Failure Modes and Effects Analysis (FMEA) Assistant Tool Feasibility Study

Melissa Flores [(1)], Jane T. Malin [(2)]

[(1)] *Project Principal Investigator, Safety and Mission Assurance Directorate, NASA Johnson Space Center, Houston, TX, 77058,* *melissa.d.flores@nasa.gov*
[(2)] *Project Co-Investigator, Engineering Directorate, NASA Johnson Space Center, Houston, TX, 77058,* *jane.t.malin-1@nasa.gov*

ABSTRACT

An effort to determine the feasibility of a software tool to assist in Failure Modes and Effects Analysis (FMEA) has been completed. This new and unique approach to FMEA uses model based systems engineering concepts to recommend failure modes, causes, and effects to the user after they have made several selections from pick lists about a component's functions and inputs/outputs. Recommendations are made based on a library using common failure modes identified over the course of several major human spaceflight programs. However, the tool could be adapted for use in a wide range of applications from NASA to the energy industry.

INTRODUCTION

In order for NASA to meet ambitious goals in space exploration using increasingly complex system designs, safety should be considered as early as possible in the design process. Program managers, design engineers, and systems safety and reliability practitioners recognize the need to identify risk early thus reducing lifecycle cost. by, However, current safety analysis methods are challenging to perform quickly enough to affect design, particularly when assessing rapidly occurring changes and large, complex systems.

This project investigated the feasibility of developing a software tool, or modifying an existing tool or suite of tools, to assist in Failure Modes and Effects Analysis (FMEA). This innovative tool uses a standardized systematic approach to failure analysis that makes it easy to capture model information while saving analysis time. This approach not only enables early risk mitigation by reducing cost and human error, but also produces a reusable system model. This model can help bridge the gap between system engineering and safety. Hardware criticality, which can drive cost and schedule due to testing and certification requirements, can be quickly and systematically identified. Undesirable consequences across subsystem interfaces can be mitigated or eliminated.

FMEA starts at the component level and evaluates what can go wrong, and how it can affect the system. It is a bottom-up and systematic method that is mostly qualitative. It is used to identify design strategies to prevent failures and improve reliability. The FMEA therefore provides input to risk assessment activities, assists in assessing compliance to safety requirements (e.g., identifying single point failures), and is used to compare the benefits of competing designs. FMEAs are required for a wide range of products designed and built by NASA from Government Furnished Equipment projects and payloads, to fully integrated human rated spacecraft or habitats. The energy industry could also benefit from mutual development and use of this tool.

In prior NASA programs, it was recommended that lists of standard "common" failure modes (CFM) be considered for use, but free text fields provided for database entry led to inconsistent failure mode identification. For example, to identify the mode where a valve "Fails to Close" some analysts would enter a failure mode of "Fails Open" while others wrote "Fails to Close". A later problem report search for occurrences of this failure mode would miss occurrences of the mode, as they were identified differently. For this reason, more recent efforts have been to standardize a CFM list of about 100 selections for use in a database [1]. However, in practice it was observed that such a long list was unwieldy, and analysts often chose failure descriptions too general to be informative, such as "fails to function," with the detailed description written in free form text. This negates the benefit of a CFM list.

The FMEA Assistant tool has been designed to overcome this problem while retaining, and even expanding, the use of the common failure mode list. The FMEA Assistant does this by guiding the analyst through a set of questions about component attributes, including subsystem type, kinds of resources used, and types of outputs. The chosen attributes narrows down the number of possible choices of failure modes that make sense for that component. The analyst need only consider a few small sets from the full list of common failure modes to find the appropriate ones. The dialogue is dynamic, so that the choices of failure modes presented change if the analyst changes the attribute selections. The tool also extends the use of standardization by offering short lists of common failure causes and effects for each failure mode.

The approach extends a prototype tool suite, the Hazard Identification Tool, developed in collaboration between Johnson Space Center's Safety and Mission Assurance (S&MA) and Engineering directorates, which uses semantic text analysis and extraction technology to create system models from requirements, FMEAs and hazard reports [2]. The requirements and safety information are integrated into system architecture visualizations for review of completeness, correctness, and consistency of the analyses. This technology was extended to generate the basis of a reliability block diagram (RBD) model from the master equipment list (MEL). The model from the extracted text shows components, connections, redundancy, and links to FMEAs.

This project addresses a recognized challenge in a FMEA competency that is needed for developing the analysis for human-rated spacecraft. This project is also relevant to analysis of reliable systems being developed for power, life support, re-entry and landing, and software systems. Early opportunities to design out failure modes prevent the need for re-design, and can save cost and schedule.

1. MODELING APPROACH

A trade study to evaluate five existing software tools against the project's objectives was completed. The Hazard Identification Tool prototype was selected as a starting point. The FMEA Assistant tool models a system's components and their connective relationships, and then assists the design engineer or safety analyst (hereafter referred to as the user) in FMEA, and finally links the FMEA data back to the model for further analysis and review.

The following describes in more detail the step-by-step procedures and how they were implemented. The component to follow in this example is a motor safety device.

1. An initial model is generated from the MEL with some manual manipulation.

   1.a. Information about component names and quantities are extracted from a MEL table for the system. The user selects the components to include in the model and to have a FMEA worksheet. An example is provided in Figure 1.

   1.b. A model canvas, as shown in Figure 2, is automatically populated with the components, in the indicated quantities.

   1.c. Consulting the schematic, the user arranges the components and creates the connections to complete a model similar to an RBD, which reads left to right and shows parallel, redundant paths.

Figure 3 shows the model after the components have been manually arranged and connected. Reachability analysis permits inspection of flow paths and redundancy from the visual model, as detailed in [2].

2. The user selects a component to analyze from the visual model. The menu for initiating a FMEA dialogue for a component is shown in Figure 4.

3. From pick lists on the dialogue page (shown in Figure 5) the user selects the component features and functions, including: the system type, resources, outputs, state sets, and hazard types. Then, small sets of candidate failure modes are offered for user-selected functions, state sets and hazard types. Trying out alternate selections enhances analysis and decision-making. The user has the option to deselect failure modes on this page or a subsequent dialogue page if some are redundant. For example, if "Inadvertent Output" and "Inadvertently Fires" are both offered for this device, the user can select the most specific wording that is correct.

The Failure Mode Library was constructed using the Constellation CFM list, which has about 100 types of component failure modes. The Constellation CFM list includes phrases that relate to functional failures and input/output (I/O) failures. Examples include high input, incorrect timing, delayed activation, fails to actuate, degraded operations, fails to operate, fails to shutdown/stop, and opens incorrectly. The most common failures in the list describe a specific type of failure to function or function correctly. The CFM also contains failures to protect or control a hazard, which are commonly named for a hazardous state such as overvoltage. There are also input/output failures that describe lost or erroneous input or output, and these can also be interpreted as causes and effects of a failure.

The library is in the form of a table of CFMs and some of their attributes, which is given in Appendix A. Constellation Common Failure Modes. The format of the table is shown in Table 1. User choices of component attributes drive the selection of rows in the CFM library table that contain information for reuse in system modeling.

H	I	J
Select for Model	DRAWING TITLE	QTY
	PYROTECHNIC INSTALLATION DRAWING	1.00
X	MOTOR IGNITER	2.00
	EXPLOSIVE TRANSFER LINES	1.00
X	ETL (MOTOR SAFETY TO IGNITER)	2.00
X	ETL (DETONATOR TO SAFETY)	2.00
	ETL CLICK STUD ASSEMBLY	1.00
	P-CLAMP	7.00
	WASHER	7.00
	NUT	7.00
	CLICK STUD	7.00
	SAFETY DEVICE	1.00
X	MOTOR SAFETY	1.00
	DETONATOR	1.00
X	DETONATOR MANIFOLD	2.00
X	DETONATOR	2.00
	DETONATOR MANIFOLD CLICK STUD ASSEMBLY	1.00
	WASHER	4.00
	NUT	4.00
	CLICK BONDS	10.00
X	MOTOR	1.00

Figure 1. MEL example, with column added to indicate which components are to be added to the system model

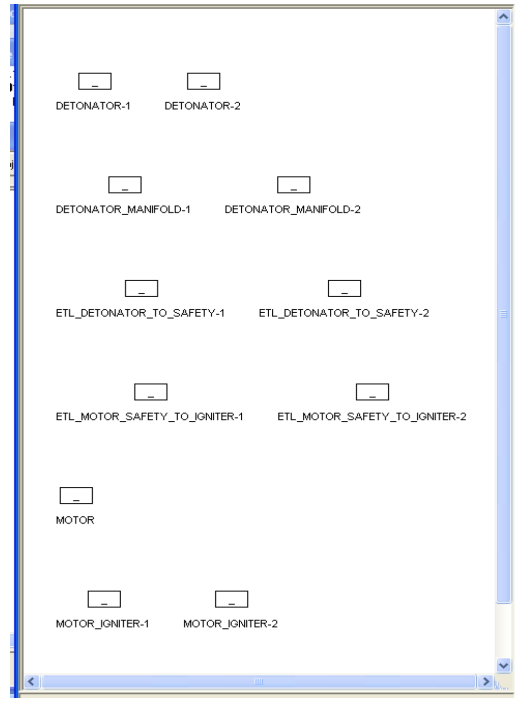

Figure 2. Model canvas populated from MEL

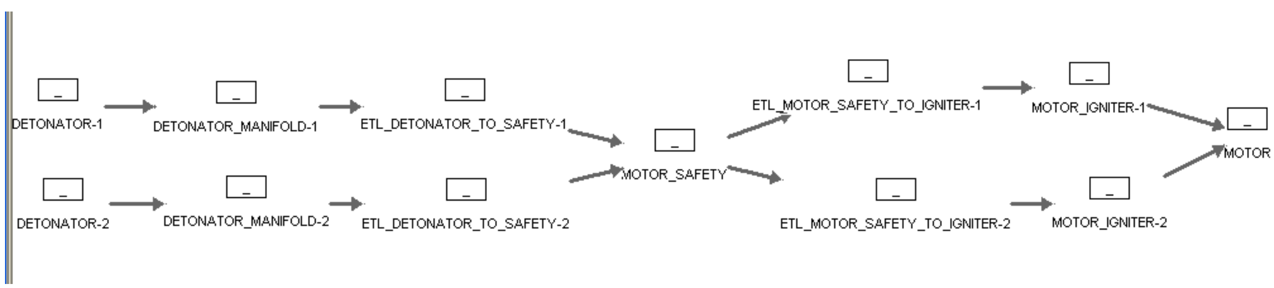

Figure 3. Model after manual arrangement of components and addition of connections

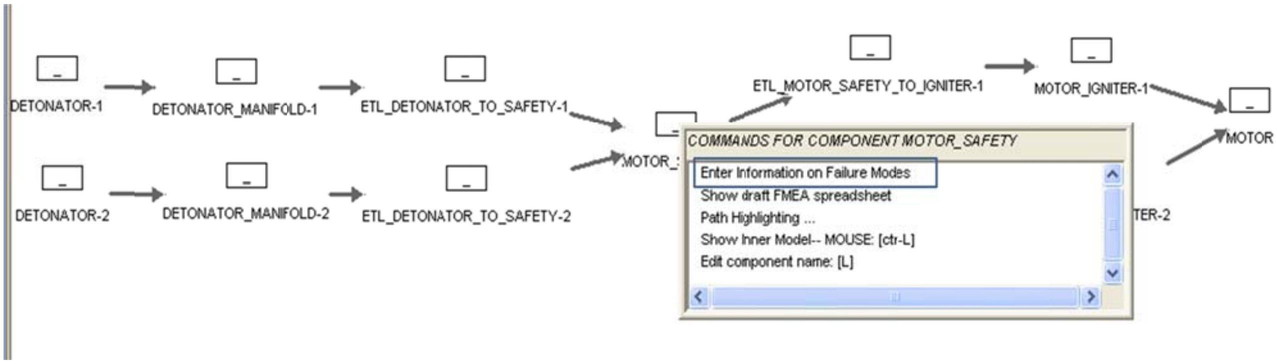

Figure 4. Selecting a component for analysis

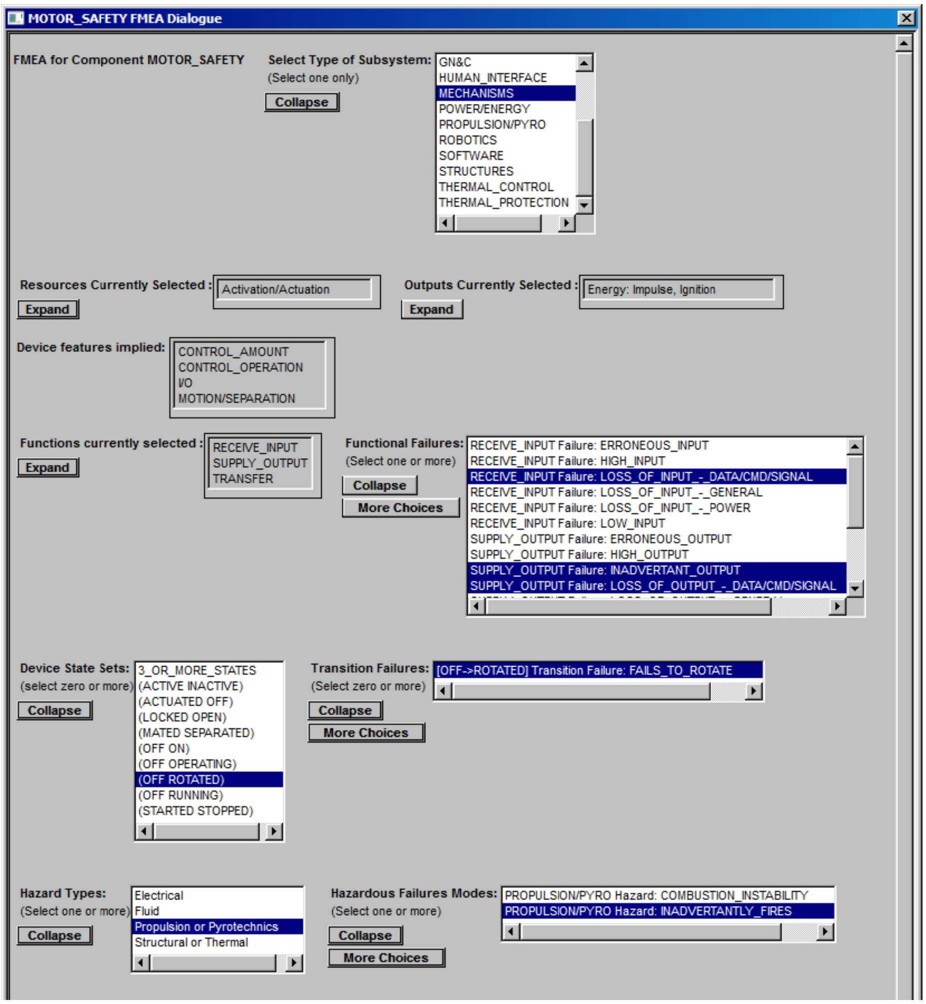

Figure 5. Failure mode dialogue user interface

The table indicates the system types, functions, device features and sets of operating states that are probably associated with each failure mode. The Table of attributes for CFMs was developed using functions and operating states mentioned in each FM, or determining the meaning of the FM phrase and associating one or more probable general functions and state sets. This information drives much of the dialogue, working back from the attributes to narrow down to failure modes.

The user's choice of the system type and other attributes determine the functional failures presented in the function pick list, which in turn determine the contents of the failure mode pick lists.

Error! Reference source not found. Figure 6 shows a diagram indicating how the pick list choices offered as possible responses to dialogue queries depend on choices made for other queries, beginning with the choice of subsystem for the component.

Recommended FM List	Function	Operating States	Device Features	System Type
Clogs	Transfer		Fluid	ECLSS, Thermal, Propulsion/Pyro
Closes at incorrect time	Lock	Open, Locked	Control Operation	Mechanisms, Structures

Table 1. Format of Table of Attributes associated with standard Common Failure Modes (Partial)

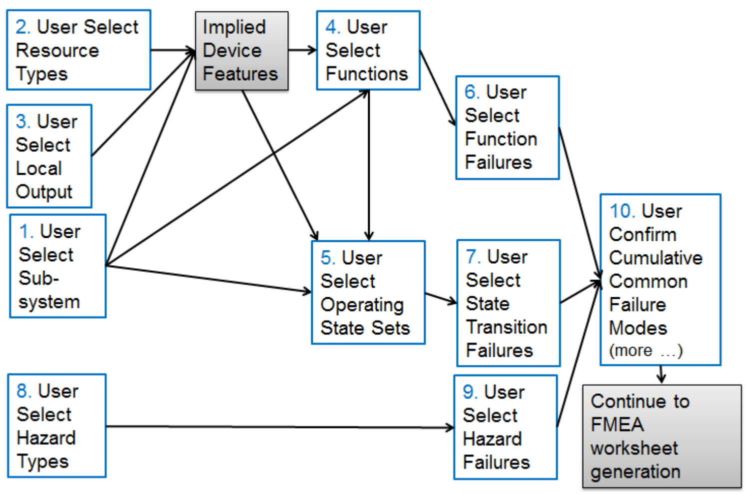

Figure 6. Diagram of Dialogue logic, illustrating how user responses determine offerings for queries

2. GENERATING THE PRELIMINARY FMEA

After selecting the set of failure modes in the dialogue page as shown in of Figure 5, the user opens a second dialogue by clicking a button at the bottom of that first dialogue. Here, the user can select types of failure mode causes and effects and can add descriptions and comments. An example of a completed second dialogue is shown in Figure 7, continuing with the motor safety component example. It contains a row for each failure mode selected in the first dialogue. Each failure mode "Description" on the far left can be extended with free form text to tailor the common failure mode with details specific to the particular component.

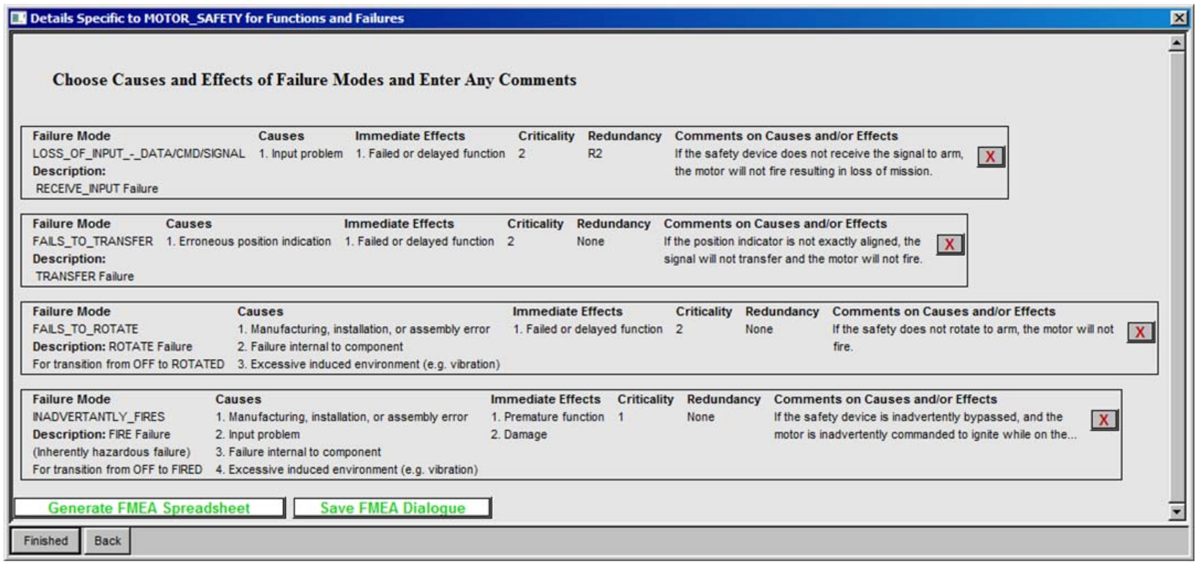

Figure 7. Second dialogue for refining and completing a component's FMEAs

2.1 Selecting Causes and Effects

By clicking on "Causes" and "Effects" columns in a failure mode row, the user then selects causes and effects from lists of common causes and common effects. The user has the opportunity to enter comments on the far right of each row for adding more detail concerning the selected causes and effects for the particular component.

The "Causes" pick list is shown in . The field at the bottom allows the user to add a failure cause not on the pick list if there is a cause for the failure in the particular component that is not covered in the pick list.

The causes pick list was developed by reviewing existing FMEAs and categorizing causes into these primary categories: Failure internal to component; Manufacturing, installation, or assembly error; Input problem; Excessive natural environment (e.g. radiation); and Excessive induced environment (e.g. vibration).

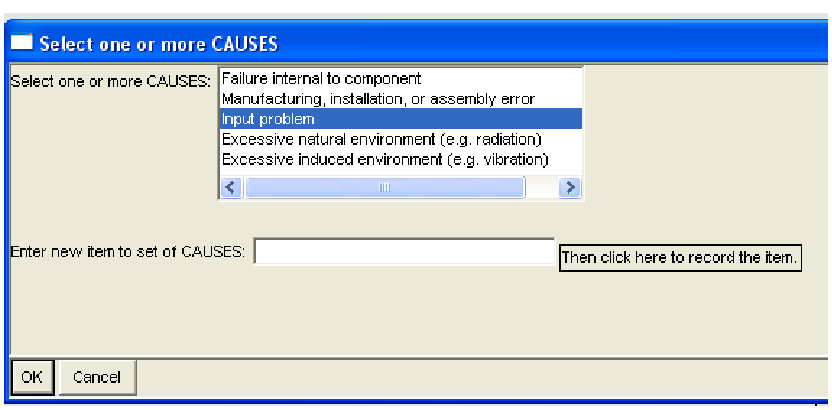

Figure 8. Causes Pick List

Similarly, the effects list includes: Failed or delayed function; Premature function; Loss of output; Premature output; Erroneous output; Damage; and Leakage. The "Effects" pick list is shown in Figure 9. As with the Causes pick list, a field is provided that allows the user to select one or more failure effects and enter a new one if there is an effect of the failure of the particular component that is not covered in the pick list.

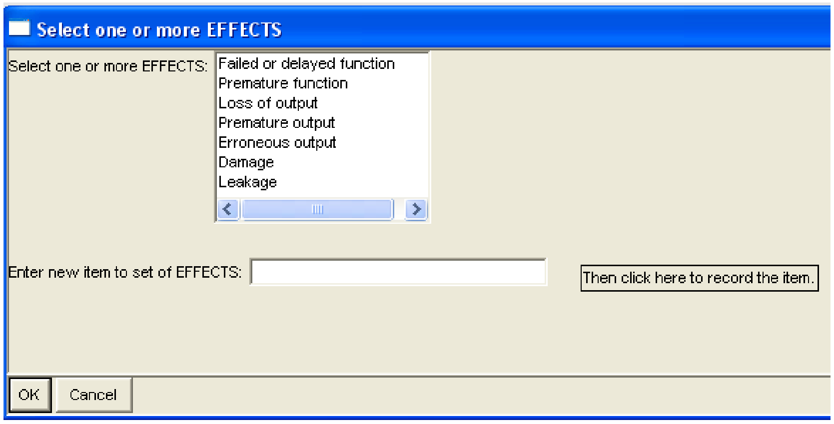

Figure 9. Effects Pick List

2.2 Criticality and Redundancy

The final fields that the user supplies in the dialogue of Figure 7 are criticality and redundancy for each failure mode. The criticality is typically assigned on the basis of worst-case potential failure effect assuming the loss of all redundancy (where applicable) [1]. Criticalities are defined as:

1 – Single failure that could result in loss of life or vehicle
2 – Single failure that could result in a loss of mission
1R# - Redundant hardware that, if all failed, could cause loss of life or vehicle. A number (#) is used to indicate the number of failures required for complete system failure
1S – Failure in a safety or hazard monitoring hardware item that could cause the system to fail to detect, combat, or operate when needed during a hazardous condition.
2R – Redundant hardware item that if all failed, could cause a loss of mission.
3 – All other failures.

2.3 Generating a FMEA worksheet

Finally, a FMEA worksheet, as shown in Figure 10, is generated in Excel, with the following fields: Subsystem, Component, Function, Failure Mode, Failure Description, Failure Causes, Immediate Effects, Criticality, and Comments.

In addition to the FMEA worksheet, a table of the rows that have been selected from the Failure Modes attributes table during the analysis process can be output and reused for modeling system components in engineering.

	A	B	C	D	E	F	G	H	I
1	Subsystem	Component	Function	Failure Mode	Failure Description	Failure Causes	Immediate Effects	Criticality	Comments
2	MECHANISMS	MOTOR_SAFETY	RECEIVE_INPUT	LOSS_OF_INPUT		1. Input problem	1. Failed or delayed function	2R2	If the safety device does not receive the signal to arm, the motor will not fire resulting in loss of the mission.
3	MECHANISMS	MOTOR_SAFETY	TRANSFER	FAILS_TO_TRANSFER		1. Erroneous position indication	1. Failed or delayed function	2	If the position indicator is not exactly aligned, the signal will not transfer and the motor will not fire.
4	MECHANISMS	MOTOR_SAFETY	ROTATE	FAILS_TO_ROTATE	For transition from OFF to ROTATED	1. Excessive induced environment (e.g. vibration); 2. Manufacturing, installation, or assembly error; 3. Failure internal to component	1. Failed or delayed function	2	If the safet device does not rotate to arm, the motor will not fire.
5	MECHANISMS	MOTOR_SAFETY	REGULATE_TIMING	INADVERTENTLY_FIRES	For transition from OFF to FIRED	1. Failure internal to component; 2. Manufacturing, installation, or assembly error; 3. Input problem; 4. Excessive induced environment (e.g. vibration)	1. Damage; 2. Premature function	1	If the safety device is inadvertently bypassed, and the motor is inadvertently commanded to ignite while on the ground could cause loss of life or major assets/facilities.
6									

Figure 10. Final FMEA Worksheet

3. CONCLUSION

The prototype FMEA Assistant tool has the potential to reduce cost and human error. It provides a standardized systematic approach to failure analysis while gathering model information. Without any tool, the user may repeatedly choose general failure modes such as "failure to function". General failure modes are rarely adequate for FMEA worksheet development and subsequent systems and safety analysis. The tool helps drive out the complete and most descriptive choices of applicable common failure modes. With the FMEA Assistant tool, the user is invited to consider the component from several perspectives (subsystem, function, inputs, outputs, operating states, and hazard types). This encourages full consideration of potential failure modes and therefore more thorough and accurate analysis. The user is able to spend more time considering safety-related issues and less time repeatedly scanning a long list of common failure modes or searching for related historical or other information. This should result in a lower error rate, less overall time preparing the FMEA, and an improved product. Furthermore, this approach not only enables early risk mitigation, but also model reuse. Using the tool to derive a single model for reuse by systems engineers, safety analysts, and others helps reduce cost and human error. Identifying single point failures allows for early opportunities to design them out, preventing the need for re-design, and can save cost and schedule.

4. FORWARD WORK

In response to feedback from potential users, a capability to identify hazards associated with particular failure modes has recently been added. This capability was developed by mapping the common failure modes list with a common or standard hazards list. This helps the analyst either identify hazards at the vehicle level caused by the component, or can help with the currently manual task of cross-referencing the FMEA to hazards already documented.

Also in response to user suggestions, a selection of common components will be selected for identification of standard failure modes. This will demonstrate the concept of building a library of standard components with failure modes, causes, and effects already identified within the tool. Additionally, integration with the existing FMEA database used by the International Space Station Program has been studied and is feasible with the proper data field mapping and funding to complete the task.

Evaluation of the benefit in time, accuracy and specificity compared to traditional FMEA practices is greatly desired. A relatively small scope NASA project would be ideal for an evaluation.

In the longer term, the FMEA Assistant tool capability could be integrated with other vehicle risk assessment tools in development at JSC for quantitative reliability assessment. It could also tie into other JSC model-based system and mission capability impact tools currently in development, as they all have the same goals of providing information on how a failure affects other systems, and how the effects propagate to affect the mission. Along those lines, the tool could be used in operational programs to help identify the potential cause(s) of a failure.

A recent effort [3] to integrate safety attributes and failure knowledge from FMEA Assistant into Systems Modeling Language (SysML) models has been initiated. This is another related area of potential forward work.

ACKNOWLEDGEMENTS

M.F. Author would like to thank Vuong Pham for encouraging development of this idea, and assistance in identifying a funding source. The authors would also like to acknowledge the JSC Joint Technology Working Group, particularly John Saiz, Ronnie Clayton, and David Brown for funding this project, encouraging it's continuation, and developing opportunities to share this idea with the JSC community through various avenues. The authors would like to thank Land Fleming for excellent application design and software development.

REFERENCES

[1] "Constellation Program Hardware Failure Modes and Effects Analysis and Critical Items List (FMEA/CIL) Methodology", *NASA*, Dec. 2009, pp. 20 – 21.

[2] Jane T. Malin, Land D. Fleming, Carroll Thronesbery, David R. Throop and Ted Bennett, "Integrated Visualization of Information from Requirements, Safety Analyses, and Hazard Reports," Proceedings of the 28th International System Safety Society Conference, Sept. 2010.

[3] Jane Malin and Sheena Miller, "Failure Mode Modeling using SysML and the Aerospace Ontology", NASA JSC White Paper, 2012.

Appendix A. Constellation Common Failure Modes Attributes Table (Partial)

Recommended FM List	Function	Operating States	Device Features	System Type
Clogs	Transfer		Fluid	ECLSS, Thermal, Propulsion/Pyro
Closes at incorrect time	Lock	Open, Locked	Control Operation	Mechanisms, Structures
Closes at incorrect time	Close	Open, Closed	Control Path	ECLSS, Thermal, Propulsion/Pyro, Power/Energy
Closes at incorrect time	Regulate Timing	Open, Closed	Control Path	ECLSS, Thermal, Propulsion/Pyro, Power/Energy
Closes incorrectly	Close	Open, Closed	Control Path	ECLSS, Thermal, Propulsion/Pyro, Power/Energy
Combustion instability	Control Vibration		Propulsion/Pyro	Propulsion/Pyro
Degraded Operations	Operate	Off, Operating	Control Operation	Any
Delayed activation	Activate	Inactive, Active	Control Operation	Any
Delayed activation	Regulate Timing	Inactive, Active	Control Operation	Any
Delayed de-activation	De-activate	Active, Inactive	Control Operation	Any
Delayed de-activation	Regulate Timing	Active, Inactive	Control Operation	Any

Delayed operation	Operate	Off, Operating	Control Operation	Any
Delayed operation	Regulate Timing	Off, Operating	Control Operation	Any
Electrostatic discharge	Insulate		Electronics/Power	Power/Energy, Electronics
Erroneous high indication	Indicate		Sensor/Indicator	Any-with Sensor/Indicator
Erroneous indication	Indicate		Sensor/Indicator	Any-with Sensor/Indicator
Erroneous Input	Receive Input		Sensor/Indicator	Any-with Sensor/Indicator
Erroneous low indication	Indicate		Sensor/Indicator	Any-with Sensor/Indicator
Erroneous output	Supply Output		Sensor/Indicator	Any-with Sensor/Indicator
Erroneous position indication	Indicate		Sensor/Indicator	Any-with Sensor/Indicator
Erroneous trip	Trip; Control Overcurrent	Closed, Open	Electronics/Power	Power/Energy, Electronics
External leakage	Contain/Isolate		Fluid	ECLSS, Thermal, Propulsion/Pyro
Fails activated	De-activate	Active, Inactive	Control Operation	Any
Fails deactivated	Activate	Inactive, Active	Control Operation	Any
Fails high	Monitor		Sensor/Indicator	Any-with Sensor/Indicator
Fails low	Monitor		Sensor/Indicator	Any-with Sensor/Indicator
Fails off	De-activate	Off, On	Control Operation	Any
Fails off	Monitor	Off, Monitor	Sensor/Indicator	Any-with Sensor/Indicator
Fails on	Activate	On, Off	Control Operation	Any
Fails partially closed	Close	Open, Closed	Control Path	ECLSS, Thermal, Propulsion/Pyro, Power/Energy
Fails partially open	Open	Closed, Open	Control Path	ECLSS, Thermal, Propulsion/Pyro, Power/Energy
Fails to actuate	Actuate	Off, Actuated	Control Operation	Any
Fails to close	Lock	Open, Locked	Control Operation	Mechanisms, Structures
Fails to close	Close	Open, Closed	Control Path	ECLSS, Thermal, Propulsion/Pyro, Power/Energy
Fails to cut	Cut		Motion/Separation	GN&C, Propulsion/Pyro, Mechanisms, Robotics
Fails to deploy	Deploy		Motion/Separation	GN&C, Propulsion/Pyro, Mechanisms, Robotics
Fails to detect	Detect		Sensor/Indicator	Any-with Sensor/Indicator
Fails to fire	Fire	Off, Fired	Propulsion/Pyro	Propulsion/Pyro
Fails to function	… other function			
Fails to ignite	Ignite	Off, Ignited	Propulsion/Pyro	Propulsion/Pyro
Fails to inflate	Inflate		Motion/Separation	GN&C, Propulsion/Pyro, Mechanisms, Robotics
Fails to initiate	Initiate	Off, Initiated	Propulsion/Pyro	Propulsion/Pyro
Fails to jettison	Jettison		Motion/Separation	GN&C, Propulsion/Pyro, Mechanisms, Robotics
Fails to mate	Mate	Mated, Separated	Motion/Separation	GN&C, Propulsion/Pyro,

				Mechanisms, Robotics
Fails to open	Open	Closed, Open	Control Path	ECLSS, Thermal, Propulsion/Pyro, Power/Energy
Fails to operate	Operate	Off, Operating	Control Operation	Any
Fails to reef	Reef		Motion/Separation	GN&C, Propulsion/Pyro, Mechanisms, Robotics
Fails to relieve	Relieve		Fluid	ECLSS, Thermal, Propulsion/Pyro
Fails to rotate	Rotate	Off, Rotated	Motion/Separation	GN&C, Propulsion/Pyro, Mechanisms, Robotics
Fails to run	Run	Off, Running	Control Operation	Any
Fails to seal	Seal		Fluid	ECLSS, Thermal, Propulsion/Pyro
Fails to separate	Separate	Mated, Separated	Motion/Separation	GN&C, Propulsion/Pyro, Mechanisms, Robotics
Fails to shutdown/stop	Shutdown/stop	Started, Stopped	Control Operation	Any
Fails to stop	Stop	Started, Stopped	Control Operation	Any
Fails to switch	Switch	Closed, Open	Electronics/Power	ECLSS, Thermal, Propulsion/Pyro, Power/Energy
Fails to switch	Switch	Off, On	Electronics/Power	Any
Fails to switch	Switch	On, Off	Electronics/Power	Any
Fails to switch	Switch	3_or_More_States	Electronics/Power	Any
Fails to transfer	Transfer		I/O	ECLSS, Propulsion/Pyro, C&DH, C&T, GN&C, Power/Energy, Thermal
Fails to trip	Trip; Control Overcurrent	Closed, Open	Electronics/Power	Power/Energy, Electronics
Flow blockage	Transfer		Fluid	ECLSS, Thermal, Propulsion/Pyro
Flow restriction	Transfer		Fluid	ECLSS, Thermal, Propulsion/Pyro
High input	Receive Input		Control Amount	ECLSS, Thermal, Propulsion/Pyro, C&DH, C&T, GN&C, Power/Energy, Mechanisms
High output	Supply Output		Control Amount	ECLSS, Thermal, Propulsion/Pyro, C&DH, C&T, GN&C, Power/Energy, Mechanisms
Inadvertant output	Supply Output		I/O	ECLSS, Thermal, Propulsion/Pyro, C&DH, C&T, GN&C, Power/Energy, Mechanisms
Inadvertant output	Regulate Timing		I/O	ECLSS, Thermal, Propulsion/Pyro, C&DH, C&T, GN&C, Power/Energy, Mechanisms
Inadvertantly fires	Fire	Off, Fired	Propulsion/Pyro	Propulsion/Pyro
Inadvertantly fires	Regulate Timing	Off, Fired	Propulsion/Pyro	Propulsion/Pyro

Incorrect timing	Regulate Timing		Control Operation	Any
Internal leakage	Contain/Isolate		Fluid	ECLSS, Thermal, Propulsion/Pyro
Loss of adhesion-cohesion	Attach		Structure	Any
Loss of input - data/cmd/signal	Receive Input		I/O	ECLSS, Propulsion/Pyro, C&DH, C&T, GN&C, Power/Energy
Loss of input - general	Receive Input		I/O	ECLSS, Propulsion/Pyro, C&DH, C&T, GN&C, Power/Energy
Loss of input - power	Receive Input		I/O	ECLSS, Propulsion/Pyro, C&DH, C&T, GN&C, Power/Energy
Loss of insulation capability	Insulate		Thermal	Any
Loss of output - data/cmd/signal	Supply Output		I/O	ECLSS, Propulsion/Pyro, C&DH, C&T, GN&C, Power/Energy
Loss of output - general	Supply Output		I/O	ECLSS, Propulsion/Pyro, C&DH, C&T, GN&C, Power/Energy
Loss of output - power	Supply Output		I/O	ECLSS, Propulsion/Pyro, C&DH, C&T, GN&C, Power/Energy
Loss of preload/loading	Attach		Structure	Any
Low input	Receive Input		Control Amount	ECLSS, Thermal, Propulsion/Pyro, C&DH, C&T, GN&C, Power/Energy, Mechanisms
Low output	Supply Output		Control Amount	ECLSS, Thermal, Propulsion/Pyro, C&DH, C&T, GN&C, Power/Energy, Mechanisms
No indication	Indicate		Sensor/Indicator	Any-with Sensor/Indicator
Nonconforming flow	Control Flow		Fluid	ECLSS, Thermal, Propulsion/Pyro
Nonconforming start	Start	Stopped, Started	Control Operation	Any
Nonconforming stop	Stop	Started, Stopped	Control Operation	Any
Open circuit	Protect Circuit		Electronics/Power	Power/Energy, Electronics
Opens at incorrect time	Open	Closed, Open	Control Path	ECLSS, Thermal, Propulsion/Pyro, Power/Energy
Opens at incorrect time	Regulate Timing	Closed, Open	Control Path	ECLSS, Thermal, Propulsion/Pyro, Power/Energy
Opens incorrectly	Open	Closed, Open	Control Path	ECLSS, Thermal, Propulsion/Pyro, Power/Energy
Overcurrent	Control Overcurrent		Electronics/Power	Power/Energy, Electronics
Overheats	Control Heat		Thermal	Any
Parameter drift	Condition Data		Sensor/Indicator	Any-with Sensor/Indicator
Passes contaminates	Control Contaminants		Fluid	ECLSS, Thermal, Propulsion/Pyro
Premature actuation	Actuate	Off, Actuated	Control Operation	Any
Premature actuation	Regulate	Off, Actuated	Control Operation	Any

	Timing			
Premature de-activation	De-Activate	Active, Inactive	Control Operation	Any
Premature de-activation	Regulate Timing	Active, Inactive	Control Operation	Any
Premature operation	Operate/Run	Off, Operating	Control Operation	Any
Premature operation	Regulate Timing	Off, Operating	Control Operation	Any
Regulates high	Regulate		Control Amount	ECLSS, Thermal, Propulsion/Pyro, C&DH, C&T, GN&C, Power/Energy, Mechanisms
Regulates low	Regulate		Control Amount	ECLSS, Thermal, Propulsion/Pyro, C&DH, C&T, GN&C, Power/Energy, Mechanisms
Reverse polarity	Protect Circuit		Electronics/Power	Power/Energy, Electronics
Separates prematurely	Separate	Mated, Separated	Motion/Separation	GN&C, Propulsion/Pyro, Mechanisms, Robotics
Separates prematurely	Regulate Timing	Mated, Separated	Motion/Separation	GN&C, Propulsion/Pyro, Mechanisms, Robotics
Short circuit	Control Overcurrent		Electronics/Power	Power/Energy, Electronics
Short to ground	Control Overcurrent		Electronics/Power	Power/Energy, Electronics
Structural failure - debond	Attach		Structure	Any
Structural failure - debris	Contain/Isolate		Structure	Any
Structural failure - deform	Protect Structure		Structure	Any
Structural failure - fracture	Protect Structure		Structure	Any
Structural failure - general	Protect Structure		Structure	Any
Structural failure - loss of containment	Contain/Isolate		Structure	Any
Structural failure - mounting	Attach		Structure	Any