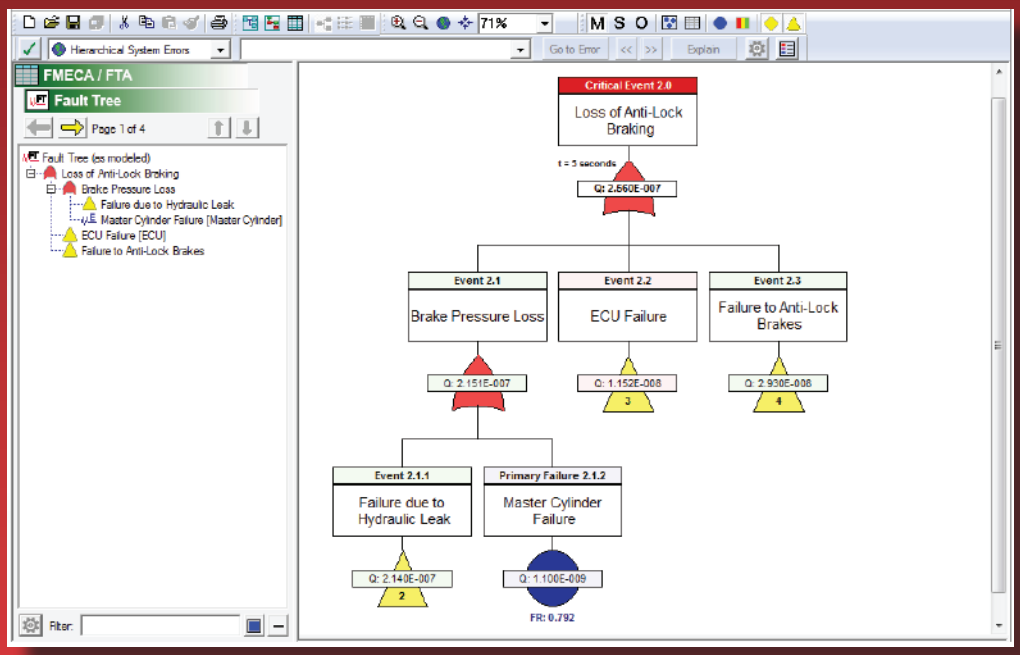
DSI International

eXpress FTA Module

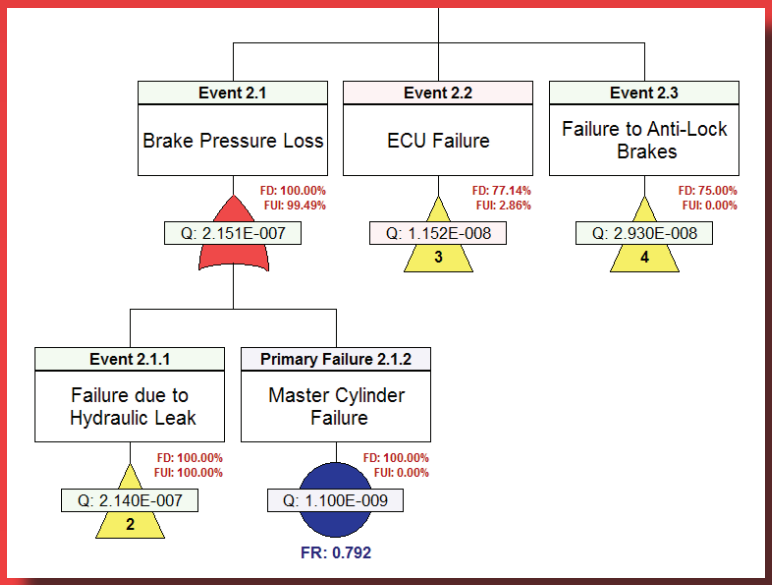
Fault Trees for Reliability and Probabilistic Risk Assessment

Interdisciplinary Fault Tree Analysis – The ***eXpress*** FTA Module automatically generates full-featured fault trees using data from an ***eXpress*** systems engineering model. Fully integrated with both **FMECA Plus** and the ***eXpress*** diagnostics/prognostics, the resulting Fault Tree Analysis not only opens up new vistas within the realm of Diagnostic Engineering, but also provides for the dovetailing of previously independent efforts expended on Diagnostic, Reliability, Risk and Safety analysis.



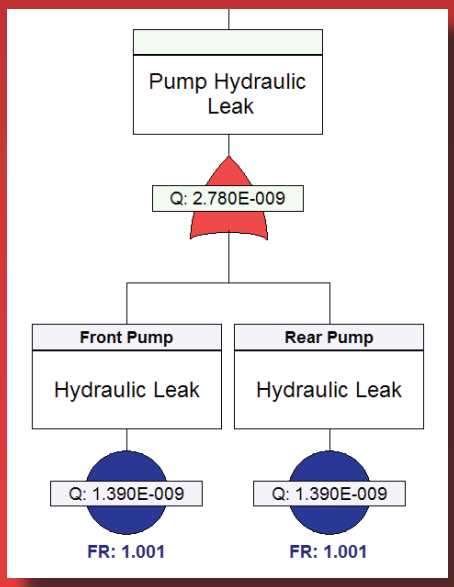
This example fault tree computes the likelihood that the Anti-Lock Brakes in an automobile will fail during the five seconds ("exposure time") in which they are applied. The yellow transfer gates indicate that lower-level details are provided on subsequent pages of the diagram.

Integration with *eXpress* Models – Because ***eXpress*** captures engineering data at a depth lower than is necessary for most FTA efforts, the failure rates for primary failures in ***eXpress*** fault trees are automatically derived from the same data used for other design analysis efforts. Even preliminary design data, when represented as a so-called "inverted FMEA", provides an excellent framework that can serve as a functional roadmap of the system hierarchy. The propagation of failure represented in this roadmap can then be studied and updated for use in the final Fault Tree Analysis.



Fault Detection & Isolation information can be displayed directly in the fault tree.

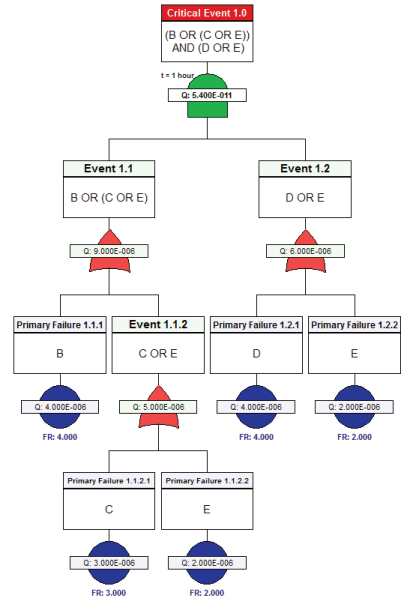
Customized Automation – Although fault trees are generated automatically within ***eXpress***, there are many ways to customize their content, order, layout and appearance. This unique blend of customization and automation greatly reduces the level of effort required to create deliverable-quality fault trees—trees that have been specifically tailored to suit your particular analysis needs.



*In this small excerpt from a customized **eXpress** fault tree, the name of the repair item associated with each primary failure is listed (in lieu of the event ID) in the header of each event box.*

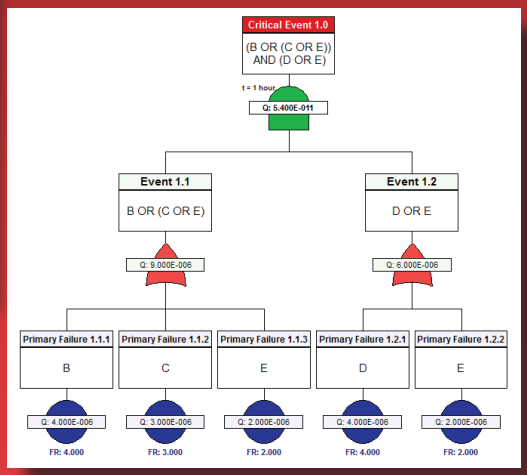
Integration with the *eXpress* Diagnostics – Because fault trees in ***eXpress*** are generated from the same data that is used for diagnostic engineering, cross-disciplinary guesswork is virtually eliminated. Reliability, Risk & Safety analysis can now confidently take into account the behavior of the actual diagnostics that will be fielded with the system. This reveals new areas of risk that result when diagnostics are unable to adequately identify or isolate the root causes that lead to critical failure. Likewise, diagnostic engineers can now take advantage of the in-depth analysis of failure performed by other disciplines. Diagnostic effectiveness can be assessed from an operational standpoint (thereby transcending the so-called "maintenance bias" that inheres in most diagnostic analysis efforts).

eXpress FTA Module

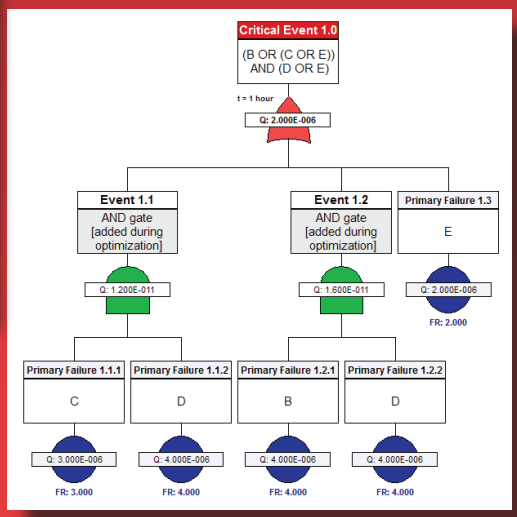


Viewing the fault tree "as modeled".

Three Views – One of the unique features of the ***eXpress*** FTA is that it provides three different ways of viewing a given fault tree. One view displays the tree "as modeled" (that is, using all relevant effects from the ***eXpress*** design). A second viewing mode displays a "simplified" fault tree, with unnecessary events removed (the degree of simplification is based on user settings). Finally, you can view the "optimized" fault tree, which not only employs the most extensive simplification, but also reorganizes the logic of the tree to account for multiple occurrences of the same event (so that displayed failure probabilities are equivalent to those calculated from the Minimal Cut Sets). In the simple example below, the top-level probability of failure for the optimized tree is **2.000E-006**, five orders of magnitude greater than the number in the *simplified* tree (**5.400E-011**). With fault tree optimization, there is no discrepancy between the numbers in the tree and those calculated from Minimal Cut Sets.

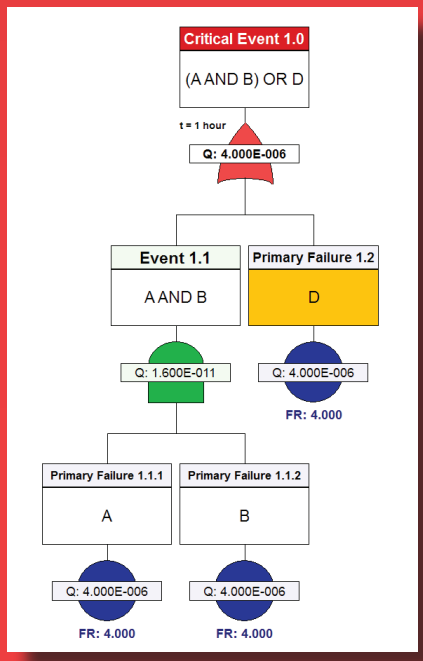


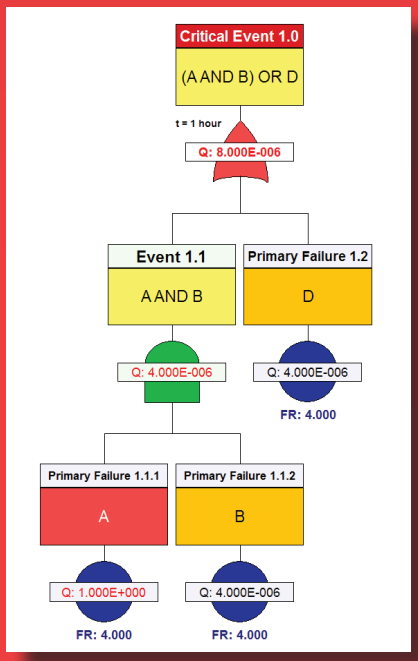
A "simplified" view of the same fault tree.

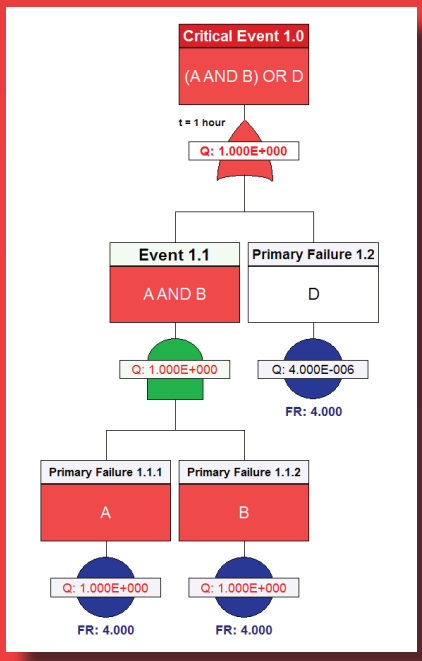


The "optimized" view of the same fault tree.

Fault Insertion – A useful feature of the ***eXpress*** FTA is the ability to assess the impact of individual failures (or sets of failures) by inserting faults and viewing the propagated effects within the fault tree. The tool's Fault Insertion capability also allows you to visually identify single points of failure—failures that, if they were to occur, would directly result in the top-level event.



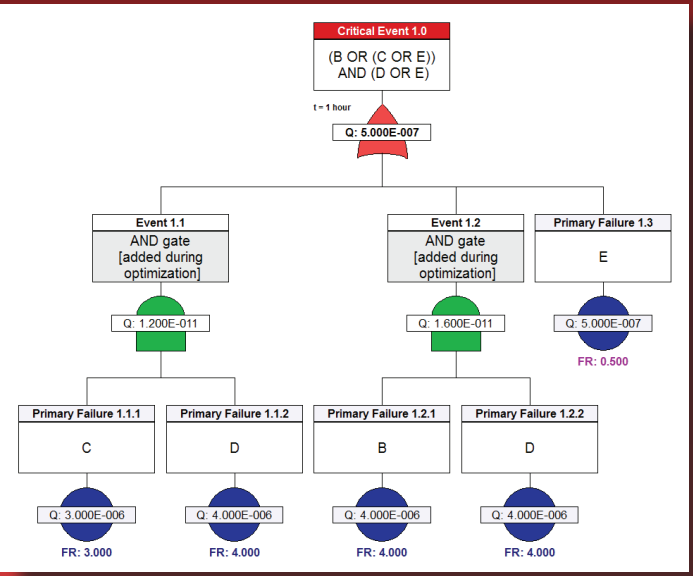




*When the Fault Insertion mode is invoked, all single points of failure are colored orange for easy identification (as shown in the first picture). When a fault is inserted, the box corresponding to the inserted fault is colored red in the tree and any higher-level events that have "partially" failed due to that fault are colored yellow (as shown in the second picture). The top-level probability is recalculated to represent the new likelihood of occurrence, given that the specified failure has occurred. Also, notice that fault insertion may result in new single points of failure. When the inserted fault(s) are sufficient to produce the top-level critical event, then the box at the top of the tree will be colored red as well and its probability of failure will be displayed as **1.000E-000** (as shown in the third picture).*

Accounting for Prognostics – When an ***eXpress*** FTA is linked to a diagnostic study that includes prognostic definitions, the expected decrease in the occurrence of failures that can be prevented using prognostics will be reflected in the fault tree (with failure rates reduced based on the specified confidence of each prognosis). Using the same example fault tree depicted on the top of the facing page, we have specified that failure E can be prognosed with 75% confidence. As a result, it is assumed that this failure will occur one-fourth as often as it would without prognostics. All calculated values (both on the screen and in reports) will be updated to reflect this change.

Reports – The ***eXpress*** FTA module offers a variety of user-customizable reports, each relating to a different aspect of Fault Tree Analysis. These reports have been designed to address key concerns for a variety of disciplines, including (but not limited to) Reliability Analysis, System Safety Analysis, Probabilistic Risk Assessment and Diagnostic Engineering. All reports created by the ***eXpress*** FTA module can be generated as RTF documents, exported as Excel spreadsheets, or saved in XML format.



When a primary failure can be partially prevented using prognostics, the effective failure rate (failures despite prognostics) is displayed in magenta.

Cut Set Details Report

Critical Event 1.0

(B OR (C OR E)) AND (D OR E)

Minimal Cut Set / Failure(s)	Failure Rate	## Failures	PoF (Q)
Cut Set 1.1		1	5.000E-007
E [BOX]	0.500		
Cut Set 1.3		2	1.600E-011
B [BOX]	4.000		
D [BOX]	4.000		
Cut Set 1.2			
D [BOX]			
C [BOX]			

*The **Cut Set Details Report** provides detailed information about each of the minimal cut sets for a given fault tree. The report can be generated as a list of cut sets (shown at left) or as a list showing the different cut sets associated with each primary failure. With user-selectable columns, sorting, grouping and filters, this report is likely to be essential to all FTA efforts.*

Failure Mitigation Report

Critical Event 1

(B OR (C OR E)) AND (D OR E)

Failure [Object]	Failure Rate	Individual PoF (Q)	Contributing PoF (Q)	Mitigating Events
E [BOX]	0.500	5.000E-007	5.000E-007	None
B [BOX]	4.000	4.000E-006	1.600E-011	AND (2) @ 1.2
D [BOX]	4.000	4.000E-006	1.600E-011	AND (2) @ 1.2
C [BOX]				

*The **Failure Mitigation Report** shows, for each primary failure, the extent to which that failure is mitigated by functional redundancy (or some other design consideration) to prevent it from acting as a single point of failure.*

Importance Measures Report

Critical Event 1

(B OR (C OR E)) AND (D OR E)

Failure [Object]	Individual PoF (Q)	Birnbaum	CIF	RAW	RRW	Fussell-Vesely
E [BOX]	5.000E-007	9.990E-001	0.998944	1999888.507	17858.246	0.999944
D [BOX]	4.000E-006	7.000E-006	0.000056	14.999	1.000	0.000056
B [BOX]	4.000E-006	4.000E-006	0.000032	8.999	1.000	0.000032
C [BOX]						

*The **Importance Measures Report** lists standard industry measures of the importance of various elements to the successful performance of a given device or system. These metrics (some of which are shown at right) are staples of Probabilistic Risk and Safety Assessments (PRA & PSA).*

Probability of Failure Report

Details

Critical Event 1.0

(B OR (C OR E)) AND (D OR E)

Minimal Cut Sets	## Failures	Probability of Critical Event	Probability of Partial Failure	Probability of No Failure
Cut Set 1.1	1	5.000E-007	N/A	0.999999
Cut Set 1.3	2	1.600E-011	8.000E-006	0.999992
Cut Set 1.2	2	1.200E-011	7.000E-006	0.999993
Overall:	4	5.000E-007	1.100E-005	0.999989

*The **Probability of Failure Report** lists the likelihoods of critical failure, "partial" failure (Fail Safe) or no failure in columns colored red, yellow & green. Probabilities are calculated for minimal cut sets or for individual failures, showing how they collectively result in the critical event's overall probability of failure. An optional summary lists the overall probabilities for each fault tree in a single table.*

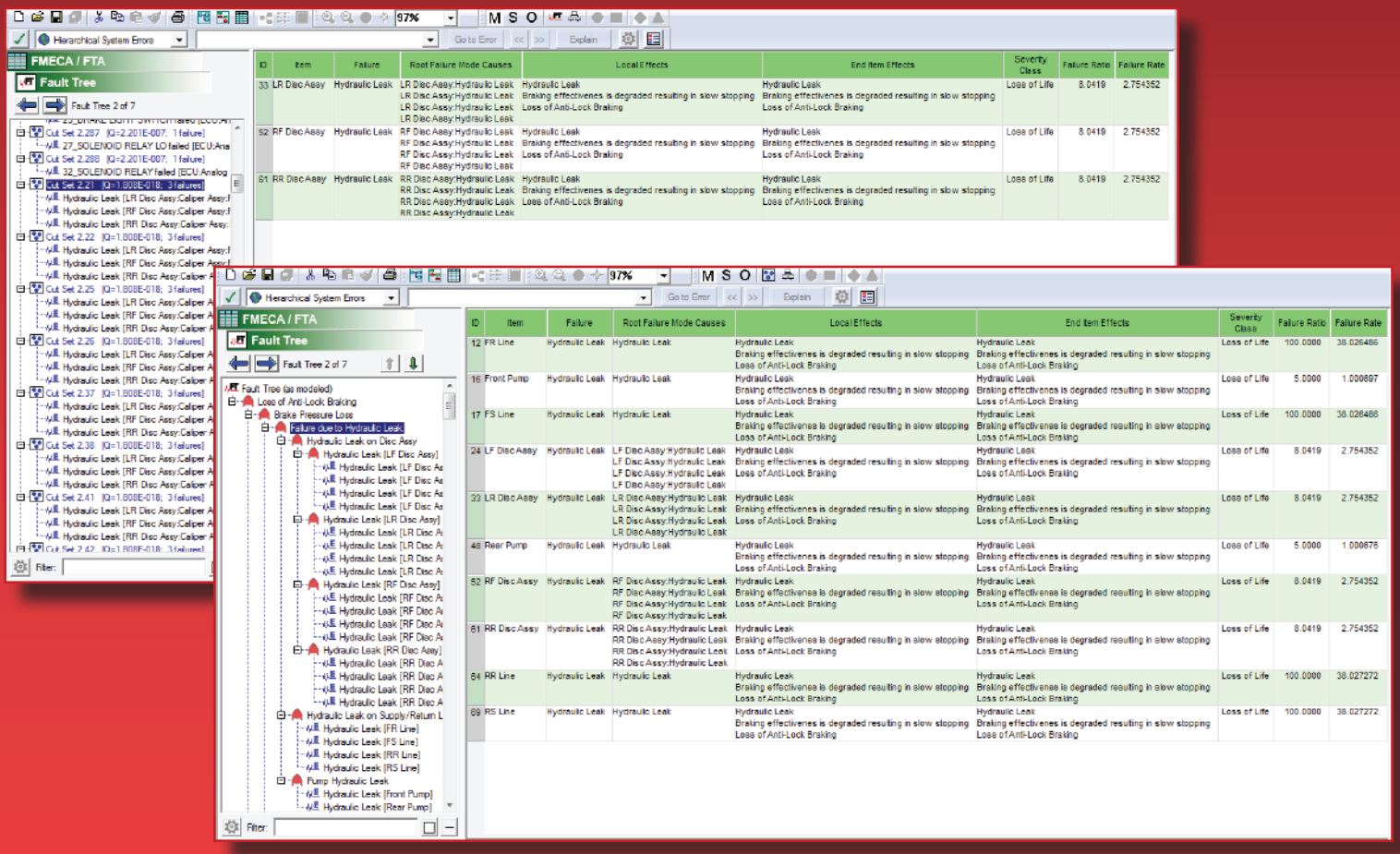
*Not depicted: the **Failure Diagnosis & Prognosis Report** and the **Fault Tree Optimization Report**.*

DSI International

eXpress FTA Module

Fault Trees for Reliability and Probabilistic Risk Assessment

Integration with FMECA Plus – In ***eXpress***, fault trees are displayed using the same graphic interface that is used to display ***eXpress*** FMECA charts. One benefit of this tight integration is that each fault tree also serves as an index to information in the corresponding FMECA. This is particularly powerful when your FMECA has custom columns containing project-specific data. Many companies treat their FMECAs as data repositories for multiple design and analysis disciplines. With the ***eXpress*** FTA module, this information remains at your fingertips as you evaluate the system-level impact of failures using fault trees.



During fault tree editing, FMECA rows that are related to the selected fault tree can be optionally displayed (instead of the fault tree diagram) on the right-hand side of the screen. When one or more entries are selected in the Explorer Tree on the left—which contains either the fault tree events (front example) or the Minimal Cut Sets (back example), then the chart will be further filtered to list only FMECA rows related to the selected entries.

Benefits & Features

- Fault trees are automatically generated from the same data used by other engineering efforts
- Incorporates the results of diagnostic & prognostic analyses from ***eXpress***
- Fully integrated with charts and calculations within **FMECA Plus**
- Calculates Minimal Cut Sets / Critical Paths
- Ability to insert faults and view their impact upon the system / identify additional single points of failure
- Viewing Modes: As Modeled, Simplified, Optimized
- Primary Events: Basic, Undeveloped/Secondary, Conditioning, External
- Gates: AND, OR, Voting OR, Inhibit, Transfer
- Reports: Probability of Failure, Cut Set Details, Importance Measures, Failure Mitigation, Failure Diagnosis & Prognosis, Fault Tree Optimization
- Importance Measures: Birnbaum, CIF, RAW, RRW, Fussell-Vesely, DIF and more

United States
DSI International, Inc.
(714) 637-9325
sales@dsiintl.com
www.dsiintl.com

United Kingdom
SPHEREA Test & Services
+44 1202 872800
chris.gorringe@spherea.co.uk
www.spherea.com

France
SPHEREA Test & Services
+33 (0)6 88 61 33 91
michel.schieber@spherea.com
www.spherea.com

Japan
Y-MAX, Inc.
+81-45-789-0701
massayo@y-max.com.jp
www.y-max.com

South Korea
Realtimewave Co, Ltd
+82-2-572-9471/2
sales@realtimewave.com
www.realtimewave.com

China
MTCS Systems Engineering Co. Ltd
+86-10-5881-6565
sales@mtcs.com.cn
www.mtcs.com.cn