Failure Modes and Effects Analysis (FMEA) Assistant Tool

IAASS Conference
May 22, 2013

Melissa Flores and Jane Malin

NASA Johnson Space Center

Introduction

Motivation: Designing safety into space vehicles

- For decades, Failure Modes and Effects Analysis (FMEA) has been used to identify risks inherent in space system designs
- Current analysis methods are challenging to perform quickly enough to affect design

Project Goal: Identify design weaknesses early in the design process with timely risk identification

- Semi-automate identification of failure modes, causes and effects
  - Extract data from early design inputs to build a system model for evaluating and displaying failure effects
  - Use pick lists and libraries to help an analyst consider relevant failure modes from a standard list, and types of causes and local effects
  - Generate draft FMEA worksheets in Excel and attach to the model
- Integrate and enable access to data used by designers and safety analysts to make risk-informed design decisions real-time

Today, we will demonstrate our prototype software tool.

Approach

Retain and expand use of a standard set of failure modes

- About 100 “Common Failure Modes” (CFMs) were selected for use in a space program database
  - In practice such a long list is unwieldy
- FMEA Assistant Tool guides the analyst through a set of questions about component attributes, which narrows down possible failure mode choices
  - Beneficial side effect is a narrowed down set of reusable model information

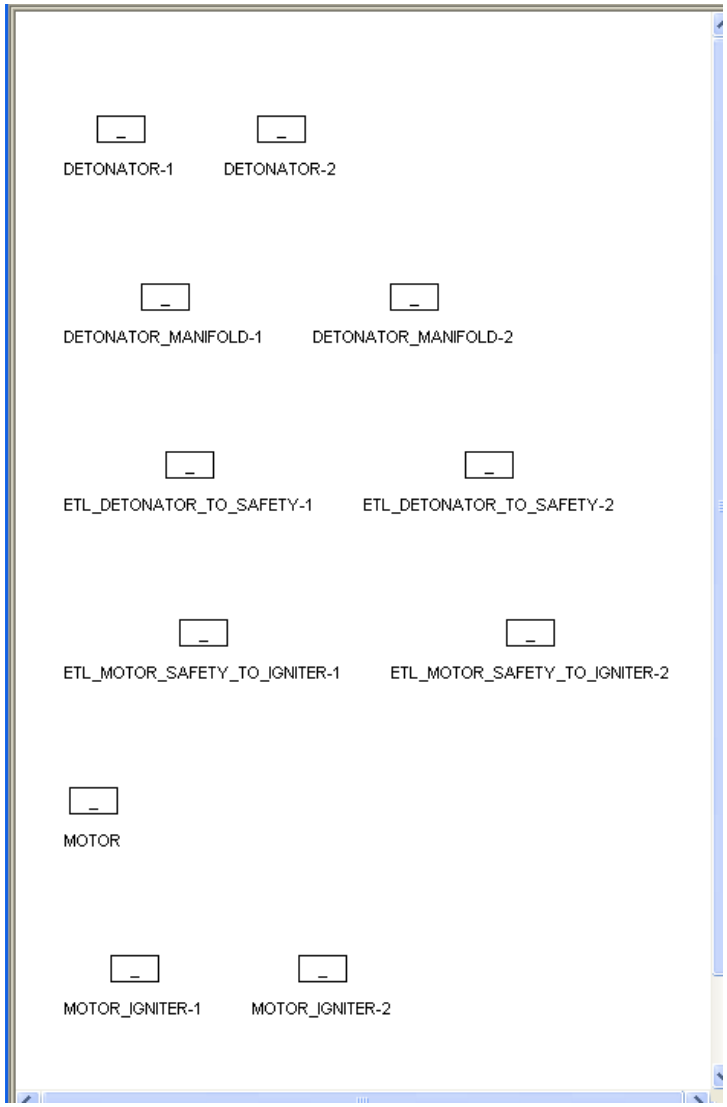
Models system components and connective relationships

- Component names and quantities are extracted from a Master Equipment List (example on next slide)

Equipment List

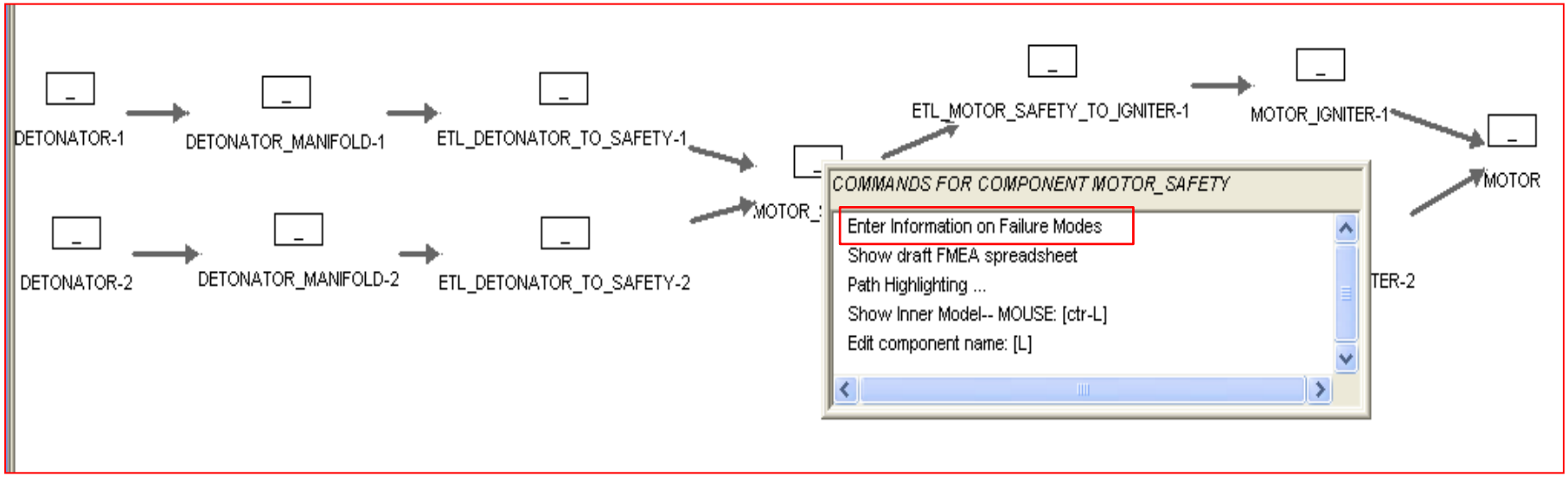
H	I	J
Select for Model	DRAWING TITLE	QTY
	PYROTECHNIC INSTALLATION DRAWING	1.00
X	MOTOR IGNITER	2.00
	EXPLOSIVE TRANSFER LINES	1.00
X	ETL (MOTOR SAFETY TO IGNITER)	2.00
X	ETL (DETONATOR TO SAFETY)	2.00
	ETL CLICK STUD ASSEMBLY	1.00
	P-CLAMP	7.00
	WASHER	7.00
	NUT	7.00
	CLICK STUD	7.00
	SAFETY DEVICE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

Model canvas



Model after manual arrangement

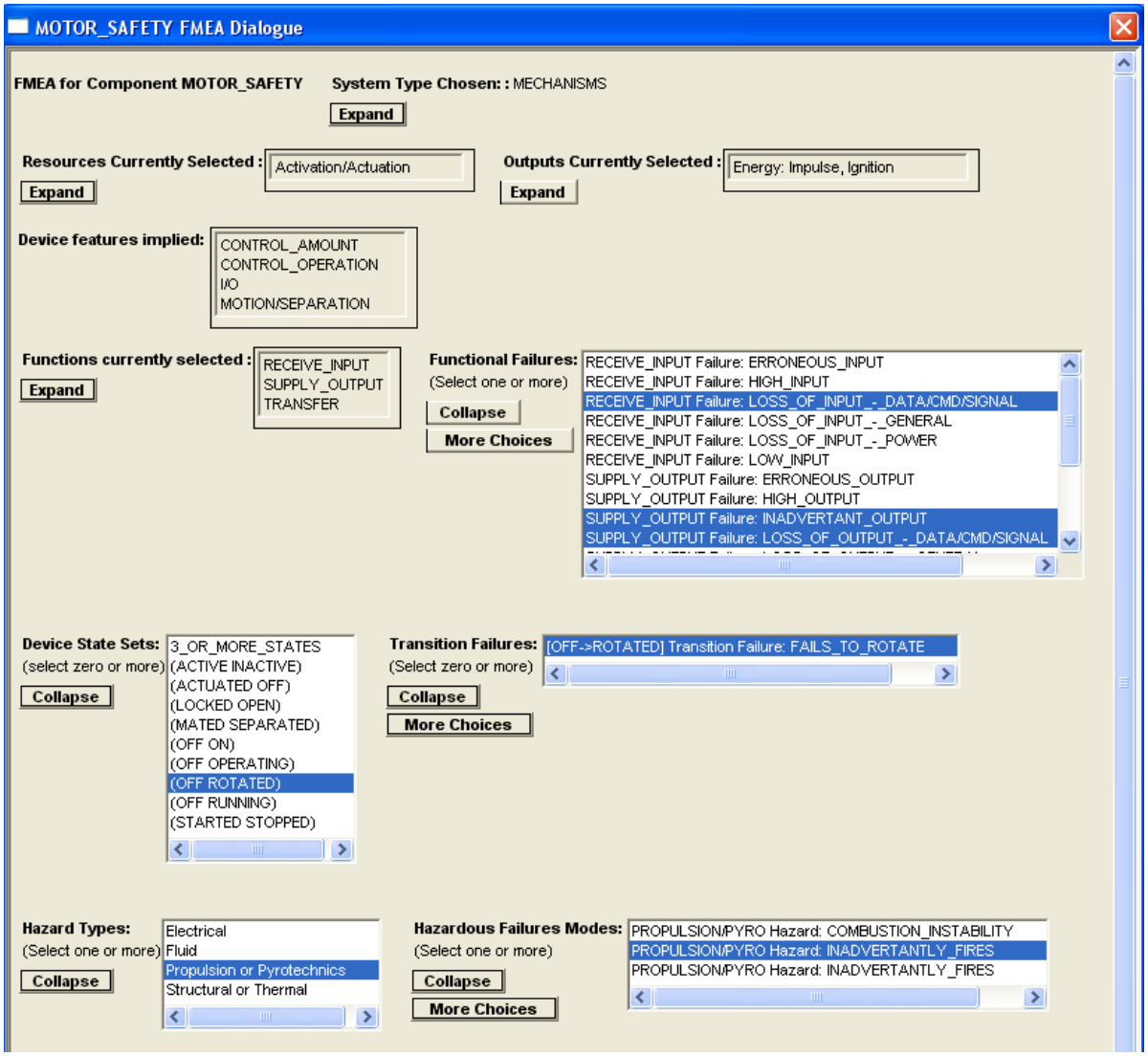
Consulting the schematic, the user arranges the components and creates the connections to complete a model similar to a reliability block diagram, which reads left to right and shows parallel, redundant paths.



The user can select a component from the model to analyze.

A mouse click over the component activates a menu, and a FMEA dialogue for the component can be initiated.

Failure Mode dialogue



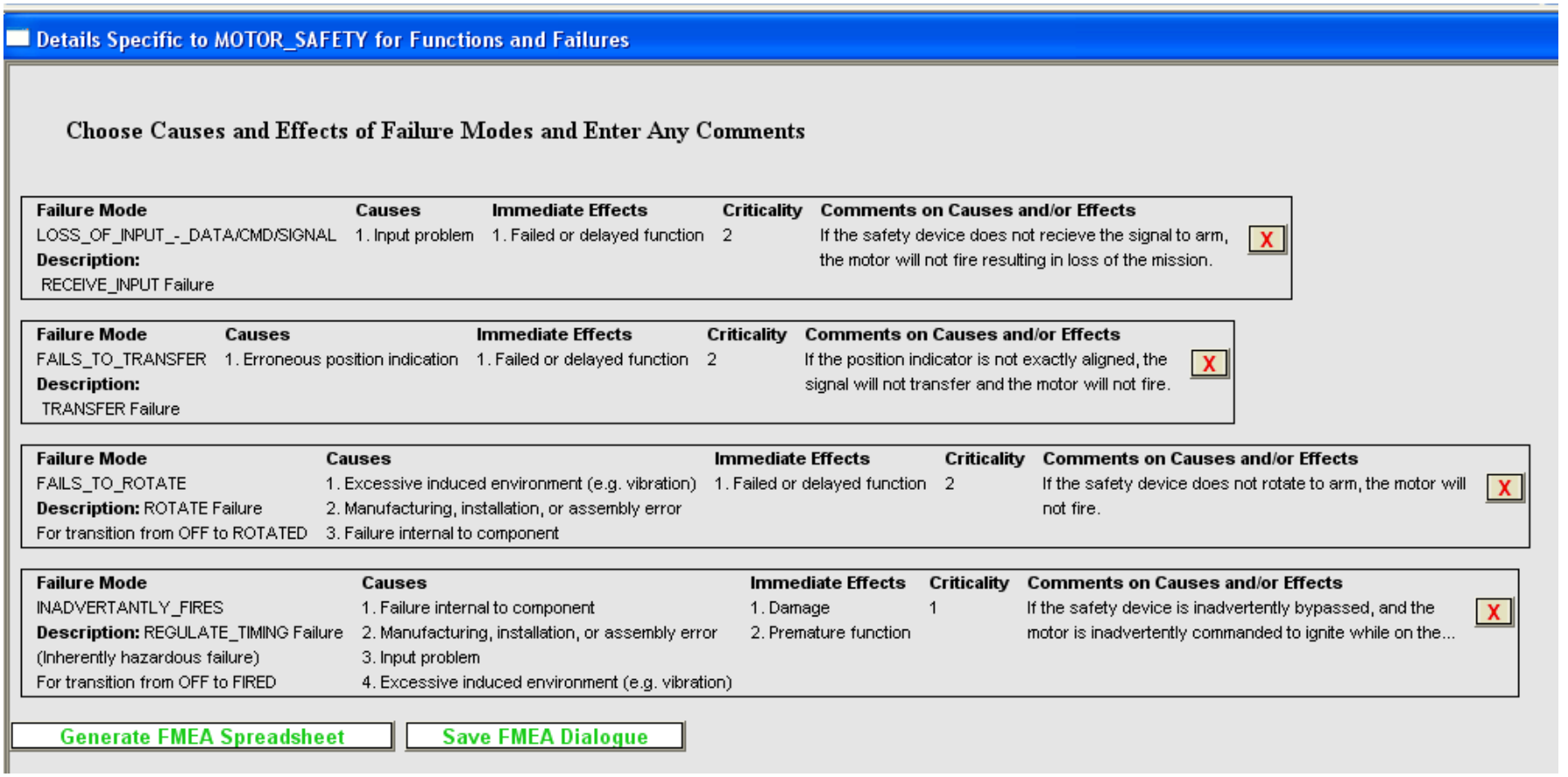
Failure Modes Library

This example table shows attributes associated with each CFM in a library, including subsystem types, functions, operating states and device features that are probably associated with each failure mode.

Common FM List	Function	Operating States	Device Features	Subsystem Type
Clogs	Transfer		Fluid	Thermal, Propulsion, Life Support…
Short to Ground	Control Overcurrent		Electronics/Power	Power/Energy, Electronics
Fails to Actuate	Actuate	Off, Actuated	Control Operation	Any

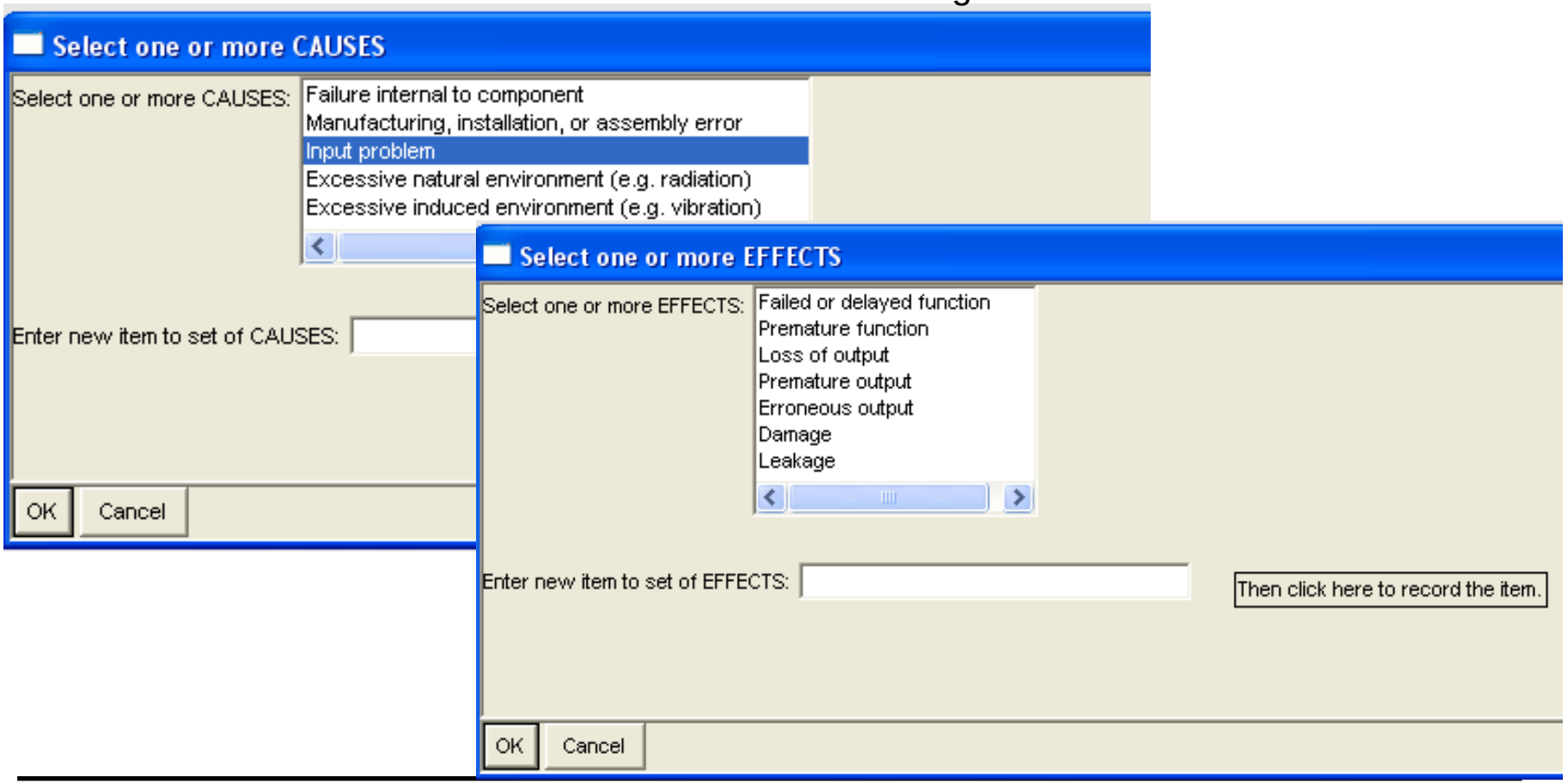
The user's choice of the subsystem type and values of other attributes determine the subsets of the CFM list that are presented in the pick lists.

Refine and complete the FMEA



Causes and Effects

- The user selects causes and effects from lists of common causes and common effects.
- The user has the opportunity to enter new items.
- The user can add comments with more detail concerning the selected causes and effects.

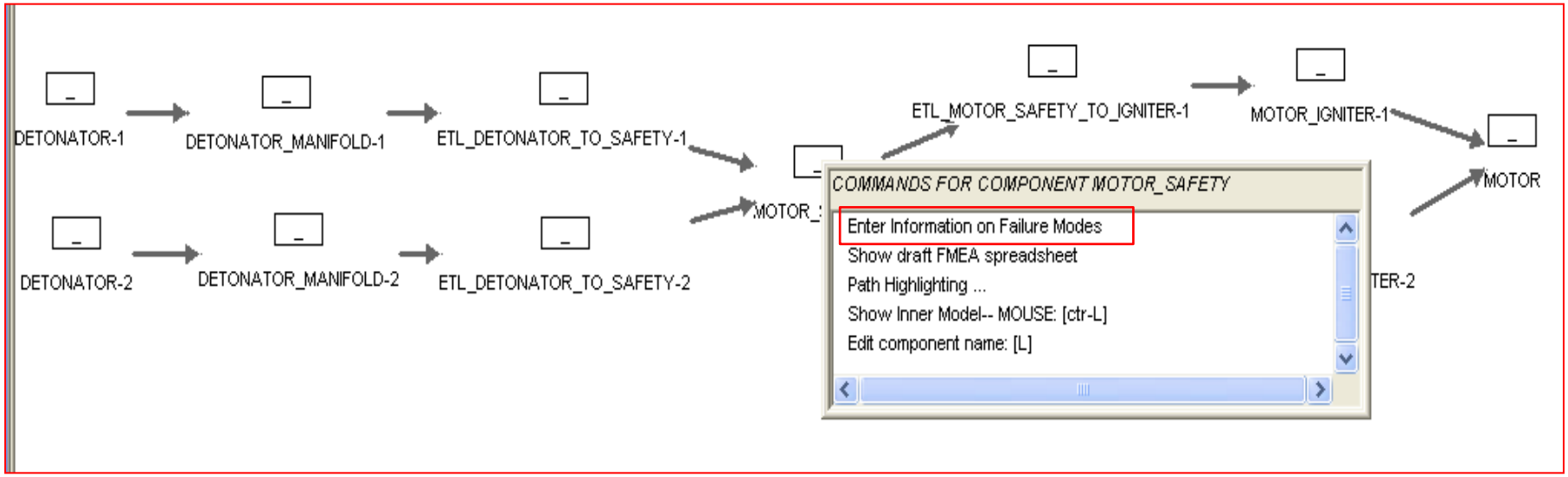


Generating a FMEA worksheet

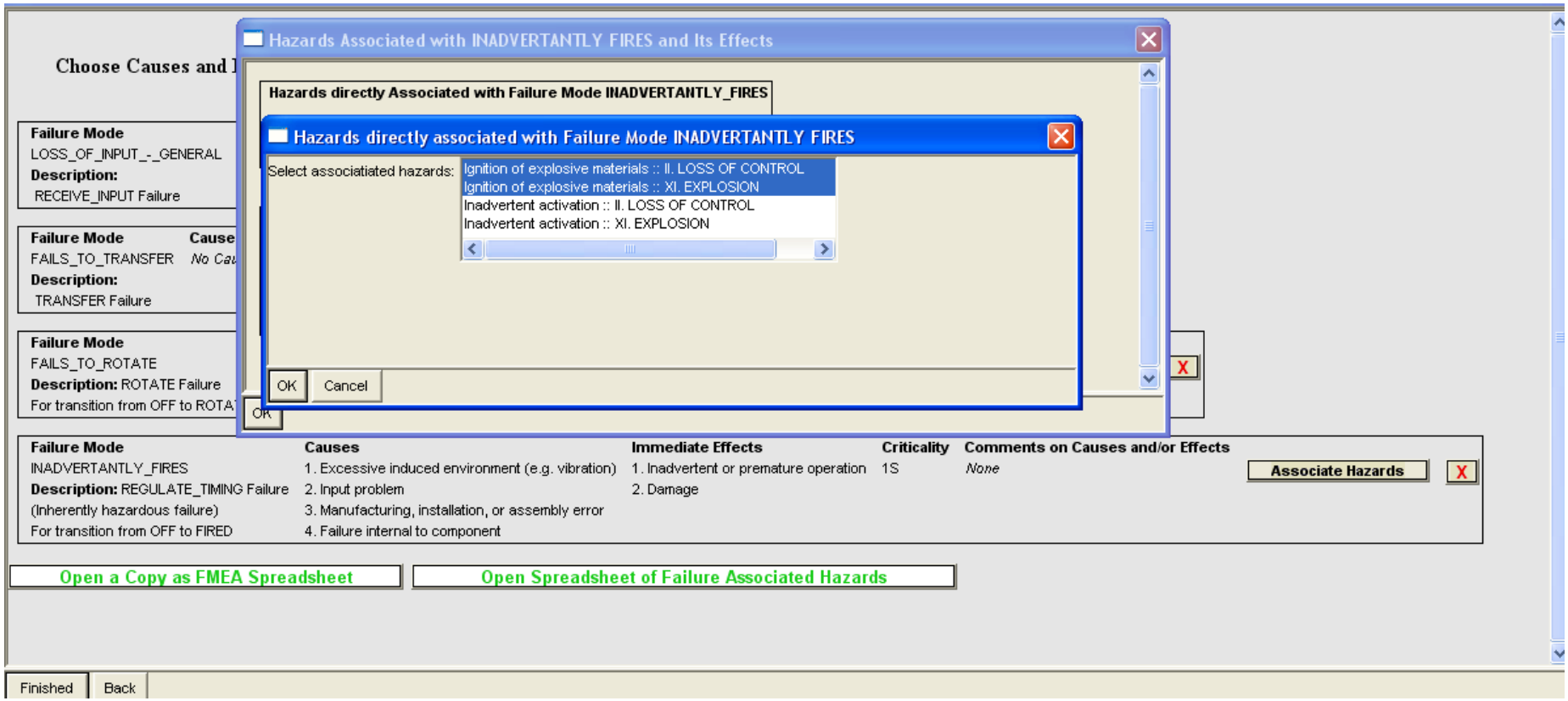
	A	B	C	D	E	F	G	H	I
1	**Subsystem**	**Component**	**Function**	**Failure Mode**	**Failure Description**	**Failure Causes**	**Immediate Effects**	**Criticality**	**Comments**
2	MECHANISMS	MOTOR_SAFETY	RECEIVE_INPUT	LOSS_OF_INPUT		1. Input problem	1. Failed or delayed function	2R2	If the safety device does 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									

Analysis from Model Canvas

- Each draft FMEA Worksheet is associated with a component on the canvas.
- Path highlighting selections show upstream, downstream or redundant paths.



Identify associated hazards



A capability to identify hazards associated with particular failure modes has recently been added.

Conclusion

The prototype FMEA Assistant tool provides a standardized, systematic approach to failure analysis while gathering model information.

- Helps drive out the complete and most descriptive choices of applicable common failure modes
- User is invited to consider the component from several perspectives (subsystem, function, inputs, outputs, operating states, hazard types)
- More time to consider design issues, and less time repeatedly scanning a long list of common failure modes or searching for connectivity information
- Enables model reuse in systems engineering
- Helps identify single point failures

Forward Work

In response to feedback from potential users:

- Select some common components for identification of standard failure modes; demonstrate library concept
- Integration with existing FMEA database used by ISS has been studied and is feasible with proper data field mapping and funding to complete the task
- Greatly desire customer(s) to evaluate the benefit in time, accuracy, and specificity compared to traditional FMEA practices – small scope project ideal

Long term:

- Integrate with other tools in development at JSC
  - Model-based system and mission capability impact tools
  - Quantitative reliability assessment

Questions?