Universal approach to

Model-Based Safety Analysis and Assessment

A Technology Process White Paper

Prepared by

DSI International, Inc.

Background

A Model-based approach to ensuring functional performance on complex systems for the warfighter has been a core objective for DSI since the mid 1970's. As computing technologies and software advanced, DSI has continued to push and lead industry in this Model-based approach to Testability and Diagnostic Analysis. DSI's founder, Ralph A. DePaul, Jr., was recognized as pioneering "Designing for Testability" by IEEE in 1994.

By 1998, DSI's Model-based Diagnostics Engineering tool, "***eXpress***", was the first fully-featured Diagnostic Design capture and analysis tool available as a PC-based commercial product. As such, "***eXpress***" has matured to be the "go-to" Diagnostics Engineering tool for those large or complex Aerospace and Military programs.

Over the past decade, many other tools have been developed by DSI to greatly expand and enriched the utility of the ***eXpress*** Model-based approach to Diagnostics Engineering. Once any design is fully captured in the ***eXpress*** Model-based environment, almost any other Model-based assessment are generated as "turnkey" outputs from the captured diagnostic design – including design or system level FMEAs, FMECAs and a myriad of stock Model-based Safety Analysis Assessments.

Interoperability – Development Lifecycle – Product Lifecycle Management (PLM)
As a prerequisite to performing a Model-Based Safety Analysis and Assessment is an environment that must be able to include any or all relevant design data from all interdisciplinary design activities. It must be able to include design data in an "interoperable" form from external suppliers and whom may use a variety of preferred design tools.

Any data to be included as input to the Model-based Systems Engineering (MBSE) approach must be able to be more than simply, "compatible" in industry or specialized data form schemas or structures – particularly when integrating Model-based Safety Analysis (MBSA) as fully integrated component to the MBSE process. Additionally, there must be an inherent Model—based design mechanism or utility that fully vets supplied data with error and validation checkers that determine completeness and accuracy before inclusion into overarching system (asset-level) model(s).

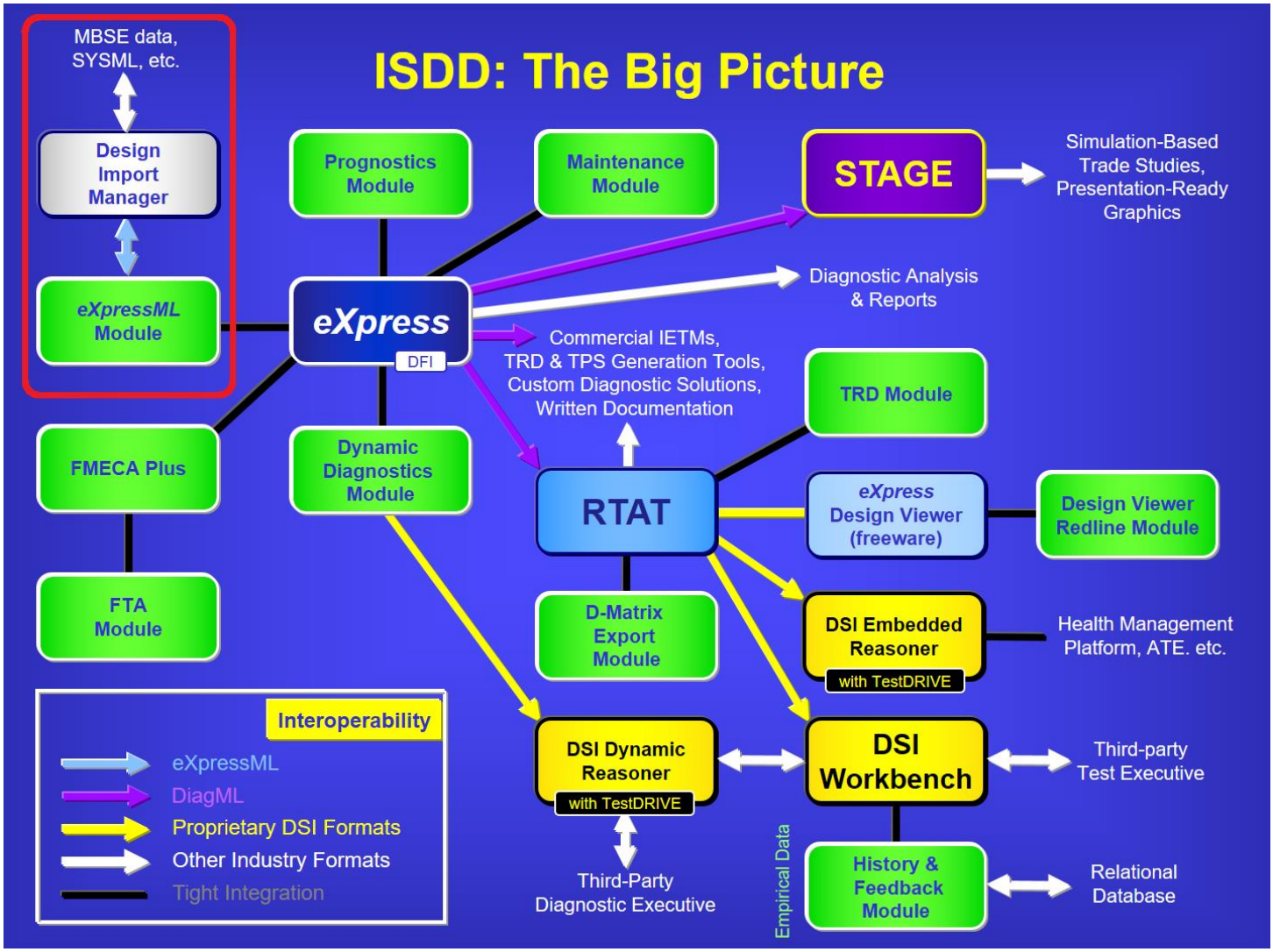
Interoperability – Sustainment Lifecycle
To ensure that any investment expended into "designing for MBSA" is capable of being directly "transitioned" to the (evolving) Sustainment paradigm, the output from the MBSA must extend beyond the boundaries of the Design Development Lifecycle. It must perform this seamless transition with ease and consistency while also being capable of migrating to future technologies before inclusion into the Development and Sustainment Lifecycle(s).

Diagnostic Engineering generates the "Trade Currency" to Support high-end MBSA

As a prerequisite for high-end MBSA requirements to become an integral layer within a variety of high-end MBSE and dynamic PLM Development environments, it must have agile "trade *currency*" that is shared at an equally robust level in order to continue to support any design or support discipline. This will enable the data to be (re)assessed, (re)optimized, updated or revised and actively "traded" against any other interdisciplinary design assessment(s) input or output data to discover the impact on the Maintenance philosophy (requirements) at any point over the sustainment lifecycle. Model-based Diagnostics Engineering must be performed at the same elite level as the MBSA to ensure the consistency, quality and reliability of the data as it transitions from the Development Lifecycle to & throughout, the Operational & Sustainment Lifecycle. To this purpose, "Diagnostics Engineering" shall provide the "currency" to trade, balance, validate and ensure that seamless, comprehensive & ongoing transition.

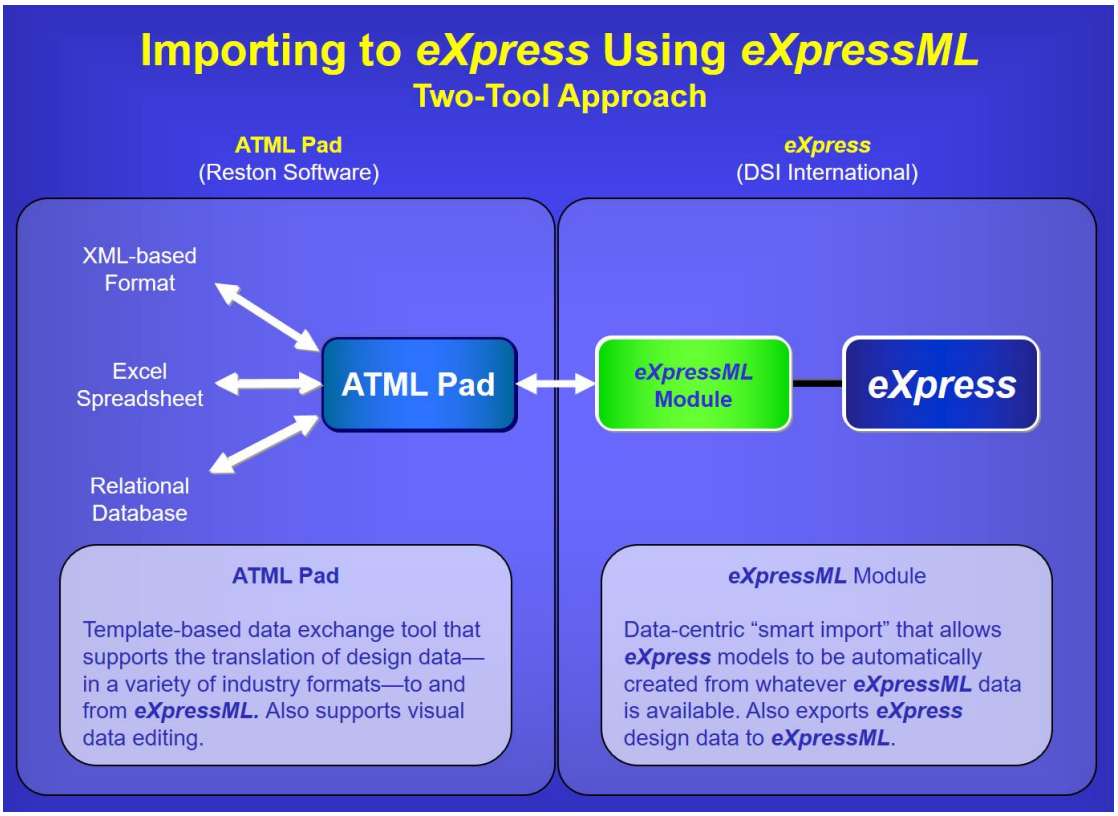
Capability to Model any Complex or Large System

DSI's *eXpress* software application is the core tool within an entire Model-Based Diagnostic Engineering environment that is highly interoperable with many other DSI Model-Based Reliability and Maintainability Engineering tools, but also with data from any other Reliability or MBSE tools commercially available in industry.



MBSE Diagnostics modeling in *eXpress*

Since ***eXpress*** is a high-end Model-based Diagnostics Engineering tool used throughout industry and also already at some level within (*your organization*) it serves as the central area of the "Integrated Systems Diagnostics Design" (ISDD) environment that enables a potpourri of alternatives to enrich any MBSE or MBSA paradigm. Notice the "double-headed" arrows on the "***eXpressML***" data import to ***eXpress***, which depicts the ***eXpressML*** export from ***eXpress*** to the MBSE environment as well.

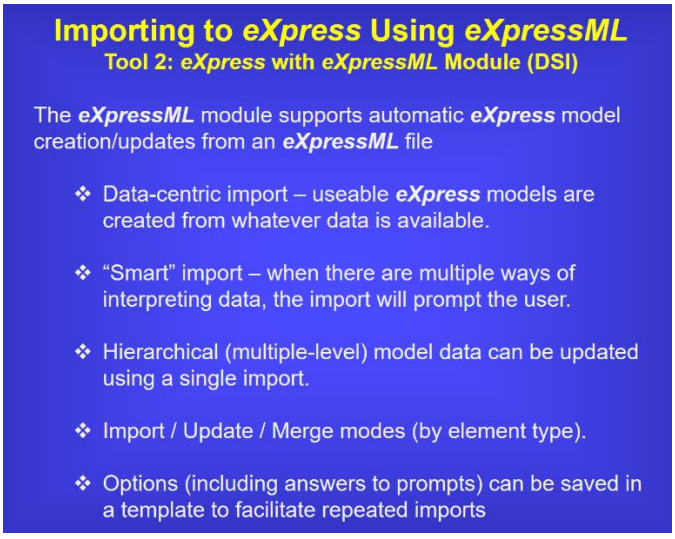


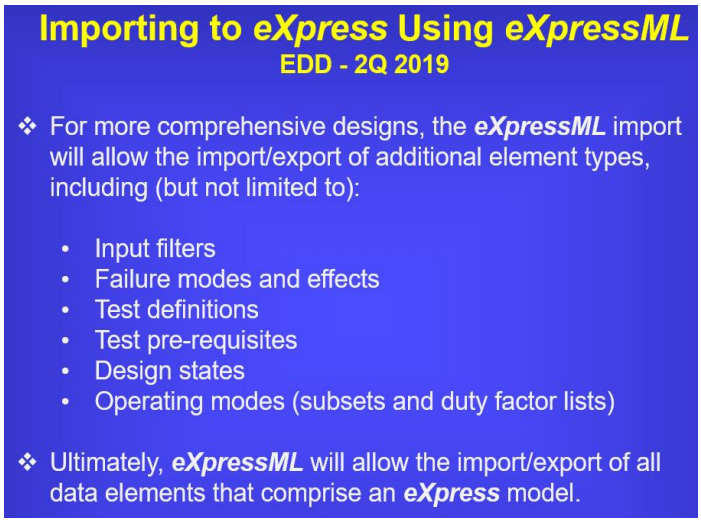
Auto-generation of the Functional Model of the designs at any hierarchical design level(s)

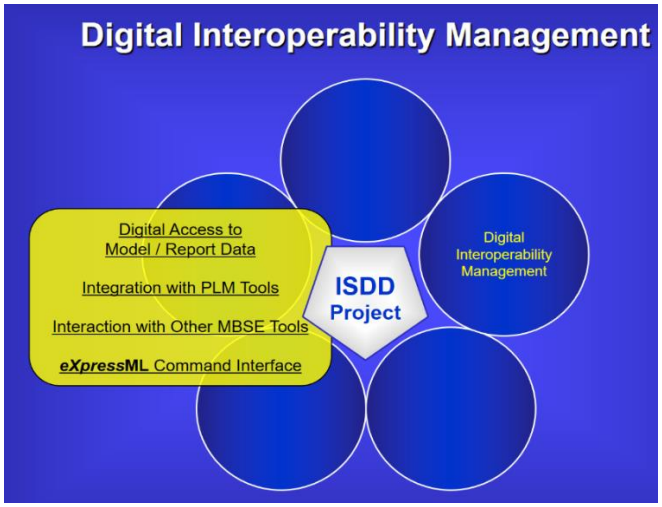
At its core, ***eXpress*** enables any or all of the functional and failure propagations to be captured in its "hybrid" dependency modeling paradigm, and can be performed at any time before, during or after design development. It's fullest capability is realized when used to "influence" design decision making as it vividly reports on the "diagnostic effectiveness" of any alternative design considerations that can be immediately shared within an MBSE or externally to a secured MBSE environment. These functional and failure propagations captured within ***eXpress*** will report on the "diagnostic value and utility" of any sensors or BIT considered within the design(s) of any of lower level assemblies cards, subsystems, etc. and/or any upper-level fully integrated systems at the operational asset level or higher.

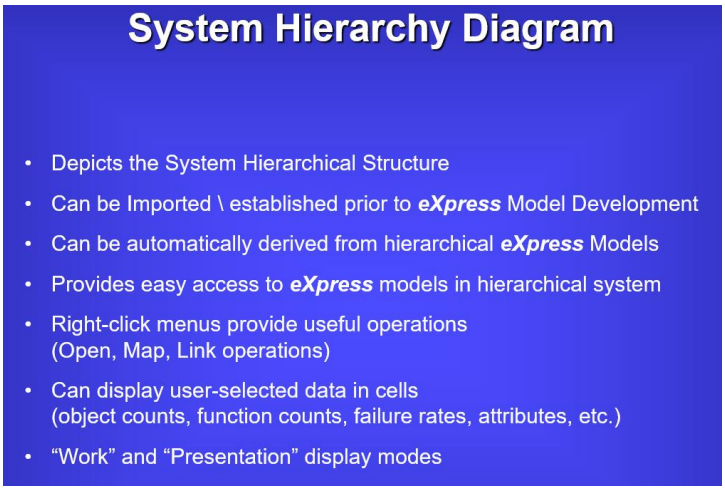
Data Validation and Analysis

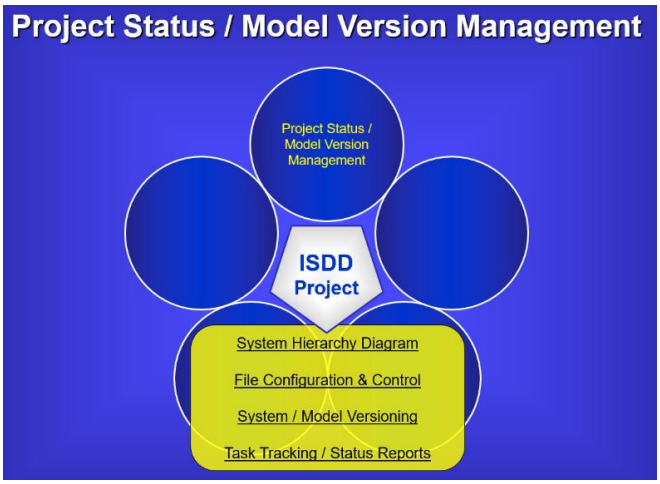
In ***eXpress***, all input and output definitions (flows and functions) are described and initially checked for modeling errors by the ***eXpress*** "Model Error Checker". As the design matures, is validated via several collaboration tools: The ***eXpress*** Design Viewer and the internal ***eXpress*** Desktop Fault Insertion capability ("DFI").











Model Scalability – a prerequisite for MBSA

Diagnostic Engineering Models of systems already performed within ***eXpress*** include complex Flight Control systems, aircraft carrier launching and arresting systems, multi-spectral targeting systems, radar and countless high-end missile systems. There is no technical limit to the domain or size of the models produced in ***eXpress*** by large military and defense, so model purpose, domain(s) or Scalability are not limitations.

Importing, reuse and repurposing of MBSE data using SysML or MS Excel

Data forms such as SysML or MS Excel (currently available) can be imported into the ***eXpress*** Model-based Diagnostics Engineering environment, which can be exported as "raw" data or "cooked" processed data for the diagnostic deployment or a myriad of purposes in the operational environment – including to the on-board or embedded diagnostic reasoning.

BIT (or Operational) "Test" Coverage

As each *test* and/or *failure* data is initially described in ***eXpress***, in terms of its "Test Coverage" – what "Diagnostic Conclusions" are learned when any test(s) (i.e. BIT, sensor, etc.) *passes*, or *fails*. This is integral expert design knowledge that ***is not***, otherwise captured in any MBSE or MBSA paradigm. This Test Coverage detail is considered throughout the system and full design and MBSA hierarchy (within ***eXpress***) and can be updated or modified at any time. Any design MBSA assessments are then computed on any aspect of the design after automatically elaborating this detail, and/or any other properties. The validation of any diagnostic BIT or sensors – at any, or all design level(s), is inherent to this approach and essential to assess and ensure operational effectiveness of MBSA.

Auto-generation of Testability Assessments – Fault Detection & Fault Isolation that impact MBSA

This is a core competency of ***eXpress*** as DSI pioneered, led, and still leads industry in the computation of Fault Detection and Fault Isolation for any design and for any purpose(s) to support any complex design – operationally or otherwise throughout the its full Product Lifecycle.

The integration of the Safety and Reliability Analysis is a capability of "*eXpress*"

Since the preponderance of the raw reliability data is available as "object attributes" within most advanced Reliability Engineering processes, typically in spreadsheet form, this data can be immediately imported into the ***eXpress*** design at any time or at any intervals in a MBSA & MBSE design environment. Such object attributes may include the typical component information such as failure rates, severities, reference ID's, port names & flow, operational states, part numbers, reference ID's, LCN, cost data, etc., or any additional attributes specified by the program. ***Attribute types are unlimited***.

Auto-generation of Functional Failure Modes, Effects

Because ***eXpress*** is a high-end Model-based engineering tool, it is able to "auto-generate" preliminary failure modes and failure effects for any design upon completion of the functional model capture in ***eXpress***. When more specific data is learned and desired to be "merged or swapped" into the model, the data can be easily imported, and (re)propagated whenever desired. This accentuates the agility inherent to this approach and further supports any PLM environment.

Select Failure Distribution "Attribute" for adjusting any Failure Probability

Since ***eXpress*** allows the inclusion of any type of failure probability calculation (Dormant, Weibull, Log Normal, Normal, Binomial, etc.) via a simple selection of a Failure Effect "Attribute", the effects of these calculations are inherently considered throughout the entire design and overarching system design hierarchy.

Auto-generation of (preliminary) Functional Hazard Analyses (SAE 4761)

Because ***eXpress*** is able to include and propagate the knowledge of root failure modes, failure effects and relevant component property attributes throughout the entire design hierarchy, the preliminary Functional Hazard Analysis can be auto-generated as an output product and/or described in a form that is traceable and mapped to the WBS.

Auto-generation of FMEA & FMECA Assessment products

Since ***eXpress*** is able to capture the functional and failure propagations within the context of discovering the diagnostic integrity of the design(s), it using any available Reliability (and Maintainability) data that also enables the automatic generation of the Traditional "standard" FMEA or FMECA's (MIL-Hdbk 1629A) but allows full customization.

Item	Failure	Mission Phases	Root Failure Mode Causes	Failure Effects			Compensating Provisions	Severity Class
				Local	Next Higher	End Item		
Fuel Pump	Fuel pump fails to pump fuel.	Landing	Mechanical Failure Electrical Failure	Engine shuts down during landing.	Loss of engine during landing.	Loss of engine during landing.	Compensated for by multiple engines and	MINOR
	Fuel pump fails to pump fuel.	Startup	Mechanical Failure Electrical Failure	Engine fails to start.	Vehicle fails to start.	Vehicle fails to start.		MINOR
	Fuel pump fails to pump fuel.	In Flight	Mechanical Failure Electrical Failure	Engine shuts down during flight.	Loss of engine during flight. Pilot/control adjustment to additional operating engine to keep vehicle running.	Loss of engine during flight. Pilot/control adjustment to additional operating engine to keep vehicle		CATASTROPHIC
Fuel Valve	Pressure restricted in valve	Landing	Valve Obstructed Mechanical Failure due to damaged or worn components	Engine shuts down during landing.	Loss of engine during landing.	Loss of engine during landing.	Compensated for by multiple engines and end-of-flight.	MINOR
	Pressure restricted in valve	In Flight	Mechanical Failure due to damaged or worn components Valve Obstructed	Erratic engine operation in flight.	Engine operates erratically during flight. Pilot compensates with power adjustments between engine.	Engine operates erratically during flight. Pilot compensates with power adjustments between engine.		CRITICAL
	Pressure restricted in valve	Startup	Mechanical Failure due to damaged or worn components Valve Obstructed	Engine fails to start.	Vehicle fails to start.	Vehicle fails to start.		MINOR
	Valve stuck open or closed.	Landing	Mechanical Failure due to damaged or worn components Electrical Failure	Engine shuts down during landing.	Loss of engine during landing.	Loss of engine during landing.	Compensated for by multiple engines and end-of-flight.	MINOR
	Valve stuck open or closed.	In Flight	Mechanical Failure due to damaged or worn components Electrical Failure	Engine shuts down during flight.	Loss of engine during flight. Pilot/control adjustment to additional operating engine to keep vehicle running.	Loss of engine during flight. Pilot/control adjustment to additional operating engine to keep vehicle		CATASTROPHIC
	Valve stuck open or closed.	Startup	Mechanical Failure due to damaged or worn components Electrical Failure	Engine fails to start.	Vehicle fails to start.	Vehicle fails to start.		MINOR
Landing Gear	Landing gear fails on ground.	Startup	Mechanical Failure	Landing gear failure on ground.	Landing gear fails on ground.	Landing gear fails on ground.		MINOR
	Landing gear fails on landing.	Landing	Mechanical Failure	Unable to extend landing gear.	Landing gear fails to extend during landing. Pilot attempts to manually extend gear.	Landing gear fails to extend during landing. Pilot attempts to manually extend gear.		CATASTROPHIC
	Landing gear fails to retract.	In Flight	Mechanical Failure Electrical Failure	Unable to automatically retract landing gear.	Landing gear fails to retract during flight. Drag on vehical performance during operation of vehical in flight.	Landing gear fails to retract during flight. Drag on vehical performance during operation of vehical in flight.		MARGINAL
VCU	Control failure prevents startup of system.	Startup	Power Supply Failure Discrete Output Buffer Failure Discrete Output Failure Controller Failed	Loss of control power during startup. Engine fails to start.	Vehicle fails to start.	Vehicle fails to start.		MINOR

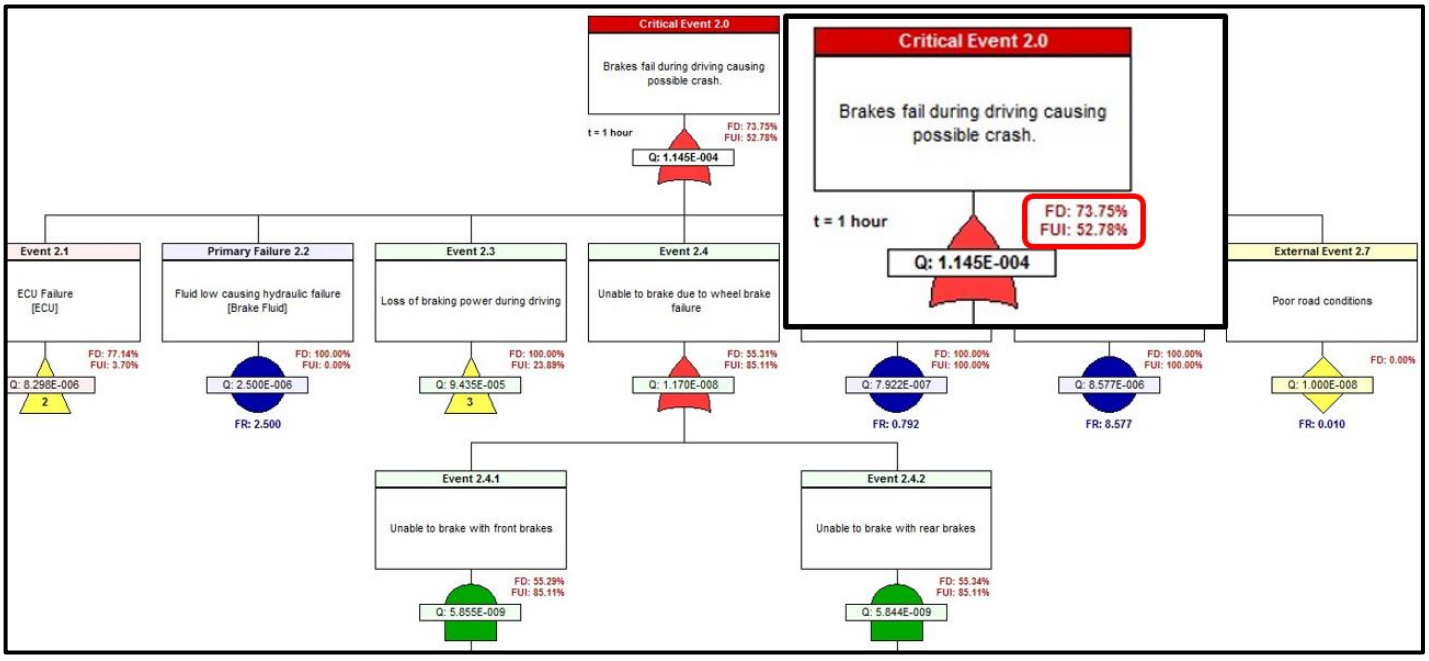
Auto-generation of FMEA & FMECA Assessment products – upon demand to Support MBSA

Additionally, ***eXpress*** enables any desired number of columns to be added and adjoined within the FMECA to describe such diagnostic details about each component as Failure Detected, Number of Root Failure Modes in each Fault Group and the size & constituency of that Fault Group. It can also describe if the Failure is "Uniquely Isolated" in this "Diagnostics-Informed" FMECA, as well as being identified as "FUI" in any Reliability Assessment products generated as outputs from the ***eXpress*** Model (see images of FTA below). Not fully discovering and considering the impact of FUI will have a negative impact on the operational value realized from any MBSA.

Failure	Item	Failure Rate	Severity Class	Relative Criticality	Diagnostic Coverage				
					Failure Detected	Fault Isolation			
						Uniquely Isolated	Number of Root FMs in Fault Groups	Fault Groups	Fault Group Sizes (Number of Items)
Hydraulic Leak	FS Line	38.026486	Loss of Life	38.0265	Yes	Yes	1	Fault Group # 88	1
Hydraulic Leak	FR Line	38.026486	Loss of Life	38.0265	Yes	Yes	1	Fault Group # 89	1
Forward Pump Failure	Front Pump	19.013243	Loss of Life	19.0132	No	N/A	N/A	N/A	N/A
Rear Pump Failure	Rear Pump	19.012853	Loss of Life	19.0129	No	N/A	N/A	N/A	N/A
L Brake Light Bulb Failure	L Brake Bulb	87.751628	Degraded Performance	17.5503	Yes	Yes	1	Fault Group # 82	1
R Brake Light Bulb Failure	R Brake Bulb	87.751628	Degraded Performance	17.5503	Yes	Yes	1	Fault Group # 84	1
W Brake Light Bulb Failure	RW Brake Bulb	87.751628	Degraded Performance	17.5503	Yes	Yes	1	Fault Group # 85	1
Battery dead	BATTERY	41.639002	Loss of Operation	16.6556	Yes	No	2	Fault Group # 0	1
Solenoid Control Relay Coil Open	Solenoid Relay	11.573041	Loss of Life	11.5730	No	N/A	N/A	N/A	N/A
Battery Fuse Blown	Fuse	11.407946	Loss of Life	11.4079	Yes	Yes	1	Fault Group # 1	1
Pump Relay Cotact Stuck Open	Pump Relay	11.129475	Loss of Life	11.1295	Yes	Yes	1	Fault Group # 23	1
Brake Light Switch Stuck Open	Brake Light SW	9.919749	Loss of Life	9.9197	Yes	No	2	Fault Group # 83	1
Pad1 Wear Beyond Limit	LR Disc Assy:PADS	9.393689	Loss of Life	9.3937	Yes	No	4	Fault Group # 105	1
Pad1 Wear Beyond Limit	LF Disc Assy:PADS	9.393689	Loss of Life	9.3937	Yes	No	4	Fault Group # 102	1
Pad1 Wear Beyond Limit	RR Disc Assy:PADS	9.393689	Loss of Life	9.3937	Yes	No	4	Fault Group # 104	1
Pad1 Wear Beyond Limit	RF Disc Assy:PADS	9.393689	Loss of Life	9.3937	Yes	No	4	Fault Group # 103	1
Tread Worn	LR Tire	45.000000	Degraded Performance	9.0000	No	N/A	N/A	N/A	N/A
Worn Tread	RF Tire	45.000000	Degraded Performance	9.0000	No	N/A	N/A	N/A	N/A
Worn Tread	LF Tire	45.000000	Degraded Performance	9.0000	No	N/A	N/A	N/A	N/A
Worn Tread	RR Tire	45.000000	Degraded Performance	9.0000	No	N/A	N/A	N/A	N/A
Pedal Linkage Failure	Brake Pedal	8.577227	Loss of Life	8.5772	Yes	Yes	1	Fault Group # 3	1
Ignition Switch Stuck Open	Ignition Switch	8.415525	Loss of Life	8.4155	Yes	Yes	1	Fault Group # 2	1
Solenoid Control Relay Ccontact stuck ATCM	Solenoid Relay	7.661896	Loss of Life	7.6619	Yes	Yes	1	Fault Group # 81	1
Solenoid Control Relay Ccontact stuck GND	Solenoid Relay	7.661896	Loss of Life	7.6619	Yes	Yes	1	Fault Group # 80	1
Hydraulic Leak	RS Line	38.027272	Degraded Performance	7.6055	Yes	Yes	1	Fault Group # 86	1
Hydraulic Leak	RR Line	38.027272	Degraded Performance	7.6055	Yes	Yes	1	Fault Group # 87	1

Auto-generation of *eXpress* Fault Tree Analysis

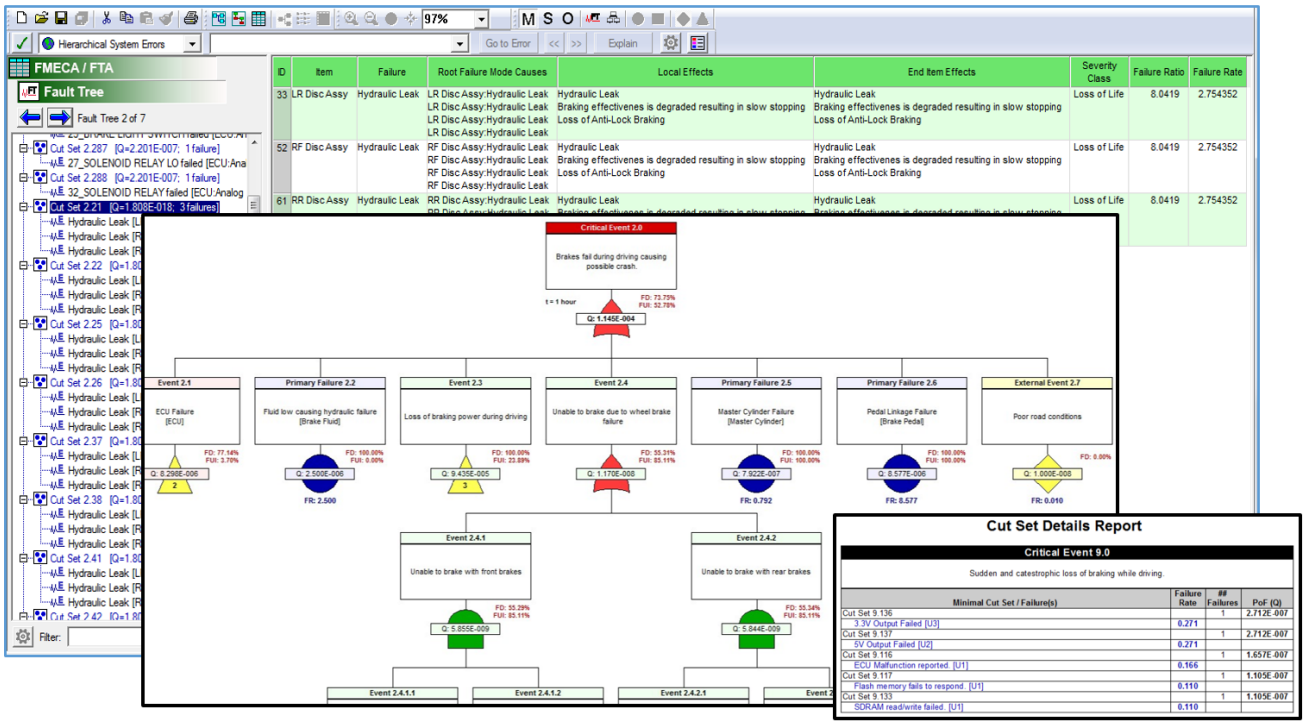
The ***eXpress*** Fault Tree Analysis (FTA) is calculated and produced as an "output" from the captured diagnostic design in ***eXpress*** (see image below). Unique to the ***eXpress*** FTA is that each node of the FTA will identify the probabilities of detecting a failure at any node ("FD") of the FTA - and the percentage of that Failure that can be "Uniquely Isolated" (identify the "root cause" to a specific Failure Mode) at that node in the FTA – integral to a high-end MBSA process. The inability to discern the specific root cause (Failure Mode) is a heavy contributor to False Alarms and Operational Aborts.



Reporting of FTA "Cut Sets" in the ***eXpress*** FTA & FMECA

Simultaneous Auto-generation of *eXpress* "Critical Failure Diagnoses Chart" (Diagnostics-Informed FMECA: second image above) and the interdependent *eXpress* Fault Tree Analysis (FTA) at any point during design development. This critical Reliability Assessment product ensures cross-validation between the FMECA and the FTA. Both the FMECA and FTA assessment products are generated using the same diagnostic knowledgebase from the *eXpress* Model. The typical "Cut Sets" are also co-identified within the FMECA and/or the FTA. Concurrently, automated detailed "Cut Set" reports produced by *eXpress* for any FMECA/FTA generated in *eXpress* along with the full breadth of traditional Safety Assessment reports (Cut Set Details, Important Measures, etc.) but also a "Failure Mitigation Report" to discover mitigated single-point failures.

Furthermore, and since all of these companion assessment products are generated as co-dependent outputs from any model or system model within *eXpress*, any variation, change or update to the *eXpress* model(s) during the development process can be immediately reported back into the PLM or high-end MBSE design development processes for SME validation and further MBSA trade study analyses. Refer to an example of the *eXpress* FMECA/FTA toggle capability and the FTA Cut Set outputs in the image below:



MBSA Value Transitioned to Operational Environment

Without equally high-end Diagnostics Engineering, any investment into MBSA within an MBSE environment, will not be able to ensure that the operational level (or any ensuing maintenance level continued thereafter) implementation of the Health Monitoring/Managing will be able to be fully realized. To discover the strengths and weaknesses of the MBSA as it corresponds to the operational environment it would require that the MBSA be compared to results learned from the performing of an operational support simulation whereby any failures can be simulated during any mode or operational state of operational vehicle or asset.

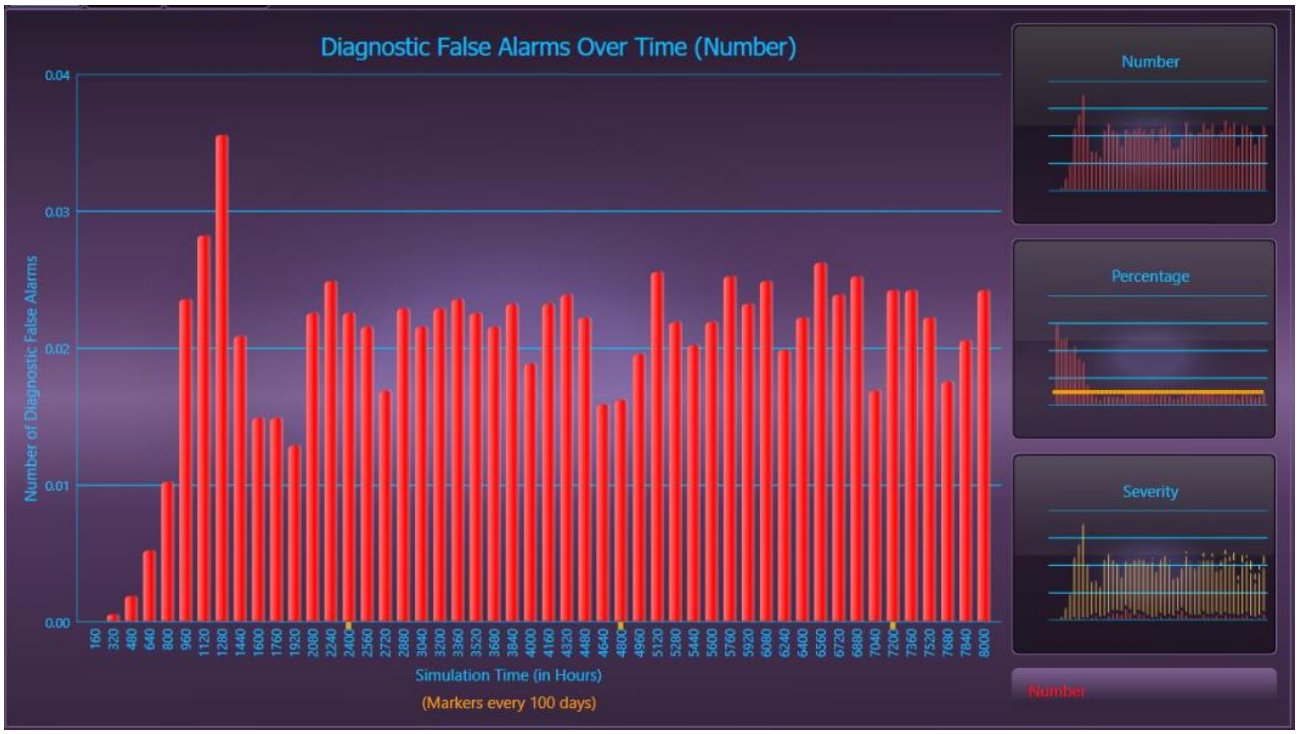
The Simulation of failures to Ensure Accuracy of Corrective Action(s)

The simulation of failures will allow us to examine if the critical failure(s) can be detected or decisively isolated to any critical root cause (failure mode) as declared in the MBSA within the companion FMECA, at the operational System's level. While the ***eXpress*** FMECA/FTA identifies such Safety Assessment metrics to be determined and included within any selection of static report forms, the "STAGE" operational support simulation will determine the impact of the occurrence of any possible failure(s), including critical failures, during any specified "Sustainment Lifetime". The "STAGE" Simulation will allow the assessing of any mixture of maintenance paradigms of Run-to-Failure (RTF), Preventative (RCM), Conditioned-Based (CBM) and Predictive (PdM) to analyses operational trades, benefits, degradations and costs in over 100 graphs.

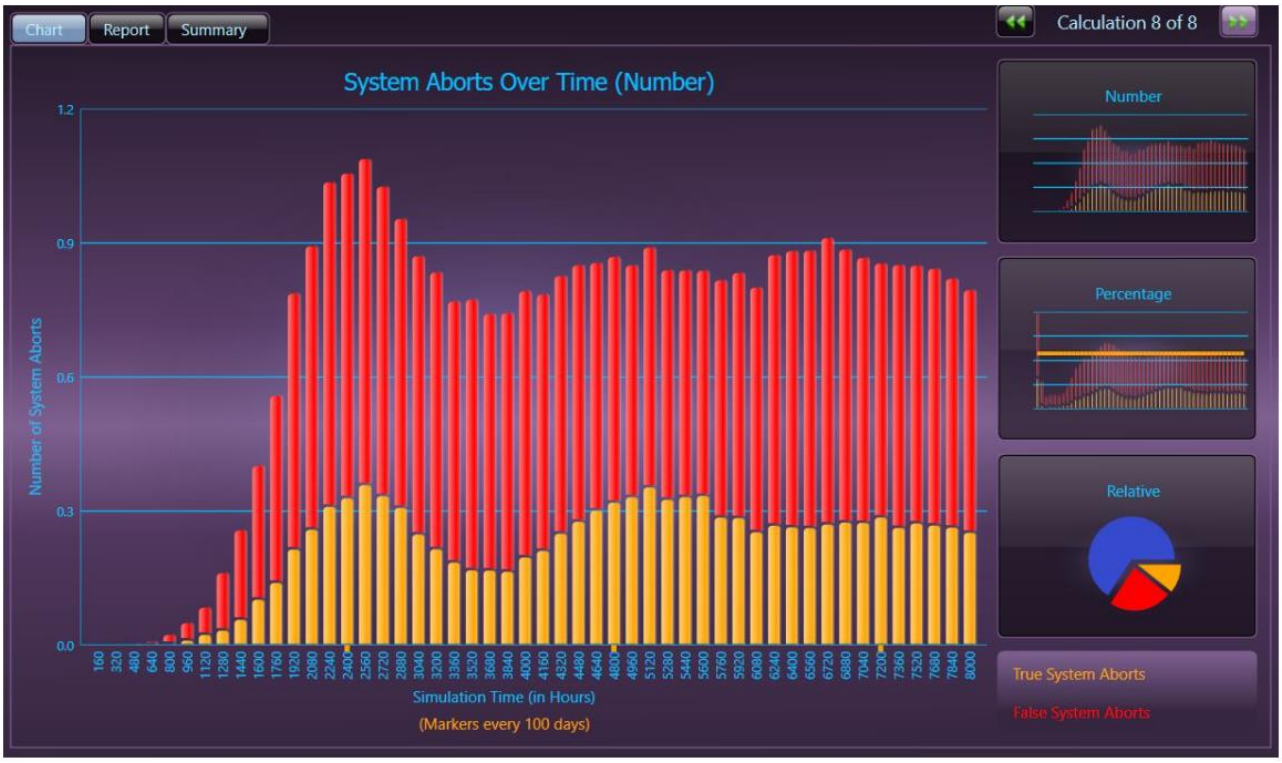
Operational Support & MBSA Simulation - Since the *STAGE* Simulation is cognizant of:

1) The "Test Coverage" of each and every sensor (BIT) & all Diagnostic Fault Group Constituency
2) All Failures that are and are not Detectable at specific periods during any Operational Diagnostic Interrogation
3) Includes all Failure Rate, Failure Modes data & computes Failure Propagation knowledge throughout the System
4) Considers the Realization of how a System is maintained impact how it fails throughout the Sustainment Lifecycle.

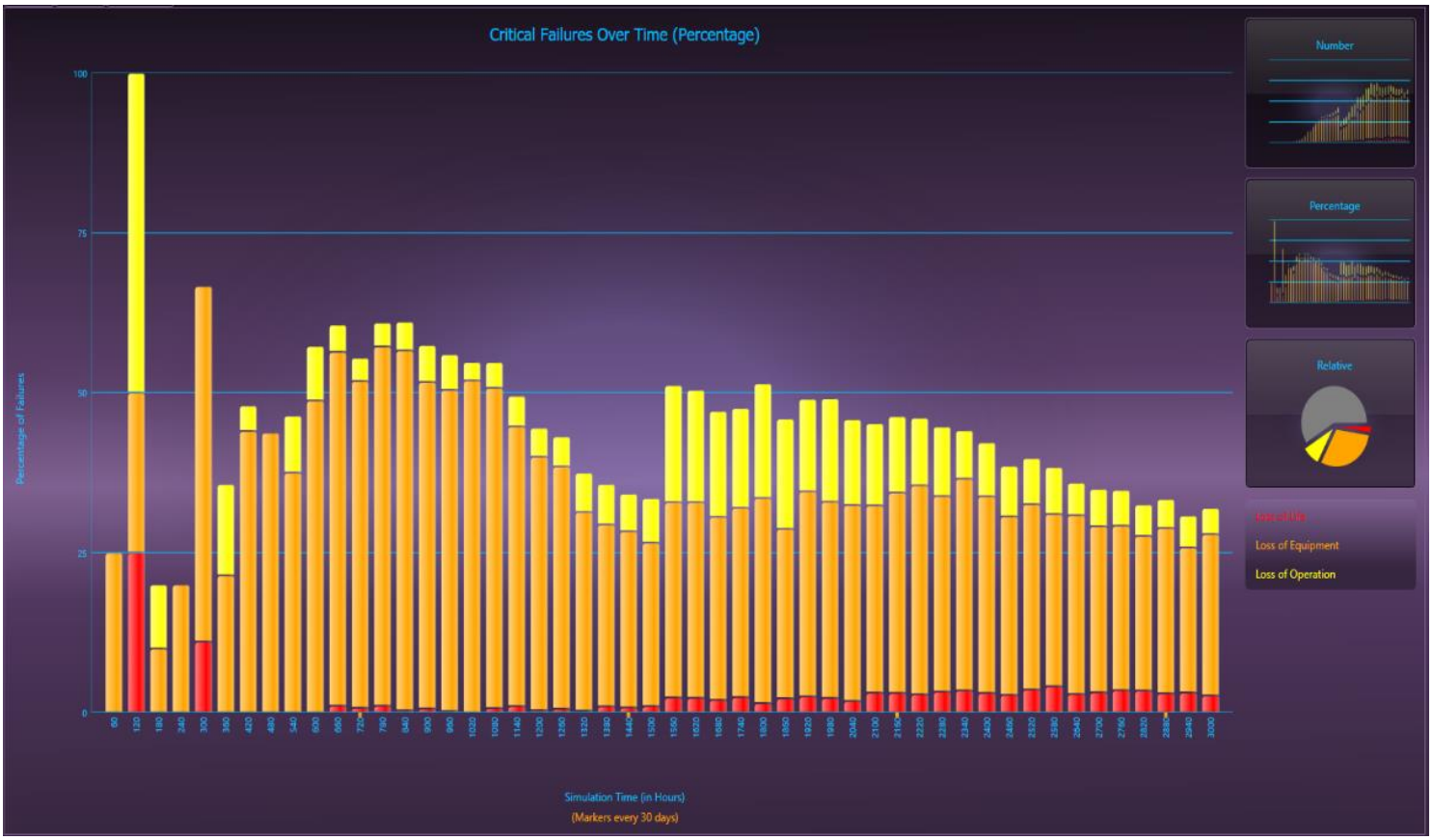
Refer to the initial outputs from the STAGE Simulation that are relevant for core MBSA metrics in the images below:



Diagnostic False Alarms (False Alarms due to constraints in Diagnostic Design)
Graph considers Replacements due to any Maintenance Activities



True and False System Aborts (Aborts due to constraints in Diagnostic Design)
Graph considers Replacements due to any Maintenance Activities



Critical Failures (Simulates the expected Critical Failures in accordance to Severity)
Graph considers Replacements due to any Maintenance Activities

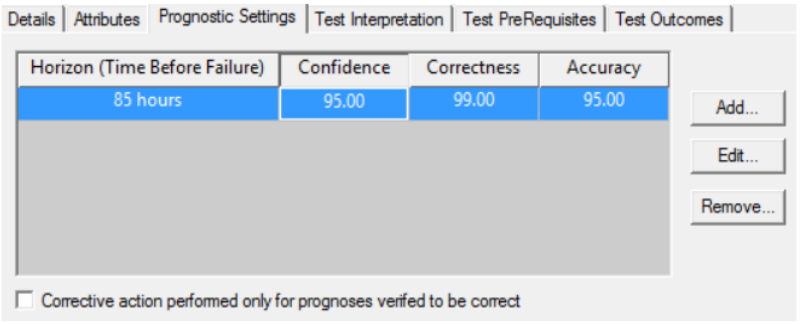
Impact of Prognostics (and PHM) on Corrective Actions as determined in MBSA

The MBSA must be able to consider the "impact of Prognostics Design" at any time during the Development Lifecycle. To this end, MBSA must be able to consider the operational effectiveness of very low-level Physics of Failure (PoF) analyses for Safety and Risk Mitigation objectives. This area of PHM can become extravagant or ineffective if not strictly worked within the structure of a full MBSE process that is around an MBSA, and is accountable to the operational effectiveness in the sustainment environment. This accountability can be examined, once again, by using Diagnostics Engineering as a means to provide operational and maintainability effectiveness assessments during design development.

Integrating Resultant Data from PoF into the MBSA

To determine the impact of PHM in the MBSA as an integral contributor to any high-end MBSE processes, common data types & formats can provide the infrastructure to perform consistent, objective and holistic data MBSA analyses and also seed the Operational Support Simulation (see above).

Any other required "attributes" (i.e. for HAZOP, etc.) are fully captured and integrated into the MBSA as needed.



Effectiveness of PHM in an MBSA

The first step is to determine the best candidates for Health Monitoring or Health Management at the operational asset level. With this approach to using MBSA, investment into development of advanced sensor technologies is based upon the "diagnostic effectiveness" of the proposed BIT to be used for any PHM application. PHM candidates can be selected on the basis of safety, risk mitigation and operational value (high non-recurring development costs), rather than solely on the size of the corresponding PHM budget.

Prognostic Candidates Report

Scope: Diagnostic Only
Hierarchy Selection: All Levels

Summary

Average Failure Probability (Top 25 FMs): 0.024798
Average Failure Probability (Entire Scope): 0.002660

Expected Repair Time (Top 25 FMs): 16.89 minutes
Expected Repair Time (Entire Scope): 93.81 minutes

Prognostic Candidates (Top 25)

Failure Mode	Item	Repair Time (in minutes)	Maximum Severity	Failure Probability	Ranking
Battery dead	BATTERY	15.00	Category III - Marginal	0.035559	107.14
Hydraulic Leak	FR Line	30.00	Category III - Marginal	0.032471	97.80
Hydraulic Leak	FS Line	30.00	Category III - Marginal	0.032471	97.80
Tread Worn	LR Tire	10.00	Category IV - Minor	0.038429	82.92
Worn Tread	RR Tire	10.00	Category IV - Minor	0.038429	82.92
Hydraulic Leak	RS Line	30.00	Category IV - Minor	0.032471	64.68
Hydraulic Leak	RR Line	30.00	Category IV - Minor	0.032471	64.68
Output Failed	ECU:U2	4.00	Category I - Catastrophic	0.000232	62.09
Output Failed	ECU:U3	4.00	Category I - Catastrophic	0.000232	62.09
Major hydaulic leak while driving.	RR Line	30.00	Category I - Catastrophic	0.000003	62.00
Major hydaulic leak while driving.	RS Line	30.00	Category I - Catastrophic	0.000003	62.00

Integrating Resultant Data from PoF into the MBSA

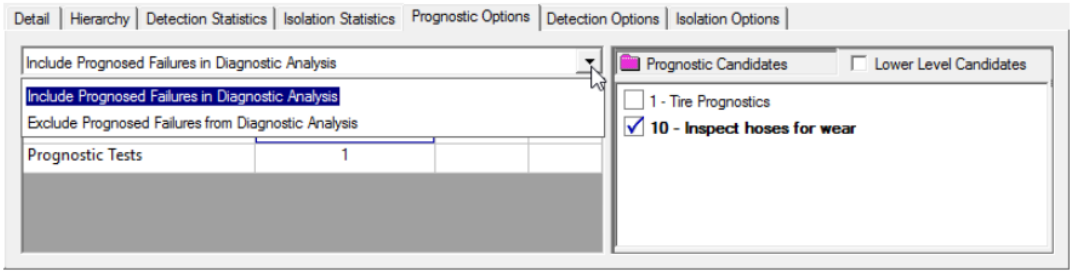
For less obvious critical, and non-single-point critical failures, a holistic diagnostic analyses will be able to fully rank the criticality of the failure(s) along with any other factor, including Failure Probability, Repair Time, Maximum Severity, etc.

All or any of these "Prognostic Candidates" that are being considered early, and throughout the MBSA & Design Development Process, can be continually (re)ranked at any time. As design modifications are considered, all of these rankings may be affected, but since all of these reports are simple one-click outputs from the same captured diagnostic knowledgebase, these reports are available upon demand.

Furthermore, any of these design alternatives that are performed during the MBSA, can also be seamlessly transferred to the Operational Support Simulation for a myriad of data analytics and costing to support Lifecycle cost/benefit objectives.

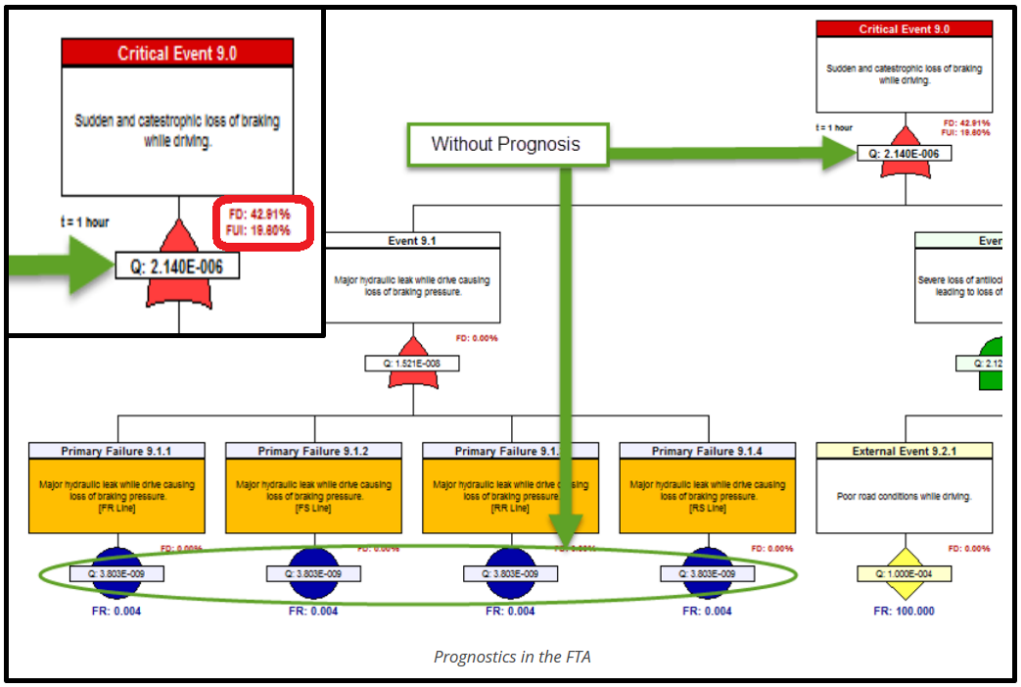
Prognostics within the Testability Analysis

Prognostics are used in *eXpress* diagnostics by selecting prognostic tests candidates and by selecting whether to include or exclude the prognosed failures in the diagnostic analysis.

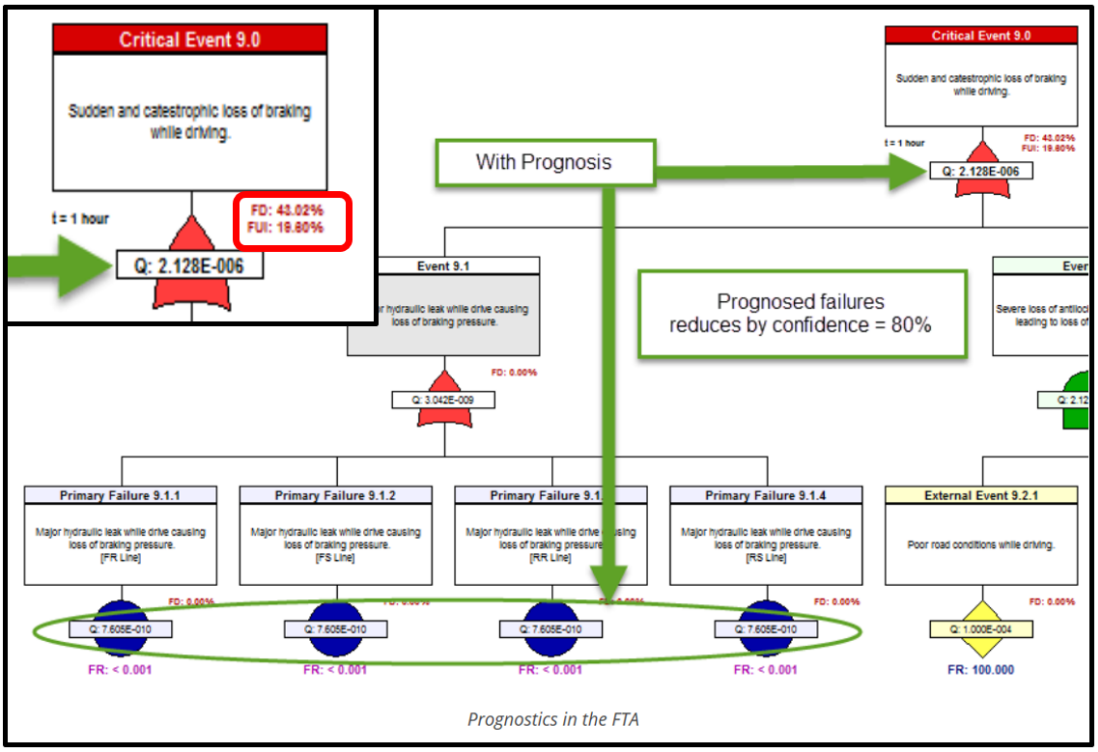


Impact of PHM in an MBSA

Since the high-end Diagnostics Engineering capability is able to determine the Test Coverage of any (proposed or deployed) sensors or BIT (per operational mode, etc.) and is fully cognizant of the propagations of any failure to the lowest root cause, it is able to immediately generate turnkey outputs of the FTA that considers PHM in the MBSA – per cut set.



Prognostics in the FTA



Prognostics in the FTA

Impact of PHM in an MBSA

In the images above, the top image easily identifies the single-point failures in a mode where the FTA fills the region with an orange color, which signifies that PHM may benefit by drawing attention to these areas. Then, when the results from any PoF analysis (or using, less specifically, historical data) are able to be factored into the captured Diagnostic Engineering knowledgebase, their contribution to the reduction in the likelihood of experiencing a critical failure is immediately computed for each impacted cut set.

The most overlooked contribution that Diagnostics Engineering brings to this FTA portion of the MBSA is that it determines the capability of the PHM to detect and identify the root failure cause(s) within each specific branch or cut set of the FTA. Too often, the Safety Analysis is performed and there's no "certainty" to the actual portion, if any, of critical failure(s) is able to be observed by the on-board BIT used with or without specifically developed PHM-targeting sensors.

Auto-Assign & Manage (BIT) Fault Codes – Accurately indict failing component(s)

In this solution, the BIT Fault Codes can be associated directly to the fault group and/or the root failure mode during MBSA. By using the full hierarchical knowledge of the system's diagnostic constraints, this approach uniquely determines which root failures are observed by the BIT, those that are not, and when certain root failures may not be covered in the BIT (see "FUI").

Enriching BIT Fault Codes "entry points" with Diagnostic Heath Status Knowledge

Additionally, when performed in a high-end MBSA application, BIT codes enable the diagnoses to be "continued" from the on-board PHM capability to the off-board Automatic or Manual Testing implementation(s). This is performed without losing any diagnostic integrity in the transitioning from one paradigm to the next. Replacing the correct failing component(s) in any ensuing maintenance activity provides an optimum method to mitigate safety risks due to mis-isolation of critical failures.

PHM-Informed MBSA

The prerequisite for the assessing of the expected operational value of PHM-informed MBSA is to, again, leverage the diagnostic engineering currency:

1) "Select" Prognostic Candidates
2) "Discover" the impact on Risk Mitigation in the FTA
3) "Balance" PHM with any other mix of maintenance requirements, strategies (RTF, RCM, CBM, PdM) and costing
4) "Transition" optimized MBSA to the operational environment using companion Diagnostic Knowledgebase

Committee members of PHM

DSI is an active (2019) participant in the IEEE SCC20 for developing an Industry Standard in support of PHM.

Existing MBSA Tools Identified in this document

Below is a chart that identifies the commercially Licensable Software tools mentioned throughout this document. While any "Product Lifecycle" ambitions will ultimately be constrained by its effectiveness to transfer such detailed design assurance to the operational environment, restricting to the scope of this inquiry, DSI has thereby not described its commercially available Diagnostic Reasoning tools to accommodate these integral objectives.

Design Tools	Plug-Ins	Generic Descriptions
eXpress	Module that allows FMECA data (either imported or developed in ***eXpress***) to be enhanced with metrics derived from ***eXpress*** diagnostics. Automatically included with all ***eXpress*** licenses.	
	eXpress**ML Module**	Module that allows ***eXpress*** model data to be imported from XML (including ***eXpress*****ML** and SysML). Local or hierarchical models can be created from a single import.
	FMECA Plus	Module that allows FMECA data (either imported or developed in ***eXpress***) to be enhanced with exhaustive attributes and metrics derived from ***eXpress*** diagnostics.
	FTA Module	Fully integrated with FMECA Plus and the ***eXpress*** diagnostics, this module allows ***eXpress*** to produce diagnostic/prognostic-informed fault trees for Reliability and MBSA (Safety analysis).
	Prognostics Module	Module that allows ***eXpress*** to analyze the impact of prognostics upon diagnostic performance. Prognostic definitions can also be exported to be used in trade studies within STAGE.
	Maintenance Module	Module that allows ***eXpress*** to support multiple levels of diagnosis. Facilitates the concurrent development of embedded diagnostics and troubleshooting procedures for Technicians (IETMs).
STAGE	Using data from ***eXpress,*** STAGE simulates failures, diagnoses and repairs that would occur in a fielded system. Over 100 Calculations (represented as graphs) show changes over time, as well as the impact of maintenance upon failure. STAGE supports case studies involving different "cocktails" of maintenance approaches (Predictive PdM, Preventative RCM, Conditioned-Based CBM, and Run-to-Failure RTF).	
RTAT	The *eXpress* Run-Time Authoring Tool (RTAT) allows diagnostic procedures exported from ***eXpress*** to be enhanced with graphic overlays and links to external documents. Diagnostics can also be reformatted (ATML, PDEL, S1000-D) for use in sequencing the diagnostics in a variety applications including, Embedded Reasoning, ATE or Portable Maintenance tools.	
	TRD Module	Plug-in module that allows RTAT to populate a Test Requirements Document (TRD) with test sequencing & attribute data from ***eXpress***
eXpress **Design Viewer**	The **eXpress** Design Viewer allows design and diagnostic data to be shared and/or reviewed on systems where *eXpress* has not been installed. This not only facilitates team collaboration and in-house reviews, but also provides a deliverable for customer evaluation.	
ATML Pad	ATML Pad manages the complexity of the ATML formats, allowing you to focus on describing your tests. It abstracts XML ID references, allowing the selection of the referenced item from a list. In addition, ATML Pad can generate XML IDs automatically and ensures that IDs remain unique while editing the data.	