom combinations of abortability tables, booster FTS delay time and LOM scenarios subjected to booster free flyers are embedded in the specific revision of the AAM to allow a unique AAM file to be adapted for specific analysis case.

The VBA macro performs the following actions upon execution.

1. Open AAM and all abortability tables Excel files
2. Step through each LOM scenario row in the AAM, checking for missing ATWTs for applicable abort triggers
3. Step through each LOM scenario row and read in identified mission phase and abortability table type used
4. For each LOM scenario row, step through all abort triggers, and perform lookup of the AE from the abortability table, based on ATWT, mission phase and abortability table ID, fill the relevant AAM cell with the AE result
5. Save the AAM and duplicate the results, and repeat Step 3 and 4 to account for booster free flyer risk if the user chooses.
6. Prompt the user that the macro has ended, and close appropriate data files.

For inputs into the PRA software, the resulting AE for each LOM scenario is reviewed and formatted as a triangular distribution. A triangular distribution was used based on a recommendation by STE based on the understanding of the physics of failure, and modeling and propagation assumptions used. The mode of the triangular distribution is set to the base AE, and the lower and upper bound are set to the worst and best AEs.

## IV. Application of Methodology

This section describes how the analysis methods described in the previous section are applied to specific SLS abort trigger-related problems.

### A. *LOC Benefit of Abort Trigger Suite*

The most important analysis that is performed using the methods described in section 3 is the selection of the abort trigger suite for the SLS vehicle. As described previously, the primary metric of value of an abort trigger is the benefit it provides for the crew to escape safety-threatening, SLS-caused hazards. If the crew successfully escapes, a potential Loss of Crew situation becomes merely a Loss of Mission, and the amount of LOC that is avoided by the existence of an abort trigger is the value of that abort trigger, its LOC Benefit value.

The SLS vehicle will use several abort triggers, which are collectively known as the abort trigger suite. To analyze the value of the suite as a collective, the suite of triggers are added to the Abort Analysis Matrix, and evaluated as described in the previous section. This analysis assigns the entire amount of LOC Benefit to an abort trigger in a failure scenario if it is the trigger that activates first. When performed in this way, the analysis of the entire suite of triggers provides an accurate assessment of the value of the entire abort trigger suite as a whole. However, the individual LOC Benefit values for each trigger might be considered somewhat misleading, as will be described in the next section. Nonetheless, this is the simplest method of LOC Benefit evaluation, and it definitely provides a clear-cut method to estimate the value of each abort trigger, with the clearest and simplest interpretation.

### B. *Delta LOC Benefit of Added Abort Trigger*

While the LOC Benefit calculation method described above in Section IV.A provides the simplest calculation and clearest interpretation of results, it is in some ways misleading. This is because the benefit of an abort trigger should ideally be measured as the change in LOC Benefit that is provided by adding this trigger to the previously existing set of triggers. This is the “Delta LOC Benefit” method. The major difficulty with this method is that the value of any single trigger depends on the value of all the previously selected triggers, and this in turn means that the order in which triggers are selected generates a different Delta LOC Benefit value for any added trigger!

Let us assume for the sake of argument that the SLS vehicle is designed initially without any abort triggers, which means that any detection of failures would occur by detection of hazards from the MPCV or Mission Operations, or when on the ground, from ground systems. These detections and resulting abort responses will provide some finite amount of LOC Benefit, which can be calculated in the manner described in Section III. To determine which abort triggers on the SLS will provide maximum improvement to LOC, one could ideally assess all possible abort triggers one by one to determine the added LOC Benefit they provide compared to the off-vehicle set of triggers. Based on this comparison, one can then select the trigger with the maximum LOC Benefit, as long as its monetary and schedule costs are low, and as long as its projected False Positive rate is low enough.

Once added, this new trigger is added to the existing suite of off-board triggers, yielding a trigger suite consisting of the off-board set plus one on-board trigger. This new suite can be assessed as a group to determine its collective LOC Benefit. The analyst can then once again assess all remaining potential triggers and calculate their Delta LOC Benefits. Again, one can select the next-best trigger, add it to the suite, assess as a group, and repeat the process. This process continues until the Delta LOC Benefits of the remaining potential triggers are all so low as to be not worthwhile to add to the suite. Because every abort trigger has a cost in additional Losses of Mission due to False Positives, once the Delta LOC Benefit of potential triggers begins to approach the probability value of the Delta LOM Cost due to the false positives of adding that trigger, it is no longer worthwhile to add the new trigger. For launch vehicle aborts, every Loss of Mission also produces a small additional Loss of Crew, because there are risks associated with every abort. Thus the added costs are the added LOM and LOC values due to the False Positive rate of the added trigger.

While the sort of analysis described below can in theory be performed, for the SLS vehicle this was not done, due to the relative complexity of the method, and also due to schedule and resource constraints to perform the work and yet meet program schedules and deliveries. However, with the right kind of tool (which does not yet exist), this Delta LOC analysis process could be automated and done cost-effectively in the future.

### *C. Free-Flying Booster Risk*

Booster free-flying (BFF) risk addresses the risk to the escaping crew module due to a breakaway, or rogue booster. Currently, there is a breakwire between the booster and the core stage to address public safety concern of a runaway solid booster. The breakwire, which is tied to the booster's Flight Termination System (FTS), is activated if it is severed when the booster becomes detached. The breakaway booster scenario can occur either due to failure of the booster to core stage attachment points during nominal flight, during a vehicle failure, such as vehicle explosion or loss of control, or after initiation of an abort. Depending on when the booster breaks away from the core stage, the average LAS acceleration and head start time, and FTS delay time, there is a chance that the booster can catch up or overtake the escaping MPCV and detonate. The FTS detonation releases booster fragments on the crew module if the booster is next to the MPCV at the time of detonation. If the booster is in front of the MPCV at the time of detonation, then the MPCV will fly into the resulting debris field. If the booster is behind the aborting MPCV at the time of detonation, then the distance and relative velocity between the two must be taken into account in the calculation of the likelihood of debris strikes on MPCV.

The time at which the booster breaks away is important, as the acceleration, velocity, and resulting position of the booster relative to the MPCV depends on the atmospheric density and the booster propellant mass fraction. For a heavier booster in low altitude, the booster has more mass to carry, reducing its acceleration and therefore reducing its ability to catch up to the MPCV, as compared to a booster breakaway higher up in the atmosphere, with less friction and less mass, and thus higher booster acceleration. For the initial assessment, a simple one-dimensional trajectory of the MPCV and rogue booster was used, and it is assumed that booster breaks away when the launch vehicle explodes. The time at which the launch vehicle explodes is also a primary factor in the calculation of the ATWTs and abortability tables, and thus using the assumption that the booster breaks away at the same time as a launch vehicle explosion occurs made the determination of the LAS head start time very easy.

For the actual AE assessment, the aforementioned Excel VBA macro is used and BFF risk is assessed in Step 5 of the aforementioned *Abortabilty Tables Lookup Script* steps. This risk is added to the risks described above for benign, loss of control, and explosion failures. If the MPCV does not survive the initial SLS failure, then LOC already exists and any additional BFF risk does not matter. If the MPCV survives the SLS failure, then the BFF risk is applied. The BFF risk is also applied to all applicable LOM scenarios, such as premature booster separation or vehicle explosion. To account for the variability in the FTS activation delay, which for a generic FTS can be up to +/- 1 sec, a bounding assessment similar to the worst ATWT on worst abortability assumptions is used. This results in worst-on-worst-on-worst or best-on-best-on-best bounding cases. That is, the worst (shortest) FTS delay time AE is operated on the worst ATWT and worst abortability table. The final AE for a particular LOM scenario *i* and trigger *j* is shown in (6):

$$\mathrm{AE}_{\mathrm{LOM\ Scenario}_{\mathrm{i,BFF}}} = AE_{LOM\ Scenario_{i,j,PreBFF}} \times AE_{BFF|MET,ATWT,FTS\ Delay} \tag{6}$$

### *D. Limitations & Caveats*

The biggest technical limitation and caveat to the sort of analysis described in this paper is the size of the uncertainties involved with these calculations. Each group performed their own calculations with their own uncertainties and assumptions, which are part of the overall abort trigger analysis process. Some of these have rather large uncertainties themselves, such as the probability of LOM calculations within S&MA PRA, the STE blast calculations, and the M&FM estimates of warning times. These uncertainties all have to be combined to yield something that has meaning when aggregated. In general, the group aimed for 5%, mode, mean, and 95% values. In practice, it is difficult to know how close the "best case" and "worst case" or "mode" values are to the ideal of 5%, mode, and 95% without performing full Monte Carlo simulations. At the "bottom" of the calculations are always engineering judgments being made by the relevant engineers and analysts, which must be vetted with other experts to ensure that they are reasonable.

The analysis described here also requires significant resources. For a human-rated launch vehicle, with existing groups that perform related work that is already required for NASA systems, the resources were available. It was helpful that many of the groups already performed analyses that generated data similar to what was ultimately needed to perform the abort trigger effectiveness calculations and related LOC Benefit. Thus S&MA already performed PRAs that mainly needed to provide a bit more detail for some failure scenarios than they would otherwise have done. GN&C analyses of abort triggers did not require any new tools beyond those used for nominal analyses, though it did require using these tools in somewhat different ways than before. STE already performed blast overpressure, debris and fireball analyses, and mainly needed to structure those analyses in a way that enabled inputs of warning times from the M&FM group to provide appropriate outputs of crew survivability in differing conditions. The M&FM group, which is historically new within NASA MSFC, required the most "new" work, for the simple reason that the quantitative analysis of abort triggers had never been done before. This entailed development of the methodology and the Abort Analysis Matrix tool to mechanize the process, and also the establishment of new relationships to the other groups to enable this analysis to be performed. For other systems such as robotic spacecraft, these resources may not be available, and so the detailed process here would need to be simplified to enable it to occur. In the long run, SHM/FM analyses of the sort described here should become a standard feature of an SHM/FM tool suite, making it cost effective for most projects.

Lastly, the analyses we have performed to date uncovered or made clear a number of issues that will need to be resolved in the future. One is the differentiation of crew survivability due to an effective abort, versus crew survivability simply due to an explosion being small or with debris by luck not hitting the MPCV. This is related to the over-simplified assumption that LOC occurs if a secondary abort trigger fails to detect an abort condition. The current method of attributing LOC Benefit to the first abort trigger that detects an abort condition in a LOM scenario needs further refinement. In other words, the more accurate method of calculating LOC Benefit is the "Delta LOC" methodology described previously, but this supposedly more accurate method does not seem to provide a single absolute number for LOC Benefit, since it depends on the order of selection of previous abort triggers. Finally, issues such as the rogue booster described in IV.C above should be directly integrated into the analysis through improved abortability tables, as opposed to being addressed with a post-processing macro as has been performed to date.

## V. Conclusion

The theory of System Health Management and of its operational subset Fault Management indicates that quantitative analysis of FM Control Loops can be performed, with metrics related to state estimation and control. This theory has been successfully applied to the selection of abort triggers for the NASA SLS vehicle to enable the crew to escape from potentially catastrophic hazards. The selection of abort triggers is now nearing completion, in which the quantitative assessment of the Loss of Crew Benefit of an abort trigger suite played a significant role in the decision process. The process is now a standard part of the overall design process in SLS, and will likely be applied to similar problems in the future at NASA MSFC. Based on the successful experience of applying SHM/FM, future improvements are envisioned to the methodology, to improve its technical accuracy and to reduce its future costs through the development of improved tools to perform these analyses.

## Acknowledgment

The work described here was performed under contracts NNM12AA41C from NASA Marshall Space Flight Center. The authors thank Michael D. Watson and Melanie Bodiford from MSFC, and John C. Day from Jet Propulsion Laboratory for helping to develop the ideas and methodology. The authors also thank our other team members, including Jim Rogers, Jesse Bales, and Mark Bigler (Johnson Space Center) from NASA PRA Group, Greg Dukeman, Ashley Hill and Dan Uckotter from SLS GN&C, Louise Strutzenberg and Scott Lawrence (Ames Research Center (ARC)) from STE, Jonathan Patterson, Joel Broome, Kevin Melcher (Glenn Research Center (GRC)), Jose Cruz (GRC), Christian Neukom (ARC) and Greg Pisanich (ARC) from M&FM. All team members are from MSFC unless otherwise stated.

## References

[1] S. B. Johnson, "The Theory of System Health Management," in System Health Management: with Aerospace Applications, S.B. Johnson, T. J. Gormley, S. S. Kessler, C. D. Mott, A. Patterson-Hine, K. M. Reichard, P. A. Scandura, Jr., Eds. Chichester, United Kingdom: John Wiley & Sons, 2011, pp. 3-26.

[2] S. B. Johnson, Goal-Function Tree Modeling for Systems Engineering and Fault Management. AIAA Infotech@Aerospace (I@A) Conference, 2013, Boston, MA. August 19-22. AIAA Paper 2013-4576.

[3] NASA Risk-Informed Decision Making Handbook (NASA/SP-2010-576)

[4] NASA Procedures Guide for NASA Managers and Practitioners, NASA-SP-2011-3421, December 2011.

[5] D.L. Mathias, S. Go, K. Gee, and S. Lawrence, Simulation Assisted Risk Assessment Applied to Launch Vehicle Conceptual Design. Annual Reliability and Maintainability Symposium, Las Vegas, NV, January 28-31, 2008.

[6] NASA Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects, NPR 8705.5A, June 7, 2010.

[7] S. Lawrence, et.al., Simulation-Assisted Risk Assessment. AIAA Aerospace Sciences Meeting and Exhibit, 2006, Reno, LA. January 9 - 12. AIAA Paper 2006-0090.