Model-based Data Integration and Process Standardization Techniques for Fault Management – A Feasibility Study

Deepak Haste, Qualtech Systems, Inc. (QSI), Rocky Hill, Connecticut

Sudipto Ghoshal, Qualtech Systems, Inc. (QSI) Rocky Hill, Connecticut

Stephen B. Johnson, Dependable System Technologies, LLC (DST), Westminster, Colorado and Jacobs ESSSA, Huntsville, Alabama

Craig Moore, National Aeronautics and Space Administration (NASA) Marshall Space Flight Center (MSFC)

***Abstract*—This paper describes the theory and considerations in the application of model-based techniques to assimilate information from disjoint knowledge sources for performing NASA's Fault Management (FM)-related activities using the TEAMS® toolset. FM consists of the operational mitigation of existing and impending spacecraft failures. NASA's FM directives have both design-phase and operational-phase goals. This paper highlights recent studies by QSI and DST of the capabilities required in the TEAMS® toolset for conducting FM activities with the aim of reducing operating costs, increasing autonomy, and conforming to time schedules. These studies use and extend the analytic capabilities of QSI's TEAMS® toolset to conduct a range of FM activities within a centralized platform.**

Keywords—FM design, architectural trade studies, multi-domain data integration, common cause failures (CCFs), Failure Effect Propagation Timing (FEPT), system health management (SHM).

I. INTRODUCTION

As science missions and human spaceflight missions are tasked with increasingly complex goals and have more pressure to reduce the overall operations costs while ensuring mission success, enhanced system autonomy is a critical component to cost reduction. Fault Management (FM) is one of the key components of system autonomy. FM consists of the operational mitigation of existing and impending failures. FM is implemented with spacecraft hardware, on-board autonomous software that controls the hardware, information and analytical redundancy, and ground-based software and task procedures. For human-crewed systems, the on-board crew can also perform task procedures. The ability to execute appropriate and timely mitigating actions as part of an FM system is thus a key enabler for satisfying complex mission goals, and for enhancing mission success.

NASA has invested significant effort and has developed a draft FM Handbook [1] to improve FM design, development, verification & validation, and operational processes. NASA's FM directives have both design-phase and operational-phase goals. The FM Handbook provides guidelines for realizing the design and operational goals with the aid of advanced Model-Based Systems Engineering (MBSE) software tools. During the design phase these tools should be able to model a system from the FM perspective, support design evaluation and validation activities, identify design shortcomings and inconsistencies, and aid FM design updates and revisions. During the operational phase, these tools should perform failure detection, fault diagnostics and prognostics; assess functional capabilities; provide information to support actionable FM decisions; facilitate optimal troubleshooting and maintenance; and assess probabilities of individual mission objective satisfaction and for overall mission success.

NASA uses a variety of tools to conduct its FM activities. These tools are varied and disjoint, and often require manual intervention to transfer data from the output of one tool to the input of another. This process is tedious and error-prone, and scales poorly for large, complex systems. Individual tools are often confined to the unique purpose for which they were designed. These tool-related issues hinder FM engineers from gaining insight into system-level design and characteristics that are key to transparency, verifiability and efficiency of implementing and testing FM. A central platform is needed that can (1) perform FM architecture trade studies of cost-effective FM design architectures and operations, (2) provide an efficient way to develop and test FM models and algorithms, (3) provide performance metrics of FM designs, (4) integrate data from multi-domain tools, (5) develop test suites automatically for verification & validation, and (6) provide visualization of FM design across the life cycle of a system.

This paper provides an overview of proposed capabilities in TEAMS® and the concomitant software tools to (1) capture diverse and disjoint data products and multi-domain modeling information into TEAMS® for standardizing FM techniques and processes, (2) improve the productivity of model (knowledge) creation and the FM design process, (3) conduct Architecture Trade Studies focusing on failure detection (including launch vehicle abort trigger) effectiveness with related sensor suite selection, and (4) introduce ancillary capabilities in TEAMS® such as assessment of Failure Effect Propagation Timing (FEPT) and Common Cause Failures (CCFs) to aid in analytical tasks.

The main objective of the efforts described in this paper is to position TEAMS® as the platform of choice for conducting many FM-related activities. Rather than replacing existing MBSE and Safety and Mission Assurance (S&MA) tools (SysML, FMECA, etc.), its purpose is to be a central platform to assimilate pertinent FM modeling information about a system from varied modeling sources. This would benefit NASA tremendously since the data and model information will be centralized, coherent and consistent, and therefore conducive to performing FM analyses.

The rest of the paper is organized as follows. Section II

describes our semantics-based multi-domain model capture and integration concept. Section III describes how TEAMS® can utilize the captured multi-domain model information to conduct various architecture trade studies. Section IV discusses various capabilities that are being, or need to be incorporated in TEAMS® to conduct these trade studies. Section V illustrates an example multi-domain model integration process from a systems engineering data source in Excel format, and a representative FM Architecture Trade study conducted by TEAMS® using the engineering data. The paper concludes with a summary in Section VI, acknowledgements in Section VII and references in Section VIII.

II. Semantic-Based Multi-Domain Model Capture

Many of NASA's current MBSE practices involve SysML [2] as the chief modeling language. Various plug-ins to import models from other sources, such as FMECA spreadsheets, have been developed within the framework of SysML authoring tools. However, SysML tools do not usually have an extensive modeling framework upon which to address FM activities and analyses that can provide information to meet needs of project managers and FM engineers early in design, or improve the efficiency of implementing and testing FM. Moreover, the models generated in SysML tools do not typically capture the intricate failure dependencies that exist among system components. For example, a fault in one component in a coupled system often creating cascades of failure effects impacting other components, thereby changing overall system health and reliability. A TEAMS®-based, system-level FM modeling platform overcomes this problem by translating the impact of component-level faults to subsystem or system-level metrics that take into account failure effect propagation in the coupled system.

A QSI-DST semantics-based approach seeks to integrate multi-domain data and models into the TEAMS® modeling framework. The approach (shown in Figure 1) leverages Eclipse Modeling Framework (EMF) [3] and uses a Model-driven approach to transform systems that are made up of different technologies.

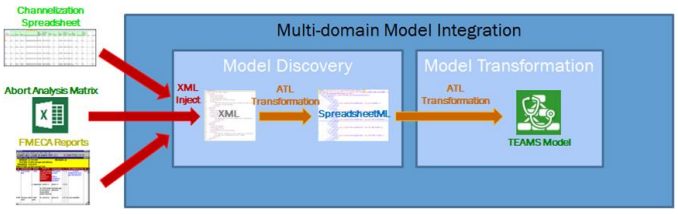

Figure 1: Multi-Domain Model Integration

The main steps involved in the transformation are:

- *Discover*: First, a metamodel that describes an existing legacy system is created. Then, based on the metamodel of the system representation, the underlying legacy model of the system is discovered.
- *Generate*: From the discovered model, a generic (domain-independent) Ecore model [4] is generated for viewing and editing.
- *Transform*: This step involves converting the generic model to the desired TEAMS® output format.

This approach involves engaging with various NASA systems engineering and FM modeling teams to identify system engineering specifications, requirements, parameters, etc. for creating the corresponding semantic meta-models from those repositories. Examples of domain models are:

- *Channelization Spreadsheet*: This document uses an Excel format, and depicts bus mapping, wiring information and hardware channelization. Using this as a basis of connections between various modules and submodules, a multi-signal TEAMS® model can be constructed. QSI already has a proprietary spreadsheet model format (dependency information) that is imported into TEAMS®. This capability can be enhanced to incorporate other spreadsheet sources.
- *Abort Analysis Matrix (AAM)*: This Excel spreadsheet contains the Mission & Fault Management (M&FM) group's model of Space Launch System (SLS) abort trigger (AT) effectiveness. It uses the Loss of Mission (LOM) scenarios provided by Probabilistic Risk Assessment (PRA) group and their associated probabilities, grouped by vehicle mission phase. Using this spreadsheet, the ATs (failure detections of conditions for which an abort response is necessary), which in TEAMS® parlance are Sensor Tests, can be imported into TEAMS® along with the detections, false-positive/false-negative properties, etc.
- *Fault Trees/FMECA Reports*: Fault trees and FMECA (Failure Modes, Effects, and Criticality Analysis) information can be captured in TEAMS® provided they can be exported into a standardized file format, such as Excel or XML, by the tools in which they are authored. NASA has several formats for these:
  - *SLS PRA Model (top down)*: The PRA fault tree model of the SLS is in SAPHIRE format and is created by the Safety and Mission Assurance (S&MA) PRA group.
  - *Element FMEAs (bottom up)*: Created by the S&MA Reliability Group, these engine specific Failure Mode and Effect Analysis (FMEA) documents pertain to Core Stage, Main Engine, Upper Stage, etc. of the SLS. The main goal is to capture common failure modes and correlations among these disparate FMEAs into an integrated TEAMS® model.
  - *Hazard Trees (top down)*: These are created by the S&MA Systems Safety group using tools such as CAFTA. The hazard tree contains causal relationships between intermediate and top-level effects.

Of particular interest are various input parameter spreadsheets (tables containing sensor properties, such as False Positives (FP), latency, etc.) for trade study of launch vehicle AT suite

selection [6]. A suitable sub-system model can be utilized for the aforementioned architecture trade studies with inputs from the parameter spreadsheets. Candidate models for these studies include a Spacecraft Propellant model, the SLS model, AMPS (AES (Advanced Exploration Systems) Modular Power System) model, and the CDS (Cascade Distillation System) model.

III. FM Architecture Trade-Studies

The main purpose of having multi-domain data captured in a TEAMS® model is to leverage its built-in analytic capabilities to quantitatively conduct FM architecture trade studies. NASA devises FM approaches, architectures, and tools for implementing and testing FM. As previously noted, the use of separate multi-domain modeling and analysis techniques can lead to expensive, disjoint and sometimes inconsistent analyses. Data integrity and consistency is needed between multi-domain tools. TEAMS®, being a Commercial Off-the-Shelf (COTS) product and already used by NASA to conduct various FM activities, is a natural fit to determine the completeness and appropriateness of FM designs and implementations. Examples of the FM architecture trade space studies currently conducted by NASA that can be assimilated into TEAMS® are described below.

A. LOC Risk Mitigation Criteria Using Abort Triggers

An AT, in the context of SLS, is the means by which the SLS detects a crew safety-related failure and sends a recommendation to the Orion vehicle (Orion consists of the Crew Module, and the supporting Service Module, and Launch Abort System) to initiate an abort response. TEAMS® software can apply quantitative criteria to assess the effectiveness of proposed ATs in order to select the most effective detection suite to protect the astronauts from catastrophic failure (e.g. Loss of Crew - LOC) of the SLS vehicle. The FM-related requirements for which effectiveness measures are needed include those for safing, abort, and redundancy management, and also for reliability, availability, and safety (RAS).

The metrics used derive from the theory of System Health Management (SHM), within which control theory can be extended to address FM, which is the operational aspect of SHM. See Chapter 1 of reference [9]. A natural extension of the various capability improvements described in this paper is to enhance and leverage TEAMS® to minimize and control the LOC likelihood via improved selection of a system's failure detection capability. Specifically, TEAMS® can compute the LOC risk reduction metric and the related AT Effectiveness (ATE) metrics that are related to the ability of a sensor suite to provide timely detection of crew-threatening failures, which in turn activates the relevant abort response for the crew to escape the launch vehicle hazard in various failure scenarios. The primary driver for computing the LOC risk mitigation ATE metrics will be built-in TEAMS® analytic capabilities, which span modeling, information interchange, and analytic computations. QSI leverages concepts and techniques described in the AIAA SciTech 2017 paper titled "FM Metrics and V&V" [7] to compute the ATE metrics.

Design engineers often use the FMECA analyses to identify potential system faults (failure modes), their probabilities of occurrence, their manifestation as functional failures (effects), monitoring mechanisms for making the effects visible, system-level implications in terms of safety, mission success, etc. PRA methodologies include logic models such as event trees and fault trees to identify, quantify and reason about risk. These models are scalable, include uncertainty in the risk assessment, and calculate the contribution of functional failures to the overall system risk. The current process of mapping FMEA to LOC/LOM end-states is done by manually examining the FMEA. This process is tedious and requires the examination of voluminous FMEA spreadsheets where the FMEA local, subsystem and system level effects are enumerated. In contrast, by capturing the FMEA spreadsheets and defined LOC/LOM events (effects) in the TEAMS® model, TEAMS® Designer can generate FMEA-based fault trees to support risk assessment that automatically traces from FMEA data to higher-level constructs such as PRA and Hazard fault trees. The fault tree computation exhaustively enumerates those FMEA initiating events that can account for a given end-state. Given the set of potential initiating events defined in the failure modes, probability splits between the classes of independent initiators can also be defined to support the logical definition of fault trees and in turn help determine (probabilistic) failure contribution to LOC/LOM events.

Both the default TEAMS® model and TEAMS® fault tree export rely on the use of failure mode modules in TEAMS® as initiating events (Figure 2). Additionally, the fault trees require the use of mission phase definition, effect nodes and AND nodes. Effect nodes in TEAMS® are defined to represent the end-states to which failure effects may propagate from the initiating event failure modes. Three types of effect nodes are defined in the models, corresponding to three effect levels: local, isolation_level and system_wide. AND nodes are used to represent redundancy. It is the modeler's responsibility to link the local effect nodes, isolation-level effect nodes, and AND nodes to the system-wide effect nodes. Disjunction occurs by default when multiple upstream links are input to an effect node – in this case, any one of the possible causes can lead to the top-level effect. Conjunction occurs by the use of AND nodes – in this case all of the possible causes need to occur to lead up to the top-level effect. In TEAMS®, a fault tree can be generated for each system-wide effect node. When the system-wide effect nodes correspond to LOC/LOM states, fault trees can be generated for each LOC/LOM scenario.

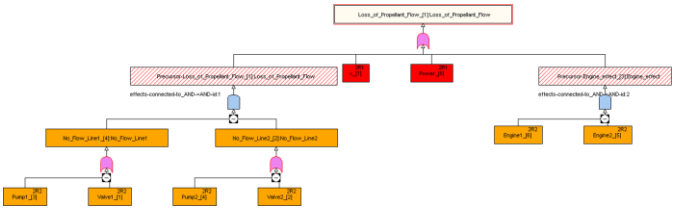

Figure 2: TEAMS® Fault Tree Analysis

Given a fault tree for a particular LOM-causing scenario (henceforth simply called a "LOM scenario"), a failure detection mechanism can be incorporated by placing appropriate sensors at the leaves of the fault tree to ensure that all paths up the tree are covered. These failure detection mechanisms can include timing information from the point that a failure occurs to the detection mechanisms, and subsequently the time to activate a response before the failure propagates to the end-effects (see Section IV.A - Failure Effect Propagation Timing (FEPT)). They may also include information about two or more detections existing along any given Fault Tree path, which means that more than one trigger can account for failures for a given LOM scenario.

TEAMS® can be employed to select an optimal AT / failure detection suite by utilizing the dependency information among systems/ subsystems/ components, failure detection, and state estimation metrics of sensors in detecting the failure conditions (namely, the "truth table" or "confusion matrix" metrics of True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN)). For the purpose of AT selection, the principal performance criteria for sensor allocation will be a "LOC Risk Mitigation" metric. This metric could be any criteria of relevance to the analyst such as detection effectiveness (fault detection probability), diagnostic effectiveness (fault isolation probability), etc. of the AT suite for the applicable failure scenarios. These failure scenario specific metrics are currently being incorporated in TEAMS®-Designer under the NASA Phase II "FM Metrics and V&V" (contract # NNX16CM10C).

The approach is elaborated in the following steps:

- NASA subject matter experts (SMEs) generate the "AT Tables" containing a library of ATs and their associated warning times—the amount of time provided between the detection time and the time of the end-effect that causes LOM or LOC), state estimation metrics (such as FP, FN, etc.), and information about potential redundant failure detections (primary vs. secondary triggers, etc.).
- Utilize the proposed multi-domain model integration capability (Section II) to import AT configuration files and the associated FMECA model.
- Import the sensor library and their associated properties including the state estimation metrics associated with the AT algorithms associated with the relevant sensors (such as FP, FN etc. of TEAMS® tests.), FEPT and redundant detection information from the AT Tables into TEAMS®.
- Import the top-level effects, mission phases, etc. from the AT Tables into TEAMS®, to form the building blocks of a FMECA model.
- Perform Fault Tree analysis in TEAMS® for each LOM scenario by generating cut sets and the initiating failure causes.
- Using the FM Metrics capabilities of TEAMS® Designer, generate the Confusion Matrix of the entire AT Suite for the LOM Failure Scenario (top-level effect).
- Using the FP/FN calculations for the AT suite, evaluate the risk mitigation criteria [6] in order to determine the suite of ATs that are most suitable for meeting the "LOC Risk Mitigation" criteria.

The implementation and demonstration of the aforementioned capability in TEAMS®-Designer was out of scope of this research paper. QSI and DST plan to demonstrate this feature in a future research effort.

B. Abort Trigger FP and FN Quantification with Sensor Data Qualification (SDQ)

On the SLS project, NASA has conducted trade studies on FP, FN quantification in the presence of SDQ mechanism in the analysis of ATs [8] related to LOC and LOM end-effects. One of the objectives for SLS is to determine the "value" of inclusion of SDQ, and in this regard two detection mechanism designs are compared, one with SDQ and one without. By comparing the FP, FN metrics between the two design architectures, NASA can determine how much benefit SDQ provides in detecting sensor failures and hence to determine whether certain SDQ algorithms should be included in the AT (failure detection) design. The trade study executes the following steps during its analysis:

- Incorporates probabilities of failure modes, such as electrical shorts, high voltage, etc., associated with failed-high (F2FS: failure-to-full-scale)/failed-low (F2Z: failure-to-zero)/failed-intermediate observations;
- Incorporates common-cause failures (redundant component failures due to common causes, i.e., cut sets of size 1 or single point failures);
- Uses SAPHIRE to compute the Fault Tree of events leading to the FP and FN of the ATs;
- Rolls up the probabilities caused by component and common-cause failures to calculate FP, FN of the AT; and
- Calculates the minimal cut sets of sizes up to 5 (risk drivers).

In this context, TEAMS® can leverage the built-in capabilities and concepts from the AIAA SciTech 2017 paper titled "FM Metrics and V&V" [7] to automate the SDQ study steps and generate AT FP/FN metrics as a special case of response effectiveness. This mechanism is elaborated in the following steps:

- Create a TEAMS® Model utilizing the proposed multi-domain model integration capability to import AT configuration (Excel) files and the associated FMECA model:
- Top level end-effects in TEAMS® would represent the overall effect due to occurrence of Failure to Zero (F2Z) and Failure to Full Scale (F2FS) (F2ZEffect, F2SEffect);
- Failure modes and their failure rates inside each component of the AT system will be gathered from FMECA documents;

- Next, the failure modes will be assigned "Functions" (F2Z, F2S, etc.) based on their contributions to the AT.
- TEAMS® AND nodes with a "threshold" can be used to specify *m*-out-of-*n* redundancy between the various components in the AT model.
- Simulate various failure scenarios (e.g. multiple sensor(s) going F2Z, etc.) and compute the end-effect (LOM, LOC) FP/FN metrics utilizing the methods described in the "FM Metrics and V&V" AIAA SciTech 2017 paper.
- TEAMS® Designer computes Fault Trees and Minimal Cut sets for the top-level Effect under different phases/operational modes, taking into account redundancies, and then rolls up probabilities of the implicated faults to the top-level end-effects.
- The SDQ mechanism can be considered as series of switches ("System Modes") that "switch out" certain failure modes from the model due to improved threshold classification. Apply appropriate mode changes to "switch in" the "SDQ mechanism" in the AT system, observe those top-level effect probabilities and their associated FP and FN reduction.
- Finally, TEAMS® will perform "Fault Tree Analysis" for the F2ZEffect, F2SEffect, etc. End-Effects with applicable "System Modes" to apply various SDQ configurations, as well as the "Mission Duration", to furnish the resulting "cut-sets" and their probabilities.

The ability in TEAMS® to perform these analyses shows that it can be an enabling platform to facilitate efficient and cost-effective FM design architectures and operations.

IV. TEAMS® TOOLSET ENHANCEMENTS

This section describes some of the TEAMS® Designer enhancements required to enable it to perform the architectural trade studies mentioned in Section III.

A. Failure Effect Propagation Timing (FEPT)

This step entails the incorporation of knowledge captured by building a FEPT table into the TEAMS® model. It intends to capture the intermediate times between a fault origination location and a failure detection location. Timing information is added to the links in a TEAMS® model. Such information is gathered from SMEs for each propagation path of interest. Critical faults must be detected, identified and acted upon within a specified time window to prevent potentially harmful ramifications.

For any FM Control Loop (FMCL), the FM analyst must assess the race condition between the failure effect propagation time (FEPT) to the "critical failure effect" (CFE) and the overall time latency of failure detection through the failure response. In general, the response function in the FMCL needs to complete before the FEPT to the critical effect. On SLS, the difference between the two is identified as the "Abortability Table Warning Time (ATWT)", which for the SLS-Orion integrated stack is defined as the difference between the occurrence of a large-scale explosion (or more generally, the directly crew-threatening failure effect) and when the Orion separates from the launch vehicle in an abort scenario. More generally, one desires the difference between the CFE time and the time to completion of the "critical failure response" (CFR). This needs to be greater than zero, where the units are those of time: CFE – CFR > 0.

Currently TEAMS®-Designer has a simplistic FEPT capability in that it allows for time to be associated with a node or an arc. There are drawbacks with this simple implementation. FEPTs can differ even on the same node or arc, depending on which failure effect it is. For example, a large propellant leak can in some cases propagate faster than a small leak. Also, different types of physics can be associated with a given node or arc, such as the propagation of electrons, which travel rapidly but also produce heat, which often propagates much more slowly. In TEAMS® this would be represented as different functions. Thus, timing effects must be associated with each relevant effect (function), not just one per node or arc. One way to account for variable timing delays along the same path (e.g. electrical property vs. thermal property) could be to attach the timing information to individual "Functions" detected by the outcomes of TEAMS® tests.

Timing effects are inherently statistical in nature, so that failure effect times should be represented as distributions with minima, modes, means, and maxima. Currently, TEAMS® is used primarily to account for the components along the Failure Effect Propagation Paths (FEPPs), and these must be accounted for in the FEPT analysis. FEPTs should ideally be modeled as function-dependent statistical distributions. Several distributions can be considered, depending on the application. These include common Gaussian and Poisson-like distributions with exponential characteristics, but also simple triangular distributions and bi-modal distributions. In practice on SLS, these statistical effects associated with individual scenarios are currently modeled as a triangular distribution. This has the advantage of requiring only three point estimate values for a worst, mode, and best value, from which a mean is easily calculated as the average of the three. This makes the estimation process simple, and given the need to estimate dozens or hundreds of these warning times for a complex system like SLS, simplicity is important.

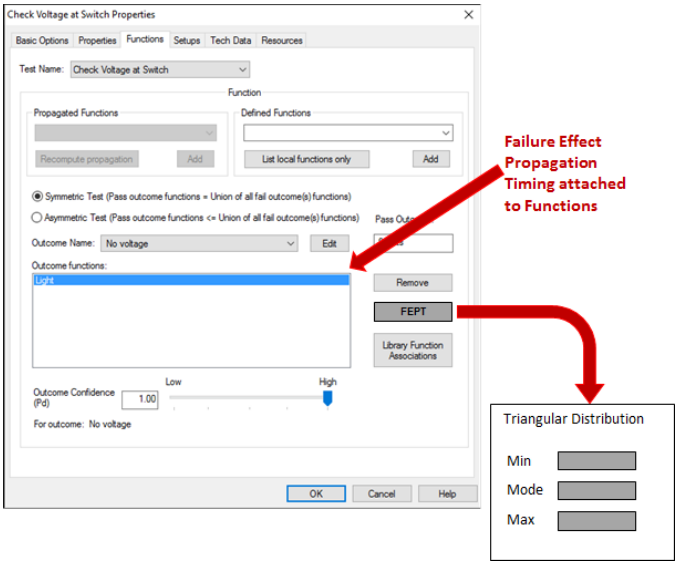

Figure 3: FEPT in TEAMS®

TEAMS®-Designer can be enhanced to associate timing with each relevant failure effect, not just one per node or arc. This is done by attaching the timing information to individual TEAMS® "Functions" detected by the outcomes of TEAMS® tests (see Figure 3). Moreover, the proposed user interface aims to capture the inherently statistical nature of timing effects by allowing the user to associate distributions to each FEPT. The interface would provide to the user the ability to specify the lower/upper bounds and the mode in the Triangular Distribution setting fields.

B. *Common Cause Failures (CCF)*

A key capability present in baseline studies undertaken by NASA to conduct FM architecture trade studies, and that TEAMS® currently lacks, is Common Cause Failures (CCFs) modeled across redundancies. CCFs are defined as the failure of multiple components, some of which could be part of the designed redundancy, due to shared identical failure modes such as a common design or manufacturing defect or from improper installation and maintenance. In redundant systems, it is very common for the system reliability rates to go lower than typical CCF rates, which are usually estimated at a blanket rate from 3% to 10% of component reliability values. Thus, CCF rates often dominate the system reliability estimates, as compared to random part failure rates. Being the dominant contributors to system unreliability, failing to model common cause failure means that system reliability estimates will be far more optimistic than warranted. Due to absence of CCFs in TEAMS®, there would be considerable mismatch in trade study analyses results provided by TEAMS® and those computed in the baseline studies by NASA. One key facet of CCFs are that when there is a failure of one of these components, the other common components' likelihood of failure needs to be adjusted dynamically while conducting reliability analyses as well as for FDIR related computations.

The NASA study to calculate the FP/FN for ATs accounted for Common Cause Failure (CCF) events in the SAPHIRE model of the FT. In that study, CCF events were modeled in the FT to account for the possible failure of AT components due to external causes. For example, multiple Flight Computers (FC) 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 support this capability, TEAMS® needs to provide a user interface to mark a set of components as part of CCFs. Furthermore, the interface needs to provide the user the ability to specify the coupling between the components of CCF sets such as common cause scaling factors. Possible methods to incorporate CCFs in TEAMS® analyses include CCF probability equations (Mosleh, Rasmuson, & Marshall, 1998) and associated alpha factor values (Atwood, Kelly, Marshall, Prawdzik, & Stetkar 1996).

V. Example Calculation

A. *Semantic-Based Multi-Domain Model Capture*

QSI implemented a rudimentary capability to import domain-independent model into TEAMS® to utilize its built-in analytic capabilities for quantitatively conducting various FM Architecture Trade Studies. Specifically, for the "LOC Risk Mitigation via selection of Abort Trigger Suite" Architecture Trade Study, QSI captured the Abort Analysis Matrix (AAM) (the AAM is a specific instantiation of an "AT Table" identified above) domain information, including mission phases, effects, Tests and FP/FN information. Based on the information contained in the AAM spreadsheet, QSI formulated the steps to enable TEAMS® to perform this study. Figure 4 shows the numbered steps, although a partial set, to incorporate the study into TEAMS®:

1. The defined LOM Failure Scenario from the "PRA Input" worksheet would be incorporated into the TEAMS® Model. Corresponding "Phases" will also be imported into the TEAMS® model. QSI developed a mechanism to import LOM Failure Scenarios (End Effects, Phases) from the "PRA Input" worksheet. Failure Modes defined for that scenario will have to come from the relevant Risk Model – could be FMECA, CAFTA or PRA – and their associations with the resulting End-Effects would be incorporated into TEAMS®.
2. Import the AT detections from the "MFM Input" worksheet as "Tests" into the TEAMS® model.
3. The FN (%) and FP (%) values would be directly imported for each Test. Since FP/FN for an AT are specified on a per scenario basis, TEAMS® may need to support specifying Test FP/FN values on a per function basis.
4. The ATWT Times for each Test will be translated into FEPT (see Section IV.A) for the detected "Function" inside that Test.

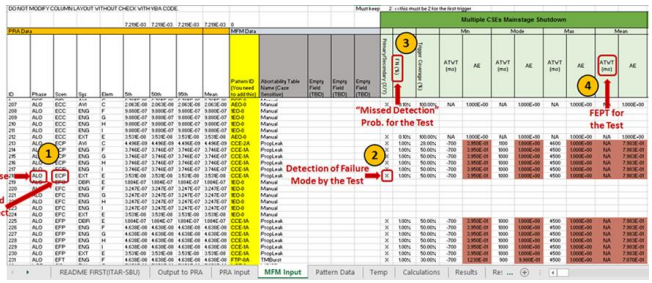

Figure 4: LOC Risk Mitigation using Abort Trigger in TEAMS®

The resulting TEAMS® model from the aforementioned exercise is shown in Figure 5.

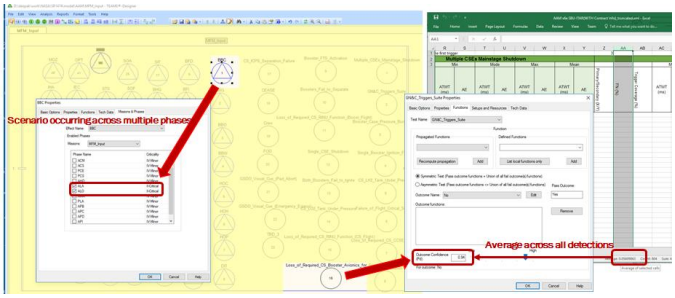

Figure 5: Translated TEAMS® Model from the AAM

In the figure above, the ATs are imported in TEAMS® Designer as Tests. As mentioned before, each AT can have a different FP/FN value in different scenarios. Since TEAMS® Designer currently does not have the facility to capture multiple FP/FN values for each test outcome, we simplified the logic by taking an average over all the scenarios to assign a single value of FP/FN for a test outcome. Each scenario was imported as a TEAMS® Designer Effect (This works because a scenario defines a specific failure effect as its "essential feature"; this effect usually has multiple causes.) with the corresponding Phase attached to it and assigned a default Criticality of "Critical". When Phase Criticality information is available, these fields will be updated. Since each scenario in the AAM appears across multiple phases, each of those phases are associated with the Effect in TEAMS® Designer.

B. Abort Trigger FP and FN Quantification with SDQ Architecture Trade Study

For the "Abort Trigger FP and FN Quantification with SDQ" study, QSI created an equivalent TEAMS® model of the AT and conducted trade study analyses in TEAMS® similar to the one in the publication [8]. This FM trade study quantifies the benefit of having the SDQ processing module on the detection process for ATs. Figure 6 shows a notional approach with numbered steps describing the process to incorporate the study into TEAMS®. The numbered steps are described below:

1. Based on the schematics of the Abort Trigger (AT) illustrated in the publication, create an equivalent model in TEAMS® Designer comprising of "Power System (PS)", "Sensor Electronics (SE)", etc. components. If models for the AT already exist, employ the "Multi-domain Model Integration" techniques to import the TEAMS® model.
2. Augment the TEAMS® model of the AT with the SDQ module in the form of component blocks and switching mechanisms ("Switch Modes"). This will enable switching in and out of various SDQ blocks associated with various AT hardware configurations.
3. Add "Failure Modes" associated with each block of the AT in the corresponding TEAMS® Components. Use published Mean Time To Failure (MTTFs) numbers. SDQ blocks can also have their own Failure Modes.
4. Assign "Functions" (F2Z, F2S, etc.) to each Failure Mode based on their contributions to the AT. Insert top level "Tests/Effects" detecting the F2Z and F2S Functions (e.g. F2ZEffect, F2SEffect, etc.) in the TEAMS® model.
5. Insert "AND Nodes" between the various components in the AT model. The "AND Node" "Thresholds" will specify the M-out-of-N fault tolerance of each sub-system.
6. Perform "Fault Tree Analysis" in TEAMS® for the F2ZEffect, F2SEffect, etc. End-Effects with applicable "System Modes" to apply various SDQ configurations, as well as the "Mission Duration", to furnish the resulting "cut-sets" and their probabilities.

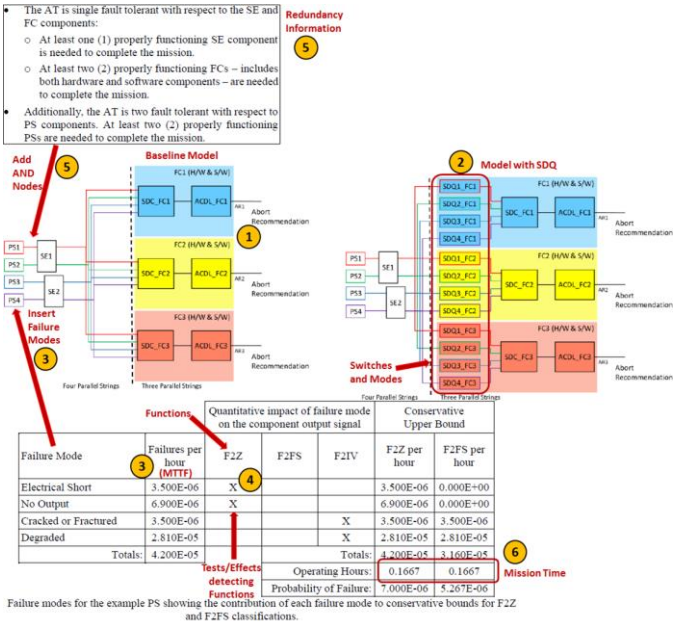

Figure 6: AT FP/FN Quantification using SDQ in TEAMS®

Based on the schematics of the AT illustrated in the publication and the approach mentioned in Section III.B, QSI created an equivalent model in TEAMS® Designer comprising of "Power System (PS)", "Sensor Electronics (SE)", etc. components. QSI also augmented the TEAMS® model of the AT with the SDQ module in the form of component blocks and switching mechanisms ("Switch Modes"). This will enable switching in and out of various SDQ blocks associated

with various AT hardware configurations. The TEAMS® model of the AT is shown in Figure 7.

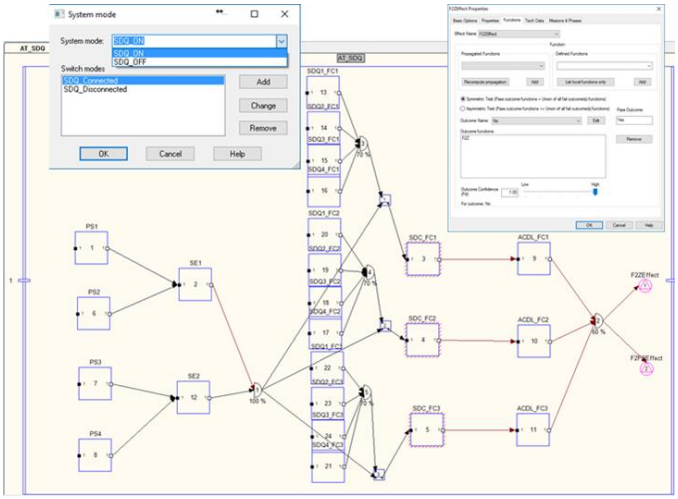

Figure 7: TEAMS® Model of the AT

There are two top level Effects that detect the F2Z and F2S Functions. The Failure Modes and their Failure Rates inside the AT components are assigned from the study (Figure 8).

Failure Mode	Failures per hour	Quantitative impact of failure mode on the component output signal: F2Z	F2FS	F2IV	Conservative Upper Bound: 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

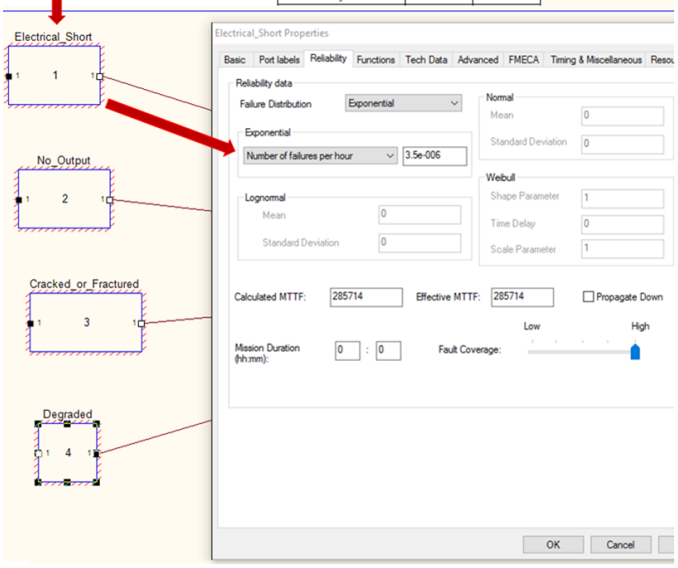

Figure 8: Assigning Failure Rates in the AT TEAMS® Model

Failure Modes are assigned "Functions" (F2Z, F2S, etc.) based on the component output signals and their contributions to the AT as defined in the study (Figure 9).

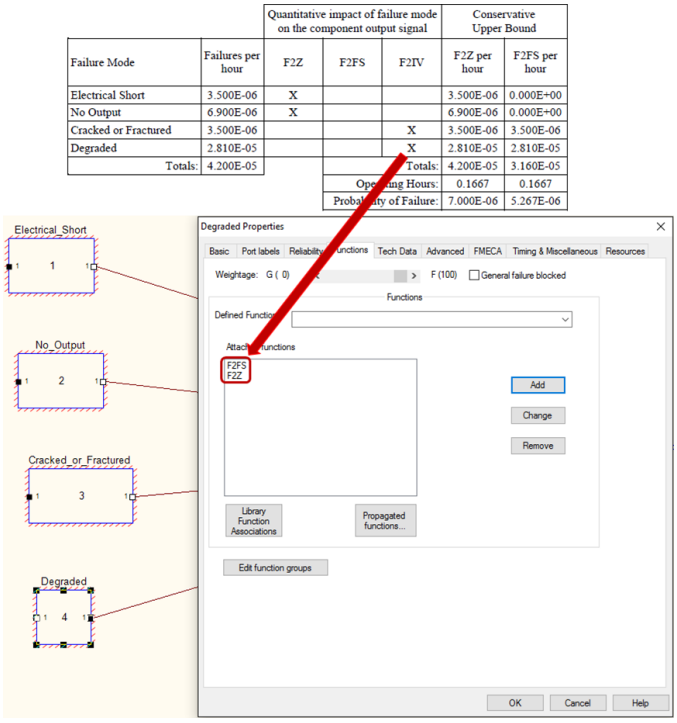

Figure 9: Assigning Functions in the AT TEAMS® Model

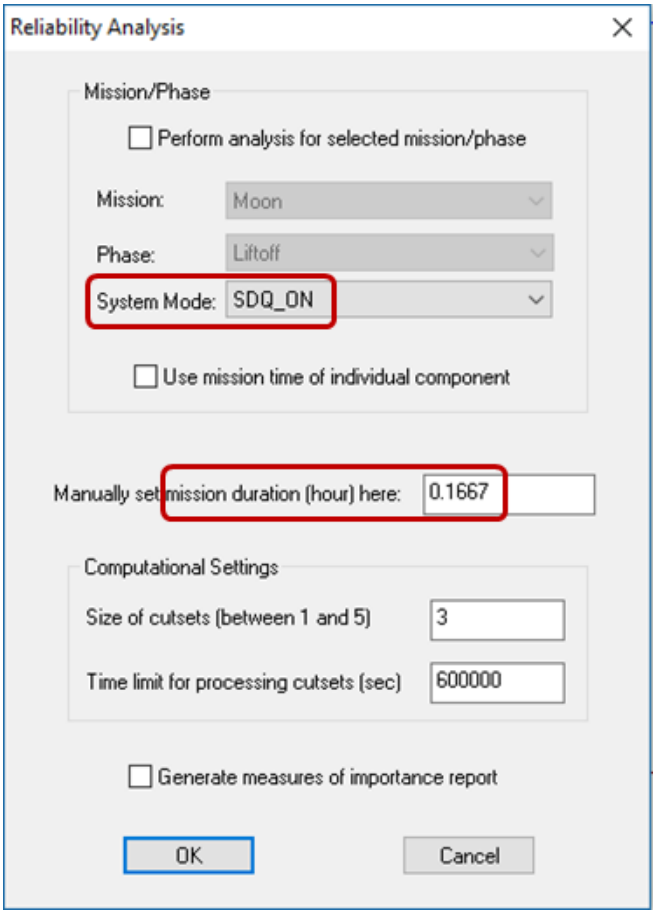

Figure 10: Performing Fault Tree Analysis for the AT Model

The results from TEAMS® Fault Tree Analysis are shown

below:

- The probability of occurrence of F2ZEffect (FP):
  - With SDQ OFF = 8.46E-10 (cutset size 2) + 6.22E-21 (cutset size 3)
  - With SDQ ON = 6.46E-10 (cutset size 2)
- The probability of occurrence of F2FSEffect (FN):
  - With SDQ OFF = 7.55E-10 (cutset size 2) + 3.66E-16 (cutset size 3)
  - With SDQ ON = 5.67E-10 (cutset size 2)
- Hence, the net benefit of having SDQ
  - For mitigating F2ZEffect (FP) = 23.64%
  - For mitigating F2FSEffect (FN) = 24.9%

All of these calculations are performed with generic, not actual SLS numbers. The lower overall probabilities for the F2ZEffect and F2FSEffect in TEAMS® compared to the study are possibly due to absence of CCFs, which are known to contribute significantly to the likelihoods of the FP and FN occurrences in the AT. The percentage benefit computed in TEAMS® was roughly double that of the study but of the same order of magnitude.

Future exercises in this study will incorporate alternate SDQ mechanisms that can be modeled using TEAMS® configuration for the trade space study.

VI. Conclusion

This paper describes ongoing work to implement FM quantification techniques in TEAMS® using metrics derived from the theory of SHM and FM, and using genericized SLS data and methods. The results were validated by comparison to actual SLS results, but again using genericized data. QSI was able to capture the domain knowledge from the AAM spreadsheet into a sparse but representative TEAMS® model. The TEAMS® analysis results from the AT FP and FN Quantification with SDQ Architecture Trade Study are in line with the ones from the NASA study. The comparison demonstrates that the methods being developed in TEAMS® generate similar, but not identical results to the actual calculations on SLS, with the primary difference likely being from TEAMS® not yet having the CCF modeling capability. This is a crucial capability for assessment of redundant systems that needs to be incorporated in TEAMS®. Some of the FM Architecture Trade studies identified in Section III such as the "AT Selection for LOC Risk Mitigation" were out of the scope and hence were not included in this paper.

VII. Acknowledgment

Some of the work that led to this paper was performed under NASA Small Business Innovative Research (SBIR) contracts NNX15CM31P, and NNX16CM10C.

QSI-DST would like to acknowledge Craig Moore for continued support during this study, and Yohon Lo for providing data formats for PRA and FMEAs.

VIII. References

[1] Fault Management Handbook, NASA-HDBK-1002, Draft 2, April 12, 2012, National Aeronautics and Space Administration, Washington, DC.

[2] SysML: Online: http://www.omgsysml.org/

[3] Eclipse Modeling Framework: Online: https://eclipse.org/modeling/emf/

[4] ECore: Online: https://en.wikipedia.org/wiki/Eclipse_Modeling_Framework#Ecore

[5] CAFTA: Online: http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001015514

[6] Lo, Yunnhon, Stephen B. Johnson, and Jonathan Breckenridge, "Application of Fault Management Theory to the Quantitative Selection of a Launch Vehicle Abort Trigger Suite," IEEE PHM Conference, Spokane, WA, June 2014.

[7] Stephen Johnson, Sudipto Ghoshal, Deepak Haste, "Fault Management Metrics", AIAA SciTech 2017, Grapevine, Texas, 9-13 January 2017.

[8] Abort Trigger False Positive and False Negative Analysis Methodology for Threshold-based Abort Detection, Kevin J. Melcher, José A. Cruz, Stephen B. Johnson, and Yunnhon Lo, PHM Society Conference 2015, Coronado, California, 18-24 October 2015.

[9] Johnson, Stephen B., Thomas J. Gormley, Seth S. Kessler, Charles Mott, Ann Patterson-Hine, Karl M. Reichard, Philip A. Scandura, Jr., eds. *System Health Management: with Aerospace Applications* (Chichester, United Kingdom: John Wiley United Kingdom, 2011).