eXpress™ Newsletter

DSI

Volume 16, Number 1

Spring 2010

Old Lettuce and Green Ice Cream

The Perishable FMECA

FMEA and FMECA activities are like heads of lettuce. Attractive when new, they can be kept fresh for a while with some diligence, yet will inevitably reach a point where they are simply no longer of use and have to be replaced by fresh heads.

If they are to remain relevant throughout the development life cycle, FMECAs must be updated regularly to reflect the changing aspects of a design as it matures. This would be fine and dandy if a new FMECA could be procured as easily as a fresh head of lettuce. Unfortunately, traditional FMECA development is notoriously time-consuming and many projects are forced to steer a path between the spiraling wastefulness of constant FMECA development and the obsolescence of static FMECA data during certain phases of the design process.

The **FMECA Plus** capability in ***eXpress*** offers an elegant solution to this dilemma—a solution perfectly suited to this funds-challenged age. In ***eXpress***, FMECAs can be derived directly from the same models that are used for the diagnostic engineering analysis. Data from the initial static FMECAs generated by standard Reliability tools can be imported into ***eXpress***, where it can be maintained along with models of the diagnostic design. When a new FMECA is needed, it can be generated from the updated model with just a few clicks of the mouse—it's as easy as going to the market!

Using **FMECA Plus** as a resource for FMECA maintenance and maturation not only eliminates duplicate work by Diagnostic and Reliability engineers, but also allows them to take full advantage of the fruit (or vegetables) of their respective labors.

Inside this Issue...

Everybody's Favorite Flavor

Ask a Reliability engineer to describe the fruit of their labor and you'll likely hear the following: "Oh, you know, it's just a standard FMEA." And yet, when it comes down to it, FMEAs come in nearly as many varieties as ice cream, with different flavors championed by different industries, projects, companies and individuals.

Nevertheless, all FMEA activities remain variations on a common theme—tracing the effects of failure upon system behavior and identifying specific failures that require special attention.

The **FMECA Plus** engine in ***eXpress*** provides a set of default configurations representing a variety of typical and atypical FMECA applications. These default configurations fall into two classes—***eXpress*** charts and "traditional" worksheets. Each of the ***eXpress*** charts is a turnkey analysis that derives all of its data from standard fields within an ***eXpress*** model. What makes these charts "special" is their extensive—and in some cases creative—use of fault detection and isolation results from the diagnostic analysis in ***eXpress***.

The "traditional" worksheet configurations offered by **FMECA Plus** rely less upon the results of diagnostic analysis and more upon custom attribute data that has been added (or imported) into the ***eXpress*** model. This allows the FMEA and Criticality Analysis worksheets created within ***eXpress*** to contain the same narrative descriptions of system behavior and fault handling that Reliability analysts are accustomed to seeing in worksheets created using conventional methods.

Of course, all of these default configurations should be thought of as templates that can be modified and extended to serve your own idiosyncratic analysis requirements. In addition to a large number of pre-defined data columns, you can also easily create custom columns based on user-defined attributes in the ***eXpress*** model.

Thanks to the flexibility of **FMECA Plus**, if you find yourself with a pressing need for green ice cream, you can still have your choice of flavors—mint, lime, pistachio, green tea or even avocado!!

Calling on the Diagnostic Design to Reduce False Alarms and System Aborts

Excessive False Alarms and unnecessary System/Mission Aborts are often the result of a poor diagnostic design. If system diagnostics do not adequately distinguish between sensor failures and operational malfunctions, for instance, then below-par diagnostic performance may become a major—in many cases primary—contributor to the overall number of False Alarms. The same is true for System and Mission Aborts. If operational diagnostics cannot distinguish between failures that necessitate an abort and other failures that produce the same fault signature, the inevitable result will be a high number of “false” aborts—situations in which an abort is effected due to the ambiguous isolation of a failure that itself should not have required an abort.

Conventional design assessment practices (including standard Reliability, Testability & Maintainability analyses) have proven to be inadequate for evaluating diagnostic inefficiencies of this kind and incapable of identifying areas where improvements to diagnostic performance could substantially reduce False Alarm and System/ Mission Abort rates.

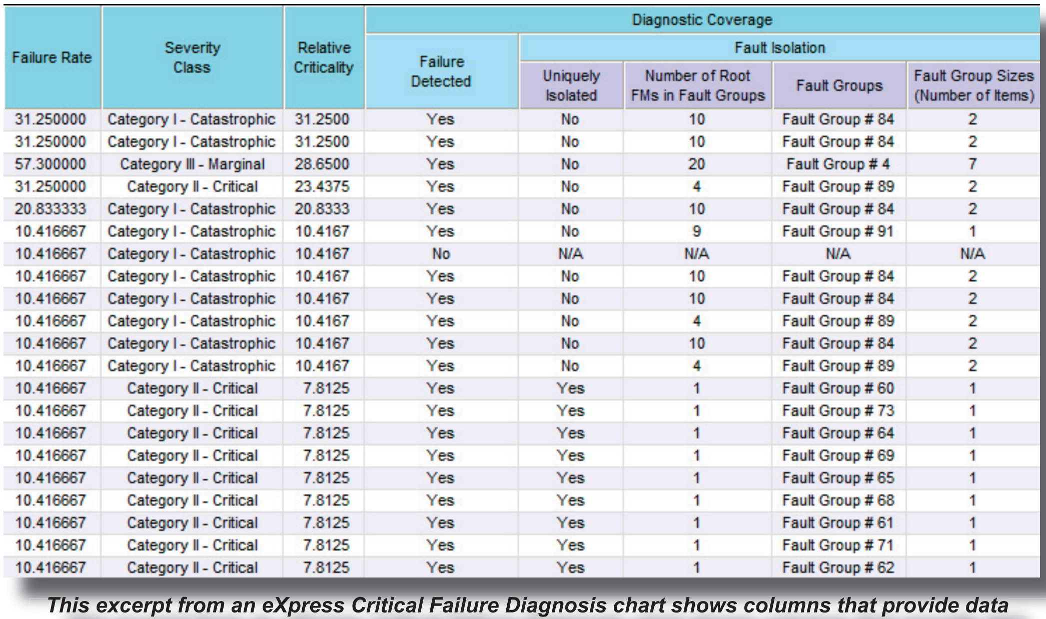
There are, of course, many reasons behind these shortcomings: an overreliance on Reliability-based models of system behavior, a near-exclusive emphasis on fault detection when analyzing the handling of critical failures, the mischaracterization of diagnostic performance using numbers that are “rolled up” from lower design levels (rather than derived from reassessments within higher-level contexts), the evaluation of diagnostic effectiveness in terms that reflect its impact upon maintenance goals rather than mission success, and the use of oversimplified analysis methodologies that do not successfully characterize the relationship between diagnostics/maintenance and future system failures.

In response to this clear need for more diagnostically-informed analyses of potential False Alarm and System/Mission Abort rates, DSI has recently introduced into its industry-leading diagnostic engineering tools ***eXpress*** and **STAGE** several new features that have been specifically designed to address these issues.

FMECA analysis has, for a long time, been the primary mechanism for representing the effects of individual failures upon system behavior and prioritizing failures that—due to their severity, frequency of occurrence, or lack of detection—require special attention. Because these three criteria (severity, frequency, detectability) can all be rolled up from lower-level analyses, they lend themselves well to spreadsheet-style analysis (as well as System Reliability Fault Diagram and Fault Tree Analysis approaches), where upper-level behavior can be represented as the aggregate or sum of constituent lower-level behavior.

To measure the impact of diagnostics upon False Alarms or System/ Mission Aborts, analysis must also take into consideration the ability of diagnostics to *isolate* detected failures. Unlike with fault detection, lower-level evaluations of the fault isolation capability of a device may not hold true when that device is tested within its system context. For instance, a given module may have excellent inherent fault isolation characteristics yet, within its subsystem context, the module’s inputs may not be directly controlled, or its outputs not directly observed, thereby resulting in additional ambiguity at the subsystem level. In short, to accurately represent the fault isolation of specific failures (and, consequently, their impact upon alarms and aborts) it is essential that fault isolation be derived from a diagnostic engineering process that takes system topology into consideration.

The **FMECA Plus** feature in ***eXpress*** incorporates details from the actual diagnostic design into its “enhanced” charts. For instance, the *eXpress Critical Failure Diagnosis* chart (depicted below at left) indicates how well each failure is both detected *and* isolated by system diagnostics.



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)
31.250000	Category I - Catastrophic	31.2500	Yes	No	10	Fault Group # 84	2
31.250000	Category I - Catastrophic	31.2500	Yes	No	10	Fault Group # 84	2
57.300000	Category III - Marginal	28.6500	Yes	No	20	Fault Group # 4	7
31.250000	Category II - Critical	23.4375	Yes	No	4	Fault Group # 89	2
20.833333	Category I - Catastrophic	20.8333	Yes	No	10	Fault Group # 84	2
10.416667	Category I - Catastrophic	10.4167	Yes	No	9	Fault Group # 91	1
10.416667	Category I - Catastrophic	10.4167	No	N/A	N/A	N/A	N/A
10.416667	Category I - Catastrophic	10.4167	Yes	No	10	Fault Group # 84	2
10.416667	Category I - Catastrophic	10.4167	Yes	No	10	Fault Group # 84	2
10.416667	Category I - Catastrophic	10.4167	Yes	No	4	Fault Group # 89	2
10.416667	Category I - Catastrophic	10.4167	Yes	No	10	Fault Group # 84	2
10.416667	Category I - Catastrophic	10.4167	Yes	No	4	Fault Group # 89	2
10.416667	Category II - Critical	7.8125	Yes	Yes	1	Fault Group # 60	1
10.416667	Category II - Critical	7.8125	Yes	Yes	1	Fault Group # 73	1
10.416667	Category II - Critical	7.8125	Yes	Yes	1	Fault Group # 64	1
10.416667	Category II - Critical	7.8125	Yes	Yes	1	Fault Group # 69	1
10.416667	Category II - Critical	7.8125	Yes	Yes	1	Fault Group # 65	1
10.416667	Category II - Critical	7.8125	Yes	Yes	1	Fault Group # 68	1
10.416667	Category II - Critical	7.8125	Yes	Yes	1	Fault Group # 61	1
10.416667	Category II - Critical	7.8125	Yes	Yes	1	Fault Group # 71	1
10.416667	Category II - Critical	7.8125	Yes	Yes	1	Fault Group # 62	1

This excerpt from an eXpress Critical Failure Diagnosis chart shows columns that provide data essential for determining the impact of diagnostics upon False Alarms and System/Mission Aborts.

Here, the isolation of each failure is characterized not only in terms of the repair items in the isolated fault group (useful information, but with a bias toward maintenance diagnostics), but also by the number of root failure mode causes included in that group. Moreover, the chart indicates whether or not each critical failure is *uniquely* isolated—whether the isolated fault group is comprised solely of root failure modes that are potential causes of that failure.

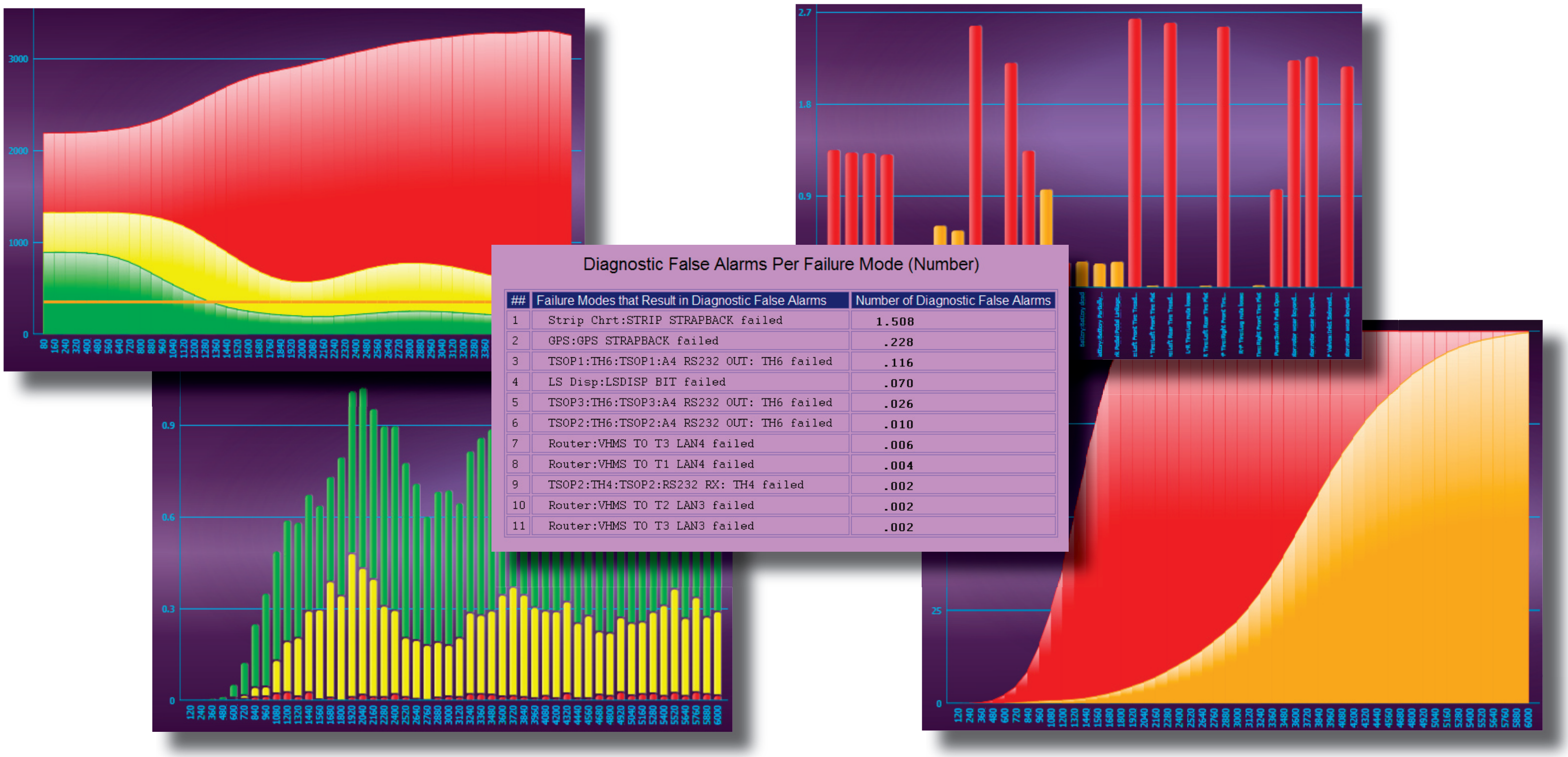
Because the ambiguous isolation of critical failures could result in unacceptable levels of False Alarms and System/Mission Aborts, it is essential that existing Reliability analyses be supplemented with a consideration of how well system diagnostics are capable of uniquely identifying critical failures.

Whereas **FMECA Plus**, by incorporating diagnostic analysis data into the Reliability engineering process, promotes the timely handling of failures that drive False Alarms and System/Mission Aborts, **STAGE** allows analysts and engineers to assess the impact that their design decisions will have upon a system's diagnostic performance (including False Alarm and System/Mission Abort rates) over time.

Using **STAGE**, for instance, analysts and engineers can assess the effects of sub-optimal fault isolation upon a system's False Alarm rate, tracking over time the frequency, likelihood and mean time between alarms of various types (including diagnostic False Alarms), as well as identifying the specific failures that are responsible for inflated alarm rates.

In a series of similar calculations, **STAGE** can also demonstrate the impact of diagnostic ambiguity upon System/Mission Aborts. In an analysis unique to **STAGE**, aborts are categorized as either "true" (resulting from failures that necessitate an abort) or "false" (resulting from failures that should not require an abort, yet which nevertheless produce an abort due to inadequate fault isolation). By recognizing the impact of fault isolation upon the System Abort rate, the analyses within **STAGE** go a long way toward bridging the gap between the artificially attractive MTBSAs estimated by standard Reliability practices and the significantly higher abort rates that might occur for a fielded system whose diagnostics have not been optimized to ensure the unique isolation of alarm-generating failures.

Unlike operational simulations based primarily on Reliability models, **STAGE** simulates not only how a system or device fails, but also how it is diagnosed and maintained. Because diagnostic and maintenance procedures are imported directly from the diagnostic engineering effort, the analyses within **STAGE** provide valuable feedback on the actual diagnostic design (rather than the best-guesses of Reliability analysts). Moreover, by taking into consideration the subtleties of maintenance-deferred-failure (where item replacement results in the postponement of specific failures), False Alarm and System/Mission Abort calculations within **STAGE** provide more accurate predictors of actual system behavior.



Diagnostic False Alarms Per Failure Mode (Number)

##	Failure Modes that Result in Diagnostic False Alarms	Number of Diagnostic False Alarms
1	Strip Chrt:STRIP STRAPBACK failed	1.508
2	GPS:GPS STRAPBACK failed	.228
3	TSOP1:TH6:TSOP1:A4 RS232 OUT: TH6 failed	.116
4	LS Disp:LSDISP BIT failed	.070
5	TSOP3:TH6:TSOP3:A4 RS232 OUT: TH6 failed	.026
6	TSOP2:TH6:TSOP2:A4 RS232 OUT: TH6 failed	.010
7	Router:VHMS TO T3 LAN4 failed	.006
8	Router:VHMS TO T1 LAN4 failed	.004
9	TSOP2:TH4:TSOP2:RS232 RX: TH4 failed	.002
10	Router:VHMS TO T2 LAN3 failed	.002
11	Router:VHMS TO T3 LAN3 failed	.002

Above are a few of the many outputs of STAGE that describe False Alarms and System Aborts. On the left are two graphs that depict the mean time between alarms and frequency of alarms over time (with alarms categorized by type). In the middle is a report listing the failure modes that result in diagnostic false alarms. On the right are two graphs showing the failure modes that result in system aborts (false and true) and the likelihood of a system abort over time.

Training Schedule

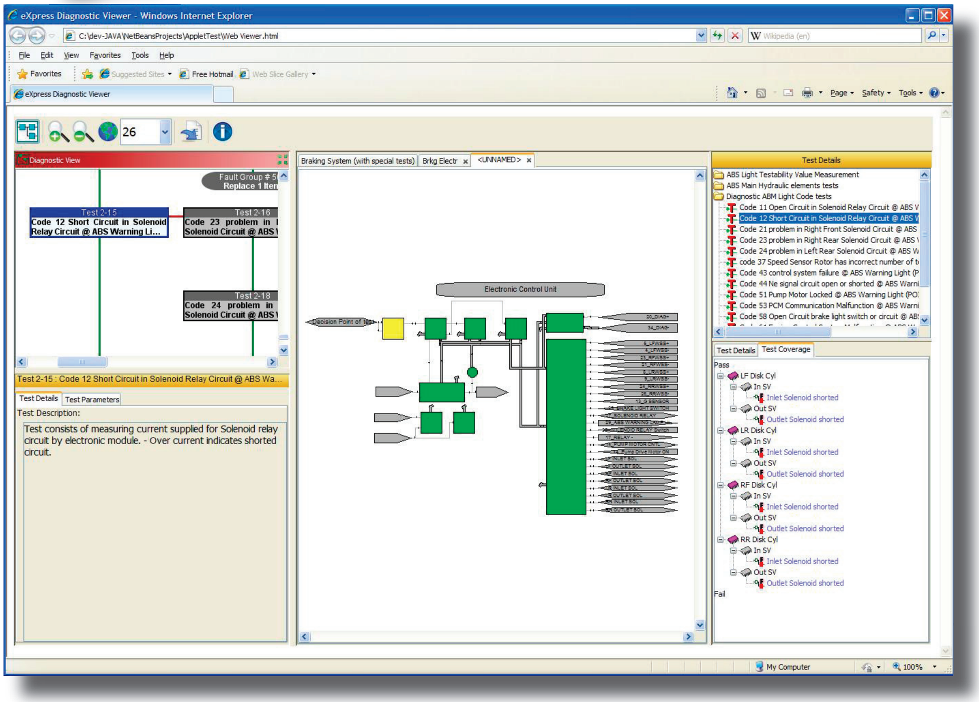
Course Number	Pre-requisite	Course Description	Dates	Location	POC
200	120	Advanced Diagnostic Development & Assessment	14 June 2010	Orange, CA	Denise Aguinaga , DSI
205	200	Advanced Test Development & Importing	16 June 2010	Orange, CA	Denise Aguinaga , DSI
210	205	Advanced FMECA Development & Assessment	18 June 2010	Orange, CA	Denise Aguinaga , DSI
250	210	STAGE Time-based Assessments & Principles	21 June 2010	Orange, CA	Denise Aguinaga , DSI
100		System Diagnostics Concepts and Applications	19 July 2010	Orange, CA	Denise Aguinaga , DSI
110	100	Basic Modeling & Introduction to Testing	19 July 2010	Orange, CA	Denise Aguinaga , DSI
120	110	Introduction to Testing & Analysis	22 July 2010	Orange, CA	Denise Aguinaga , DSI

Beyond Compliance: DSI and Industry Standards

DSI is often asked whether our tools are compliant with various Testability-related standards, such as **IEEE Standard 1522-2004** or **MIL-STD-2165**. Many people don't realize that DSI was instrumental in the development of both of these documents and that most of the metrics documented in these standards describe calculations that had first been performed within DSI's own analyses and were first commercially available (sometimes using a different name) within one or another of DSI's products. As the result of our involvement in standards development, we at DSI can say with confidence that these standards are indeed compliant with the techniques that we have championed for the last 35 years!!

Of course, these standards describe baseline calculations that often must be modified to address the unique requirements of a given project. That's why ***eXpress*** provides analysts with a wide variety of ways to constrain and categorize "standard" fault detection and isolation statistics. That's also why in **STAGE** "standard" metrics are calculated over time, demonstrating how diagnostic performance changes as a system ages. Rather than settle with mere compliance, DSI continues to pioneer ways of creatively assessing the diagnostic capability of your system—providing you with the means of analyzing the full life-cycle impact of your diagnostic or prognostic engineering decisions.

Available *NOW!* — the *eXpress* Run-Time Authoring Tool


eXpress Diagnostic Viewer - Windows Internet Explorer
C:\dev-JAVA\NetBeansProjects\AppletTest\Web Viewer.html
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Free Hotmail
Web Slice Gallery
eXpress Diagnostic Viewer
Page Safety Tools
26
Diagnostic View
Braking System (with special tests)
Brkg Electr
<UNNAMED>
Electronic Control Unit
Decision Point of Isol
My Computer
100%

Fault Group # 5
Replace 1 Item

Test 2-15
Code 12 Short Circuit in Solenoid Relay Circuit @ ABS Warning Li...

Test 2-16
Code 23 problem in Solenoid Circuit @ ABS

Test 2-18
Code 24 problem in Solenoid Circuit @ ABS

Test 2-15 : Code 12 Short Circuit in Solenoid Relay Circuit @ ABS Wa...

Test Details | Test Parameters

Test Description:

Test consists of measuring current supplied for Solenoid relay circuit by electronic module. - Over current indicates shorted circuit.

Test Details

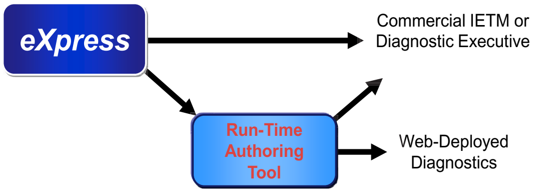
- ABS Light Testability Value Measurement
- ABS Main Hydraulic elements tests
- Diagnostic ABM Light Code tests
  - Code 11 Open Circuit in Solenoid Relay Circuit @ ABS W
  - Code 12 Short Circuit in Solenoid Relay Circuit @ ABS W
  - Code 21 problem in Right Front Solenoid Circuit @ ABS
  - Code 23 problem in Right Rear Solenoid Circuit @ ABS W
  - Code 24 problem in Left Rear Solenoid Circuit @ ABS W
  - code 37 Speed Sensor Rotor has incorrect number of t
  - Code 43 control system failure @ ABS Warning Light (P
  - Code 44 Ne signal circuit open or shorted @ ABS Warni
  - Code 51 Pump Motor Locked @ ABS Warning Light (PO
  - Code 53 PCM Communication Malfunction @ ABS Warni
  - Code 58 Open Circuit brake light switch or circuit @ AB

Test Details | Test Coverage

Pass
- LF Disk Cyl
  - In SV
    - Inlet Solenoid shorted
  - Out SV
    - Outlet Solenoid shorted
- LR Disk Cyl
  - In SV
    - Inlet Solenoid shorted
  - Out SV
    - Outlet Solenoid shorted
- RF Disk Cyl
  - In SV
    - Inlet Solenoid shorted
  - Out SV
    - Outlet Solenoid shorted
- RR Disk Cyl
  - In SV
    - Inlet Solenoid shorted
  - Out SV
    - Outlet Solenoid shorted

Fail

***eXpress* Design and Diagnostic data viewed using Internet Explorer**



Run-Time Authoring Tool

- Reads DiagML files from ***eXpress***
- Provides options for customizing the display of exported data
- Publishes data for the ***eXpress*** Java Applet

eXpress Java Applet

- Supports viewing using any Web Browser
- Facilitates the sharing of diagnostic design data with individuals who don't have ***eXpress***
- Allows work to be posted on the Internet, shared on a local network, or emailed to selected individuals
- Displays hierarchical and fully-graphical representations of objects, nets, F/FMs, tests and diagnostic sequences

World Wide Representatives

EADS Test Engineering Services (UK) Ltd.
29-31 Cobham Road
Ferndown Industrial Estate
Wimborne
Dorset BH21 7PF
United Kingdom

Tel: +44 1202 872800
Contact: Penri Jones (Gen Mgr)
Fax: +44 1202 870810
E-Mail:
penri.jones@eads-ts.co.uk
www.eads-ts.com

EADS TEST & SERVICES /EL/S
MetaPole; 1 Boulevard Jean Moulin
CS 40001 - 78996
ELANCOURT *CEDEX*
France

Tel: +33 (0) 6 88 61 33 91
Contact: Michel Schieber
Fax: +33 1 61 38 58 34
E-Mail: michel.schieber@eads.com
www.eads.com

Y-MAX Inc.
2-16 Tsurumaki 5-chome
Setagaya-ku, Tokyo
Japan
154-0016

Tel: 81-3-5451-0085
Fax: 81-3-3429-0089
E-Mail: ate@y-max.co.jp
www.y-max.com

MTCS Systems Engineering Co Ltd.
Room 1905 Block C1
Yi Cheng Plaza
No. 11 Chang Chun Qiao Road
Haidian District
Beijing 100089 China

Tel: 86-10-5881-6565
Fax: 86-10-5881-6566
E-Mail: sales@mtcs.com.cn
www.mtcs.com.cn

www.dsiintl.com

DSI International, Inc.
1574 N. Batavia St., Bldg. 3
Orange, California 92867
Phone: (714) 637-9325
Fax: (714) 637-0584
E-mail: info@dsiintl.com

The *eXpress*™ Newsletter is published semi-annually by DSI International

All information in this publication is used and covered by copyright and/or Trademark of DSI and/or respective manufacturers. Readers are encouraged to reproduce articles, giving credit to DSI. Additional copies may be obtained by writing to DSI at the above address

Information relative to products or services of products described herein or of other manufacturers is accurate to the best of knowledge of DSI and does not necessarily indicate that such manufactures endorse any products or services described herein.

Interested individuals should investigate any products or service completely before making final judgment.