

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

Authors: Deepak Haste, Sudipto Ghoshal, QSI
Stephen B. Johnson, DST
Craig Moore, NASA MSFC

AIAA SciTech: Jan 09, 2018

Presenter: Dr. Stephen B. Johnson, DST



Deepak Haste, Sudipto Ghoshal
Qualtech Systems Inc.
100 Corporate Place Suite 220,
Rocky Hill, CT 06067

<http://www.teamqsi.com>

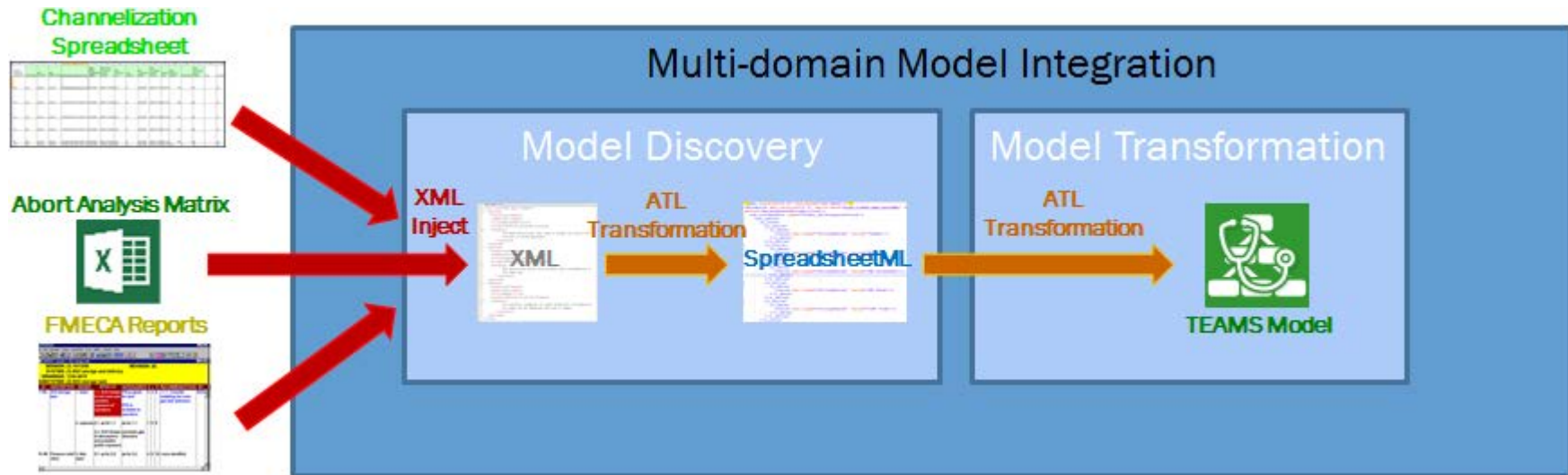
Stephen B. Johnson
Dependable System
Technologies, LLC
Westminster, CO 80234
& Jacobs ESSSA, Huntsville,
AL 35812

Craig Moore
NASA Marshall Space Flight Center
Huntsville, AL 35812

The Shortest Path to Uptime

- ∞ NASA uses a variety of tools to conduct its Fault Management (FM) activities crucial to ensuring that a system achieves mission goals while functioning within the tolerable limits
 - However, 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.
 - This prevents SHM engineers from gaining insight into the overall system level design and characteristics that are the key to transparency, verifiability and efficiency of implementing and testing FM
- ∞ There is a need for an FM Modeling and Analysis Tool that can
 - Integrate data from multi-domain tools
 - Perform FM architecture trade studies of cost-effective FM design architectures and operations
- ∞ Employing SHM/FM metrics in Commercial Off-the-Shelf (COTS) software such as TEAMS[®] often saves time and money
 - TEAMS[®] Toolset is already being used in several NASA programs and projects for SHM/FM-related purposes.

- ∞ **Capture diverse and disjoint data products and multi-domain modeling information into TEAMS[®] for standardizing FM Techniques and Processes**
 - Fault Management Requirements: “Multi-discipline FM Interoperation”
 - ✓ TEAMS[®] provides a common modeling framework in which complementary information is fused into a system-wide model and “standardization of data products, techniques and analyses” related to FM
 - Integrate multi-domain models/data from various sources into a central TEAMS[®] model of a system.
 - ✓ Semantics-based model-driven technique to discover legacy systems, generate models from the source systems, and aggregate and translate models into TEAMS[®] format.
- ∞ **Conduct Architecture Trade Studies focusing on failure detection (abort trigger) effectiveness with related sensor suite selection**
 - Enable NASA FM engineers to study designs related to sensor implication specifically for improving failure detection (e.g. abort triggers) effectiveness
 - Transition the process from a loosely coupled Excel based and disparate analytic tools into a central TEAMS[®] platform utilizing its built-in analytic capabilities
- ∞ **Capabilities in TEAMS[®] to support the main tasks such as assessment of Failure Effect Propagation timing (FEPT)**
 - To account for the time from fault initiation until detection, and from detection until it affects the end-goal (effect)



- ☞ Utilize TEAMS[®] for conducting extensive Fault Management (FM) activities
 - Leverage NASA's existing Systems Engineering (SE) sources as the basis for the TEAMS[®] models
 - Model-driven approach
- ☞ Integrate multi-domain data and models into the TEAMS[®] modeling framework using modern model-discovery/transformation/generation methods such as MoDisco.
- ☞ The main steps involved in the multi-domain integration are:
 - Discover: 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) model is generated for viewing and editing.
 - Transform: This step involves converting the generic model to the desired TEAMS[®] output format.

- ∞ **Sources of NASA model repositories for multi-domain integration**
 - Channelization Spreadsheets - Documents created by the JSC group in Excel format, showing bus mapping, wiring information and hardware channelization.
 - Abort Analysis Matrix (AAM) - Contains the Mission & Fault Management (M&FM) group's model of Space Launch System (SLS) abort trigger (AT) effectiveness
 - FMEA and Fault Trees from NASA
 - ✓ *SLS PRA Model (top down)*: The Probabilistic Risk Assessment (PRA) fault tree model of the Space Launch System (SLS) is in SAPHIRE format and is created by the S&MA group.
 - ✓ *Element FMEAs (bottom up)*: Created by the Reliability Group, these engine specific Failure Mode and Effect Analysis (FMEA) documents pertain to Core Stage, Main Engine, Upper Stage, etc. The FMEAs for various stages may come from different vendors and could potentially differ in format. The aim 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 Systems Safety group using tools such as CAFTA. The hazard tree mainly has causal relationships between intermediate and top level effects.
- ∞ **Example Discovery and Transformation from an Excel workbook containing Abort Analysis Matrices into TEAMS[®] model entities and analyses.**
 - Model Discovery – XML Injector using XML metamodels injects Excel file into XML format.
 - Model Translation/Transformation
 - ✓ First transformation is based on a simplified subset of Microsoft's SpreadsheetML metamodel used to import/export Excel workbook's data to a SpreadsheetML format.
 - ✓ Second transformation is from SpreadsheetML to TEAMS XML format

- ∞ **NASA devises FM approaches, architectures, and tools for implementing and testing FM.**
 - However, the use of separate, multi-domain modeling and analysis techniques can lead to expensive, disjoint and sometimes inconsistent analyses.
 - Leverage built-in analytic capabilities of TEAMS[®] to quantitatively conduct FM architecture trade studies.
- ∞ **Two of the FM architecture trade space studies currently conducted by NASA can be assimilated into TEAMS[®] utilizing its analytic capabilities**
 - LOC Risk Mitigation Criteria Using appropriate Abort Trigger Suite
 - ✓ Abort Trigger “detects” a crew safety-related anomaly and sends recommendation to the Multi-Purpose Crew Vehicle (MPCV) to initiate an abort response
 - ✓ TEAMS[®] software can apply quantitative criteria to assess the effectiveness of Abort Triggers to select the most effective sensor (Abort Trigger) suite
 - Abort Trigger FP and FN Quantification with Sensor Data Qualification (SDQ)
 - ✓ Effect of SDQ mechanism on False Positive/False Negative metrics of Abort Trigger
 - ✓ Leverage “FM Metrics” capability for computing FD/FI Effectiveness for LOC/LOM end effects.
 - The two trade studies will rely on importing the relevant sensor library, associated parameter, timing and redundancy spreadsheets, FMECA, etc. into TEAMS[®]
- ∞ **Apply the multi-domain model integration process to perform this assimilation of relevant information into TEAMS[®] for the trade study**
 - Develop appropriate Discoverers and Transformers for model discovery and model understanding for usage in TEAMS[®]

FM Architecture Trade Studies – LOC Risk Mitigation using Abort Triggers



The Shortest Path to Uptime

∞ LOC Risk Mitigation via selection of Abort Trigger Suite

- An Abort Trigger is the means by which the SLS detects a crew safety-related failure and sends a recommendation to the Orion vehicle to initiate an abort response.
- Most effective detection suite to protect astronauts from catastrophic effects (e.g. Loss of Crew – LOC) of failures in the SLS vehicle.
- Typically, failures in the system are identified and quantified using Probabilistic Risk Assessment (PRA) methodologies and FMEA analyses.
- Current process of mapping FMEA to end-states (LOC/LOM) is manual
 - ✓ Involves cross-referencing voluminous FMEA spreadsheets
- Utilize TEAMS[®] fault trees to enumerate initiating events (failures) and their probabilistic contribution to the end-states (effects)

FM Architecture Trade Studies – LOC Risk Mitigation using Abort Triggers



The Shortest Path to Uptime

∞ LOC Risk Mitigation via selection of Abort Trigger Suite (contd.)

- Approach utilizing TEAMS[®] to assess the effectiveness of the ATs in order to select the most effective detection suite
 - ✓ NASA subject matter experts (SMEs) generate the “AT Tables” containing a library of ATs and their associated warning times, state estimation metrics (such as FP, FN, etc.), and information about potential redundant failure detections (primary vs. secondary triggers, etc.).
 - ✓ Utilize the multi-domain model integration capability 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 in order to determine the suite of ATs that are most suitable for meeting the “LOC Risk Mitigation” criteria
 - Any relevant criteria such as detection effectiveness (fault detection probability), diagnostic effectiveness (fault isolation probability), etc. of the AT suite for the applicable failure scenarios.

FM Architecture Trade Studies – LOC Risk Mitigation using Abort Triggers



The Shortest Path to Uptime

DO NOT MODIFY COLUMN LAYOUT WITHOUT CHECK WITH VBA CODE. Must keep 2 << this must be 2 for the first trigger

PRA Data										MFM Data										Multiple CSEs Mainstage Shutdown									
				7.219E-03	7.219E-03	7.219E-03	7.219E-03	0						Primary/Secondary (X/N)	Trigger Coverage (%)	ATWT (ms)	AE	ATWT (ms)	AE	ATWT (ms)	AE	ATWT (ms)	AE	ATWT (ms)	AE				
ID	Phase	Scen	Sys	Elem	5th	50th	95th	Mean	Pattern ID (You need to add this)	Abortability Table Name (Case Sensitive)	Empty Field (TBD)	Empty Field (TBD)	Empty Field (TBD)																
207	ALO	ECC	AVI	C	2.063E-08	2.063E-08	2.063E-08	2.063E-08	AEO-0	Manual				X	0.10%	100.00%	NA	1.000E+00	NA	1.000E+00	NA	1.000E+00	NA	1.000E+00	NA	1.000E+00			
208	ALO	ECC	ENG	F	9.880E-07	9.880E-07	9.880E-07	9.880E-07	IED-0	Manual																			
209	ALO	ECC	ENG	G	9.880E-07	9.880E-07	9.880E-07	9.880E-07	IED-0	Manual																			
210	ALO	ECC	ENG	H	9.880E-07	9.880E-07	9.880E-07	9.880E-07	IED-0	Manual																			
211	ALO	ECC	ENG	I	9.880E-07	9.880E-07	9.880E-07	9.880E-07	IED-0	Manual																			
212	ALO	ECC	EXT	E	3.531E-08	3.531E-08	3.531E-08	3.531E-08	AEO-0	Manual				X	0.10%	100.00%	NA	1.000E+00	NA	1.000E+00	NA	1.000E+00	NA	1.000E+00	NA	1.000E+00			
213	ALO	ECP	AVI	C	4.496E-09	4.496E-09	4.496E-09	4.496E-09	CCE-2A	PropLeak				X	1.00%	28.00%	-700	3.950E-01	1100	1.000E+00	4600	1.000E+00	NA	7.983E-01					
214	ALO	ECP	ENG	F	3.746E-07	3.746E-07	3.746E-07	3.746E-07	CCE-1A	PropLeak				X	1.00%	50.00%	-700	3.950E-01	1000	1.000E+00	4500	1.000E+00	NA	7.983E-01					
215	ALO	ECP	ENG	G	3.746E-07	3.746E-07	3.746E-07	3.746E-07	CCE-1A	PropLeak				X	1.00%	50.00%	-700	3.950E-01	1000	1.000E+00	4500	1.000E+00	NA	7.983E-01					
216	ALO	ECP	ENG	H	3.746E-07	3.746E-07	3.746E-07	3.746E-07	CCE-1A	PropLeak				X	1.00%	50.00%	-700	3.950E-01	1000	1.000E+00	4500	1.000E+00	NA	7.983E-01					
217	ALO	ECP	ENG	I	3.746E-07	3.746E-07	3.746E-07	3.746E-07	CCE-1A	PropLeak				X	1.00%	50.00%	-700	3.950E-01	1000	1.000E+00	4500	1.000E+00	NA	7.983E-01					
218	ALO	ECP	EXT	E	3.531E-08	3.531E-08	3.531E-08	3.531E-08	CCE-1A	PropLeak				X	1.00%	50.00%	-700	3.950E-01	1000	1.000E+00	4500	1.000E+00	NA	7.983E-01					
219	ALO	EFC	DBR	E	1.884E-07	1.884E-07	1.884E-07	1.884E-07	IED-0	Manual																			
220	ALO	EFC	ENG	F	3.247E-07	3.247E-07	3.247E-07	3.247E-07	IED-0	Manual																			
221	ALO	EFC	ENG	G	3.247E-07	3.247E-07	3.247E-07	3.247E-07	IED-0	Manual																			
222	ALO	EFC	ENG	H	3.247E-07	3.247E-07	3.247E-07	3.247E-07	IED-0	Manual																			
223	ALO	EFC	ENG	I	3.247E-07	3.247E-07	3.247E-07	3.247E-07	IED-0	Manual																			
224	ALO	EFC	EXT	E	3.531E-08	3.531E-08	3.531E-08	3.531E-08	IED-0	Manual																			
225	ALO	EFF	DBR	E	1.884E-07	1.884E-07	1.884E-07	1.884E-07	CCE-1A	PropLeak				X	1.00%	50.00%	-700	3.950E-01	1000	1.000E+00	4500	1.000E+00	NA	7.983E-01					
226	ALO	EFF	ENG	F	4.638E-08	4.638E-08	4.638E-08	4.638E-08	CCE-1A	PropLeak				X	1.00%	50.00%	-700	3.950E-01	1000	1.000E+00	4500	1.000E+00	NA	7.983E-01					
227	ALO	EFF	ENG	G	4.638E-08	4.638E-08	4.638E-08	4.638E-08	CCE-1A	PropLeak				X	1.00%	50.00%	-700	3.950E-01	1000	1.000E+00	4500	1.000E+00	NA	7.983E-01					
228	ALO	EFF	ENG	H	4.638E-08	4.638E-08	4.638E-08	4.638E-08	CCE-1A	PropLeak				X	1.00%	50.00%	-700	3.950E-01	1000	1.000E+00	4500	1.000E+00	NA	7.983E-01					
229	ALO	EFF	ENG	I	4.638E-08	4.638E-08	4.638E-08	4.638E-08	CCE-1A	PropLeak				X	1.00%	50.00%	-700	3.950E-01	1000	1.000E+00	4500	1.000E+00	NA	7.983E-01					
230	ALO	EFF	EXT	E	3.531E-08	3.531E-08	3.531E-08	3.531E-08	CCE-1A	PropLeak				X	1.00%	50.00%	-700	3.950E-01	1000	1.000E+00	4500	1.000E+00	NA	7.983E-01					
231	ALO	EFT	ENG	F	4.638E-08	4.638E-08	4.638E-08	4.638E-08	FTP-0A	TMburst				X	1.00%	30.00%	-700	1.230E-01	900	3.980E-01	4500	1.000E+00	NA	7.070E-01					

Phase →
End Effect →

3
FN (%)
"Missed Detection"
Prob. for the Test

2
Detection of Failure
Mode by the Test

4
ATWT (ms)
FEPT for the Test

LOC Risk Mitigation via selection of Abort Trigger Suite (contd.)

1. Incorporate defined LOM Failure Scenarios (End Effects) from the "PRA Input" worksheet into the TEAMS[®] Model. Import corresponding "Phases" into the TEAMS[®] model. Failure Modes defined for the scenarios (end effects) will be imported from relevant Risk Model e.g. FMECA, CAFTA or PRA.
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 for the detected "Function" inside that Test.

FM Architecture Trade Studies – LOC Risk Mitigation using Abort Triggers



The Shortest Path to Uptime

Scenario occurring across multiple phases

Average across all detections

Outcome Confidence (Pd) 0.94

Average of selected cells

☞ LOC Risk Mitigation via selection of Abort Trigger Suite (contd.)

- Importing Tests and Effects
 - ✓ Effects (and associated Phases) were imported from the Failure Scenarios
 - ✓ Failure Modes will be imported from FMEAs and connected to the tests

∞ Abort Trigger FP and FN Quantification with SDQ

- Study quantifies the benefit of having the Sensor Data Qualification (SDQ) processing module on the detection process for Abort Triggers
- 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).

FM Architecture Trade Studies – Abort Trigger FP and FN Quantification



The Shortest Path to Uptime

∞ Abort Trigger FP and FN Quantification with SDQ (contd.)

- Approach leveraging TEAMS®
 - ✓ 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.
 - ✓ Assign “Functions” (F2Z, F2S, etc.) to Failure Modes 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,
 - ✓ 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.
 - Observe the top-level effect probabilities and their associated FP and FN reduction.

FM Architecture Trade Studies – Abort Trigger FP and FN Quantification

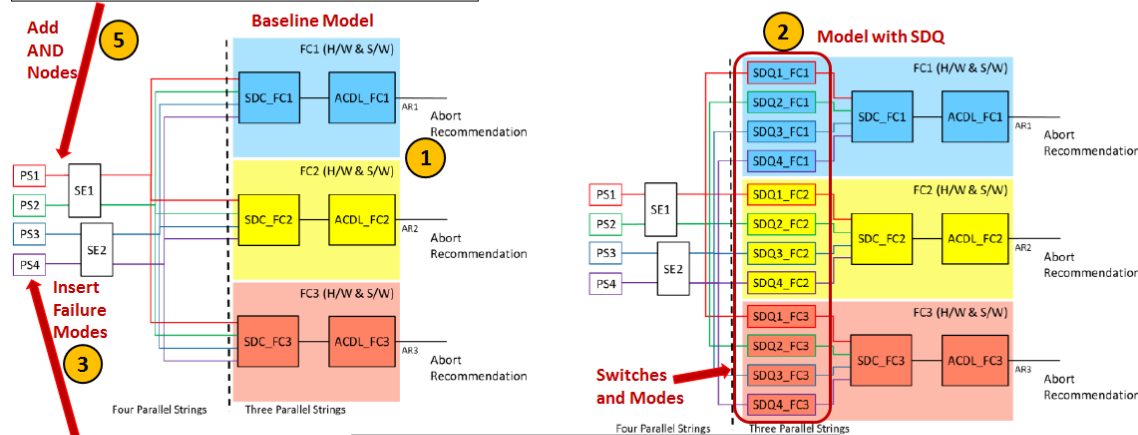
The Shortest Path to Uptime

Abort Trigger FP and FN Quantification with SDQ (contd.)

➤ Numbered steps in the next slide

- 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.

Redundancy Information
5



Failure Mode	Failures per hour (MTTF)	Functions			Quantitative impact of failure mode on the component output signal		Conservative Upper Bound	
		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	

Tests/Effects detecting Functions

Mission Time

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

FM Architecture Trade Studies – Abort Trigger FP and FN Quantification



The Shortest Path to Uptime

∞ Abort Trigger FP and FN Quantification with SDQ (contd.)

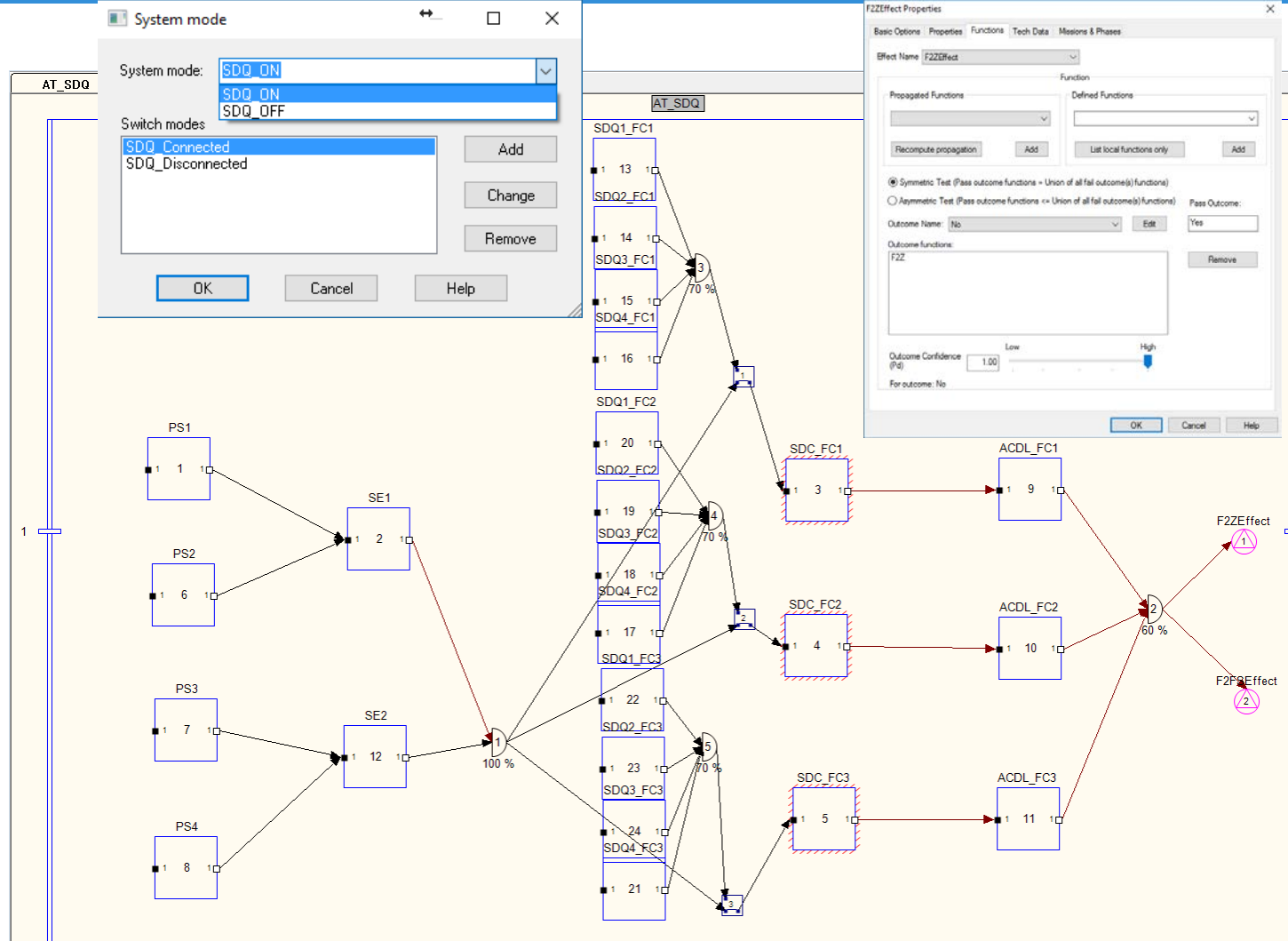
1. Create a TEAMS[®] model from the AT schematics, comprising of “Power System (PS)”, “Sensor Electronics (SE)”, etc. components. If models for the AT exist, use “Multi-domain Model Integration” techniques to create the TEAMS[®] model.
2. Augment the AT TEAMS[®] model with SDQ component blocks, and switching mechanisms (“Switch Modes”) to enable/disable SDQ blocks associated with various AT hardware configurations.
3. Add “Failure Modes” of AT components in the TEAMS[®] model. Use published Mean Time To Failure (MTTFs) numbers. SDQ blocks can have their own Failure Modes.
4. Add “Functions” (F2Z, F2S, etc.) to Failure Modes based on their contributions to the AT. Insert top level “Tests/Effects” detecting the F2Z and F2S Functions (e.g. F2ZEffect, F2SEffect, etc.).
5. Insert “AND Nodes” with “Thresholds” to specify the M-out-of-N fault tolerance.
6. Generate “Fault Trees” for F2ZEffect, F2SEffect, etc. End-Effects and for given “Mission Duration”, with applicable “System Modes” for various SDQ configurations, to get the resulting “cut-sets” and their probabilities.

FM Architecture Trade Studies – Abort Trigger FP and FN Quantification

The Shortest Path to Uptime

Abort Trigger FP and FN Quantification with SDQ (contd.)

- Model of the Abort Trigger comprising of “Power System (PS)”, “Sensor Electronics (SE)”, components.
- ✓ SDQ switched in and out with the use of System Modes
- ✓ AND Nodes specify M-out-of-N fault tolerance of each sub-system.
- ✓ Top level Effects detect the F2Z and F2S Functions



FM Architecture Trade Studies – Abort Trigger FP and FN Quantification



The Shortest Path to Uptime

Abort Trigger FP and FN Quantification with SDQ (contd.)

- Failure Modes and their Failure Rates assigned from the literature

Failure Mode	Failures per hour	Quantitative impact of failure mode on the component output signal			Conservative Upper Bound	
		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	3.160E-05
					Operating Hours:	0.1667
					Probability of Failure:	7.000E-06

The screenshot shows the 'Electrical_Short Properties' dialog box in the SDQ software. The 'Reliability data' section is active, showing an 'Exponential' failure distribution with a 'Number of failures per hour' set to 3.5e-006. The 'Calculated MTTF' and 'Effective MTTF' are both 285714. The 'Mission Duration' is set to 0:0. The 'Fault Coverage' slider is positioned towards the 'High' end. On the left, a diagram shows four failure modes: 'Electrical_Short' (1), 'No_Output' (2), 'Cracked_or_Fractured' (3), and 'Degraded' (4), with red arrows pointing from the table above to their respective boxes.

FM Architecture Trade Studies – Abort Trigger FP and FN Quantification

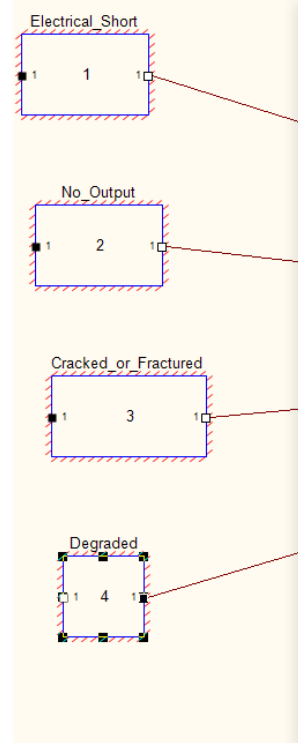


The Shortest Path to Uptime

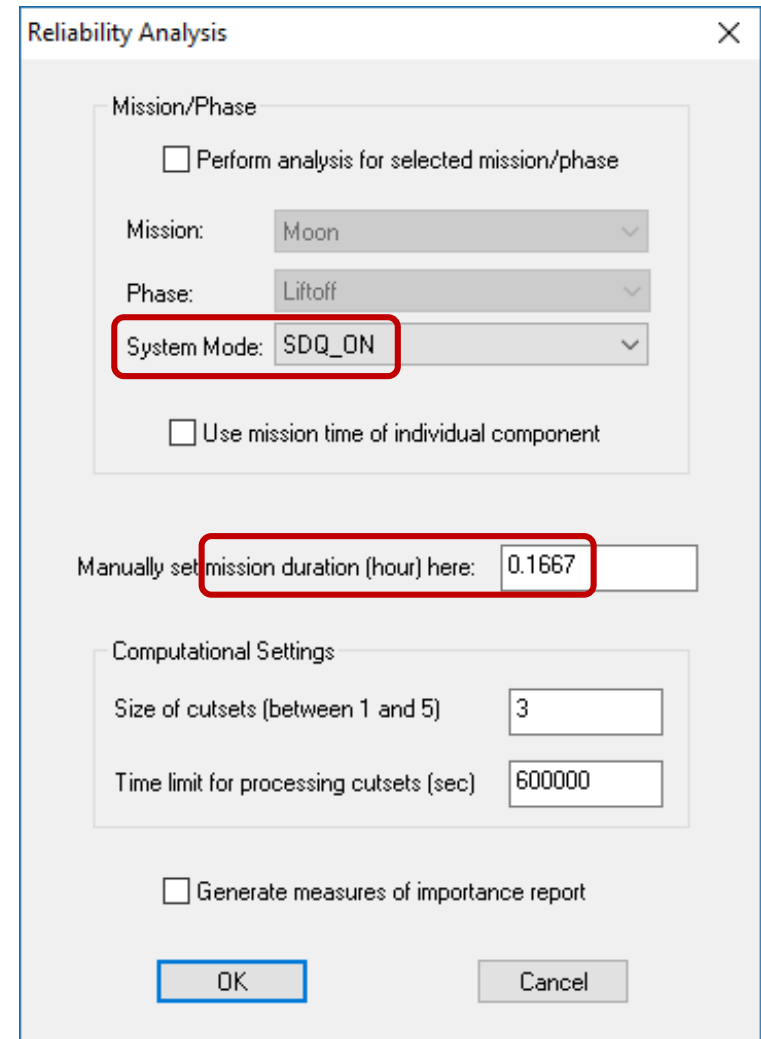
Abort Trigger FP and FN Quantification with SDQ (contd.)

- 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 .

Failure Mode	Failures per hour	Quantitative impact of failure mode on the component output signal			Conservative Upper Bound	
		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
					Opening Hours: 0.1667	0.1667
					Probability of Failure: 7.000E-06	5.267E-06



- ∞ Abort Trigger FP and FN Quantification with SDQ (contd.)
 - Perform “Fault Tree Analysis” for the F2ZEffect, F2SEffect End-Effects with applicable “System Modes” to include/exclude the SDQ mechanism, as well as the “Mission Duration”, to furnish the resulting “cut-sets” and their probabilities.
 - ✓ The main “contributors” to the top level effect are the computed “cutsets” and their “probabilities”
 - ✓ Common cause failure (CCF) not modeled
- ∞ Include Common Cause Failure (CCF) in TEAMS[®] in the future to facilitate these trade studies



∞ Abort Trigger FP and FN Quantification with SDQ (contd.)

➤ Results

✓ Probability of occurrence

▪ F2ZEffect

- With SDQ OFF = $8.46E-10$ (cutset size 2) + $6.22E-21$ (cutset size 3)
- With SDQ ON = $6.46E-10$ (cutset size 2)

▪ F2FSEffect

- With SDQ OFF = $7.55E-10$ (cutset size 2) + $3.66E-16$ (cutset size 3)
- With SDQ ON = $5.67E-10$ (cutset size 2)

✓ Net benefit with SDQ

- F2ZEffect = 23.64%
- F2FSEffect = 24.9%

✓ Lower probabilities possibly due to absence of CCFs

✓ % benefit numbers roughly double the values but of the same order as in the study

FM Architecture Trade Studies – Abort Trigger FP and FN Quantification



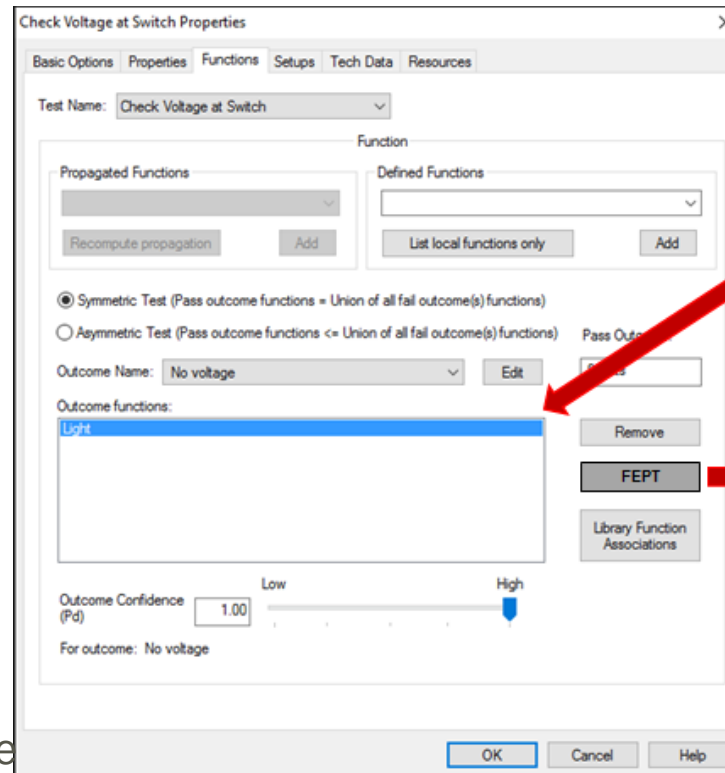
The Shortest Path to Uptime

∞ Abort Trigger FP and FN Quantification with SDQ (contd.)

➤ Future exercises

- ✓ Alternate SDQ mechanisms can be included using TEAMS[®] configuration for the trade space study
- ✓ Leverage effort from the “FM Metrics and V&V” NASA Phase II SBIR to create “Failure Scenarios” and generate various “Metrics” in a “Batch” fashion for the redundancies present in the AT model.

- ∞ FEPT captures the time between a fault origination location and a failure detection as well as a failure effect location
- ∞ Currently TEAMS[®] Designer allows for one time to be associated with a node or an arc
- ∞ Associate Timing information with each relevant function, not just one per node or arc
 - Attach the timing information to individual “Functions” detected by the outcomes of TEAMS[®] tests.
 - Timing report will enhance the Reliability Analysis Reports to include timing information for singletons and doubletons for the selected Effect
- ∞ Timing effects are inherently statistical in nature, hence these are really distributions.
 - Allow FEPTs modeled as function-dependent statistical distributions depending upon available information (e.g., bounds and the mode → Triangle distribution)



Failure Effect Propagation Timing attached to Functions

Triangular Distribution

Min

Max

Mode

- ∞ Inclusion of Common Cause Failure (CCF) In TEAMS[®]
 - Several NASA analyses related to Risk Assessment and FM Architecture Studies incorporate Common Cause Failures (CCFs)
 - ✓ 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 manufacturing defect
 - ✓ Given a failure of one of these components, the other common components' likelihood of failure needs to be adjusted
 - TEAMS[®]-Designer and TEAMS-RDS[®] Capability Enhancements
 - ✓ Allow user to define multiple CCF sets and indicate components that are part of each of the CCF sets
 - ✓ Methods for likelihood of failure adjustment for the CCFs
 - ✓ Capability to specify the adjustments such as common cause scaling factors for the CCF components

- ∞ The paper describes FM quantification techniques in TEAMS[®] using metrics derived from the theory of SHM and FM.
- ∞ 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 difference in results are due to TEAMS[®] not having Common Cause Failures (CCF) modeling capability.

Questions & Comments