Introduction to Diagnostic Engineering using the ISDD Tool Suite

January 2020

DSI international, inc.

Who We Are

DSI International

40 Years of Diagnostic Engineering

Logic Modeling

MIL-M-24100B
Functionally-Oriented Maintenance Manuals
(1974)

LOGMOD (1978)

MIL-STD-2165
Testability
(1985)

STAT (1988)

MIL-HDBK-1814
Integrated Diagnostics
(1991)

***eXpress* (1998)**

IEEE 1522
Testability & Diagnosability
(2004)

***STAGE* (2008)**

40 Years of Run-Time Solutions

LOGMOD ("GiB")
(1977)

SAMA
(1981-1985)

SPIFI
(1989)

DiagML
(2001)

GADDS / DOKTOR
(1992)

Run-Time
Authoring Tool
(2010)

DSI Workbench
(2011)

DSI Embedded
Reasoner
(2017)

DSI Dynamic
Reasoner
(2018)

Desktop Fault
Insertion
(2005, 2016, 2018)

DSI is the World's Leading Provider of Diagnostic Engineering Software

Current U.S. Customers

Aerospace & Defense

BAE Systems
Boeing
General Atomics
General Dynamics
Honeywell
Lockheed Martin
Northrop Grumman
Raytheon
Sikorsky

Government

U.S. Army
U.S. Navy
- NAVAIR/NAVSEA

Commercial

GE Transportation
Thermo King

Over 500 licenses sold worldwide

DSI is the World's Leading Provider of Diagnostic Engineering Software

International Customers

Europe

SPHEREA [FR / UK]
MBDA [FR / UK]
NEXTER (GIAT) [FR]
Safran (SAGEM / Zodiak) [FR]
THALES [FR]
French DGA

Middle East

Hewlett-Packard (Israel)

Asia

Aviation Technologies (China)
Dongfanghong Aircraft (China)
Ishikawajima HI (Japan)
Kingswell Enterprises (China)
Mitsubishi HI (Japan)
Shiji Electronics (China)
Tianwei Industry (China)
Xi'an Industries (China)
Yuntong Technology (China)

DSI Has Extensive Experience on Major Programs

2nd Gen RLV

Future Combat Systems

F-35 (JSF)

TSAT Satellites

CVN-76 Nimitz-Class Supercarrier

Comanche Helicopter

AIM-9X Evolved Sidewinder Missile

X-33 VentureStar

New Evolution Locomotive

Eurofighter

Space Operations Vehicle (SOV)

Crusader Self-Propelled Howitzer

Fire Scout UAV

Recent Programs That Have Used *eXpress*

JLENS (Raytheon)

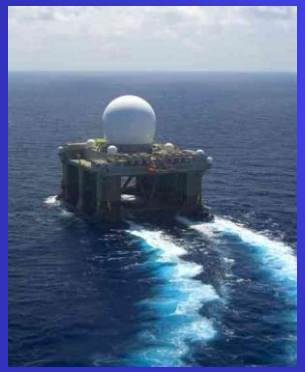
Global Hawk (Northrop)

CH-53K (Sikorsky)

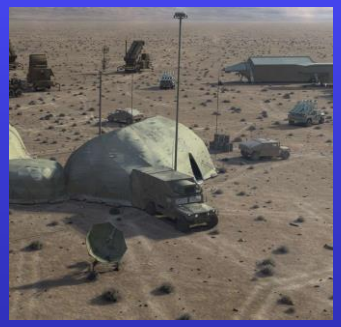
JASSM (Lockheed)

GCV (BAE Systems)

Predator – MTS (Raytheon)



X-Band Radar
(Raytheon)



IBCS
(Boeing / Northrop)

Standard Missile
(Raytheon)

Current Programs Using *eXpress*

Triton (Northrop)

Small Diameter Bomb
SDB-II & III (Raytheon)

KC-767 Refueling Tanker
(Boeing)

CVN-78 – EMALS/AAG
(General Atomics)

Bradley Vehicle
(BAE Systems)

Standard Missile (Raytheon)

What We Do

Four Main Goals of Diagnostic Engineering

Subsidiary Benefits of Diagnostic Engineering

Availability

Cost of Ownership

Effective Isolation to
Optimum Repair Level

Lower MTTI / MTTR

Reduced False Removals

Improved MTBF

Lower Maintenance Costs

Improved Fault Detection

Reduced False Alarms

FMECA / Fault Tree Analysis

Reduced System / Mission Aborts

Probabilistic Risk Assessment

Unique Isolation of
Critical Failures

Mission Success

Safety

Fault Detection & Isolation in *eXpress*

Detection Order Report

Summary

Total Detection Tests:	17
Total Functions Detected:	92.68%
Total Probability Detected:	97.34%
Aggregate Failure Rate:	34634.054901
Mean Time Between Failures (MTBF):	28.87 hours

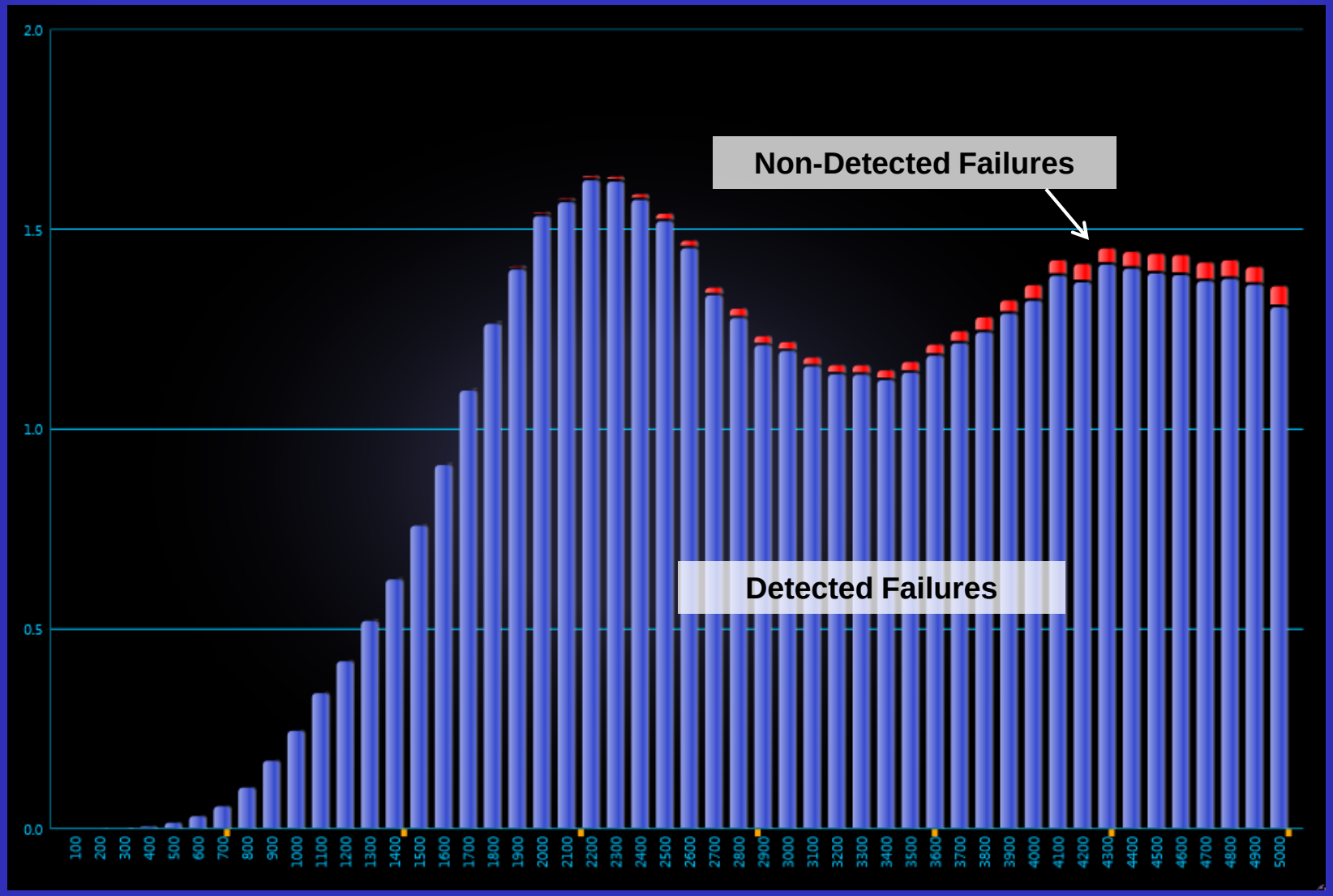
Fault Isolation Report

Multiple Failure
Fault Group Size Statistics

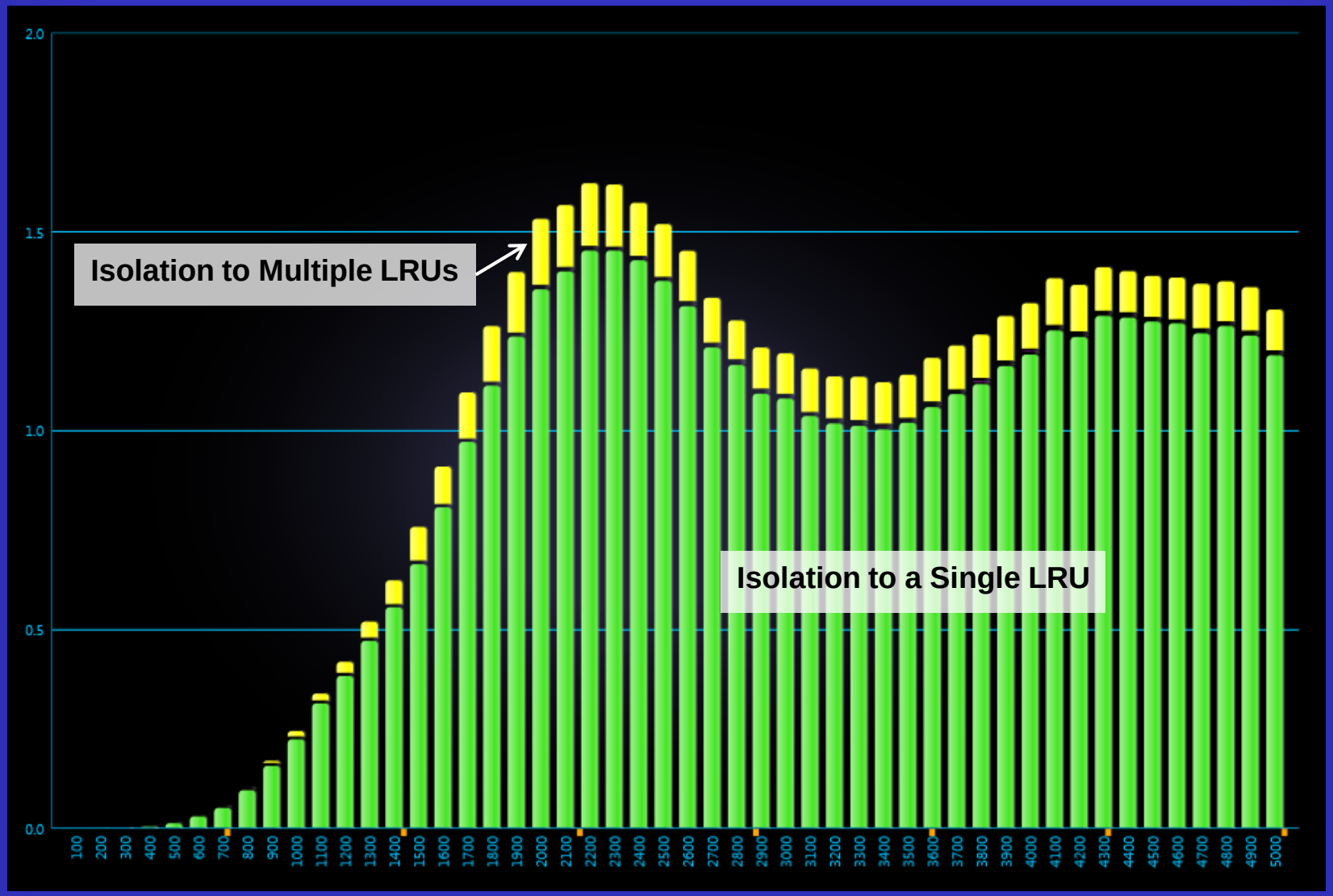
	Isolation Percentages Using Testing Only			Isolation Probabilities Using Testing Only		Resolution Probabilities Using Lambda Search	
Size	Qty	%	Cum %	%	Cum %	%	Cum %
1	77	78.57	78.57	81.04	81.04	92.72	92.72
2	11	11.22	89.80	8.97	90.00	3.37	96.09
3	0	0.00	89.80	0.00	90.00	2.01	98.10
4	0	0.00	89.80	0.00	90.00	1.29	99.39
5	2	2.04	91.84	7.22	97.22	0.57	99.96
6	0	0.00	91.84	0.00	97.22	0.03	99.98
7	7	7.14	98.98	2.16	99.38	0.01	99.99
8	1	1.02	100.00	0.62	100.00	< 0.01	100.00

Simulation-based Analysis in STAGE

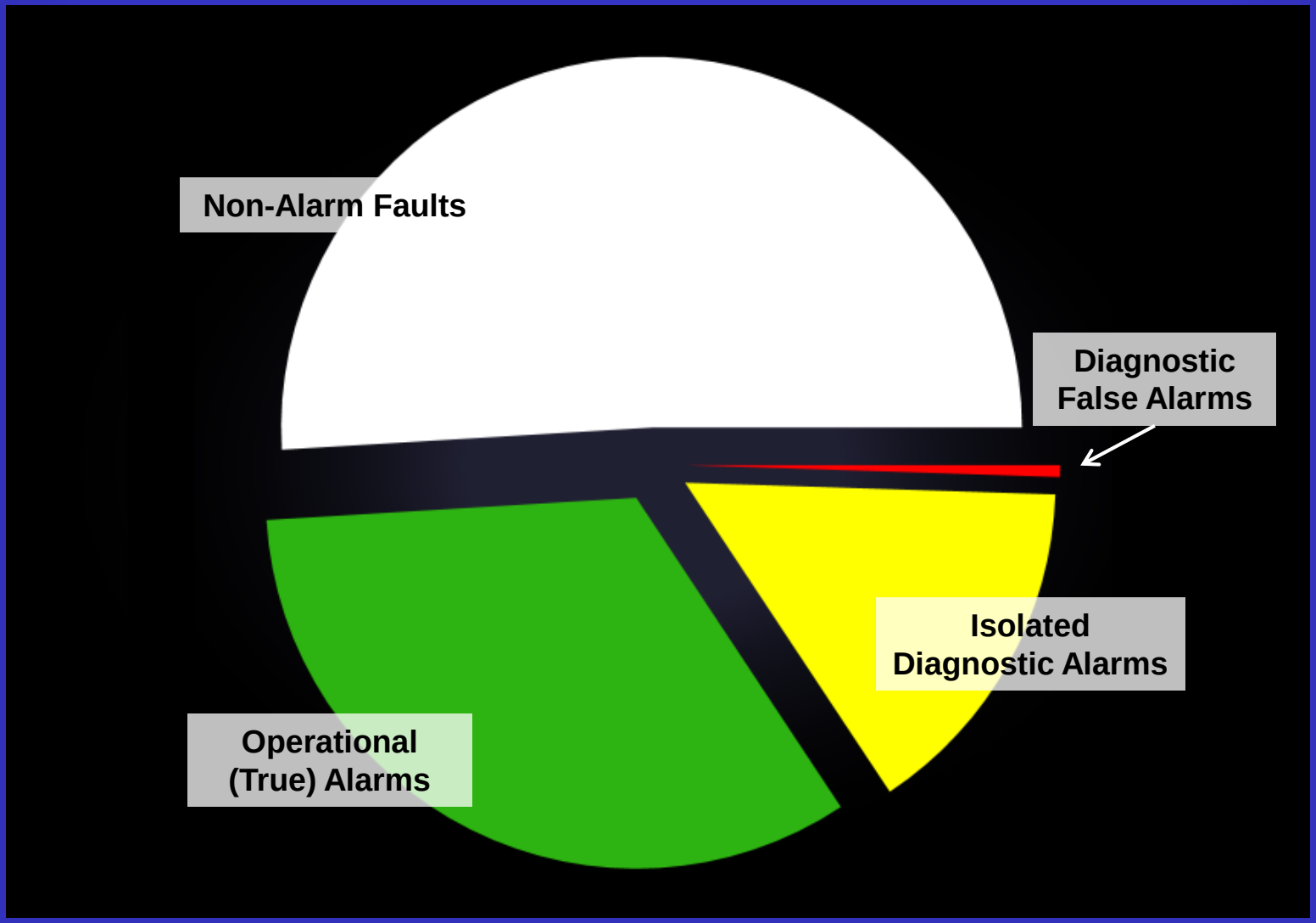
Fault Detection in STAGE



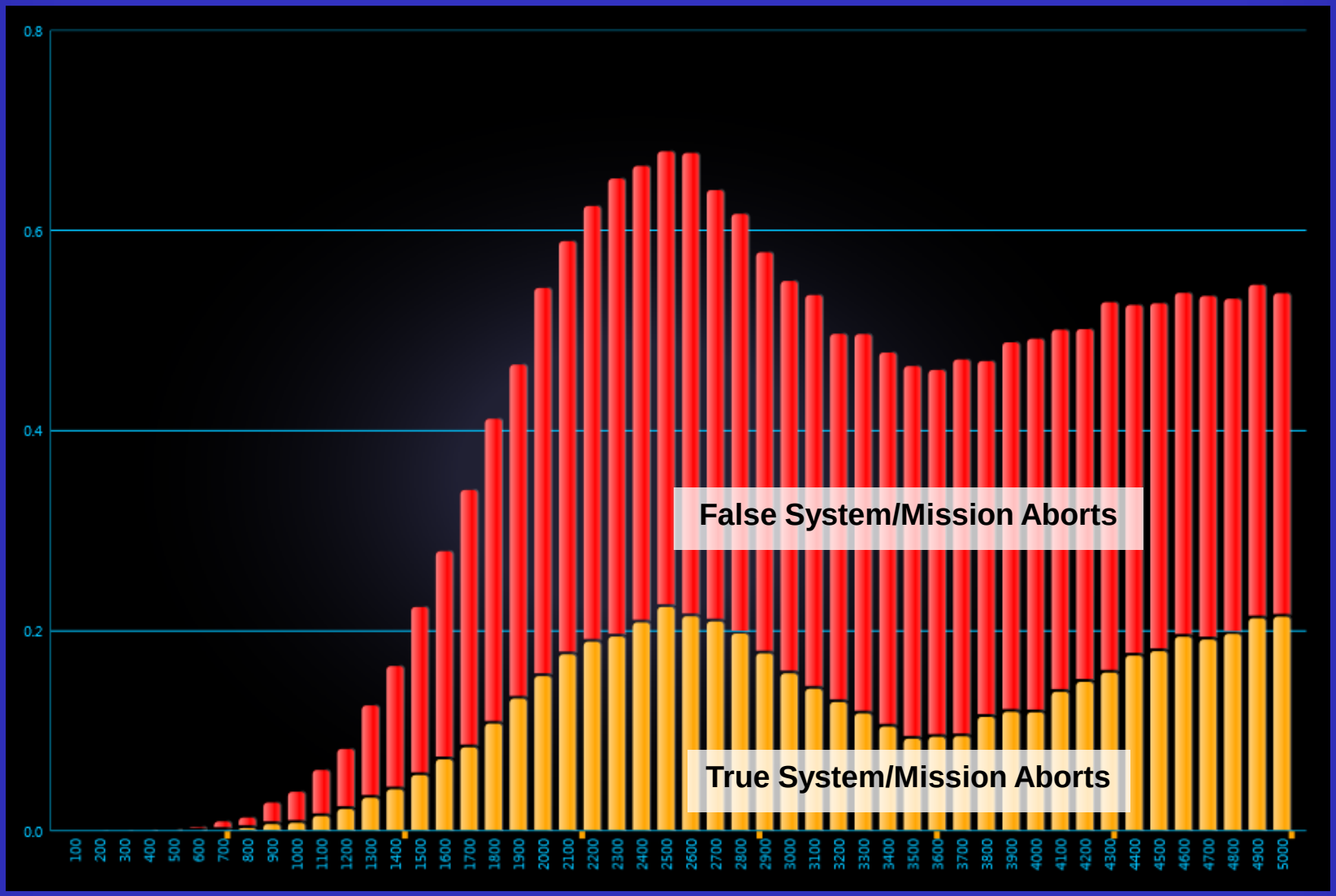
Fault Isolation in STAGE



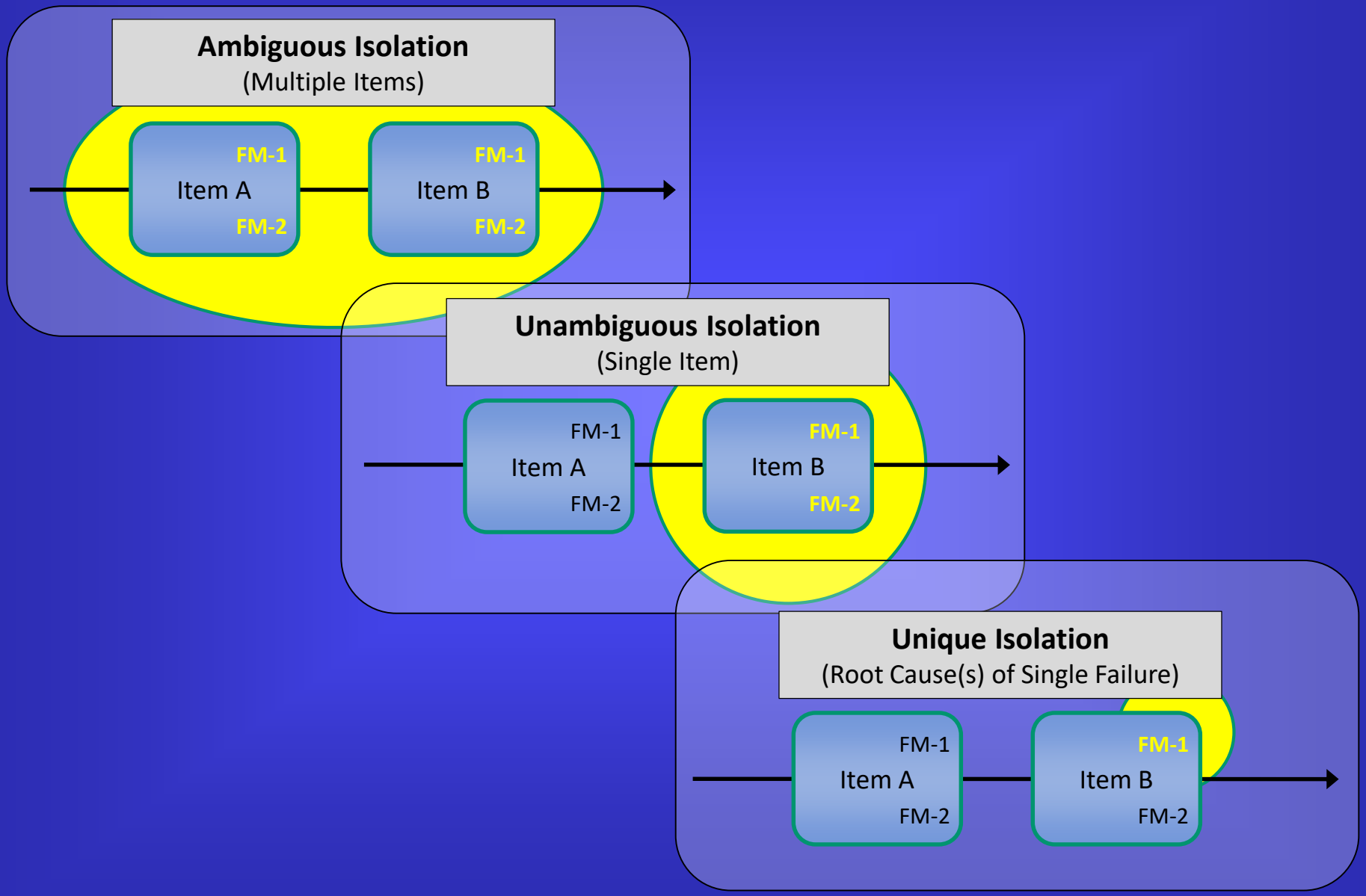
False Alarms in STAGE



System/Mission Aborts in STAGE



Unambiguous vs. Unique Isolation

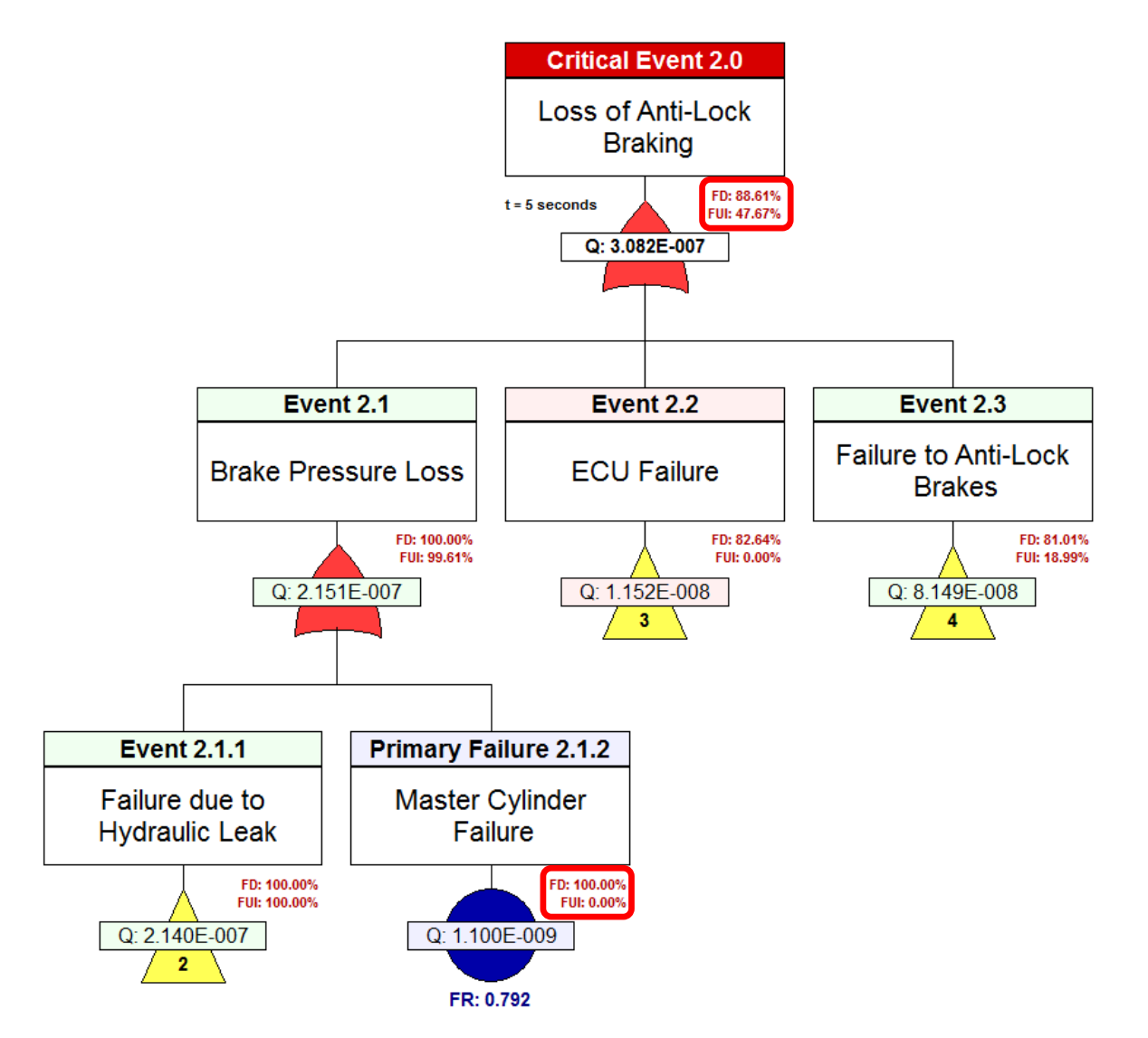


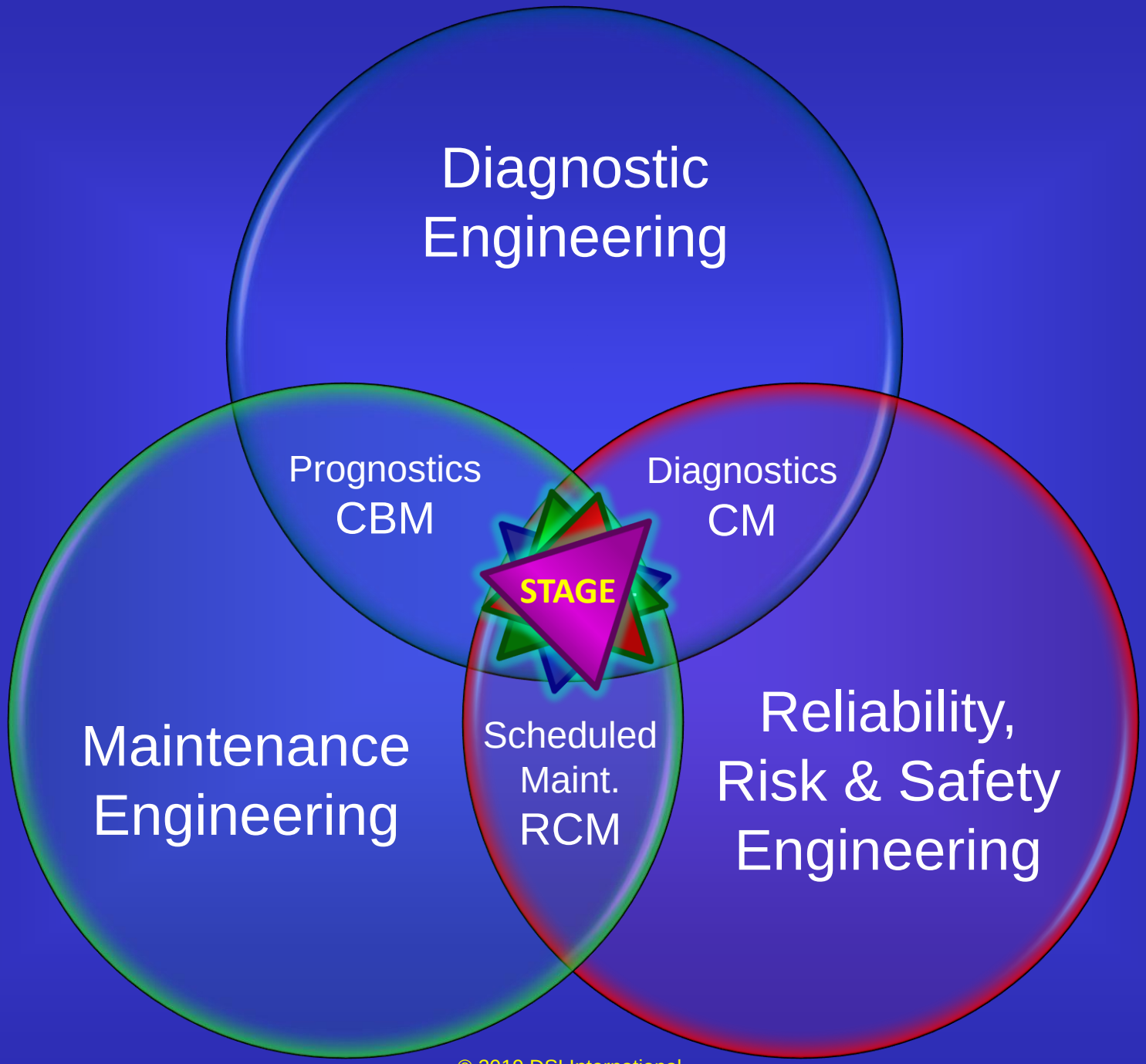
FMECA Plus: Critical Failure Diagnosis Chart

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

The “Uniquely Isolated” column indicates whether the fault group that is isolated for this failure contains only root causes of the given failure. If the fault group contains any failure modes that are not a root cause of that failure, then the failure has not been uniquely isolated by the diagnostics. The non-unique isolation of critical failures is a primary driver of false alarms and unnecessary system or mission aborts.

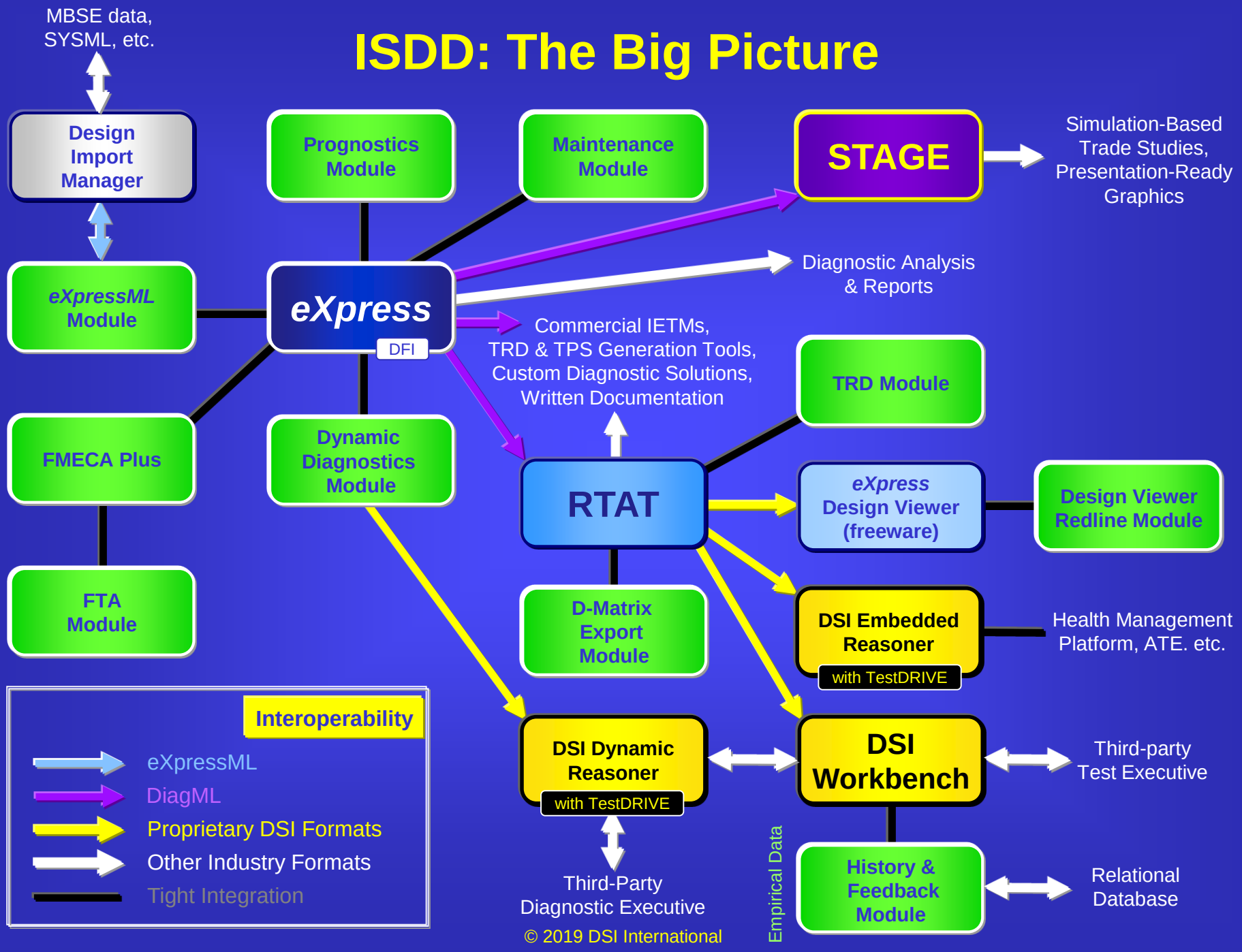
eXpress FTA Module: Fault Tree with FD/FUI



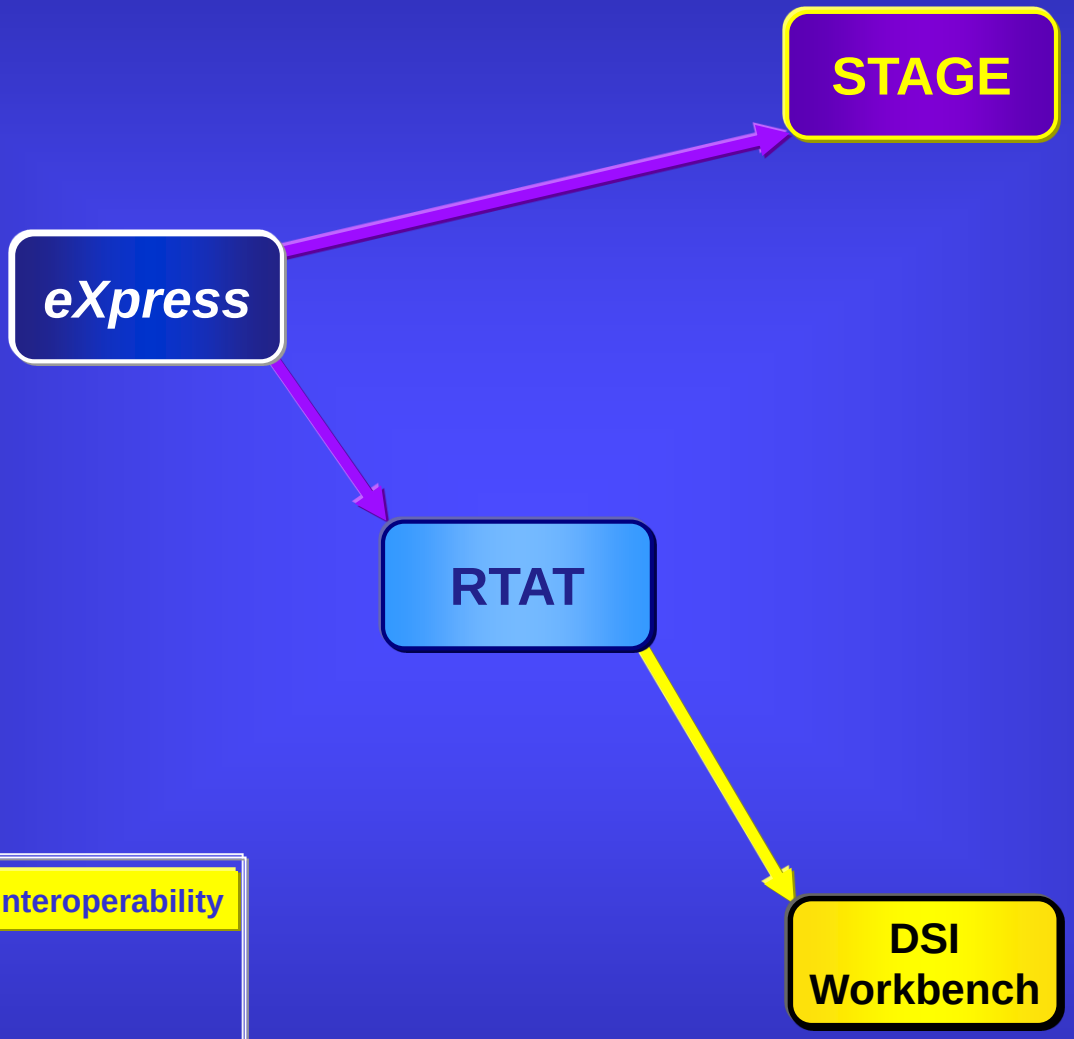


What is ISDD?

ISDD: The Big Picture



ISDD: The Core Tools

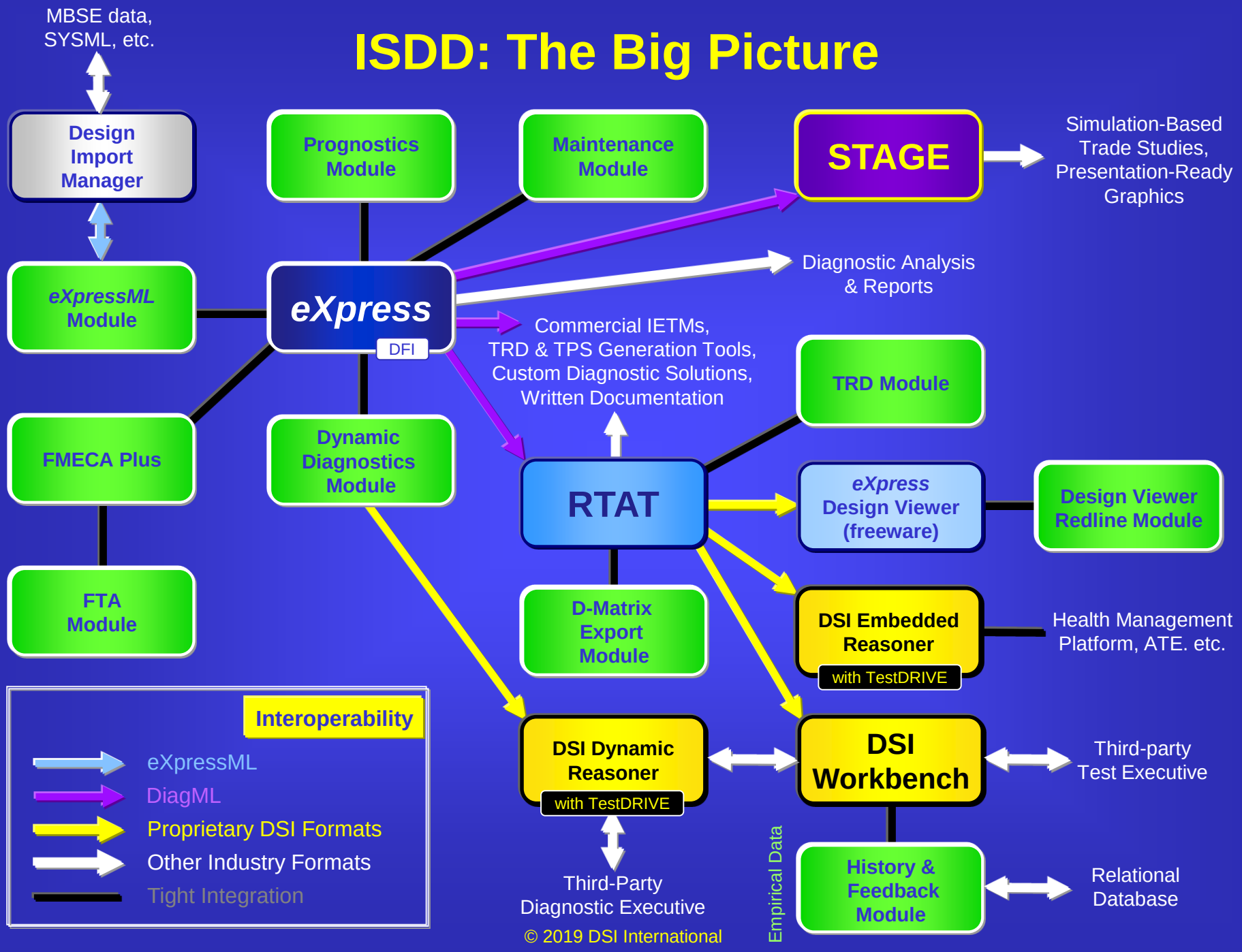


Interoperability

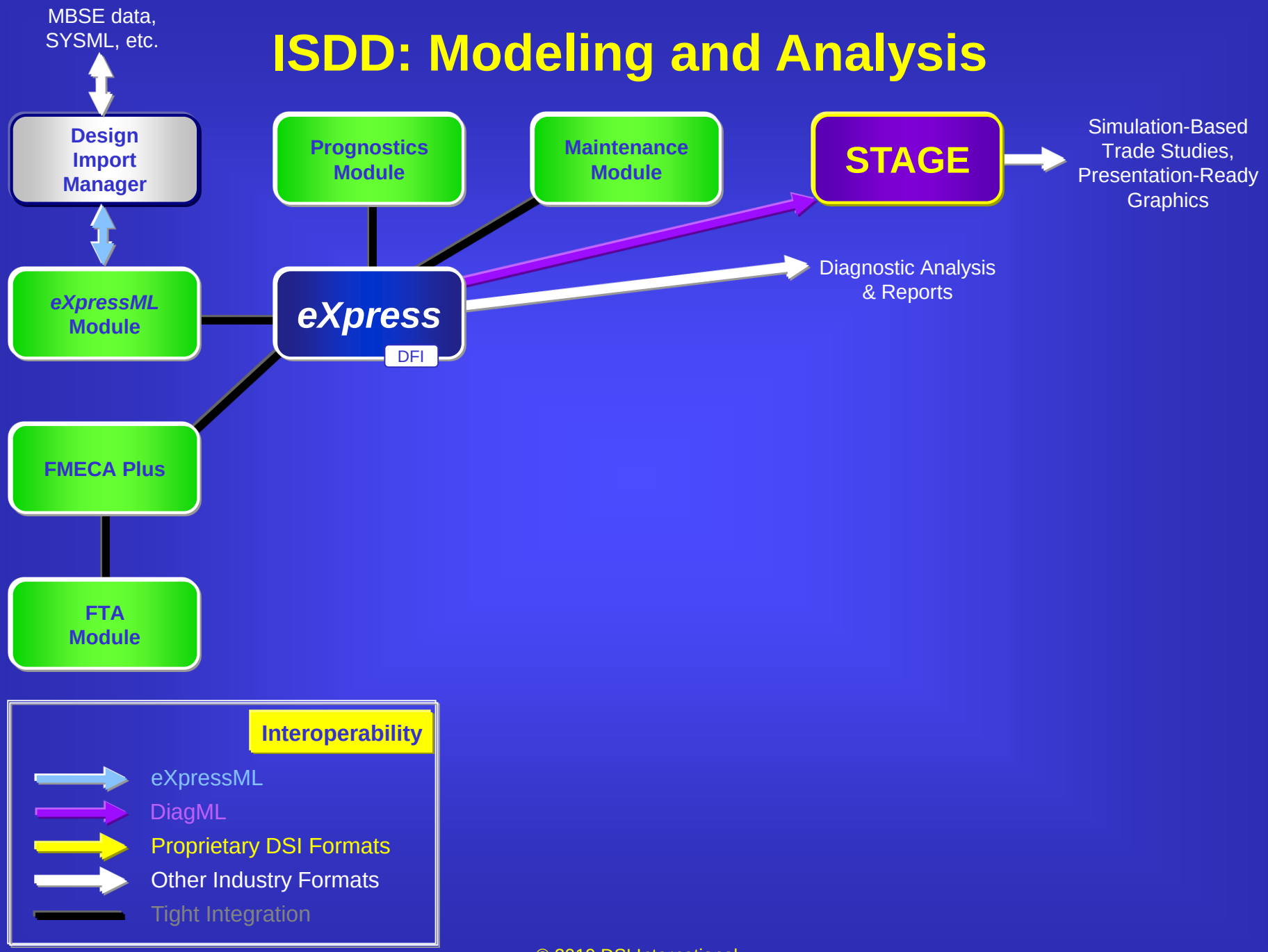
DiagML

Proprietary DSI Formats

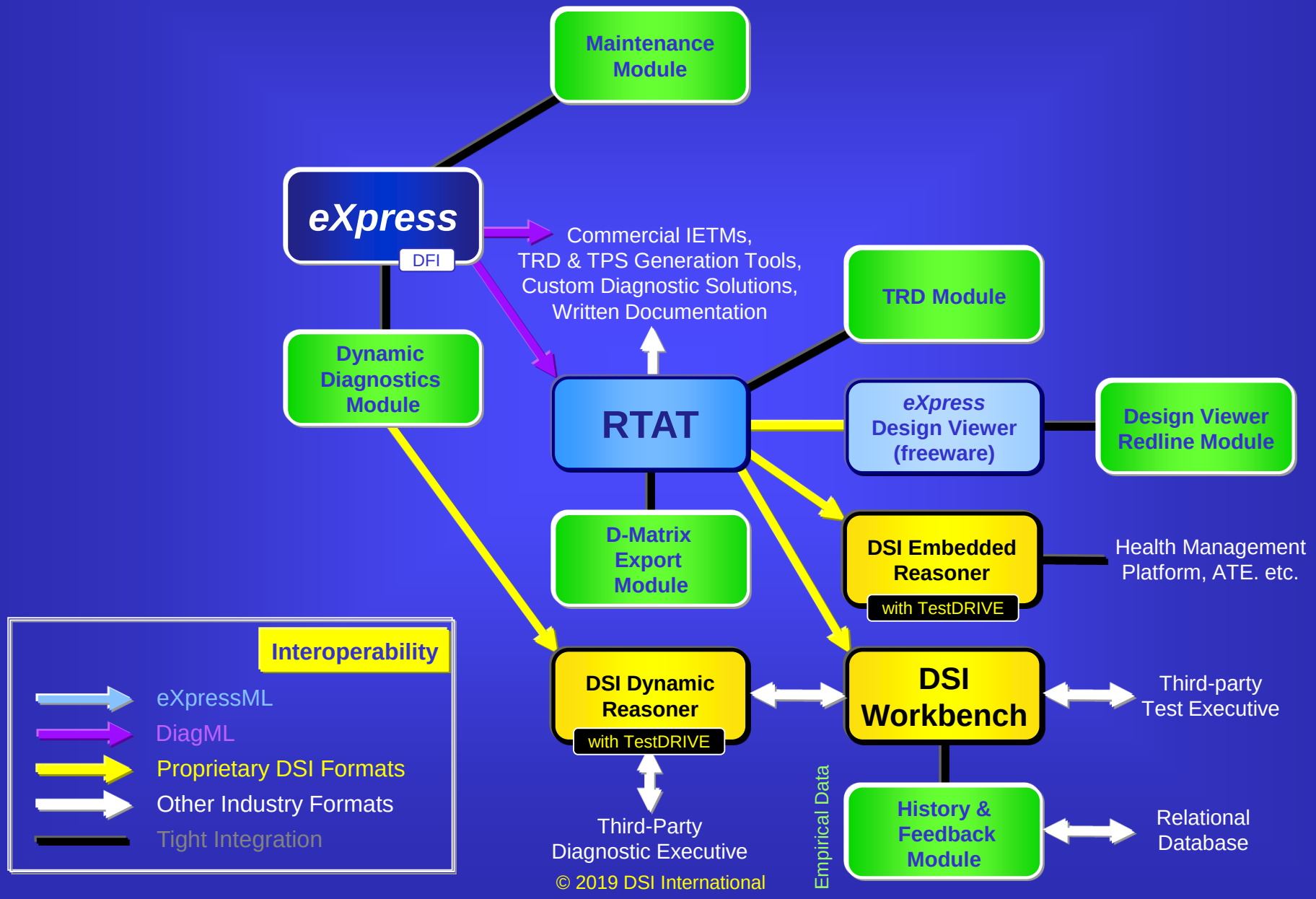
ISDD: The Big Picture



ISDD: Modeling and Analysis



ISDD: Diagnostic Development & Deployment



The ISDD Tool Suite

eXpress

Diagnostic Modeling and Analysis

eXpress creates the models used by all tools in the ISDD tool suite. It also performs standardized analyses to help engineers optimize and assess system diagnostics/prognostics, as well as the design's ability to support effective HM.

STAGE

Simulation-based Analysis

Using data from ***eXpress***, **STAGE** simulates failures, diagnoses and repairs that would occur in a fielded system. Calculations (represented as graphs) show changes over time, as well as the impact of maintenance upon failure.

RTAT

Enhancing Exported Diagnostics

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 for use in a variety of tools. This tool includes the ***eXpress*** Design Viewer.

DSI Workbench

Run-Time Diagnostic Executive

DSI Workbench allows diagnostics developed in ***eXpress*** to be fielded in a maintenance or production environment. DSI Workbench supports integration with a test executive, as well as guided troubleshooting and free-form test entry.

eXpress Modules

eXpress

Diagnostic Modeling and Analysis
eXpress creates the models used by all tools in the ISDD tool suite. It also performs standardized analyses to help engineers optimize and assess system diagnostics/prognostics, as well as the design's ability to support effective HM.

FMECA Plus

FMECA Plus (*eXpress* Reliability Module)
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.

FTA Module

***eXpress* 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 Safety analysis.

Prognostics Module

***eXpress* 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

***eXpress* Maintenance Module**
Module that allows ***eXpress*** to support multiple levels of diagnosis. It has been designed to facilitate the concurrent development of embedded diagnostics and troubleshooting procedures (IETMs).

Dynamic Diagnostics Module

***eXpress* Dynamic Diagnostics Module**
Module that allows ***eXpress*** to export resource files to be used by the ***eXpress*** Dynamic Reasoner. It also allows Dynamic Diagnostics to be validated using the eXpress Desktop Fault Insertion capability.

RTAT and Design Viewer Modules

RTAT

Enhancing Exported Diagnostics
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 for use in a variety of tools.

D-Matrix Export Module

D-Matrix Export Module
Plug-in module that allows RTAT to export test dependency data from ***eXpress*** in a Dependency Matrix format

***eXpress* Design Viewer**

***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.

Design Viewer Redline Module

***eXpress* Design Viewer Redline Module**
Plug-in module that allows users to add comments and feedback within the ***eXpress*** Design Viewer.

Diagnostic Engineering Applications

Design Assessment & Influence

- Assess ability to meet contracted requirements
- Optimize design for effective supportability
- Support interoperability with other model-based design activities

New Systems

Legacy Systems

- Identify weaknesses in current diagnostic capability
- Generate case studies evaluating the impact of proposed upgrades
- Create models to incorporate into MBSE databases

Diagnostic Development & Deployment

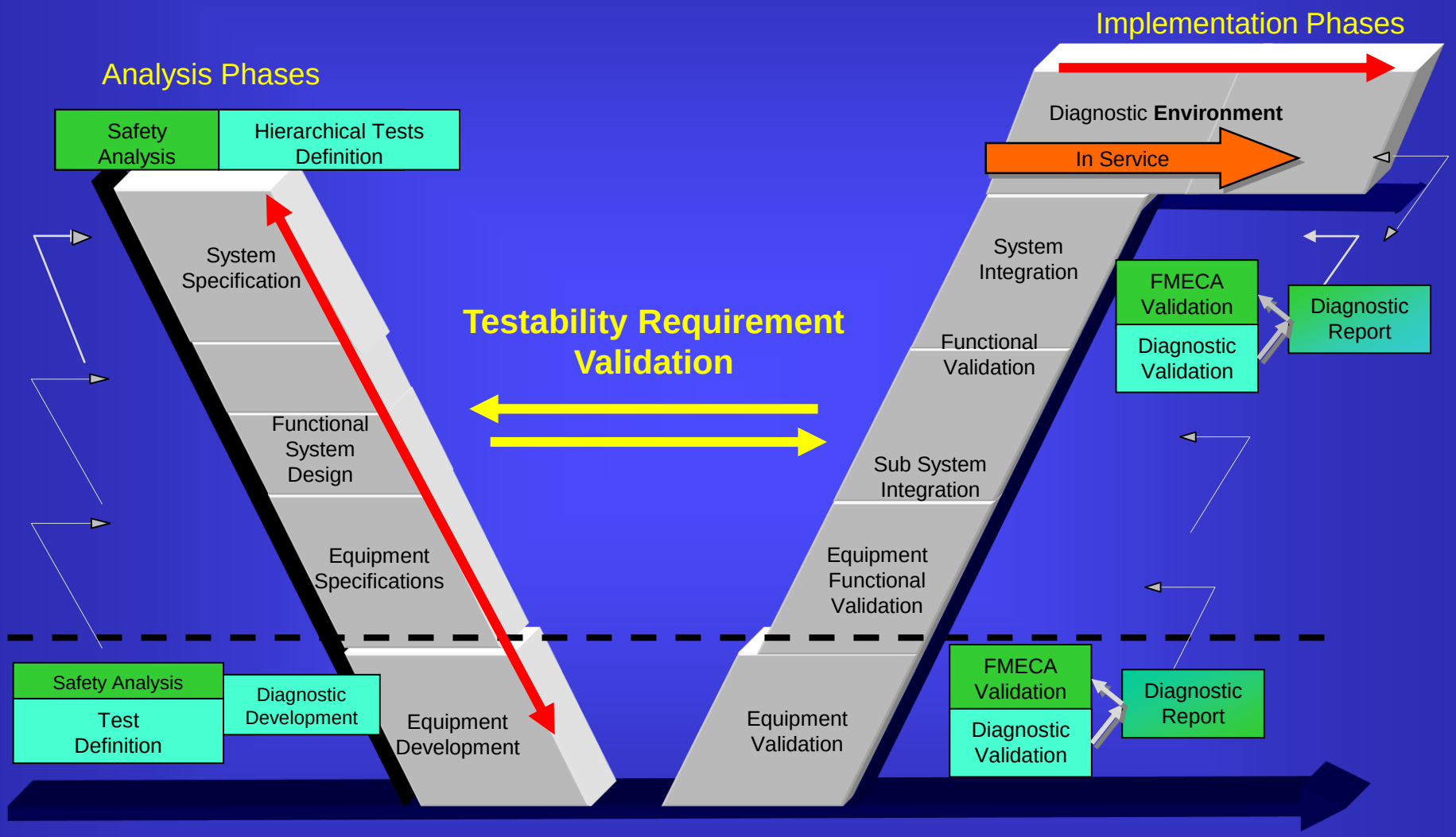
- Generate optimized diagnostics based on ***eXpress*** analysis
- Link HM to troubleshooting and/or maintenance procedures
- Determine successful mixes of corrective, predictive and periodic maintenance.

New Systems

Legacy Systems

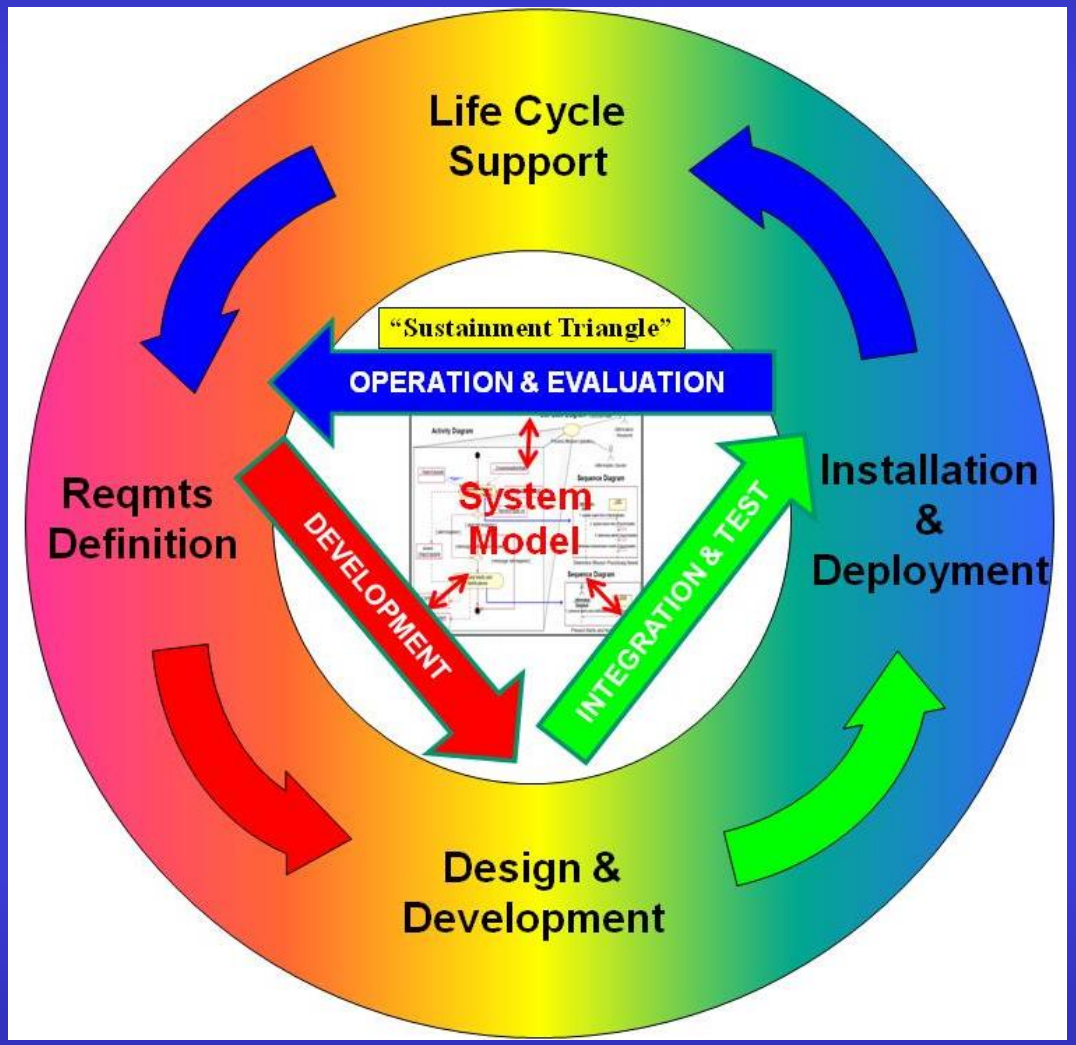
- Improve existing diagnostics based on ***eXpress*** analysis
- Repurpose existing diagnostics for new run-time platforms
- Develop empirical diagnostics from field analytics

Systems Engineering Vision



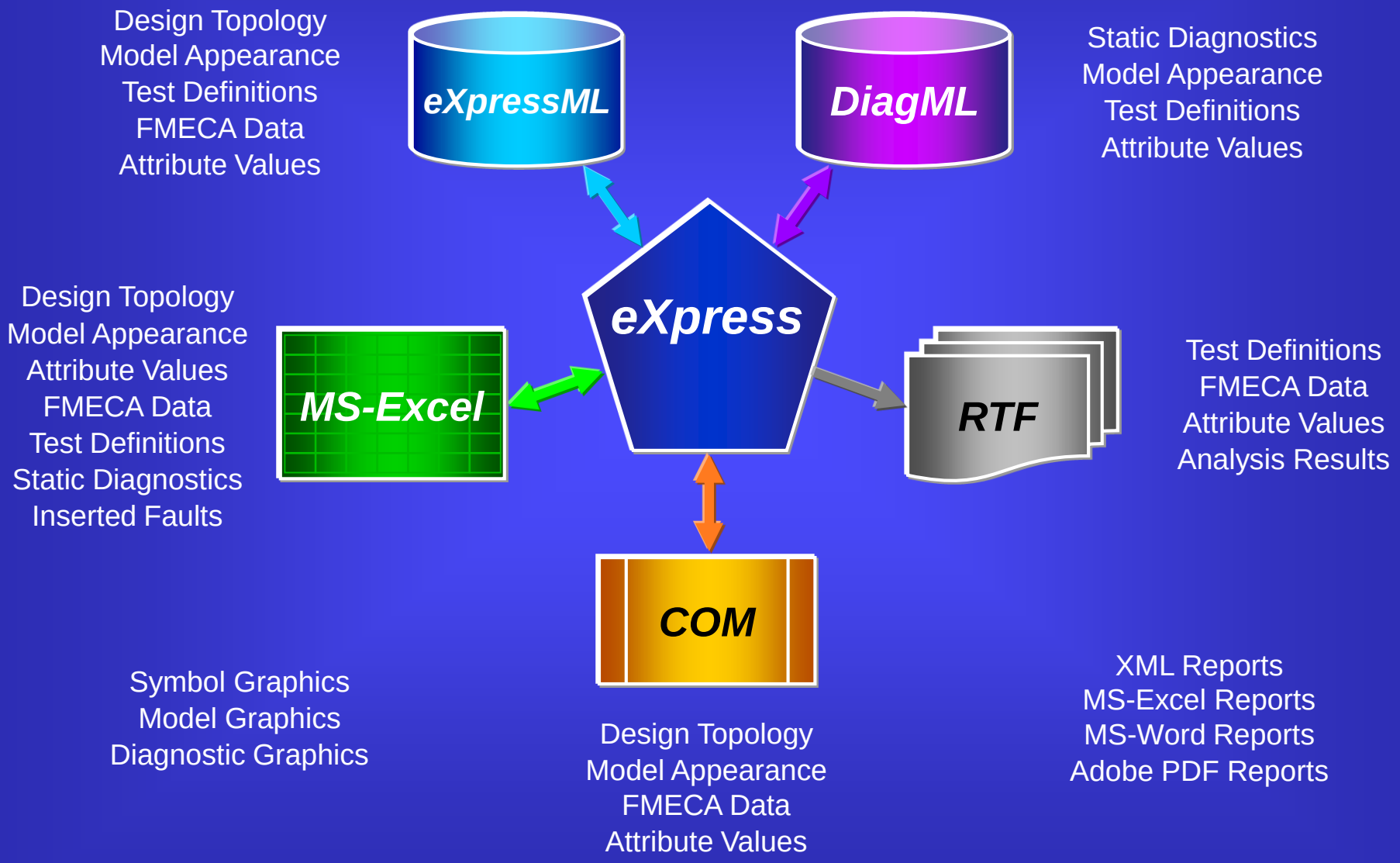
Requirements to Test / Diagnostics

Model-based Sustainment



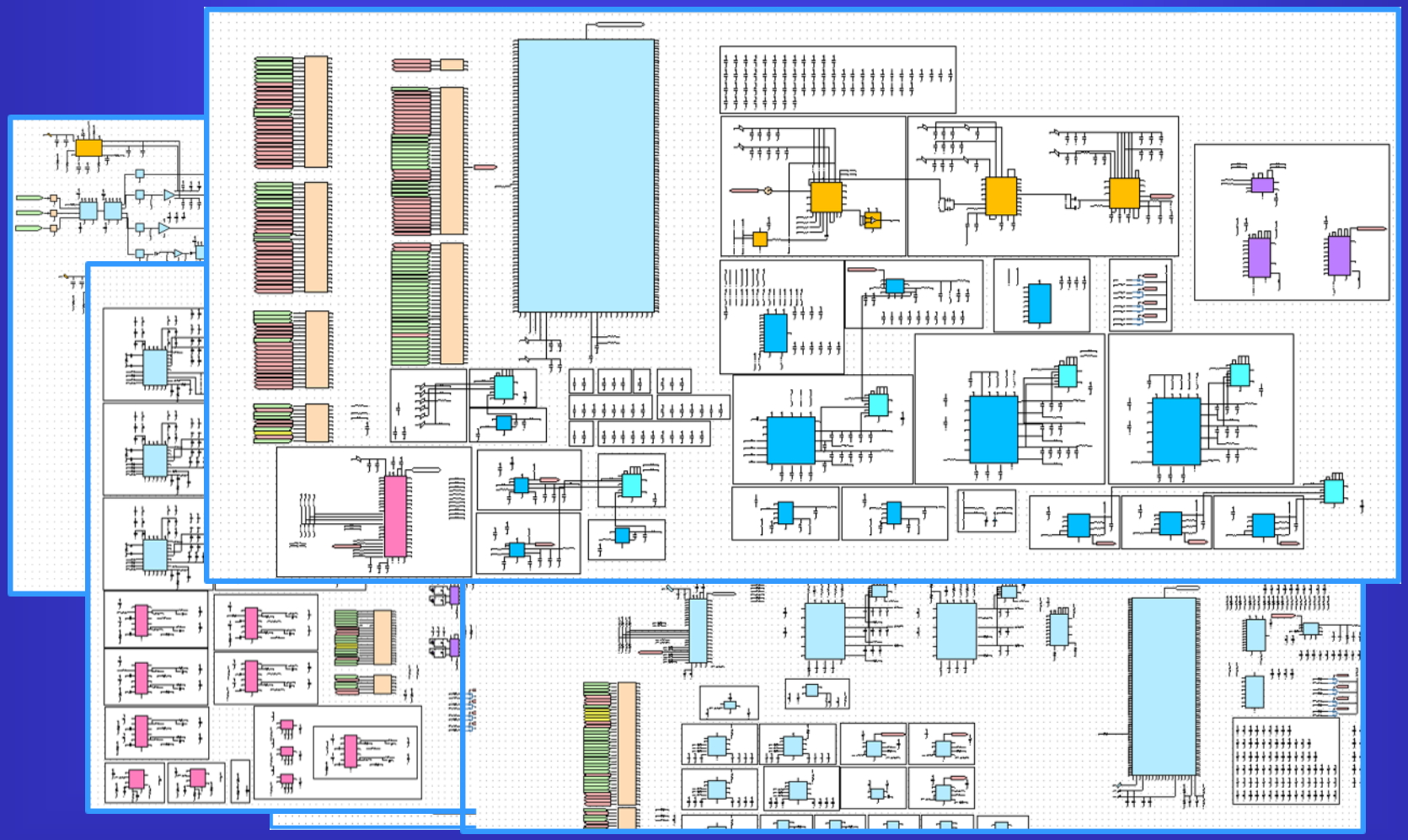
How We Do It

eXpress Interoperability



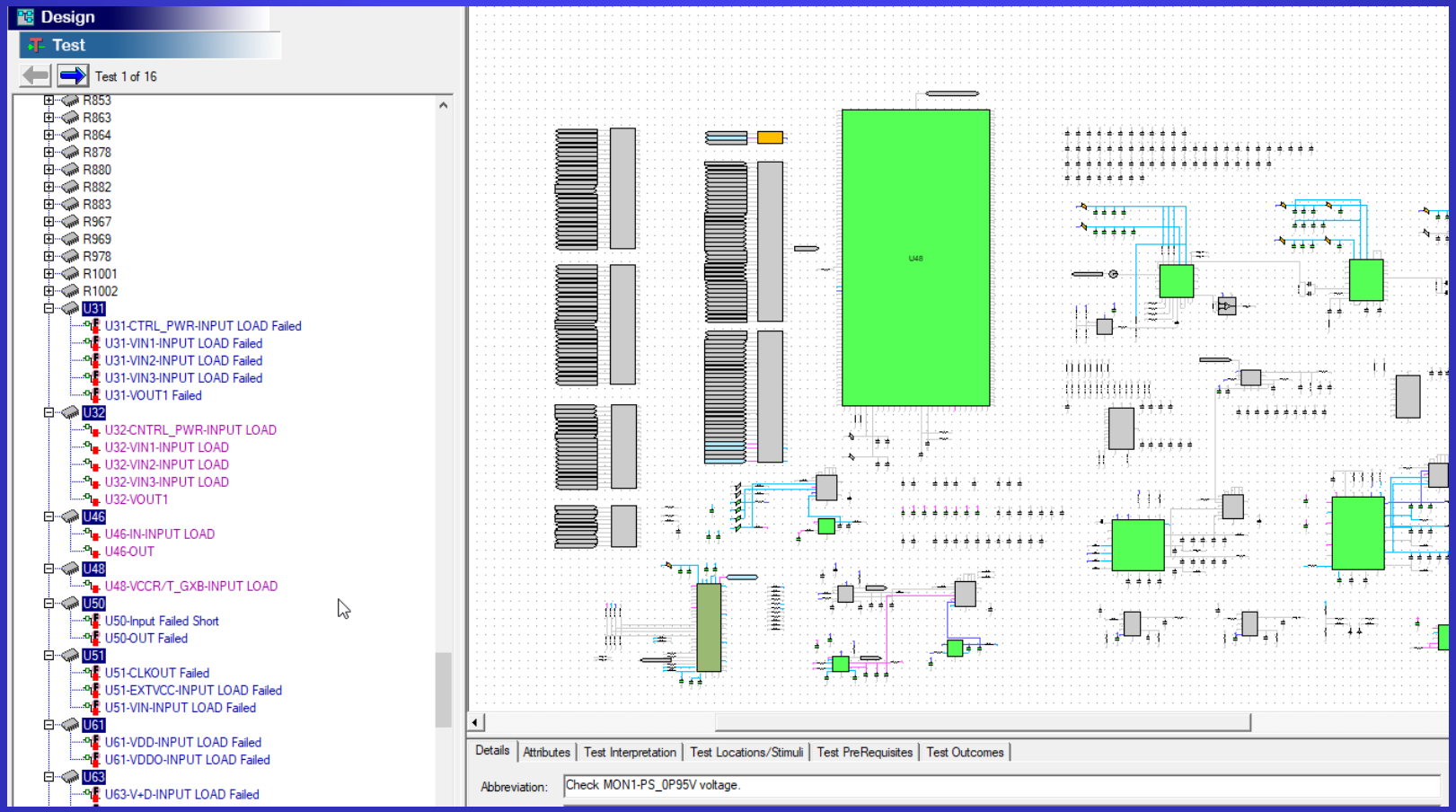
Hierarchical System Model

- Linked models representing different levels of indenture in the system hierarchy
- Diagnostic & FMECA/FTA analyses can be performed for (and to) any level of the hierarchy



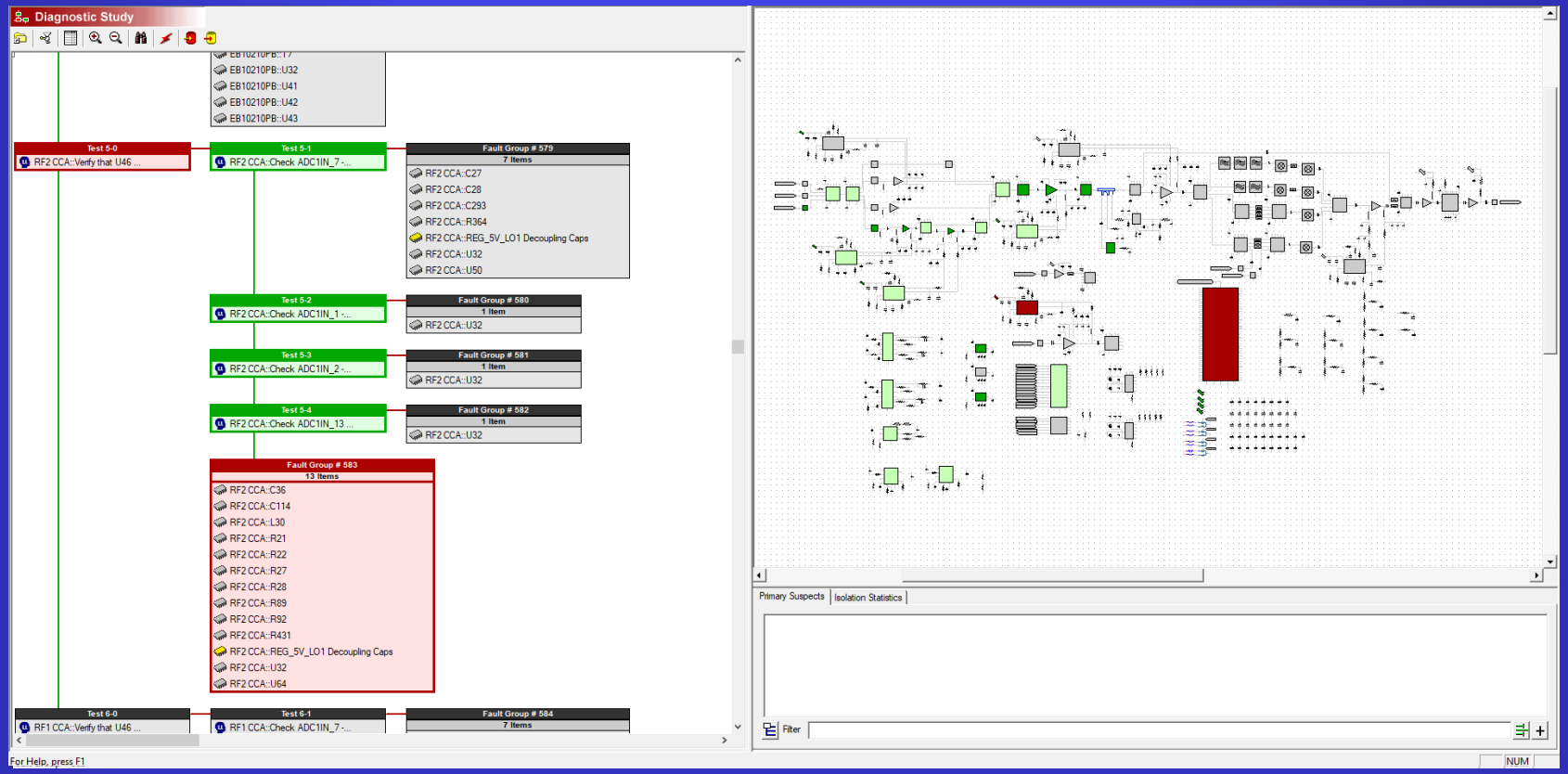
Dependency-Based Test Definitions

- Test coverage defines what diagnostics “learns” when a test passes or fails
- Initially, coverage can be based upon the modeled dependencies
- Test definitions can be reviewed both graphically and in the Explorer tree



Hierarchical Diagnostics

- Diagnostic Sequences can developed for different levels of the system hierarchy
- You can descend within the hierarchy to view suspected elements or isolated fault groups at different levels of indenture



Diagnostic / Design Assessment

- ***eXpress*** reports provide a variety of analysis results, designed to help you meet diagnostic requirements for testability, reliability, system availability, maintainability and safety.

Fault Isolation Report

Hierarchy Selection: Single Level

Common Cause
Fault Group Size Statistics

	Isolation Percentages Using Testing Only			Isolation Probabilities Using Testing Only		Resolution Probabilities Using Lambda Search	
Size	Qty	%	Cum %	%	Cum %	%	Cum %
1	140	83.83	83.83	66.91	66.91	95.74	95.74
2	25	14.97	98.80	30.44	97.35	3.30	99.04
3	0	0.00	98.80	0.00	97.35	0.34	99.39
4	0	0.00	98.80	0.00	97.35	0.31	99.69
5	2	1.20	100.00	2.65	100.00	0.31	100.00

Total Fault Groups:	167
Average Fault Group Size:	1.20
Isolation Effectiveness:	70.90
Expected Fault Group Size:	1.41
Resolution Effectiveness:	94.22
Expected Repairs per Isolation:	1.06

Fault Group Counting Method: Each individual fault group instance is separately counted
Lambda Search: Max. of 25 items, where the comparison with the next highest item is at least 1.00 to 1

Integration of Functional & Failure Propagation

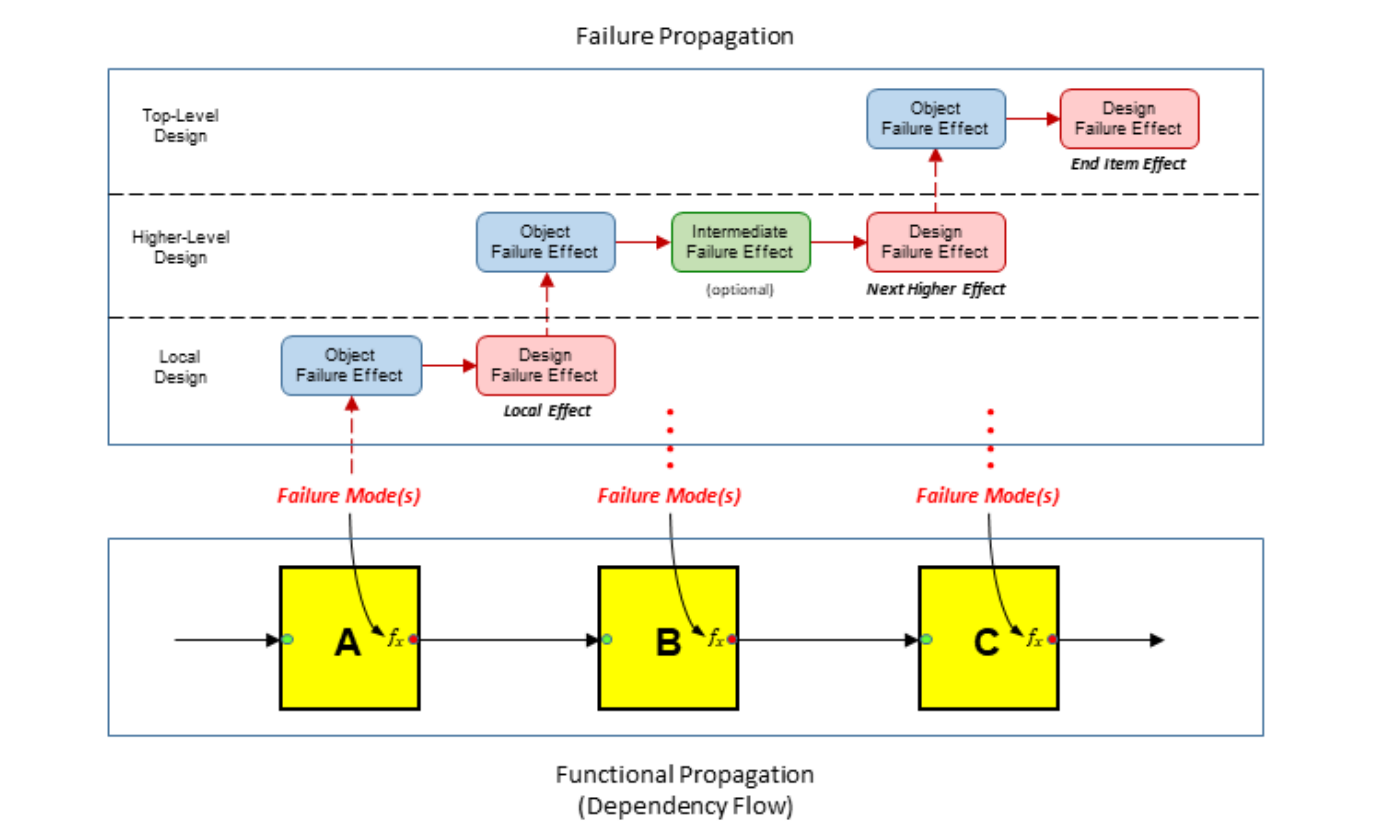
- **Functional Propagation** (horizontal) model

  Functional dependencies show how functions are impacted by other functions.

  Relationship settings show how functions are impacted by specific failures modes.

- **Failure Propagation** (vertical) model

  Failure effects show how failure modes manifest themselves at different design levels



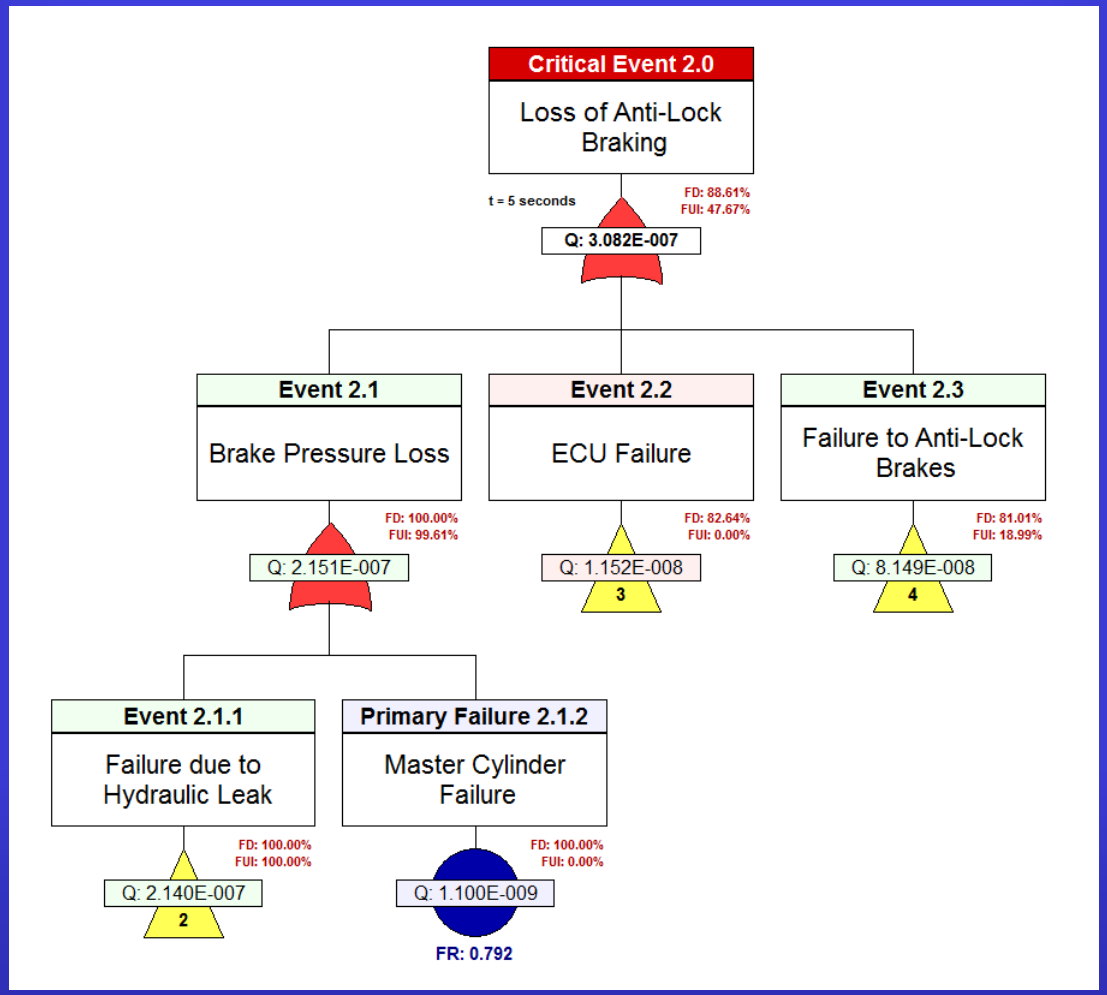
Diagnostics-Informed Reliability Analysis

- FMEA/FMECA charts can be developed within ***eXpress*** or imported from external tools.
- ***eXpress*** FMECA charts can contain a variety of columns detailing how and when failures are detected and isolated by the actual diagnostics.

	Item	Description	Value	Failure	Failure Effects			Severity Class	Failure Rate	Diagnostic Coverage	
					Local	Next Higher	End Item			Failure Detected	Fault Group Sizes
1804	T8	SURFACT MOUNT	TC4-1W-7ALN+	Open	RF out channel 1 - J11 failed for U43 Out C DSP only.		RF out channel 1 - J11 failed for U43	Category I - Catastrophic	< 0.000001	Yes	27
1805	U1	IC REG LDO ADJ 5A 28QFN	LT3070MPUFD	U1-OUT failed open	DSP_1P2VA POWER FAILED	Failure of all ADC	Failure of all ADC channels.	Category I - Catastrophic	< 0.000001	Yes	7
1806				U1-OUT failed short	DSP_1P2VA POWER FAILED	Failure of all ADC	Failure of all ADC channels.	Category I - Catastrophic	< 0.000001	Yes	1
1807				U1-power Input failed short	DSP_1P4V POWER FAILED	DSP_1P2VA POWER FAILED	Failure of all ADC channels.	Category I - Catastrophic	< 0.000001	Yes	3
1808				U1-PWRGD failed	Failure to monitor DSP_1P2VA voltage.		Failure to monitor DSP_1P2VA voltage.	Category I - Catastrophic	< 0.000001	Yes	3
1809	U2	IC REG LDO ADJ 5A 28QFN	LT3070MPUFD	U2-OUT failed open	DSP_1P2V POWER FAILED	Failure of all ADC	Failure of all ADC channels.	Category I - Catastrophic	< 0.000001	Yes	7
1810				U2-OUT failed short	DSP_1P2V POWER FAILED	Failure of all ADC	Failure of all ADC channels.	Category I - Catastrophic	< 0.000001	Yes	1
1811				U2-power Input failed short	DSP_1P4V POWER FAILED	DSP_1P2VA POWER FAILED	Failure of all ADC channels.	Category I - Catastrophic	< 0.000001	Yes	3
1812				U2-PWRGD failed	Failure to monitor DSP_1P2V voltage.		Failure to monitor DSP_1P2V voltage.	Category I - Catastrophic	< 0.000001	Yes	3
1813	U3	High Performance Wide Band PLLatinum RF Synthesizer With Integrated VCO	LMX2582	Lock Detect Failed	Invalid indication of failure of U3 PLL lock.		Invalid indication of failure of U3 PLL	Category I - Catastrophic	0.000002	Yes	1
1814				RF Output failed.	Failure of ADC and Interlinken clocks.	Failure of all ADC	Failure of all ADC channels, ILK and	Category I - Catastrophic	0.000003	Yes	17
1815				Serial communications failed.	Failure to communicate with U3 serial interface.		Failure to communicate with U3 serial	Category II - Critical	0.000002	Yes	1
1816	U4	Ultra Low-Noise Clock Jitter Cleaner with Dual Loop PLLs w/ Enhanced Performance	LMK04828EP	PLL1 Failed	Invalid indication of failure of U4 input signal.	None	None	Category IV - Minor	< 0.000001	Yes	3
1817				PLL2 Failed	Invalid indication of failure of U4 input signal.	None	None	Category IV - Minor	< 0.000001	No	N/A
1818				REGISTERS Failed	Failure to communicate with U4 serial interface.		Failure to communicate with U4 serial	Category II - Critical	< 0.000001	Yes	4
1819				U4-DCLKOUT0 - PADC_1_DEVCLK failed	Failure of ADC channel 1.		Failure of ADC channel 1.	Category I - Catastrophic	< 0.000001	Yes	34
1820				U4-DCLKOUT2 - ILK_CLK failed	RF out channel 3 - J9 failed for all both U39 Out C DSP and ILK_SDO1_N through RF. RF out channel 2 - J8 failed for all both U39 Out A DSP and ILK_SDO1_P through RF.		RF out channel 3 - J9 failed for all both U39 Out C DSP and ILK_SDO1_N through RF. RF out channel 2 - J8 failed for all both	Category I - Catastrophic	< 0.000001	Yes	3
1821				U4-DCLKOUT4 - PADC_2_DEVCLK failed	Failure of ADC channel 2.		Failure of ADC channel 2.	Category I - Catastrophic	< 0.000001	Yes	34
1822				U4-DCLKOUT6 - PADC_3_DEVCLK failed	Failure of ADC channel 3.		Failure of ADC channel 3.	Category I - Catastrophic	0.000001	Yes	34
1823				U4-DCLKOUT8 - JESD_RCLK failed	Failure of all ADC channels.		Failure of all ADC channels.	Category I - Catastrophic	0.000001	Yes	4
1824				U4-DCLKOUT10 - JESD_DCLK failed	Failure of all ADC channels.		Failure of all ADC channels.	Category I - Catastrophic	0.000001	Yes	3
1825				U4-DCLKOUT12 - PADC_0_DEVCLK failed	Failure of ADC channel 0.		Failure of ADC channel 0.	Category I - Catastrophic	0.000001	Yes	34
1826				U4-SDCLKOUT1 - PADC_1_SYSRF failed	Failure of ADC channel 1.		Failure of ADC channel 1.	Category I - Catastrophic	< 0.000001	Yes	34
1827				U4-SDCLKOUT5 - PADC_2_SYSRF failed	Failure of ADC channel 2.		Failure of ADC channel 2.	Category I - Catastrophic	< 0.000001	Yes	34
1828				U4-SDCLKOUT7 - PADC_3_SYSRF failed	Failure of ADC channel 3.		Failure of ADC channel 3.	Category I - Catastrophic	0.000001	Yes	34
1829				U4-SDCLKOUT11 - JESD_SYSREF failed	Failure of all ADC channels.		Failure of all ADC channels.	Category I - Catastrophic	0.000001	Yes	3
1830				U4-SDCLKOUT13 - PADC_0_SYSRF failed	Failure of ADC channel 0.		Failure of ADC channel 0.	Category I - Catastrophic	0.000001	Yes	34
1831				U4-SDIO failed	Failure to communicate with U4 serial interface.		Failure to communicate with U4 serial	Category II - Critical	0.000001	Yes	2
1832				U4-STATUS_LD1 failed	Invalid indication of failure of U4 PLL lock. Failure of one or more LED indicators		Invalid indication of failure of U4 PLL lock.	Category I - Catastrophic	0.000001	Yes	3
1833				U4-STATUS_LD2 failed	Failure of one or more LED indicators		Failure of one or more LED indicators	Category IV - Minor	0.000001	No	N/A
1834	U5	FPGA, Arria 10, SX660, 48TXVR, -55/+125, F40 package	A10SOC_1517	ADC_0 Over Range 0 failed	Failure to indicate that ADC channel 0 is over range.		Failure to indicate that ADC channel 0 is	Category I - Catastrophic	0.000001	No	N/A
1835				ADC_0 Over Range 1 failed	Failure to indicate that ADC channel 0 is over range.		Failure to indicate that ADC channel 0 is	Category I - Catastrophic	0.000001	No	N/A
1836				ADC_0 Voltage [D0..7] failed	Failure of ADC channel 0.		Failure of ADC channel 0.	Category I - Catastrophic	0.000001	Yes	34
1837				ADC_1 Over Range 0 failed	Failure to indicate that ADC channel 1 is over range.		Failure to indicate that ADC channel 1 is	Category I - Catastrophic	0.000001	No	N/A
1838				ADC_1 Over Range 1 failed	Failure to indicate that ADC channel 1 is over range.		Failure to indicate that ADC channel 1 is	Category I - Catastrophic	0.000001	No	N/A

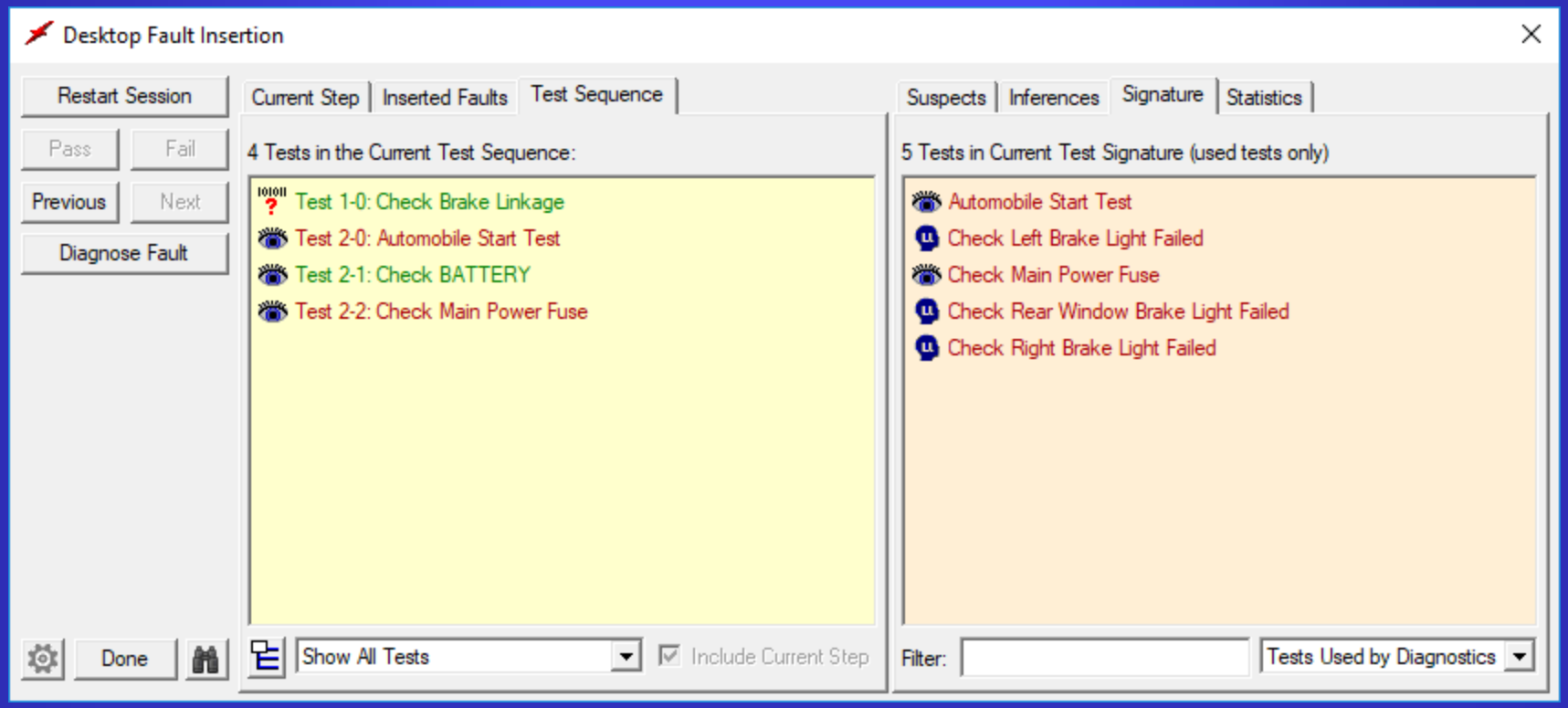
Diagnostics-Informed Fault Tree Analysis

- Fault Trees include diagnostic metrics that indicate how well diagnostics can detect and isolate individual failures that lead up to a critical event.
- Allows you to assess the overall Risk of having less-than-perfect diagnostics

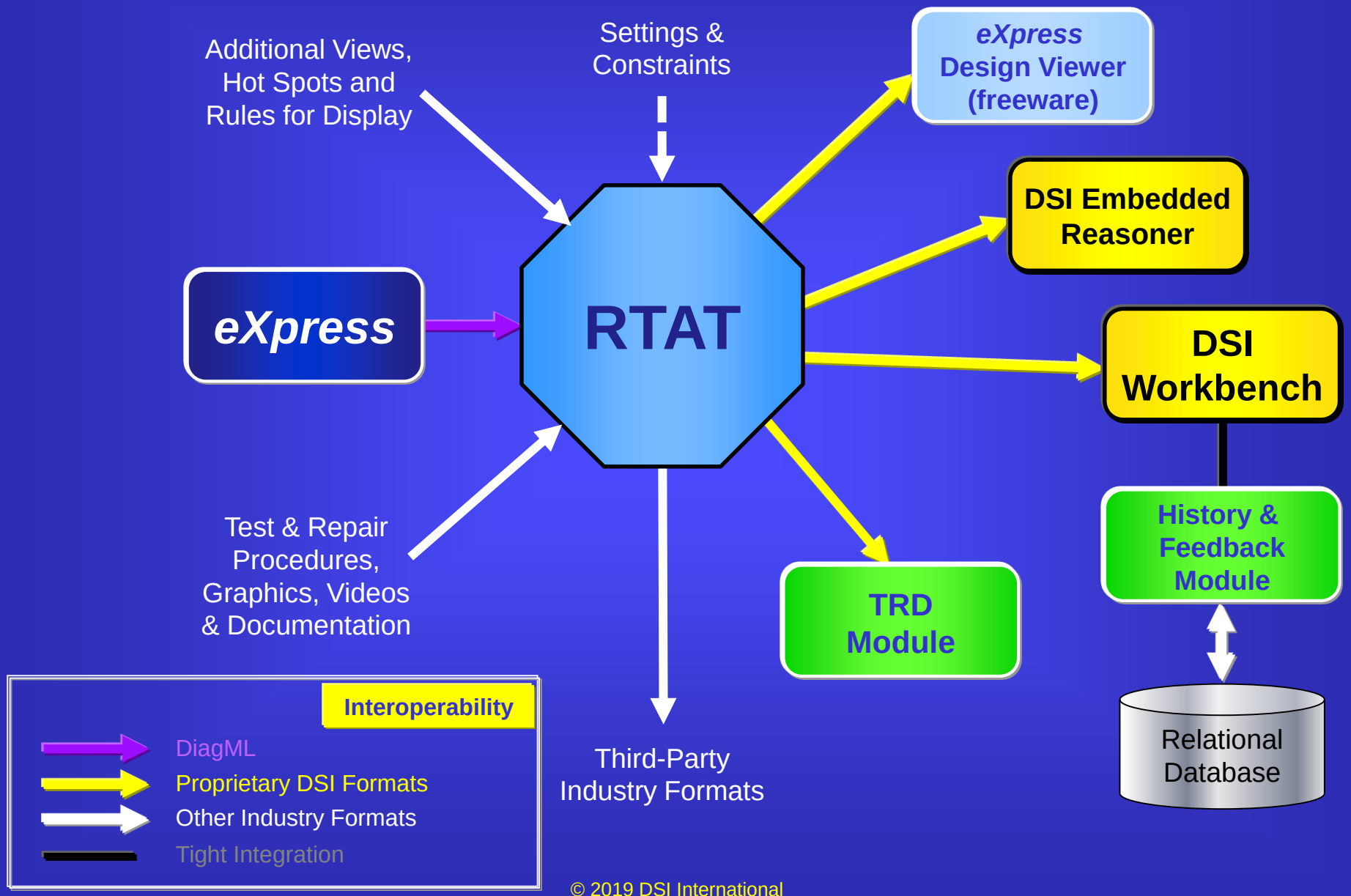


Desktop Fault Insertion

- Consists of an interactive dialog and corresponding report
- Allows analysts to validate diagnostics developed in ***eXpress*** by examining how inserted faults are detected and isolated
- Provides a variety of features to support both in-house and customer reviews
- Supports the troubleshooting of issues identified during maintenance demos or for fielded systems

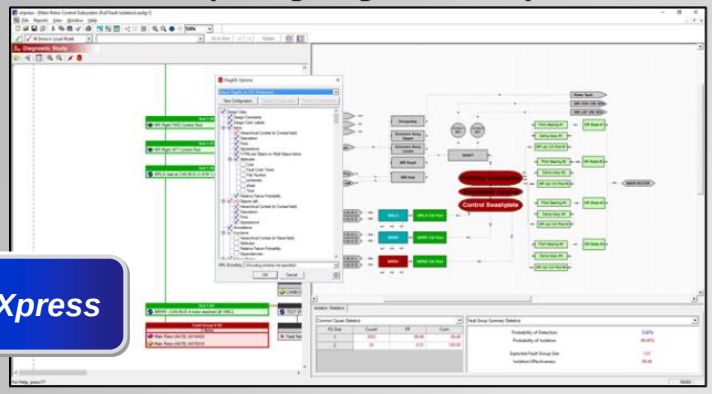


Diagnostic Interoperability via RTAT

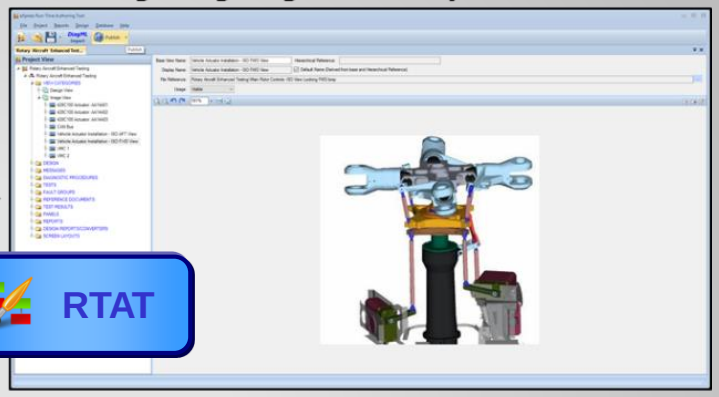


Diagnostic Deployment using DSI Workbench

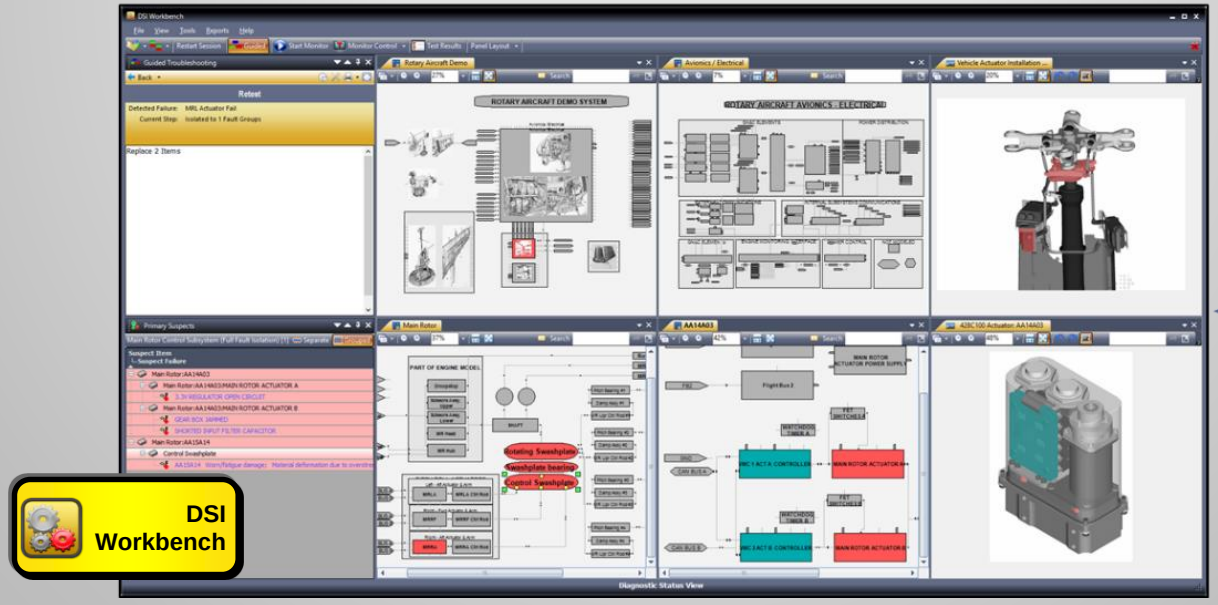
Exporting Diagnostic Study



Integrating Diagnostic Study & Resources

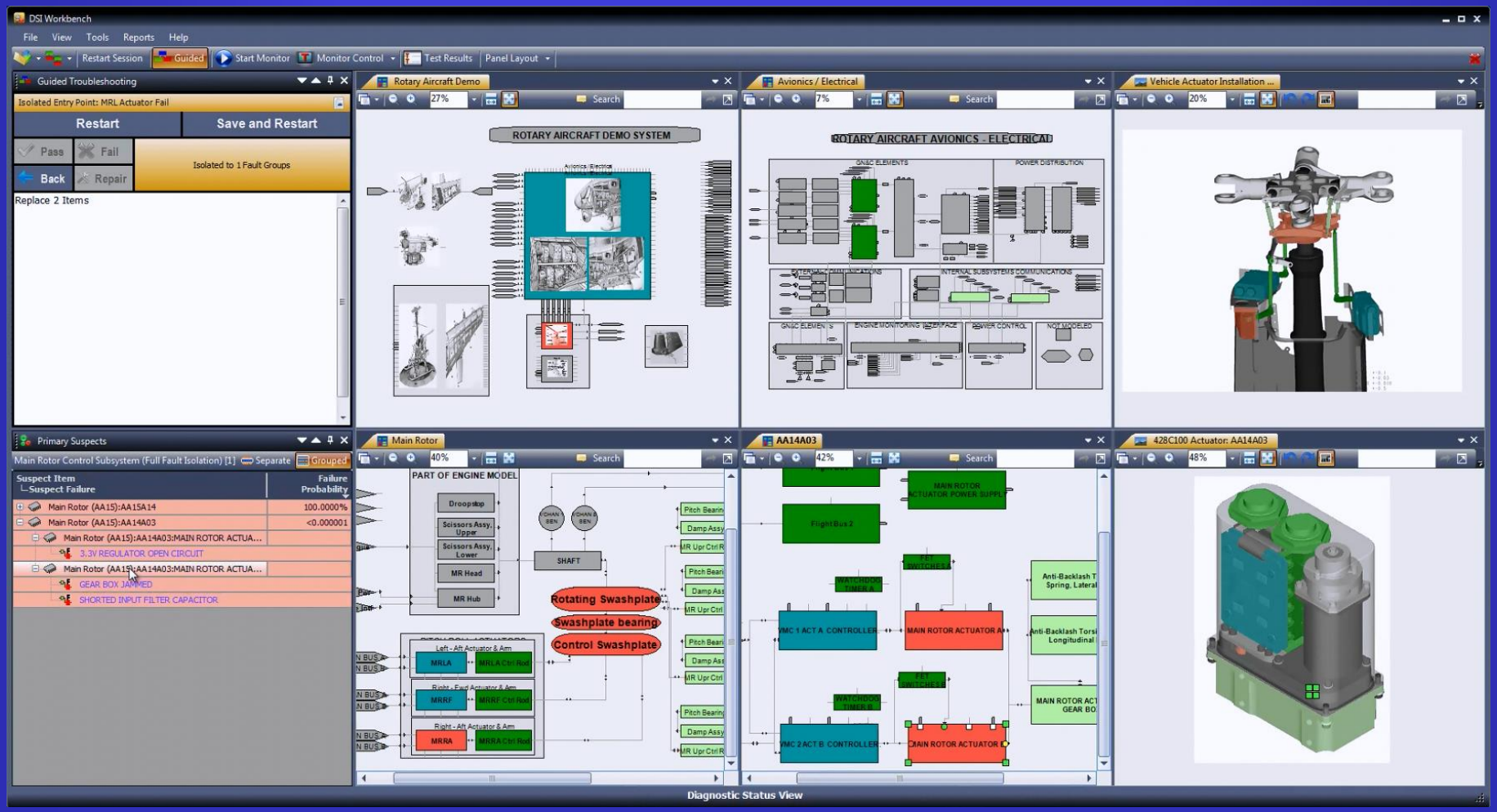


Implementing Diagnostic Strategy in Run-Time Environment



Run-Time Diagnostics in DSI Workbench

- DSI Workbench is a full-featured diagnostic executive for maintenance and production environments
- With minimal effort, you can field the same diagnostics you used to evaluate your system Testability



eXpress Fly-Over