Abort Trigger False Positive and False Negative Analysis Methodology for Threshold-based Abort Detection

Kevin J. Melcher[1], José A. Cruz[2], Stephen B. Johnson[3], and Yunnhon Lo[4]

[1,2]*NASA Glenn Research Center, Cleveland, OH, 44135, U.S.A.*
kevin.j.melcher@nasa.gov
jose.a.cruz@nasa.gov

[3]*Jacobs ESSSA Group / Dependable System Technologies, LLC, Larkspur, CO, 80118, U.S.A.*
stephen.b.johnson@nasa.gov

[4]*Jacobs ESSSA Group / Ducommun Miltec, Huntsville, AL, 35806, U.S.A.*
yohon.lo@nasa.gov

Abstract

This paper describes a quantitative methodology for bounding the false positive (FP) and false negative (FN) probabilities associated with a human-rated launch vehicle abort trigger (AT) that includes sensor data qualification (SDQ). In this context, an AT is a hardware and software mechanism designed to detect the existence of a specific abort condition. Also, SDQ is an algorithmic approach used to identify sensor data suspected of being corrupt so that suspect data does not adversely affect an AT's detection capability. The FP and FN methodologies presented here were developed to support estimation of the probabilities of loss of crew and loss of mission for the Space Launch System (SLS) which is being developed by the National Aeronautics and Space Administration (NASA). The paper provides a brief overview of system health management as being an extension of control theory; and describes how ATs and the calculation of FP and FN probabilities relate to this theory. The discussion leads to a detailed presentation of the FP and FN methodology and an example showing how the FP and FN calculations are performed. This detailed presentation includes a methodology for calculating the change in FP and FN probabilities that result from including SDQ in the AT architecture. To avoid proprietary and sensitive data issues, the example incorporates a mixture of open literature and fictitious reliability data. Results presented in the paper demonstrate the effectiveness of the approach in providing quantitative estimates that bound the probability of a FP or FN abort determination.

1. Introduction

This paper describes a quantitative methodology for bounding the false positive (FP) and false negative (FN) probabilities associated with abort triggers (ATs) that include sensor data qualification and constant abort detection thresholds during a given phase of flight. The methodology was developed to support the verification of design requirements for NASA's Space Launch System (SLS).

Flight systems may have thousands of failure modes. These failure modes – typically identified via a failure modes and effects analysis (FMEA) – can be broadly classified as "hard" failures and "soft" failures. Hard failures occur rapidly and typically result in sustained large changes in the measured system states, e.g., a sensor failing to zero or to full-scale. Soft failures occur more slowly and typically result in gradual changes in the measured system states, e.g., a sensor drift that results in an intermediate value between zero and full-scale. Hard failures are fairly easy to detect while soft failures can be difficult to detect without significant FP and FN results. However, many failure modes are defined broadly enough that they are difficult to classify as either hard or soft failures. For example, a power supply failure may result in no power or reduced power depending on the exact nature of the failure.

The uncertainty associated with understanding the impact of failures on the abort detection system provides motivation for bounding the FP and FN probabilities. A Monte-Carlo simulation and physics-based model of the system are typically used to estimate FP and FN rates. However, significant time and effort are required to develop the simulation and conduct this kind of analysis. A more cost-effective and sufficiently accurate approach for SLS purposes is to use a simpler bounding estimate. In the approach proposed here, the failure rates and probabilities associated with both soft failures and broadly-defined failure modes are first classified as failure-to-intermediate value (F2IV). F2IV values are then allocated to both failure to zero (F2Z) and failure to full-scale (F2FS). The aggregate F2Z and F2FS data then become the basis for calculating bounds on the FP and FN probabilities for a given AT.

To facilitate the discussion embodied in this paper, a clear understanding of the following terms is necessary.

Abort condition (AC): The state or behavior of a launch vehicle which indicates that a threat to the crew exists and that an abort response is required to mitigate the threat. A successful abort response during ascent enables the crew to escape from a failed or failing vehicle and return safely to Earth.

Abort trigger (AT): A mechanism that is used to detect an AC. Each AT includes all of the hardware and software components required to detect a specific AC. The success or failure of an AT is ultimately measured by the probability that the crew returns safely to Earth when vehicle system failures threaten their safety.

Defined below, two key attributes of an AT's performance are the probability of a FP detection and the probability of a FN detection. Ideally, these probabilities will be zero or an acceptably low value.

False positive (FP): Occurs when, despite the fact that an AC does not exist, the associated AT indicates that it has detected the AC and sends an abort recommendation.

False negative (FN): Occurs when an AC exists and the associated AT does not detect the AC.

Sensor data qualification (SDQ): This is software that monitors the sensor data at the Flight Computer (FC). It classifies data suspected of being corrupt as disqualified. Disqualified data are not used by ATs and, consequently, do not adversely affect an AT's detection of its associated AC. SDQ is intended to reduce the probability of FPs and FNs.

Abort Condition Detection Logic (ACDL): The ACDL is part of the AT software. On each FC, it compares the consolidated value to an AC detection threshold. If the consolidated value exceeds the threshold on a given FC for a pre-specified persistence period, that FC makes an immediate abort recommendation.

Sensor data consolidation (SDC): These are algorithms that combine multiple time-synchronous measurements into a single data value that is typically used by higher-level operations and control algorithms, e.g. ADCL.

This paper assumes that the threshold values used in abort detection result from analyses not discussed in this paper. From an academic point of view, the selection of abort detection thresholds has previously been addressed by a number of authors including Vachtsevanos, Lewis, Roemer, Hess, & Wu (2006).

This paper is organized as follows. Section 2 provides a brief overview of the theory behind fault management as an extension of control theory. It describes how this theory applies to ATs and the calculation of FP and FN probabilities. In Section 3, a methodology for calculating FP and FN probabilities for threshold-based ATs is described. Section 4 presents an example showing how the FP and FN calculations are performed in practice using the methodology described in Sec. 3. Because actual SLS data cannot be disclosed for general publication, a combination of fictitious and open-literature reliability data provide the basis for this example. In Sec. 5 Discussion, observations about the methodology and modifications toward improving the approach are discussed. Concluding remarks are presented in Section 6 which gives a summary of the paper and briefly describes plans for applying the methodology to the SLS.

2. BACKGROUND

The term System Health Management (SHM) addresses activities that are described under several names, including: Prognostics and Health Management; Fault Protection; Vehicle Health Monitoring and Management; Fault Detection, Isolation, and Response; Diagnostics; Maintainability; Reliability; Availability; aspects of Safety; as well as others. SHM has historically been a relatively ad hoc set of processes and technologies focused on predicting, detecting, diagnosing, and responding to failures. The core idea that the operational aspects of SHM are related to control theory goes back 20 years (Albert, Alyea, Cooper, Johnson, & Ulrich, 1995). More recently, a unifying theory of SHM was developed and published (Johnson & Day, 2010) (Johnson & Day, 2011) (Johnson, 2011) (Day & Johnson, 2014). This theory provides a conceptual framework for the field and for its operational subset, Fault Management (FM) theory. The unifying theory is based on the idea that FM theory and practice is essentially an extension of control theory and practice.

The purpose of SHM is to provide capabilities to preserve a system's ability to function as intended. SHM 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, termed Fault Management, are implemented as control loops, known as FM control loops (FMCLs). The FMCL detects system degradation or failure, and then determines which part of the system has failed or will fail (prognosis). Here, failure implies that all or part of the system cannot be controlled within acceptable limits to achieve its objectives. Having detected or predicted a failure, FMCLs then decide what control action (response) to take. The objective being to return the system to a controllable state or take an action to prevent or mitigate the predicted failure (Johnson, 2011).

This extension to control theory is used in this paper to assess the failure detection portion of FMCLs in a human-rated launch vehicle application. In control theory, state space control loops can be separated into two major portions: state estimation and state control. Calculation of overall control loop performance is also divided into two parts, 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 (FP), false negative (FN), true positive (TP), and true negative (TN). State control success is based on the ability of the system to correctly determine the correct response action to take, and then assess the performance or effectiveness of that action. Effectiveness of the FM response typically estimated by comparing the speed of the FM response and the time available to correct for a current or impending failure. If the response completes before the failure effects compromises relevant systems goals, the response is effective; else, it is considered to be either less or not effective. This aspect of the use of ideas that extend control theory will not be pursued further in this paper.

For human-rated launch vehicles (LV), the effectiveness of the FM mechanisms called ATs are measured in terms of their ability to protect the crew, which is estimated by determining the change in loss of crew (LOC) probability that occurs if an AT or suite of ATs is implemented. Taking classical control theory concepts of state estimation and state control, the metric of this change in LOC probability, the LOC Benefit, is calculated by subdividing it into state estimation and state control elements. These are calculated separately and used to calculate the LOC Benefit numbers associated with proposed AT implementations. The LOC Benefit value provides a quantitative basis for deciding which ATs will be provided on the human-rated LV and for measuring their effectiveness in particular scenarios and across all relevant scenarios.

A human-rated LV can have many ATs with varying types of failure detection approaches. Calculation of the LOC Benefit contribution for each AT is key to an accurate accounting of the total LOC probability. The sum of the LOC Benefit of each AT across all relevant scenarios provides the LOC Benefit of the entire suite of ATs, which is the measure of their benefit to the system.

3. FP AND FN METHODOLOGY

In this section, a general methodology is briefly described for (a) quantitatively determining the performance of threshold-based ATs used to detect abort conditions and (b) estimating the improvement or degradation of that performance due to the inclusion of SDQ (Maul, Melcher, Chicatelli, & Sowers, 2006) as a component of the AT.

Quantitatively estimating the probabilities of FP and FN abort detections is crucial. High FP and FN probabilities indicate that the AT has high loss of mission (LOM) costs, or is ineffective (i.e., fails to decrease Loss of Crew probability), and, hence, should not be incorporated into the design at all.

A methodology for calculating FP and FN probabilities for threshold-based ATs is composed of the following five steps.

1. *Define the AT* – Construct a functional block diagram integrating all of the hardware and software components included in the AT architecture. The diagram is useful for understanding the data flow from each sensor to the AC Detection Logic (ACDL).
2. *Analyze the Physics of Failure* – Analyze how failures upstream of the ACDL can result in FP and FN detections. This analysis is helpful in understanding the effects of redundancy on the FP and FN probabilities of ATs.
3. *Determine Bounds on Component Failure Probabilities* – Calculate the probability of failure for each component included in the AT architecture. Here, "component" is a general term used to describe the individual functional blocks that comprise the AT architecture, which in the case of SLS is composed of both hardware and software. A list of failure modes and their probability of occurrence are required to complete Step 4.
4. *Conduct Analysis of FP and FN Probabilities for the Baseline System* – In this step, a fault tree (FT) is created to estimate the probability of a FP or FN abort detection based on the probability that known failure modes may occur. The FT is typically created using an available Probabilistic Risk Assessment (PRA) software tool which is programmed to analyze the AT failure space.
5. *Determine the Benefit Provided by SDQ* – This step is similar to Step 4, however, the analysis is focused on an AT architecture that includes the SDQ function. Resulting FP and FN abort probabilities are subtracted from those for the baseline AT calculations (step 4) to calculate the FP and FN benefit of the SDQ function.

The novelty of this methodology is as follows. First, PRA and reliability block diagrams are applied to the failure detection problem of FP and FN. Second, the benefit of SDQ is estimated as part of a failure detection process. Third, these methods are developed and applied to the failure detection portion of FMCLs within the overall theory of SHM and FM. To see an example of performance calculations for entire FMCLs for the human-rated launch vehicle application; and thus, how the FP and FN calculations fit into the overall LOC benefit calculation, see (Lo, Johnson, & Breckenridge, 2014).

In general, the calculations described in this paper are a key part of the LOC benefit analysis used to estimate the value of ATs. These calculations help to quantitatively determine whether or not SDQ algorithms are beneficial to ATs. This allows the AT design to be optimized and reduces unnecessary design complexity.

4. APPLICATION OF FP AND FN METHODOLOGY

In this section, the methodology described in Sec. 3 is applied to a generic AT designed to detect a low-pressure AC. The description is provided as a practical example of how the FP and FN methodology may be used to detect and respond to an AC resulting, for instance, from a propellant leak. To avoid data proprietary and sensitivity issues associated with the SLS, actual SLS data are not used. Instead, a mixture of open literature and fictitious data are utilized.

Human-rated flight hardware typically contains significant redundancy to protect the crew. The example is intended to illustrate that redundancy without duplicating it. Further, although the example presented here is intended to be simple for illustrative purposes, it should be fairly easy to see how the complexity of an AT in a real system can escalate.

4.1. Step 1: Define the AT

As a first step, it is necessary to identify all of the hardware and software components required to detect a specific AC. These components comprise the AT – both collectively and through the manner in which they are connected (i.e., the architecture). As part of the subsequent methodology for estimating SDQ benefit, a baseline AT that does not include SDQ is required. The baseline AT is used to determine the reduction in the FP and FN probabilities provided by SDQ. This is accomplished by comparing results for an AT that includes SDQ against results for a baseline AT.

The main function of the AT presented here is to monitor a pressure and provide actionable knowledge to the crew so they can initiate an abort action if necessary. Low pressure conditions are a well-known issue for liquid-propellant-based LVs. Inordinately low propellant tank pressures during flight are indicative of a course of events that may result in catastrophic explosions with loss of the vehicle and/or crew.

Figure 1 presents the baseline functional block diagram of the architecture for the threshold-based AT used in this paper. To facilitate the calculation of the SDQ benefit, the baseline architecture does not include the SDQ function. Figure. 2 presents a block diagram for the same AT, but with the addition of SDQ. In the following discussion, previously undefined elements of the AT diagrams are described and the specific SDC implementation is detailed.

Pressure Sensors (PSs): The AT architecture contains four (4) redundant pressure sensors – PS1, PS2, PS3, and PS4. Each pressure sensor transducer generates analog voltage signals proportional to the sensed pressure. Said signals are inputs to the Sensor Electronics (SE). PS1 and PS2 are connected to SE1, while PS3 and PS4 are similarly connected to SE2.

Sensor Electronics (SEs): There are two sets of SEs which include (a) signal conditioning equipment required to power the pressure sensors, (b) hardware and firmware required to digitize and discretize the sensor's analog signal, and (c) hardware and firmware required to interface to a digital data bus. The SE outputs for each sensor are cross-strapped to each of the FCs via the data buses.

Flight Computers (FCs): There are three (3) FCs – FC1, FC2, and FC3. The FC functional block represents both hardware and software implemented to support operation of the launch vehicle.

Sensor Data Consolidation (SDC): For the baseline system shown in Fig. 1, sensor measurements PS1, PS2, PS3, and PS4 are averaged on each FC to obtain a single consolidated measurement that is used by the ACDL. Averaging was selected as the SDC algorithm to simplify the example. Other approaches (e.g., mid value select) could be used in place of averaging.

Some broad assumptions and ground rules that are used to analyze this example AT follow.

- The mission time is 10 minutes or $0.1\overline{66}$ hrs.

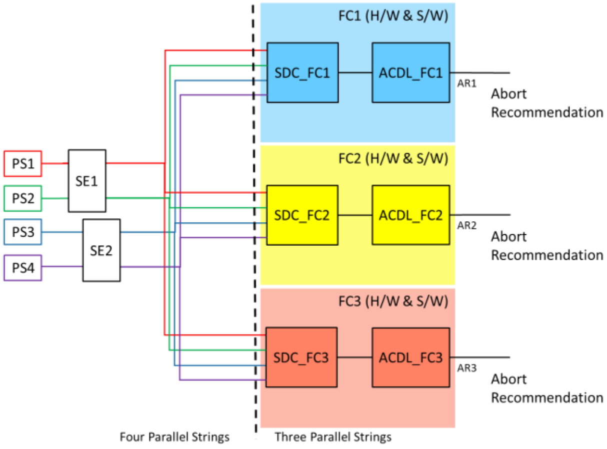

Figure 1. AT Baseline Architecture showing relevant components and data links.

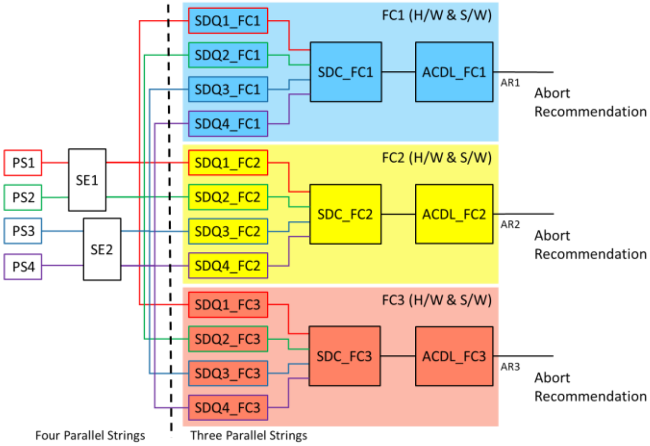

Figure 2. AT+SDQ Architecture showing relevant components and data links

- During the mission, components are considered to be in either an operational or failed state. In other words, an AT with a degraded response is not considered.
- The AT is single fault tolerant with respect to the SE and FC components:
  - At least one (1) properly functioning SE component is needed to complete the mission.
  - At least two (2) properly functioning FCs – includes both hardware and software components – are needed to complete the mission.
- Additionally, the AT is two fault tolerant with respect to PS components. At least two (2) properly functioning PSs are needed to complete the mission.
- Random part failure and the common cause failure (CCF) of redundant components are considered.
- Single-point estimates, rather than distributions, are used to represent component failure rates. This simplifies the analysis and discussion of the results.
- The limit of resolution of the analysis is at the component level. Analysis is not performed below that level.

4.2. Step 2: Analyze the Physics of Failure

Given a complete description of the components and architecture of the AT, the next step is to develop a clear understanding of the failure modes associated with those components and how the physics of failure may modify data used by the ACDL.

Here, an approach based on Receiver Operating Characteristic (ROC) theory (Vachtsevanos, et al, 2006) is used. The analysis was first simplified by defining three classifications for the effect of failures. Then, the impact of each of those classifications on the probability of a FP or FN abort detection was explored.

The probability of FP and FN aborts may be bounded by considering the following three common classifications for the effect of failures: Failure to Zero (F2Z), Failure to Intermediate Value (F2IV), and Failure to Full-Scale (F2FS). A discussion of each of these classifications follows and addresses the potential for the failure class to generate a FP or FN abort detection.

Failure to Zero (F2Z) – Occurs when data associated with one or more of the PSs fails to a value at or near zero. Small variations about zero may result from improper sensor calibration or from ambient noise. Further, when averaging is the consolidation algorithm – see Eqs. (1) and (2) – this failure classification has the effect of driving both the consolidated measurement value, $u_{j,c}$, and the standard deviation of the consolidated measurement value, $\sigma_{j,c}$, toward zero.

$$u_{j,\mathrm{c}} = \tfrac{1}{4}\sum_{i=1}^{4} u_{j,i} \tag{1}$$

$$\sigma_{j,\mathrm{c}} = \tfrac{1}{4}\sum_{i=1}^{4} \sigma_{j,i} \tag{2}$$

Here, u represents a measured or calculated system state; σ indicates the standard deviation of u; i is an index associated with the individual data buses that deliver sensor data to the FCs; j is an index that indicates a specific FC; and “c” indicates that the associated value is the result of the SDC calculation. For the example presented in this paper, $u_{j,i}$ and $\sigma_{j,i}$ respectively represent the individual pressure measurements and their standard deviations.

Failure to Full Scale (F2FS) – Occurs when data associated with one or more of the PSs fails to a value at or near full-scale. F2FS will not contribute to a FP abort detection of low pressure. It may however, contribute to a FN abort detection if the following three conditions exist.

- a system failure has occurred, and
- the system failure results in a low pressure condition, and
- the value of the pressure data, $u_{j,i}$, resulting from that failure are less than, yet sufficiently close to, the low pressure detection threshold, u_{TH}.

If these three conditions exist, then an F2FS of one or more pressure sensor data signals will result in a FN abort detection.

Failure to Intermediate Value (F2IV) – This more complicated and often more likely case occurs when occurs when data associated with one or more of the PSs fails to values greater than zero but less than full-scale. This situation could be caused, for example, by a partially blocked sensing port or by intermittent short or open circuits. In reality, failures associated with this failure effect classification may or may not result in an AC. As a result, quantification of the FP and FN probabilities associated with these failures typically requires significant Monte Carlo analysis. Since tools and resources are not currently available to conduct the required analysis, other approaches are needed to estimate and bound the probabilities. One means of providing a conservative bound for assessing the FP rate is to attribute all of the F2IV failure rate to the F2Z classification. That is:

$$\mathrm{FR(F2Z)}_{\mathrm{Upper\ Bound}} = \mathrm{FR(F2Z)} + \mathrm{FR(F2IV)}, \tag{3}$$

where FR is the failure rate. Reasoning in a similar (but “opposite” in terms of using the data) manner for FN, one means of providing a conservative bound for assessing the FN rate is to attribute all of the F2IV failure rate to the F2FS classification, so that:

$$\mathrm{FR(F2FS)}_{\mathrm{Upper\ Bound}} = \mathrm{FR(F2FS)} + \mathrm{FR(F2IV)}. \tag{4}$$

For the purposes of the analyses described in this report, all F2IV probabilities are estimated conservatively as F2Z for FP calculations and F2FS for FN calculations. This logic follows from the observations that assigning F2IV cases to F2Z will always create a FP, and assigning F2IV to F2FS for FN calculations will always create a FN. As F2IV cases will in reality only sometimes create these conditions, but at rates difficult to predict, we deliberately create overestimates of FP and FN cases to ensure a conservative estimate.

4.2.1. Failure to Zero and FP Analysis

To show the impact of an F2Z on the ACDL, cases for the F2Z of 0, 1, and 2 sensors were examined. Relevant parameters are identified in Table 1. A nominal value of $u_{i,\mathrm{nom}} = 40$ pounds per square inch (psi) was selected for the pressure sensor and a value of $\sigma_{i,\mathrm{nom}} = 0.75$ psi for the standard deviation. For F2Z sensor signals, both the signal value and the signal standard deviation are assumed to be zero. To calculate the probability that the consolidated pressure is less than the AC detection threshold, a Gaussian probability distribution is assumed and an AT threshold, $u_{\mathrm{TH}} = 25$ psi, is used. The results for each of the three cases examined are given in Table 2. Of primary interest are the consolidated values, $u_{j,\mathrm{c}}$ and $\sigma_{j,\mathrm{c}}$, and $P\left(u_{j,\mathrm{c}} < u_{\mathrm{TH}}\right)$ which is the probability that an F2Z of the signals will result in a FP abort detection.

Table 1. Parameters used in example AT for FP analysis.

Variable	Value	Units	Description
$u_{i,\mathrm{FS}}$	60	psi	Full-scale pressure
$u_{i,nom}$	40	psi	Nominal pressure
$\sigma_{i,nom}$	0.75	psi	Standard deviation of nominal pressure
u_{TH}	25	psi	Detection threshold for low pressure AC

Note here the effect of failures on the value of the consolidated signal. As more signals F2Z, both the consolidated signal value and the consolidated standard deviation move closer to zero. Also, for this example, an F2Z does not result in an overlap between the nominal and failed probability distributions as would be typical for F2IV.

Further, Fig. 3 shows the probability distribution of the consolidated signal, $u_{j,c}$, for no F2Z signals, for one F2Z signal, and for two F2Z signals. An important observation from both Table 2 and Fig. 3 is that the AT is single fault tolerant. The F2Z of a single sensor data signal is not sufficient to cause a FP abort detection. The F2Z of two or more sensor data signals on the same FC are required to generate a FP abort detection.

4.2.2. Failure to Full-scale and FN Analysis

The impact of F2FS on the ACDL is illustrated by looking at cases for 0, 1, and 2 sensors failing to full-scale. As shown in Table 3, a nominal value of $u_{i,\mathrm{nom}} = 20$ psi was selected for the pressure sensor and a value of $\sigma_{i,\mathrm{nom}} = 0.75$ psi for the standard deviation. The nominal value is assumed to be the result of an AC, as an AC must exist for a FN to occur. For F2FS sensor signals, the signal value and standard deviation are assumed to be 60 psi and 0.75 psi, respectively. To calculate the probability that the consolidated pressure is greater than the AC detection threshold, a Gaussian

Table 2. Impact of F2Z on example ACDL.

	Case 1	Case 2	Case 3
No. Data Values:	4	4	4
No. Nominal Data Values:	3	2	1
No. F2Z Data Values:	1	2	3
$u_{j,1}$	40	40	40
$u_{j,2}$	40	40	0
$u_{j,3}$	40	0	0
$u_{j,4}$	0	0	0
$u_{j,\mathrm{c}}$	30	20	10
$\sigma_{j,1}$	0.75	0.75	0.75
$\sigma_{j,2}$	0.75	0.75	0
$\sigma_{j,3}$	0.75	0	0
$\sigma_{j,4}$	0	0	0
$\sigma_{j,\mathrm{c}}$	0.56	0.38	0.19
$P\left(u_{j,\mathrm{c}} < u_{\mathrm{TH}}\right)$:	3.08E-19	1.0000	1.0000

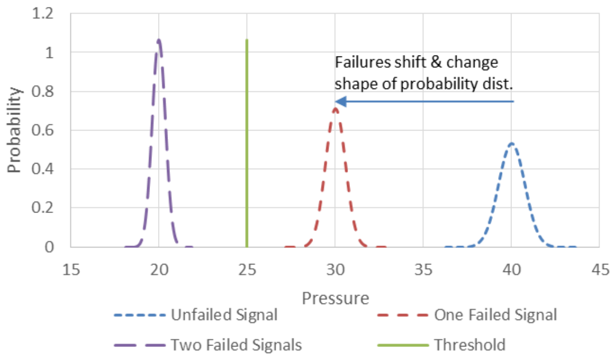

Figure 3. Probability distribution vs. pressure for $u_{j,c}$ given 0, 1, and 2 pressure signals failing to zero without the application of SDQ.

probability distribution and an AT threshold value of $u_{\mathrm{TH}} = 25$ psi were also assumed. Results for each of the three cases examined are given in Table 4. Of primary interest are the consolidated values, $u_{j,\mathrm{c}}$ and $\sigma_{j,\mathrm{c}}$, and $P(u_{j,\mathrm{c}} > u_{\mathrm{TH}})$ which is the probability that an F2FS of the signals will result in a FN abort detection.

Further, Fig. 4 shows the probability distribution of the consolidated signal, $u_{j,\mathrm{c}}$, for the three cases. An important observation from both Table 4 and Fig. 4 is that, if the low pressure AC exists and the pressure is sufficiently close to the detection threshold, the F2FS of a single sensor is enough to generate a FN abort detection.

4.3. Step 3: Determine Bounds on Component Failure Probabilities

The overall goal of this step is to calculate the probability of failure for each component that is part of the AT architecture. The process for accomplishing this goal is described below.

Step 3.1 Identify the failure modes and associated failure rates for each component in the AT architecture. Failure modes and failure rates (i.e., reliability data) are typically determined by referencing a system-specific failure modes and effects analysis or similar documents. Reliability data used in this paper are given in the first two cols. of Tables 5 through 8. In Table 8, the FC software failure rates are presumed not to include the flight application software.

Step 3.2 Classify the effect of each failure mode identified in Step 3.1 as F2Z, F2IV, or F2FS. This is typically accomplished through discussions with one or more subject matter experts who understand the failure modes and the impact of those failures on the data used to detect a given AC.

Step 3.3 Conservative (i.e., upper) bounds for the component's F2Z and F2FS probabilities are determined. To do this, failure rates classified as F2Z are only allocated to the F2Z rate (i.e., F2Z per hour). Those classified as F2FS are only allocated to the F2FS rate. And, those classified as F2IV are allocated to both the F2Z and F2FS rates. An example showing how this is done for the F2Z case is given in Table 5 where, for the Electrical Short failure, the failure rate (col. 2) is allocated to F2Z rate (col. 6), while a failure rate of zero is allocated to the F2FS rate (col. 7). Similarly, an example of how this is done for the F2FS case is shown in Table 6 where, for the High Voltage failure, the failure rate (col. 2) is allocated to F2FS rate (col. 7), while a failure rate of zero is allocated to the F2Z rate (col. 6). Finally, an example showing allocation for the F2IV case is given in Table 5 where, for the degraded failure, the failure rate is allocated to both the F2Z rate and the F2FS rate.

Step 3.4 Calculate the F2Z and F2FS total failure rates for each component by summing the rates for each failure mode in cols. 6 and 7, respectively. In Table 5, the total F2Z rate is 4.2E-05 failures per hour and the F2FS rate is 3.16E-05

Table 3. Impact of F2FS on example ADCL.

	Case 1	Case 2	Case 3
No. Data Values:	4	4	4
No. Nominal Data Values:	3	2	1
No. F2FS Data Values:	1	2	3
$u_{j,1}$	20	20	20
$u_{j,2}$	20	20	60
$u_{j,3}$	20	60	60
$u_{j,4}$	60	60	60
$u_{j,\mathrm{c}}$	30	40	50
$\sigma_{j,\mathrm{c}}$	0.75	0.75	0.75
$P(u_{j,\mathrm{c}} > u_{\mathrm{TH}})$:	1.0000	1.0000	1.0000

Table 4. Parameters used in example AT for FN analysis.

Variable	Value	Units	Description
$u_{i,\mathrm{FS}}$	60	psi	Full-scale pressure
$u_{i,nom}$	20	psi	Nominal pressure
$\sigma_{i,nom}$	0.75	psi	Standard deviation of nominal pressure
u_{TH}	25	psi	Detection threshold for low pressure AC

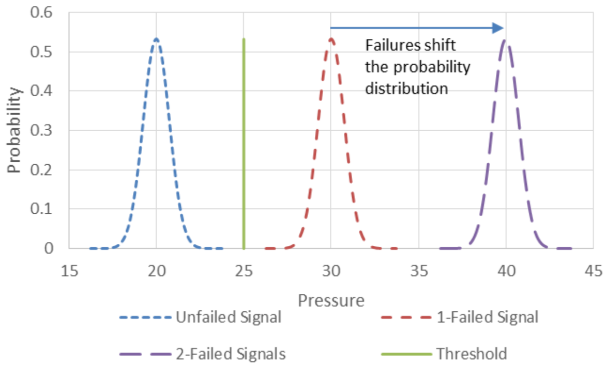

Figure 4. Probability distribution vs. pressure for $u_{j,\mathrm{c}}$ given 0, 1, and 2 pressure signals failing to full-scale without the application of SDQ.

Table 5. Failure modes for the example PS showing the contribution of each failure mode to conservative bounds for F2Z and F2FS classifications.

		Quantitative impact of failure mode on the component output signal			Conservative Upper Bound	
Failure Mode	Failures per hour	F2Z	F2FS	F2IV	F2Z per hour	F2FS per hour
Electrical Short	3.500E-06	X			3.500E-06	0.000E+00
No Output	6.900E-06	X			6.900E-06	0.000E+00
Cracked or Fractured	3.500E-06			X	3.500E-06	3.500E-06
Degraded	2.810E-05			X	2.810E-05	2.810E-05
Totals:	4.200E-05		Totals:		4.200E-05	3.160E-05
			Operating Hours:		0.1667	0.1667
			Probability of Failure:		7.000E-06	5.267E-06

Table 6. Failure modes for the example SE showing the contribution of each failure mode to conservative bounds for F2Z and F2FS classifications.

		Quantitative impact of failure mode on the component output signal			Conservative Upper Bounds	
Failure Mode	Failures per hour	F2Z	F2FS	F2IV	F2Z per hour	F2FS per hour
Defective Component	4.290E-07	X			4.290E-07	0.000E+00
Fails During Operation	1.430E-07			X	1.430E-07	1.430E-07
Connection Failure	7.133E-08	X			7.133E-08	0.000E+00
Failed to Operate	7.133E-08	X			7.133E-08	0.000E+00
High Voltage	7.133E-08		X		0.000E+00	7.133E-08
Improper Output	7.133E-08			X	7.133E-08	7.133E-08
Inoperative	7.133E-08	X			7.133E-08	0.000E+00
Logic Fault	7.133E-08			X	7.133E-08	7.133E-08
Totals:	1.000E-06		Totals:		9.287E-07	3.570E-07
			Operating Hours:		0.1667	0.1667
			Probability of Failure:		1.548E-07	5.950E-08

failures per hour. These are shown in the totals row in cols. 6 and 7, respectively.

Step 3.5 Multiply the conservative total failure rate for the F2Z and F2FS classifications by the time in the mission phase to obtain the probability of failure for each classification. The goal of this step is to calculate the probability of F2Z and F2FS for each of the components represented in Tables 5 through 8. To do that, the failure rates calculated in the previous step are multiplied by the operating time–for this example 10 minutes or $0.1\overline{66}$ hours is assumed. Results for probability of failure calculations are given in the last row of cols. 6 and 7 in each of the failure mode tables.

When appropriate, Steps 3.1 through 3.5 may be repeated for each mission phase.

4.4. Step 4: Conduct Analysis of FP and FN Probabilities for the Baseline System

In this Section, the methodologies and modeling approaches used to derive the probability of a FP and a FN abort recommendation are discussed. A FT analysis methodology was used to provide a systematic means of identifying system component failure events that lead to these undesired recommendations.

4.4.1. Fault Tree Development

FT models were constructed using the NASA fault tree analysis guidelines (Stamatelatos and Homayoon, 2011). The Systems Analysis Programs for Hands-on Integrated

Table 7. Failure modes for the example FC hardware showing the contribution of each failure mode to conservative bounds for F2Z and F2FS classifications.

		Quantitative impact of failure mode on the component output signal			Conservative Upper Bounds	
Failure Mode	Failures per Hour	F2Z	F2FS	F2IV	F2Z per Hour	F2FS per Hour
Power Supply Failure	1.540E-05	X			1.540E-05	0.000E+00
I/O Board Failure	7.700E-06			X	7.700E-06	7.700E-06
Processor Failure	3.850E-05			X	3.850E-05	3.850E-05
Data Bus Failure	1.540E-05	X			1.540E-05	0.000E+00
Totals:	7.700E-05			Totals:	7.700E-05	4.620E-05
				Operating Hours:	0.1667	0.1667
				Probability of Failure:	1.283E-05	7.700E-06

Table 8. Failure modes for the example FC software showing the contribution of each failure mode to conservative bounds for F2Z and F2FS classifications.

		Quantitative impact of failure mode on the component output signal			Conservative Upper Bounds	
Failure Mode	Failures per hour	F2Z	F2FS	F2IV	F2Z per hour	F2FS per hour
Computational	1.350E-06			X	1.350E-06	1.350E-06
Logic	1.710E-06			X	1.710E-06	1.710E-06
Data I/O	7.300E-07			X	7.300E-07	7.300E-07
Data Handling	1.090E-06			X	1.090E-06	1.090E-06
Interface	9.800E-07			X	9.800E-07	9.800E-07
Data Definition	7.300E-07			X	7.300E-07	7.300E-07
Data Base	2.470E-06			X	2.470E-06	2.470E-06
Other	9.400E-07			X	9.400E-07	9.400E-07
Totals:	1.000E-05			Totals:	1.000E-05	1.000E-05
				Operating Hours:	0.1667	0.1667
				Probability of Failure:	1.667E-06	1.667E-06

Reliability Evaluations (SAPHIRE) software was used to generate the failure combination of events that lead to a FP or FN abort recommendation, quantify probability of those recommendations, and identify the major failure contributors or risk drivers to those recommendations. SAPHIRE is a publically-available, government-developed software tool that is useful for performing Probabilistic Risk Assessment (PRA). SAPHIRE is documented in a number of reports including a summary manual by the NRC (Wood, Smith, Kvarfordt, & Beck, 2008). The SAPHIRE FT is not shown due to complexity and space limitations.

4.4.2. Common Cause Event Modeling

Common Cause Failure (CCF) events are accounted for in the SAPHIRE FT model. CCFs have been shown by many reliability studies to contribute significantly to the overall unreliability of complex systems. A CCF event is defined as the failure of multiple redundant components due to shared causes. The incorporation of CCF events into the FT model results in more realistic estimates of system unreliability. In this work, CCF events are modeled in the FT to account for the possible failure of AT components due to external causes. For example, multiple FCs might fail simultaneously or generate erroneous signal output indicating the occurrence of an abnormal system state. This type of failure event can be caused by loose connections of interface cables. Cable connection errors can be attributed to installation or assembly errors (human error), high levels of vibration during launch vehicle ascent, or by design faults in FC hardware, firmware or software. To reduce the underestimation of probabilities for FP and FN abort recommendations, combinations of multiple CCF events were considered for each AT component. The CCF probability equations (Mosleh, Rasmuson, & Marshall, 1998) and associated alpha factor values (Atwood, Kelly, Marshall, Prawdzik, & Stetkar 1996) used in this study are given in Table 9.

Table 9. CCF probability equations and α values for CCF alpha factor model (non-staggered testing scheme).

Success Configuration (k-out of- n)	Common Cause Failure Probability Equations	α factor Values
1 out 2 (CCSE)	P(CCF_2) = α_2 / 1.0257 x P_t	α_1 = 0.97430 α_2 = 0.02570
2 out 3 (FC Hardware /FC Software)	P(CCF_2)= 1/2* x α_2 / 1.0303 x P_t P(CCF_3) = α_3 / 1.0303 x P_t	α_1 = 0.97550 α_2 = 0.01870 α_3= 0.00579
2 of 4 (PS)	P(CCF_2) = 1/3 x α_2 / 1.0376 x P_t P(CCF_3) = 1/3 x α_3 / 1.0376 x P_t P(CCF_4) = α_4 / 1.0376 x P_t	α_1 = 0.97410 α_2= 0.01700 α_3= 0.00589 α_4= 0.00298

4.4.3. Estimation Approach for FP and FN Abort Detection

The methodology in this section is developed by first considering the FN case. The occurrence of a FN detection depends on the occurrence of two events.

1. A system failure of sufficient magnitude to exceed prescribed detection thresholds and
2. A failure of the AT to detect that system failure.

The occurrence of a FN event may then be represented using the following Boolean algebraic expression:

$$\mathrm{FN} = \mathrm{AC} \cap \mathrm{AT}|\mathrm{AC}. \qquad (5)$$

Here, FN is true if an abnormality event occurred and an abort trigger occurred given that an abort condition is true.

The probability of a FN event is given by,

$$\begin{aligned} \mathrm{P(FN)} &= \mathrm{P(AC \cap AT|AC)} \\ &= \mathrm{P(AC)\ x\ P(AT|AC)}. \end{aligned} \qquad (6)$$

Here P(AC) denotes the probability of an AC and P(AT|AC) denotes the conditional probability of failure of the AT given that an AC event has occurred.

If various ACs are considered, a general expression for the overall system probability of a FN detection can be obtained by applying the additive rule of probability as shown below. This expression assumes the occurrences of FN scenarios are mutually exclusive.

$$\mathrm{P(FN)} = \sum_{k=1}^{n} \mathrm{P}(\mathrm{AC}_k)\ \mathrm{x}\ \mathrm{P}(\mathrm{AT}|\mathrm{AC}_k) \qquad (7)$$

For the remainder of this paper, $\mathrm{AC}_k = 1$ implies that the probability a given AC will occur was accounted for as part of a separate analysis. This approach has the added benefit that the structure and failure logic of FP and FN events become identical. As a consequence, the SAPHIRE model and results used to analyze a FN abort recommendation may also be used to estimate the probability of a FP abort recommendation.

For each AT component, Table 10 lists the success configuration (i.e., the minimum redundancy required) and the single-point failure rates to be used in conducting reliability analyses for both F2Z and F2FS. Success configurations are based on the assumptions stated at the end of Sec. 4.1. For components other than SDQ, single-point failure rates were obtained from the bounded F2Z and F2FS failure rates listed in Tables 5 through 8. Failure rates were not available for SDQ, so a failure rate equivalent to the FC software failure rate was assumed. Although this is believed to be a very conservative estimate, it is useful for explaining the FP and FN methodology.

4.4.4. Probabilistic Risk and Reliability Analysis

After constructing the FT and entering the required data for the component and CCF probability estimates into SAPHIRE, the software can be used to perform probabilistic risk and reliability analysis. SAPHIRE initially performs a FT reduction using Boolean reduction techniques. FT reduction is performed to eliminate redundant basic failure events so as to avoid over estimation of top event probability. The results of FT reduction are a set of basic failure events

Table 10. Individual component failure rates for F2Z and F2FS

	AT Component	PS	SE	FC Hardware	FC Software	SDQ
	Success Configuration	2 out 4	1 out 2	2 out 3	2 out 3	2 out 3
F2Z	Failure Rate (failures/hour)	4.2E-05	8.57E-07	7.70E-05	1.00E-05	1.00E-05
F2FS	Failure Rate (failures/hour)	3.16E-06	3.57E-07	4.62E-05	1.00E-05	1.00E-05

that, should they occur, lead to the top event occurring. In this paper, members of this set of events are called Minimal Cut Sets (MCS) or Risk Drivers (RDs).

The FP and FN probabilities of occurrence obtained from SAPHIRE are shown in Tables 11 and 12, respectively. To consolidate the data for presentation, results for both the AT baseline and the AT+SDQ architectures are given in the same table. All of the risk drivers in these tables are CCF events associated with the AT's redundant components. For this example, the probability of random component failure is negligible. The data, which represents the top risk drivers for each classification, will be discussed in more detail in Sec. 4.5.

Table 11. Top risk drivers for an AT FP detection due to F2Z.

Set No.	AT Baseline FP Probability	AT+SDQ FP Probability	Basic Event Description
1	1.19E-07	1.19E-07	FC1 & FC2 hardware CCF
2	1.19E-07	1.19E-07	FC1 & FC3 hardware CCF
3	1.19E-07	1.19E-07	FC2 & FC3 hardware CCF
4	7.39E-08	7.39E-08	FC1, FC2, & FC3 hardware CCF
5	2.06E-08	2.06E-08	PS1, PS2, PS3, & PS4 CCF
6	1.55E-08	1.55E-08	FC1 & FC2 software CCF
7	1.55E-08	1.55E-08	FC1 & FC3 software CCF
8	1.55E-08	1.55E-08	FC2 & FC3 software CCF
9	1.36E-08	1.36E-08	PS1, PS2, & PS3 CCF
10	1.36E-08	1.36E-08	PS1, PS2, & PS4 CCF
11	1.36E-08	1.36E-08	PS1, PS3, & PS4 CCF
12	1.36E-08	1.36E-08	PS2, PS3, & PS4 CCF
13	9.60E-09	9.60E-09	FC1, F2, & FC3 software CCF
14	N/A	*4.92E-09*	*SDQ1, SDQ2, SDQ3, & SDQ4 CCF*
15	3.67E-09	3.67E-09	SE1 & SE2 CCF
16	N/A	*3.24E-09*	*SDQ1, SDQ2, & SDQ3 CCF*
17	N/A	*3.24E-09*	*SDQ1, SDQ2, & SDQ4 CCF*
18	N/A	*3.24E-09*	*SDQ1, SDQ3, & SDQ4 CCF*
19	N/A	*3.24E-09*	*SDQ2, SDQ3, & SDQ4 CCF*

Table 12. Top risk drivers for an AT FN detection by the AT due to F2FS.

Set No.	AT Baseline FN Probability	AT+SDQ FN Probability	Basic Event Description
1	7.16E-08	7.16E-08	FC1 & FC2 hardware CCF
2	7.16E-08	7.16E-08	FC1 & FC3 hardware CCF
3	7.16E-08	7.16E-08	FC2 & FC3 hardware CCF
4	4.44E-08	4.44E-08	FC1, FC2, & FC3 hardware CCF
5	1.55E-08	1.55E-08	PS1, PS2, PS3, & PS4 CCF
6	1.55E-08	1.55E-08	FC1 & FC2 software CCF
7	1.55E-08	1.55E-08	FC1 & FC3 software CCF
8	1.55E-08	1.55E-08	FC2 & FC3 software CCF
9	1.02E-08	1.02E-08	PS1, PS2, & PS3 CCF
10	1.02E-08	1.02E-08	PS1, PS2, & PS4 CCF
11	1.02E-08	1.02E-08	PS1, PS3, & PS4 CCF
12	1.02E-08	1.02E-08	PS2, PS3, & PS4 CCF
13	9.60E-09	9.60E-09	FC1, F2, & FC3 software CCF
14	N/A	*4.92E-09*	*SDQ1, SDQ2, SDQ3, & SDQ4 CCF*
15	N/A	*3.24E-09*	*SDQ1, SDQ2, & SDQ3 CCF*
16	N/A	*3.24E-09*	*SDQ1, SDQ2, & SDQ4 CCF*
17	N/A	*3.24E-09*	*SDQ1, SDQ3, & SDQ4 CCF*
18	N/A	*3.24E-09*	*SDQ2, SDQ3, & SDQ4 CCF*
19	1.53E-09	1.53E-09	SE1 & SE2 CCF

4.5. Step 5: Determine the Benefit Provided by SDQ Algorithms

The overall goal of this step is to determine the benefit provided by SDQ. For this example, the SDQ algorithm would be composed of two thresholds. One threshold near zero to detect F2Z and one near full-scale to detect F2FS.

The goal of this step is accomplished by calculating probability of a FP or FN abort for the AT+SDQ architecture and comparing the results to those for the baseline AT architecture. In a process similar to that used to analyze baseline AT, calculation of the SDQ FP and FN probabilities and the SDQ benefit may be achieved as follows:

Step 5.1 Revise the baseline AT architecture to include SDQ. The revised architecture is shown in Fig. 2.

Step 5.2 Analyze the physics of failure for the AT+SDQ architecture. This can be accomplished with a cursory review of Figs. 3 and 4 and Tables 2 and 4. If SDQ successfully identifies and disqualifies the failed signal, the shift in the consolidated signal value required to generate a FP or FN abort detection will not exist. As a result, the probability of a FP abort detection due to a double failure or a FN abort detection due to a single failure then changes from a certainty to zero.

Step 5.3 Create and analyze an FT for the AT+SDQ architecture. This can be accomplished by revising the baseline FT in SAPHIRE to include SDQ components and related failure data. Then perform the SAPHIRE analysis to identify cut sets that are the top risk drivers for this architecture.

As noted previously, the FP and FN probabilities of occurrence obtained from SAPHIRE are shown in Tables 11 and 12, respectively. These data represent the top risk drivers for the FP and FN classifications. In both of these tables, risk drivers are numbered as shown in column 1. For each of these cut sets, FP or FN probabilities for the AT baseline architecture is given in column 2; while probabilities for the AT+SDQ architecture are given in column 3. Column 4 lists the basic failure events that are the cause of the FP or FN abort detection.

Step 5.4 Determine the net SDQ benefit – the reduction in FP and FN probabilities that results from including SDQ in the AT architecture.

First, calculate the FP and FN probabilities for the AT Baseline. For the example used in this paper, this is accomplished by summing the values in column 2 of Tables 11 and 12. Results of these calculations are given in row 2 of Table 13.

Second, determine the SDQ benefit by identifying risk drivers that will be mitigated by SDQ and separately summing the FP and FN probabilities associated with those risk drivers. Risk drivers mitigated by SDQ are typically associated with components downstream – in terms of information flow – of the SDQ component. For the example used in this paper, SDQ mitigated risk drivers are identified in Tables 11 and 12 by cells with a gray background. The SDQ FP benefit is obtained from Table 11 by summing the values in column 3 (or column 2 since the values are the same) for only the gray cells. A similar calculation is applied to Table 12 to obtain the SDQ FN benefit. Results of these calculations are given as SDQ benefits in row 3 of Table 13.

Third, the addition of SDQ to the AT architecture comes at the cost of increasing the FP and FN probabilities. The SDQ cost is determined by identifying the risk drivers added by SDQ and summing the probabilities of those risk drivers. SDQ risk drivers are identified by italicized text in Tables 11 and 12. The FP SDQ cost is then determined by summing the probabilities (Table 11, column 3) for the identified SDQ risk drivers. A similar calculation is applied to Table 12 to obtain the FN SDQ cost. The FP and FN SDQ costs are given in row 4 of Table 13.

Table 13. Summary of SDQ benefit calculations for AT FP and FN detections.

		FP	FN
Probability	AT Baseline	5.66E-07	3.73E-07
	SDQ Benefit	7.87E-08	5.63E-08
	SDQ Cost	1.79E-08	1.79E-08
Net SDQ Benefit	Probability	6.08E-08	3.84E-08
	%	10.7%	10.3%

Finally, metrics for the SDQ benefit can be calculated as shown in Eqs. 8 and 9.

$$\text{Net SDQ Benefit} = \text{SDQ Benefit - SDQ Cost} \qquad (8)$$

$$Net\ SDQ\ Benefit\ \% = 100\ \times \frac{Net\ SDQ\ Benefit}{AT\ Baseline} \qquad (9)$$

Using Eq. 8, the net SDQ benefit to the FP probability may be calculated by subtracting the FP SDQ cost from the FP SDQ benefit. Similarly, the net SDQ benefit to the FN probability may be calculated by subtracting the FN SDQ cost from the FN SDQ benefit. The percent improvement in the FP and FN net SDQ benefit over the baseline AT may then be calculated using Eq. 9 in conjunction with the previously calculated values in Table 13. The FP and FN results of for Eqs. 8 and 9 are given in the next to last row and last row of Table 13, respectively.

5. DISCUSSION

Some observations based on data resulting from application of the FP and FN methodology to the example application are given in this Section.

First, because this methodology uses a conservative upper bound for the component failure rates, the FP and FN probabilities for the AT baseline and AT+SDQ architecture are also upper bounds. This means that the actual FP and FN rates and probabilities will likely be less than those presented in the first two rows of Table 13. The practical significance of the estimate is that if the upper bound values meet requirements for FP and FN probabilities, then more detailed FP and FN analyses are not needed.

Second, the methodology presented used single-point probability estimates for the reliability analysis. The analysis could be made more rigorous by performing the analysis with probability distributions instead of the single-point estimates.

Another observation is that, a significant amount of uncertainty in the failure rates results from the classification process that was applied. The sum of the F2IV for each component is essentially the failure rate uncertainty for that component. For example, in Table 8, all of the FC software failure modes are characterized as F2IV resulting in a failure rate uncertainty of 100% for that component. Proper classification of the failure modes is necessary to ensure that the uncertainty in the FP and FN probabilities is minimized and the accuracy maximized. Another option might be to consider a different classification approach.

The impact of the SDQ failure rate used in the example application is another important consideration. Given that the failure rate for SDQ is likely to be lower than that for the flight software, one might consider the bounding case where the SDQ failure rate and resulting cost are both zero. In that case, the SDQ Benefit given in row 4 of Table 13 becomes the upper bound for the net SDQ Benefit.

The methodology could also be expanded to examine the uncertainty in the net SDQ Benefit by considering the case where failure rates associated with F2IV are allocated to neither F2Z nor F2FS. Results for FTs associated with these cases could be compared to those already presented to arrive at an uncertainty bound for the net SDQ FP and FN benefits.

6. CONCLUDING REMARKS

This paper presented a methodology that was developed to calculate quantitative bounded estimates of the false positive (FP) and false negative (FN) detection probabilities for an abort trigger (AT) with sensor data qualification (SDQ) and a constant abort threshold during a given flight phase. To illustrate the methodology, an example application was given that included the type of redundancy typically found in human space flight hardware and software. The example starts with the definition of the AT architecture. It then analyzes the AT's physics of failure to arrive at three failure classifications: failure to zero, failure to intermediate value, and failure to full scale. These classifications are used to bound the component failure rates. Using the Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) software, a fault tree is created that captures the component failure modes. The SAPHIRE fault tree is used in concert with the single-point estimates for the failure rates, and parametric common cause failure models to conduct a risk and reliability analysis as a means to identify the probabilities of and top risk drivers for FP and FN abort detections. Finally, reliability analysis results for a baseline AT without SDQ are compared to an AT that includes SDQ components. This provides a means of determining the net SDQ benefit in terms of reduced FP and FN probabilities of abort detection.

Observations resulting from the example application and ways to improve the methodology are also discussed. Two key means of improving the methodology are: (1) replacing single-point probability estimates with probability distributions and (2) by a more detailed investigation of the impact on the methodology of uncertainty in the component failure rates.

Current plans are to apply a version of this methodology to all SLS threshold-based ATs with the intent of refining calculations for loss of mission and loss of crew probabilities. Further, these calculations are and will be used to select the appropriate ATs for the vehicle, the SDQ algorithms for the ATs, and for verification and validation of the AT designs.

ACKNOWLEDGEMENT

The authors wish to acknowledge the support for this effort provided by the SLS project and the Mission and Fault Management team at the NASA Marshall Space Flight Center, Huntsville, AL.

NOMENCLATURE (ACRONYMS)

AC	abort condition
AT	abort trigger
ACDL	abort condition detection logic
CCF	common cause failure
F2FS	failure to full-scale
F2IV	failure to intermediate value
F2Z	failure to zero
FC	flight computer
FDIR	fault detection, isolation, and response
FM	fault management
FMCL	fault management control loops
FN	false negative
FP	false positive
FT	fault tree
LOC	loss of crew
LOM	loss of mission
LV	launch vehicle
NRC	nuclear regulatory commission
PRA	probabilistic risk assessment
PS	pressure sensor
ROC	receiver operator characteristic
SAPHIRE	systems analysis programs for hands-on integrated reliability evaluations
SDC	sensor data consolidation
SDQ	sensor data qualification
SE	sensor electronics
SHM	systems health management
SLS	Space Launch System
TN	true negative
TP	true positive
psi	pounds per square inch

REFERENCES

Atwood, C.L., Kelly, D.L., Marshall, F.M., Prawdzik, D.A., & Stetkar, J.W. (1996). Evaluation of loss of offsite power events at nuclear power plants, NUREG/CR-5496, CCF parameter estimations (2007), p. 216.

Washington, D.C.: U.S. Nuclear Regulatory Commission.

Albert, J., Alyea, D., Cooper, L., Johnson, S., & Uhrich, D., (1995). Vehicle health management (VHM) architecture process development. *Proceedings of SAE Aerospace Atlantic Conference*, May, Dayton, OH. doi: 10.4271/951385.

Day, J. C., & Johnson, S. B. (2104). System health management design strategies. Proceedings of the AIAA SpaceOps Conference, May 5-9, Pasadena, CA. doi: 10.2514/6.2014-1819.

Johnson, S. B., & Day, J. C. (2010). Conceptual framework for a fault management design methodology. *Proceedings of the AIAA Infotech@Aerospace Conference*, April 20-22, Atlanta, GA. doi:10.2514/6.2010-3431.

Johnson, S. B., & Day, J. C. (2011). System health management theory and design strategies. *Proceedings of the AIAA Infotech@Aerospace Conference*, March 29-31, St. Louis, Missouri. doi: 10.2514/6.2011-1493.

Johnson, S. B. (2011). The theory of system health management. In Johnson, S. B., Gormley, T. J., Kessler, S. S., Mott, C. D., Patterson-Hine, A., Reichard, K. M., & Scandura, P. A., Jr. (Eds.) *System Health Management: with Aerospace Applications (*pp. 3-26), Chichester, United Kingdom: John Wiley & Sons, Inc.

Lo, Y., Johnson, S.B., & Breckenridge, J.T. (2014). Application of fault management theory to the quantitative selection of a Launch Vehicle Abort Trigger Suite. *Proceedings of the IEEE Conference on Prognostics and Health Management (PHM)*, June 22-25, Cheney, WA. doi: 10.1109/ICPHM.2014.7036380.

Maul, W. A., Melcher, K. J., Chicatelli, A. K., & Sowers, T.S. (2006). Sensor data qualification for autonomous operation of space systems. *Proceedings of the American Association for Artificial Intelligence 2006 Fall Symposiums, Spacecraft Autonomy*, October 13-15, Arlington, VA. http://aaaipress.org/Papers/Symposia/ Fall /2006/FS-06-07/FS06-07-008.pdf.

Mosleh, A., Rasmuson, D.M., Marshall, F.M. (1998). Guidelines on modeling common-cause failures in probabilistic risk assessment, NUREG/CR-5485. Washington, DC: U.S. Nuclear Regulatory Commission.

Stamatelatos, M. and Homayoon, D. (2011). Probabilistic risk assessment procedures guide for NASA managers and practitioners, NASA/SP-2011-3421. Washington D.C.: National Aeronautics and Space Administration (NASA).

Wood, S.T., Smith, C.L., Kvarfordt, K.J., & Beck, S.T. (2008). Systems analysis programs for hands-on integrated reliability evaluations (SAPHIRE), Vol. 1, Summary Manual, NUREG/CR-6952. Washington, DC: U.S. Nuclear Regulatory Commission.

Vachtsevanos, G., Lewis, F. L., Roemer, M., Hess, A., & Wu, B. (2006). *Intelligent fault diagnosis and prognosis for engineering system*. Hoboken, NJ: John Wiley & Sons, Inc.

BIOGRAPHIES

Kevin J. Melcher is the technical team lead for exploration systems health management activities in the Intelligent Control and Autonomy Branch at the NASA John H. Glenn Research Center (GRC), Cleveland, OH. In that role, he is responsible for coordinating GRC support of the Space Launch System (SLS) Mission and Fault Management (M&FM) project. Mr. Melcher and his team are responsible for developing algorithms for nominal and off-nominal operation of the electrical power system (EPS) and the thrust vector control (TVC) systems, for developing algorithms to qualify and consolidate sensor data, for developing fault propagation models of the EPS and TVC systems, and for developing and conducting M&FM supporting analyses. In 1983, he received a Bachelor of Science degree in Applied Mechanics from the University of Cincinnati, Cincinnati, OH. And in 1996, he received a Master of Science degree in Mechanical Engineering from Cleveland State University. He is a member of the IEEE and a senior member of the AIAA. He currently participates as co-chair of the Awards Subcommittee for the AIAA Intelligent Systems Technical Committee. He also serves on the AIAA Northern Ohio Section Council as Past Chair having served as Section Chair from June 2012 to May 2014.

Mr. José Cruz is currently a reliability engineer in the NASA Glenn Safety and Mission Assurance Division. During the past 15 years, he has provided reliability engineering and risk analysis support to various space flight projects and agency-wide efforts including the International Space Station Fluid Combustion Facility design project, the Ares 1 upper stage power system, the Ares V payload shroud, the Crew Exploration Vehicle (CEV) Smart Buyer, and the Constellation Altair lunar lander. Mr. Cruz holds a Bachelor of Science degree in Industrial Engineering from the University of Puerto Rico (1983), a Master of Science degree in Reliability Engineering from the University of Maryland (1995), and a Master of Business Administration (MBA) degree from Cleveland State University (2010). Additionally, Mr. Cruz holds a Professional Engineer (PE) license from the State of Ohio.

Dr. Stephen Johnson is the analysis lead for Mission and Fault Management on NASA's Space Launch System program, led by NASA's Marshall Space Flight Center. He is also an associate research professor with the Department of Mechanical and Aerospace Engineering at the University of Colorado, and the President of Dependable System Technologies, LLC. Among many publications, Dr. Johnson is the general editor for System Health Management: with Aerospace Applications (2011), the author of *The Secret of Apollo: Systems Management in American and European Space Programs (2002)*, and many other articles and books in system health management, systems engineering, space history, and space economics.

Dr. Yunnhon (Yohon) Lo is a senior systems engineer with Ducommun Miltec supporting the Mission and Fault Management (M&FM) team on the NASA space launch system (SLS) program, led by NASA's Marshall Space Flight Center where he is the M&FM Abort and Safing lead. During the past 15 years, he has provided critical support for the Space Shuttle, Ares I, and Ares I-X probabilistic risk assessment, SLS fault management and flight software development for NASA. Dr. Lo holds Bachelor of Science, Master of Science, and Ph.D. degrees in nuclear engineering from the University of Tennessee, Knoxville. He is also an avid space advocate who is actively involved in the National Space Society and is a member of the Board of Directors for the Tennessee Valley Interstellar Workshop.