ETDPO

Integrated Fault Detection, Isolation and Recovery for Ground Operations

April 27-28, 2010

Barbara Brown/ARC @ KSC
barbara.l.brown@nasa.gov
Bob Waterman/KSC
bob.waterman@nasa.gov

Contents

CxP FDIR Background

- Fault Detection, Isolation and Recovery (FDIR) required by CARD
  - [CA0216-PO] **The Constellation Architecture shall provide fault detection, isolation and recovery.** *Rationale:* NPR 8705.2, Human-Rating Requirements for Space Systems, mandates FDIR for faults of human-rated systems that affect critical functions. FDIR is required for crew safety and mission success by enabling recovery of such critical functions. In addition, fault detection enables crew abort or flight termination (in case of non-recoverable failures). Fault isolation further enables common-mode failure identification, in-flight maintenance and fleet supportability.
- Launch Availability required by CARD
  - **CA3064-PO]** Ground Systems shall have a probability of crewed launch of no less than 99 (TBR-001-1412)%, during the period beginning with the decision to load cryogenic propellants and ending with the close of the day-of-launch window for the initial planned attempt.
- FDIR requirements are flowed down to all systems (CEV, CLV, GS, MS) as separate Detection, Isolation and Recovery requirements
- Current GOP Baseline is to allocate fault detection, isolation (diagnostics) and recovery to individual subsystem application software (Isolation/Recovery are operator provided functions)
  - Detailed requirements derived from:
    - TVR-O (OMRS testing requirements)
    - LCC (Launch Commit Requirements)
    - KSC Engineering knowledge of system operation

Launch Availability

- [CA123-PO] The Constellation Architecture shall have a probability of crew launch of not less than 99% (TBR-001-021) during the period beginning with the decision to load cryogenic propellants and ending at the expiration of the EDS and LSAM loiter
- [CA3064-PO] Ground Systems shall have a probability of crewed launch of no less than 99% (TBR-001-014) during the period beginning with the decision to load cryogenic propellants and ending with the close of the day-of-launch window for the initial planned attempt

Launch Availability:
Ground Operations Historical Perspective

$$p_{LAUNCH} >= p_{CEV-AVAIL} * p_{CLV-AVAIL} * p_{WEATHER} * p_{RANGE} * p_{MS-AVAIL} * p_{GS-AVAIL}$$

	Launch Success	Weather	Flight Hardware	Launch Vehicle	Spacecraft	Infrastructure	Operational Perogative	Range	SSME aborts
Shuttle (STS-1 through STS-116)	54.3%	19.2%	18.5%			4.8%	0.9%		2.3%
Delta (1989 through 2001)	55.7%	18.7%		9.2%	3.8%			12.6%	
CxP Requirements	**88.0%**	**5.0%**		**2.0%**	**2.0%**	**<1%**		**<1%**	

- There were 11 launch delays / scrubs in Shuttle history related to ground support equipment failures.
- CxP requires at least a 5x improvement in ground system availability over the Shuttle.

The analysis above was performed in 2008

- The CxP availability requirement has since been updated to 99%

(Courtesy of Grant Cates, Russ Rhodes, Edgar Zapata, Jennifer Lyons and Amanda Mitskevich)

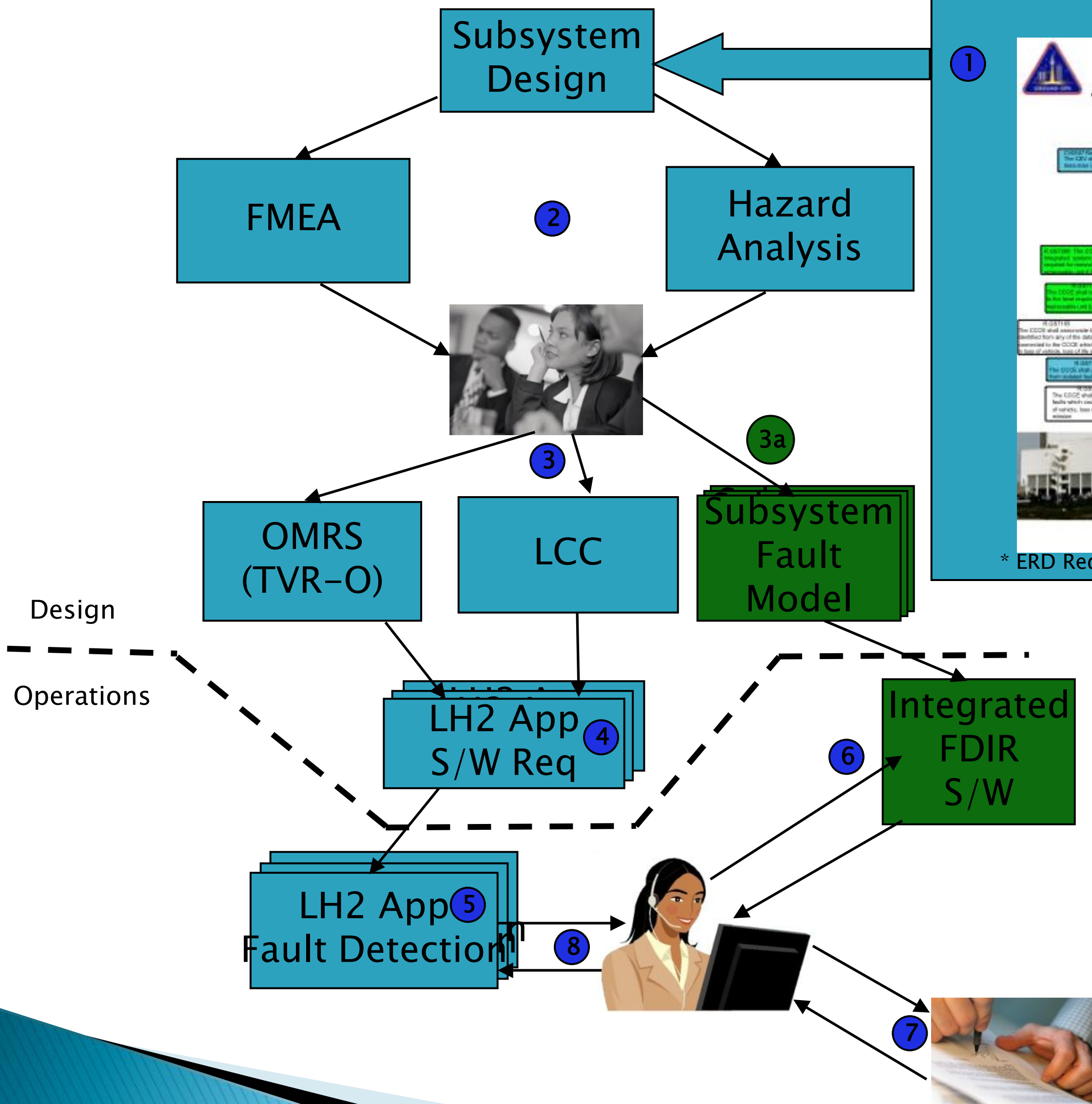
Launch Availability :
Availability versus Reliability

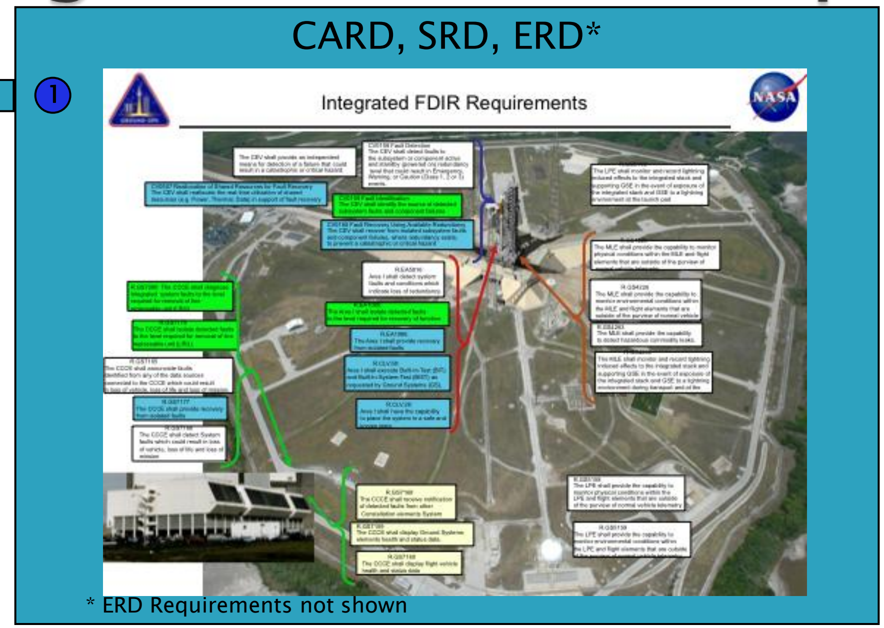
- In order to meet the CxP challenge of meeting the 99% overall launch availability, we need a five-fold improvement in ground system availability.
- Availability requirements cannot be met solely through reliability.
  - An unreliable system may be highly available if it is repaired quickly whenever it breaks.
  - Conversely, a highly reliable system may not meet availability requirements if it takes a long time to repair.
- Given the state-of-the-art in reliability of complex electromechanical systems, the major improvement for CxP has to come from MTTR.
- Total recovery time = time to detect + time to isolate + time to repair

$$\text{Availability}(A) = \frac{MTBF}{(MTBF + MTTR)} \qquad \text{Reliability}(R) = \frac{MTBF}{MTBF + 1}$$

ISHM technologies prove a systematic methodology to reduce these and increase ground system availability.

Ground Operations Integrated FDIR Concept





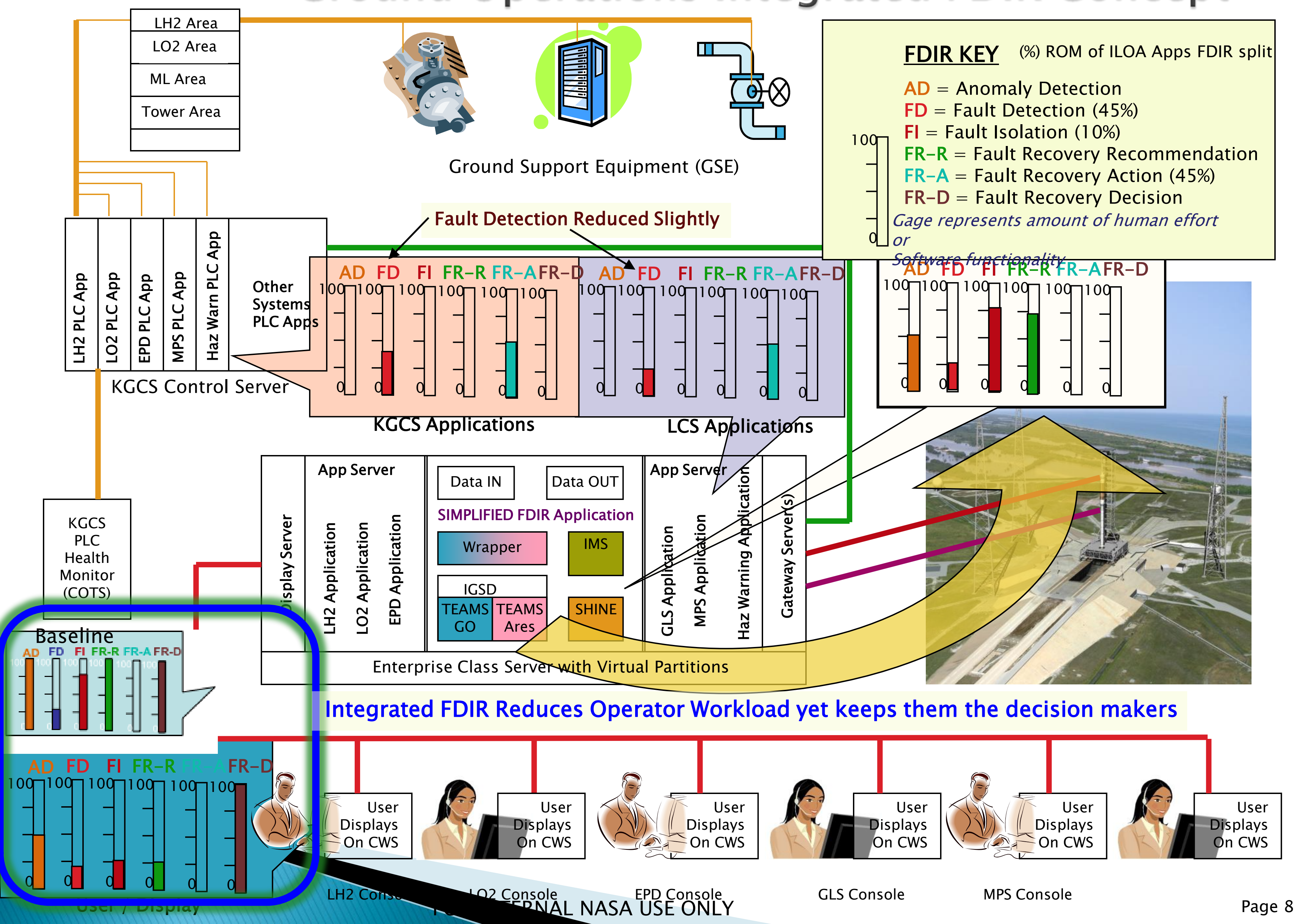
1) CARD, SRD and ERD Requirements flow into Subsystem Design
2) FMEA & Hazard Analysis Performed on Subsystem Design
3) Technical Community develops Operational Test Requirements and if applicable Launch Commit Criteria

3a) **Technical Community captures subsystem design, FMEA and Hazard Analysis into Subsystem Fault Model**

4) Operational *Fault Detection* Requirements are captured in Subsystem S/W Requirements
5) Subsystem S/W performs Fault Detection
6) **Integrated FDIR performs Fault Isolation and Recovery Recommendation to Console Operator**
7) **Console Operator makes Recovery Decision and documents in PRACA**
8) Console Operator Initiates Recovery Steps either manually or through LH2 Application

Blocks in green added for Integrated approach

Ground Operations Integrated FDIR Concept

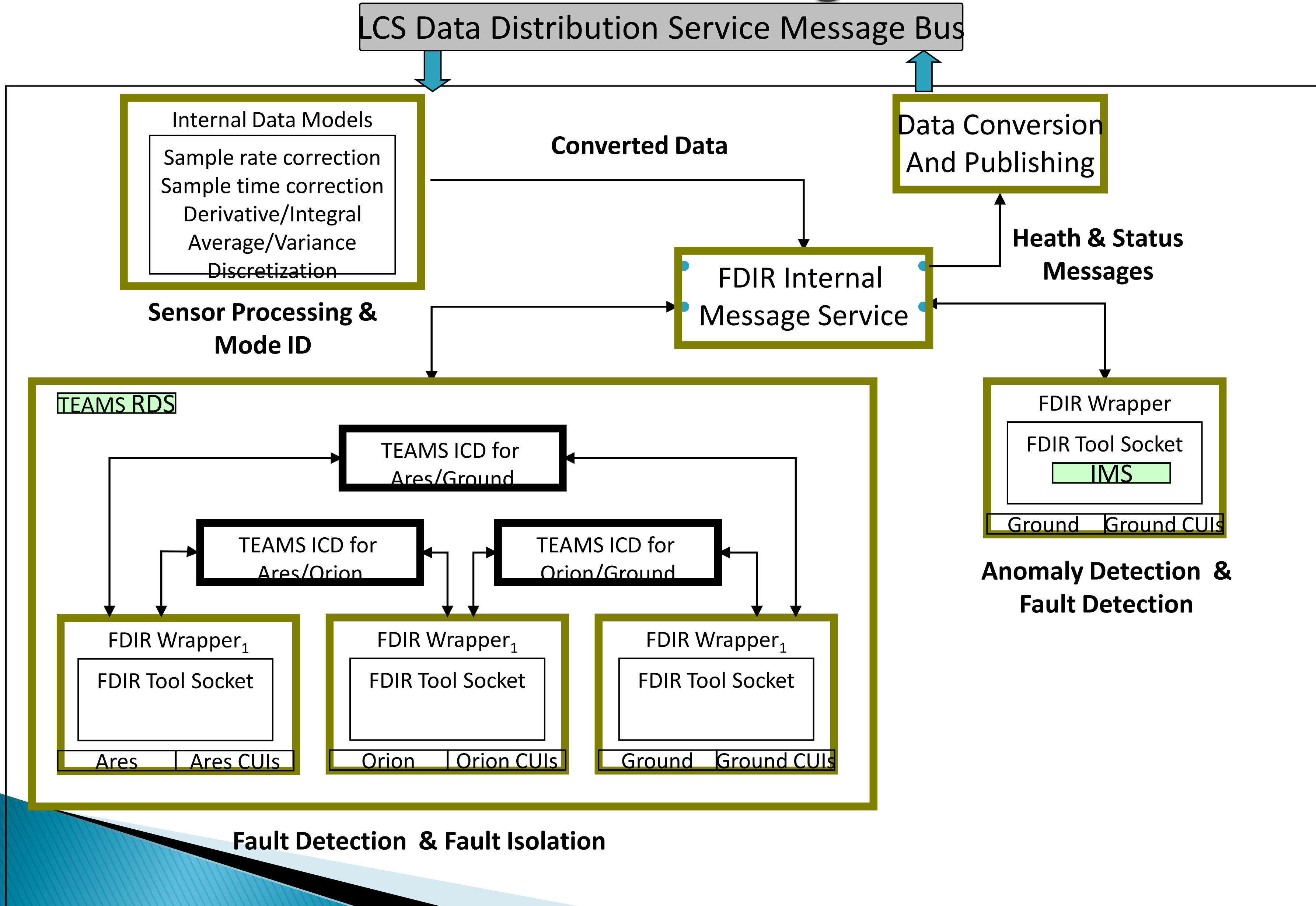


Key Objectives

- Develop certifiable Ground Operations capability to meet CARD requirements for FDIR for Initial Operating Capability (IOC)
  - Approach for integrated FDIR across ground subsystems and across vehicle/ground elements
  - Architecture, Tools, Configuration
- Develop and validate an LH2 FDIR application within LCS
- Assess Integrated FDIR capability
  - Scalability, Performance, Cost, Benefit, etc.
- Leverage Ares I-X Ground Diagnostic Prototype (GDP) Task
  - Pathfinder for architecture concept and model integration approach

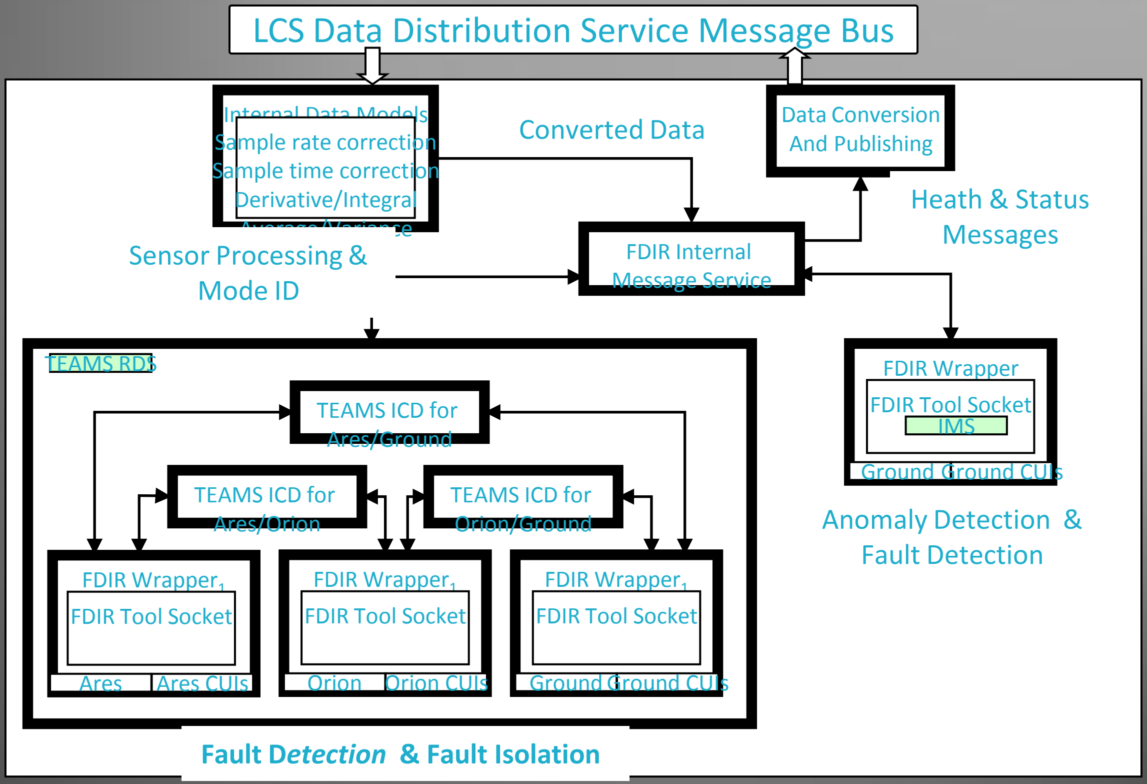
- "Recovery" capability is initially intended to be fault recovery recommendation only and is not included in IOC

Notional Architecture for Integrated FDIR

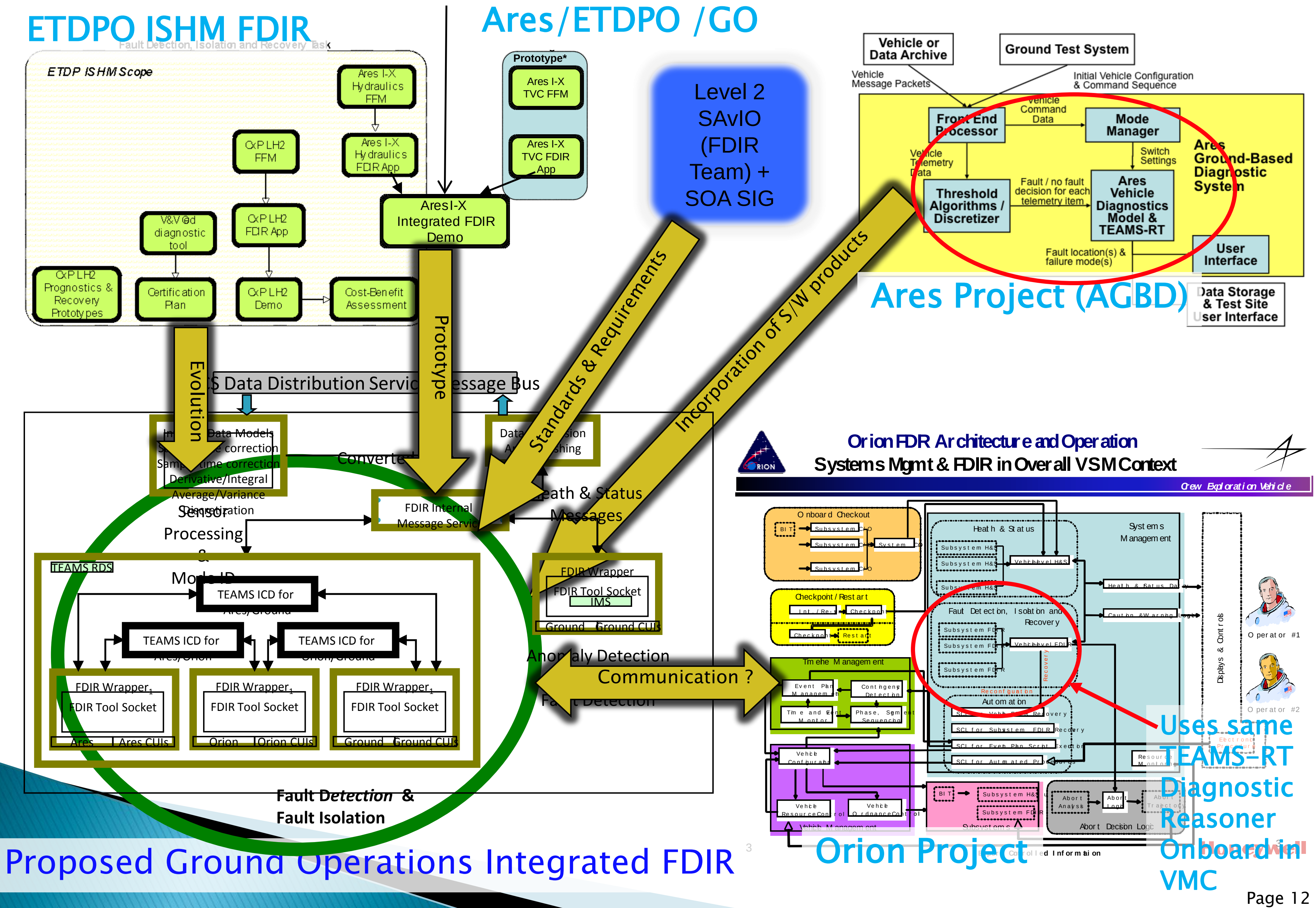


Architecture for Integrated FDIR

- Internal Data Models prepare incoming telemetry for FDIR application
- FDIR Wrappers encapsulate FDIR Tools to provide reliable interface and control
- Data Conversion And Publishing makes diagnosis, health/status, recommendations available to other LCS applications



Architecture for Integrated FDIR



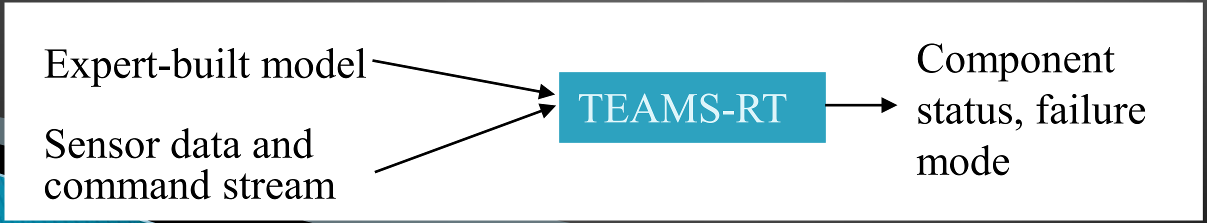
Summary of Implementation Approach

- Fault Detection / Isolation
  - For IOC, accredit GSE functional fault models and certify FDIR applications for the cryo systems
    - LH2, LO2, GHe, GN2, CHe
  - Integrate Ares Vehicle Diagnostic Model (AVDM)
    - Received as V&V'd data product from Ares Project
  - Subsystem Application Software still performs Fault Detection
  - Phase remainder of GSE subsystems for Lunar time frame to support Availability requirement
- Anomaly Detection
  - Develop knowledge bases and applications for cryo systems
  - Evaluate performance against operational data for 5 (TBR) flights and assess readiness to certify capability
- Integrated FDIR applications will be V&V'd and certified as would any other critical Integrated Launch Operations Application (ILOA)
- Subsystem models developed and maintained by GSE designers
  - Vehicle model will be developed and maintained by vehicle design agent
- Recovery Recommendation (and Prognostics)
  - Continue to mature capability and concepts within Exploration Technology Development/ISHM Project
  - Re-evaluate near IOC for follow on capability

Fault Detection and Fault Isolation Using TEAMS

(Testability Engineering And Maintenance System)

- TEAMS is a suite of tools for developing model-based fault isolation systems
  - TEAMS-Designer, TEAMS-RT, and TEAMS-RDS
- Model captures a system's structure, interconnections, tests, procedures, and failures
  - Functional dependency model captures the relationships between various failure modes and system instrumentation
- TEAMS-Designer used to create functional fault models from FMEA reports, fault trees, schematics, instrumentation lists, operational use cases, and other technical documentation
  - Can be developed incrementally, adding knowledge as designs mature
  - Model-building requires system knowledge and modeling expertise
- TEAMS-RT used for real-time isolation
  - Input is set of health status indicators (pass/fail test results) + Dependency matrix (D-Matrix)
    - e.g.: exceedances, operator observables, manual tests
  - Output is a list of bad, suspect, good, and unknown components
- TEAMS-RDS used for real-time operations
  - Provides Session Management and Archival Service
  - Includes TEAMS-RT



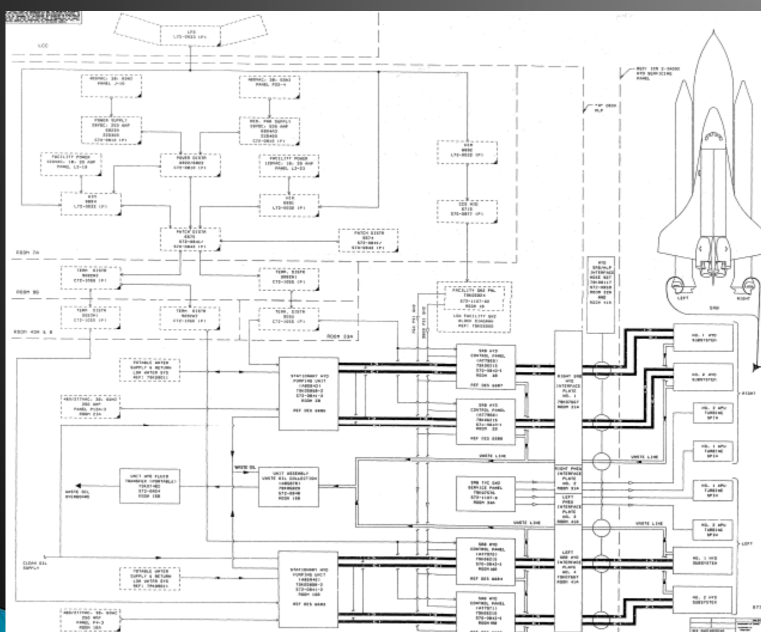
QSI QUALTECH SYSTEMS INC.

Fault Modeling Using TEAMS:
Modeling Process

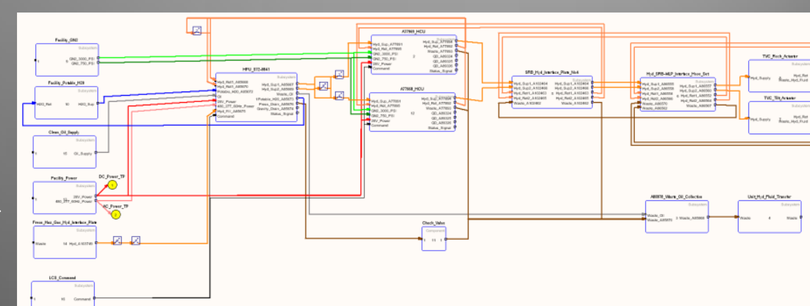
Step 1: Build subsystem functional fault model

- Transformation of energy, material, signal within the system
- Basic system connectivity, interfaces, interactions
- Insufficient to do any analysis or to be a diagnostic engine

Knowledge captured from subsystem schematics/diagrams/etc. and converted into TEAMS model



Hydraulic Support System Block Diagram



Functional Model in TEAMS

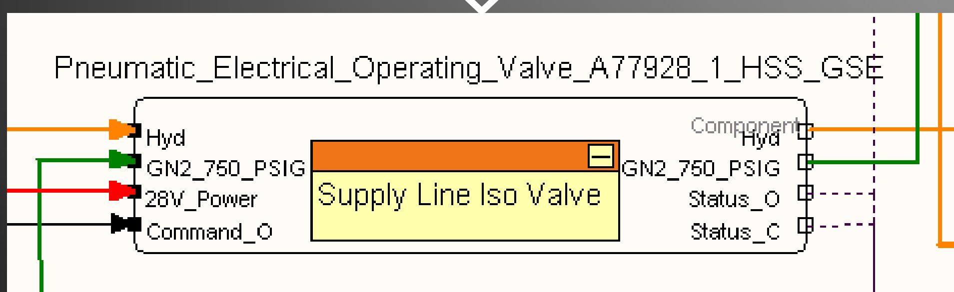
(Modeling process courtesy of Ares FFA Team)

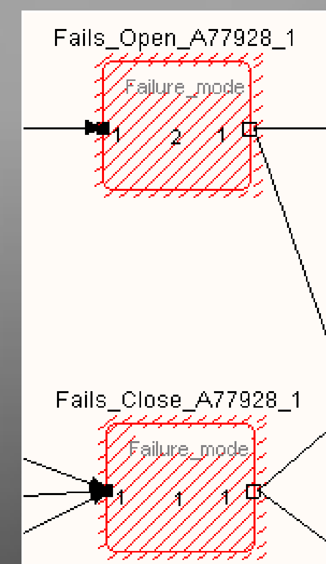
Fault Modeling using TEAMS :
Modeling Process

Step 2: Populate failure modes of components

- Extracted from FMEA
- Added as "lowest level" nodes inside each component

A77928	Pneumatic / Electrical Operating Valve	Remotely control flow of hydraulic fluid to SRB	Fails open	Loss of hydraulic flow control to the SRB could delay operations.	No effect.	3
			Fails close	Inability to flow hydraulic fluid to SRB would delay operations.	No effect.	3

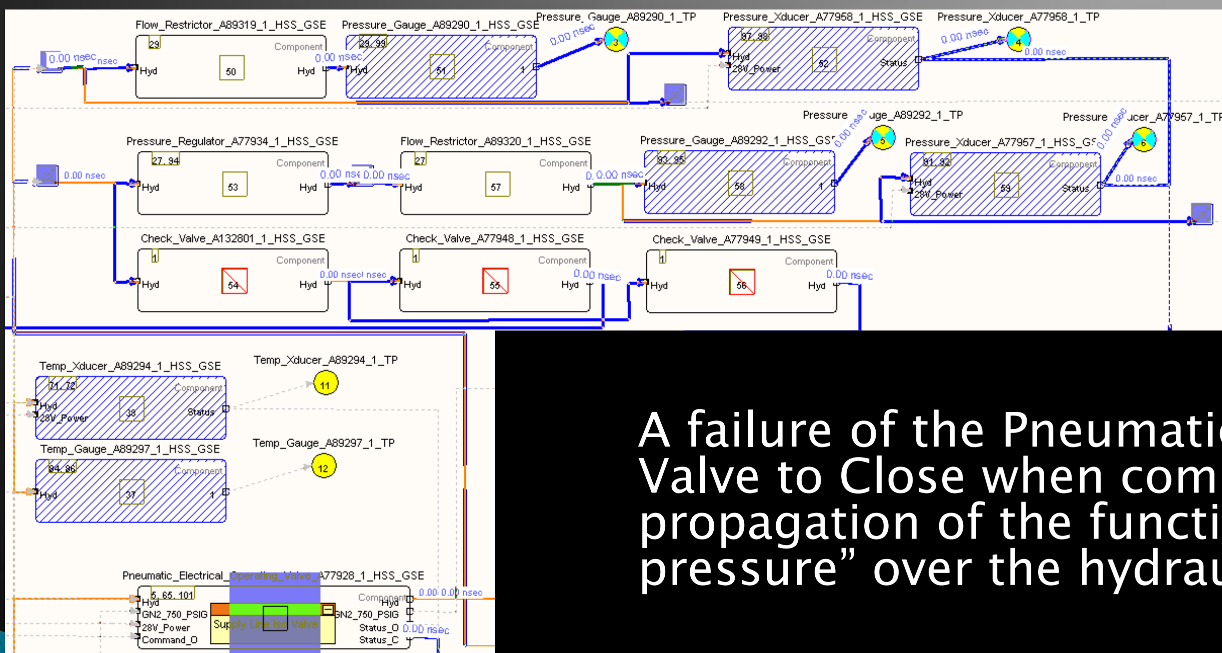




Fault Modeling using TEAMS : Modeling Process

Step 3: Determine failure effect propagation paths

- **Each failure mode produces a specific effect / set of effects**
  - Propagate along physical paths (fluid, thermal, electrical)
  - Implemented using TEAMS functions
  - Formalization of FMEA

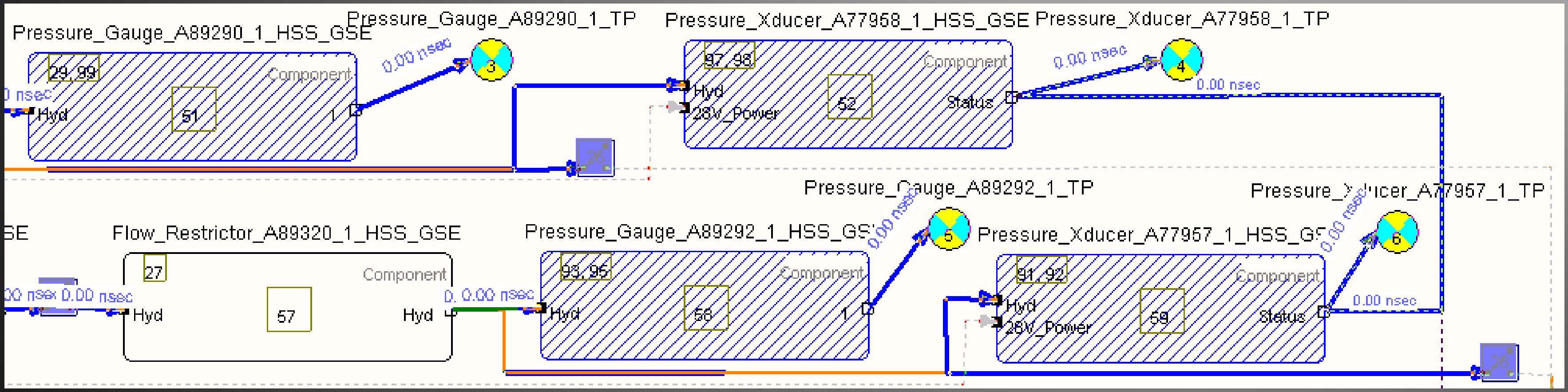


A failure of the Pneumatic Electrical Operating Valve to Close when commanded results in the propagation of the function "high supply pressure" over the hydraulic signal paths.

Fault Modeling using TEAMS : Modeling Process

Step 4: Identify sensors and test points

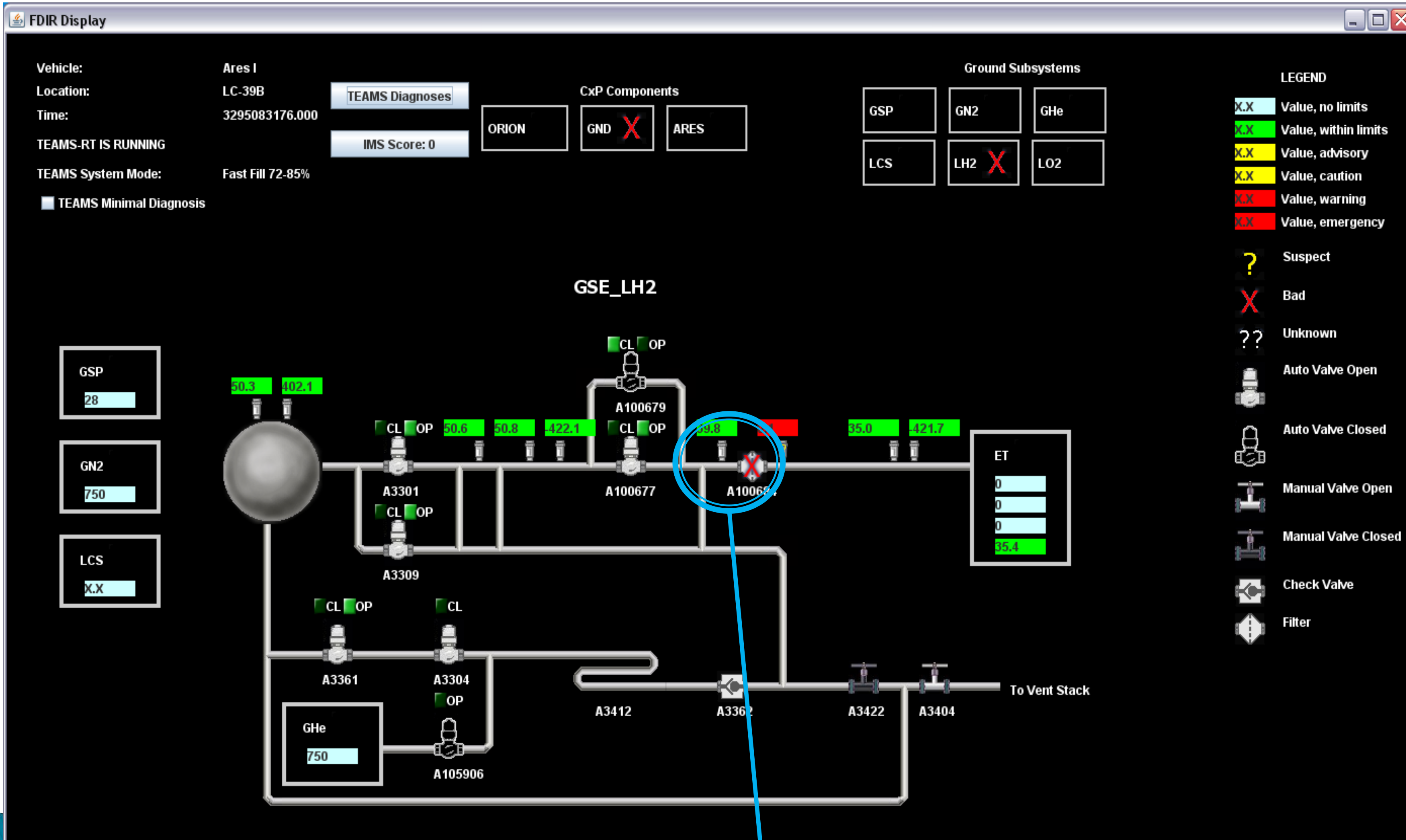
- Function model represent the location of all sensors
- The sensors are represented using nodes
- Each sensor is associated with TEAMS “test points”



The test points that represent pressure gauges and transducers detect the function “high supply pressure,” as indicated by the cyan and yellow coloring of the circular nodes.

LH2 FDIR Fault Isolation using TEAMS:

Diagnosis of Clogged Liquid Hydrogen Filter

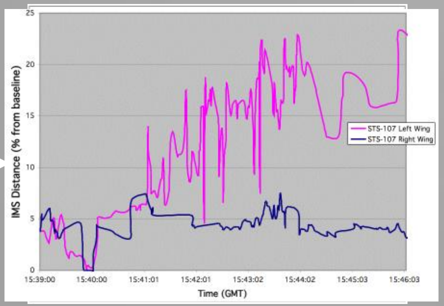


Red X and red highlighted measurement indicates component and corresponding measurement is bad.

Display From FDIR Dev 2 Build Demonstration: Using Simulated Data

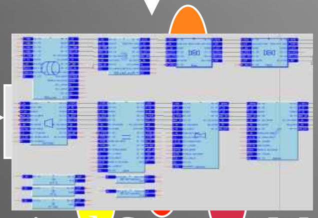
Anomaly Detection Using Inductive Monitoring System (IMS)

Inductive Monitoring System



Deviation from nominal

Sensor Data



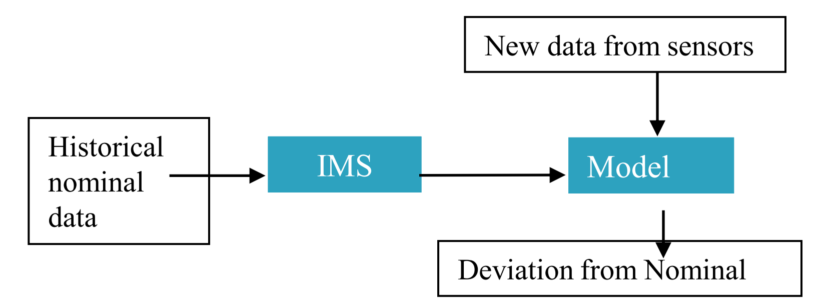
Nominal System Model

Automatically learns how the system behaves and tells you if current behavior is out-of-family

IMS developed at NASA/ARC by David Iverson

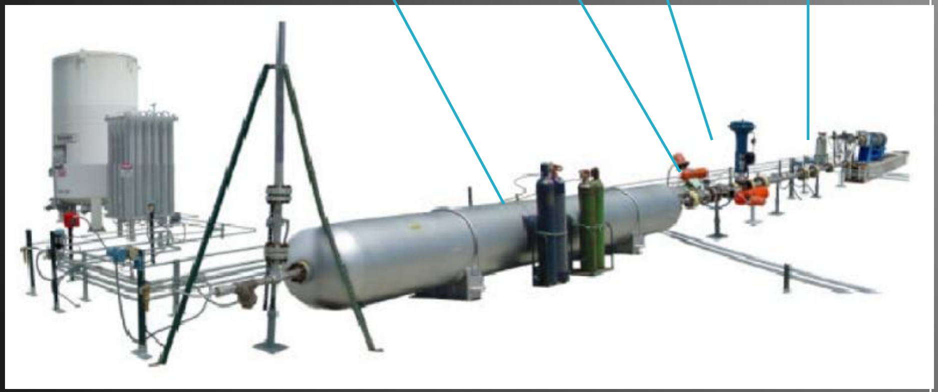
Anomaly Detection using IMS

- Automatically derives models (off-line) from archived or simulated nominal operations data
  - Does not require off-nominal data
  - Does not require knowledge engineers or modelers to capture details of system operations
- Anomaly detection module can catch anomalies whose signatures are not known ahead of time
- Can detect subtle anomalies or anomalies that are not listed in the FMEA
- On-line monitoring takes as input observations about the physical system (parameter values) & produces “distance from nominal” anomaly score
- Analyzes multiple parameter interactions
  - Automatically extracts system parameter relationships and interactions
  - Detects variations not readily
  - apparent with current individual
  - parameter monitoring practices



Anomaly Detection using IMS:
Nominal Data Vectors

(PresA POV CV% PresB delta_PresA delta_PresB)



- Nominal sensor data is used to establish general relationships between parameters
- Training data can be collected from the system and from high fidelity simulations
- Derived vector parameters, such as rate of change, can be computed from raw data values

Anomaly Detection using IMS:
Data Clustering Concept

Nominal data points are grouped into clusters of nearby points that specify acceptable ranges for parameters in a vector.

(PresA	POV	CV%	PresB	dA	dB)
(2995	0.97	0.50	2000	1	5)
(2994	0.98	0.52	2005	1	5)
(2993	0.98	0.55	2007	1	2)
(2992	0.98	0.62	2009	1	2)
(2990	0.98	0.64	2012	2	3)
(2988	0.98	0.65	2015	2	3)
(2986	0.98	0.66	2018	2	3)
(2984	0.98	0.66	2020	2	2)
(2982	0.98	0.67	2023	2	3)
(2980	0.98	0.67	2025	2	2)

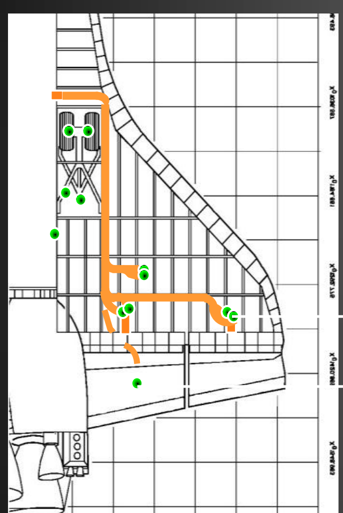
Archived Nominal Data Points

	(PresA	POV	CV%	PresB	dA	dB)
H:	(2995	0.98	0.52	2005	1	5)
L:	(2994	0.97	0.50	2000	1	5)
H:	(2993	0.98	0.62	2009	1	2)
L:	(2992	0.98	0.55	2007	1	2)
H:	(2990	0.98	0.66	2020	2	3)
L:	(2984	0.98	0.64	2012	2	2)
H:	(2982	0.98	0.67	2025	2	3)
L:	(2980	0.98	0.67	2023	2	2)

Generated Nominal Clusters

Anomaly Detection using IMS:
Modeling Example

Step 1: Determine sensors of interest for subsystem & form into vectors.



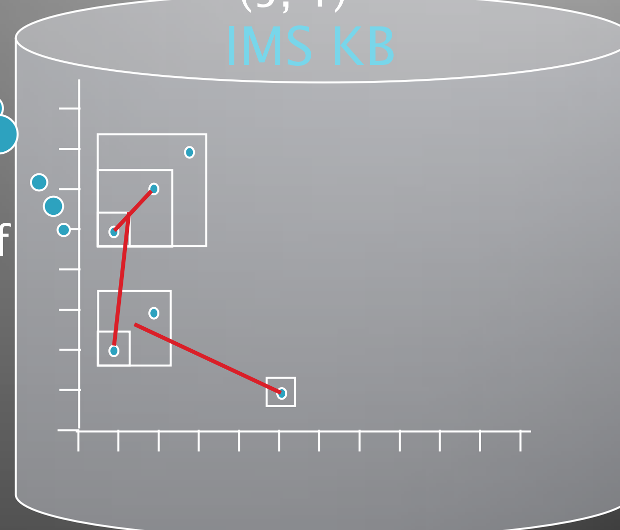
2	3
s1	s2

Step 2: Train on archived data representative of expected nominal operations…Training data set:

(s1, s2)
(1, 5)
(2, 6)
(1, 2)
(2, 3)
(3, 6)
(5, 1)

The user can customize the distance that determines whether a point is "close enough" to an existing cluster to expand the cluster vs. creating a new one.

… Create clusters of nominal operations.



Anomaly Detection using IMS:
Monitoring Concept

For Each Input Vector: Find the closest nominal cluster in the database and report the distance of the vector from that cluster.

(PresA POV CV% PresB dA dB)

(2995 0.97 0.51 2002 1 5)

.
.

(2986 0.98 0.62 2011 2 2)

.
.

(2983 0.99 0.67 2015 2 8)

.
.

Real Time or Archived Data Samples

(PresA POV CV% PresB dA dB)

H: (2995 0.98 0.52 2005 1 5)
L: (2994 0.97 0.50 2000 1 5)

H: (2993 0.98 0.62 2009 1 2)
L: (2992 0.98 0.55 2007 1 2)

H: (2990 0.98 0.66 2020 2 3)
L: (2984 0.98 0.64 2012 2 2)

H: (2982 0.98 0.67 2023 2 3)
L: (2980 0.98 0.67 2025 2 2)

.
.

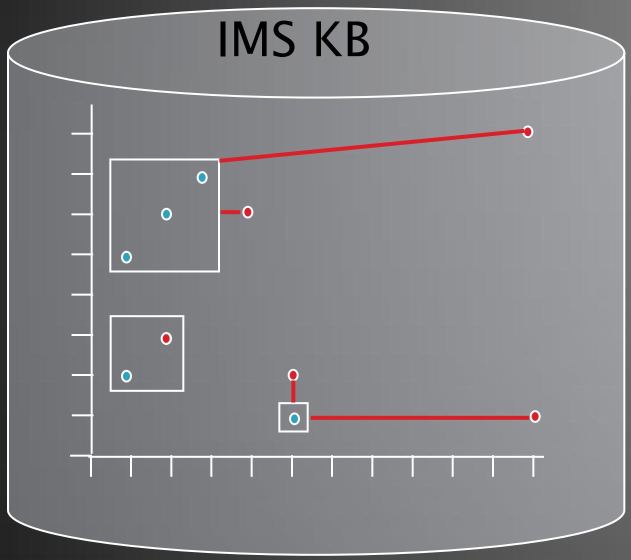
Nominal Cluster Knowledge Base

0.0
.
.
1.0002
.
.
11.225
.
.
.
.
.

IMS Distance From Nominal

Anomaly Detection using IMS:
Monitoring Example

Step 3:
Using nominal operations clusters created in modeling step…

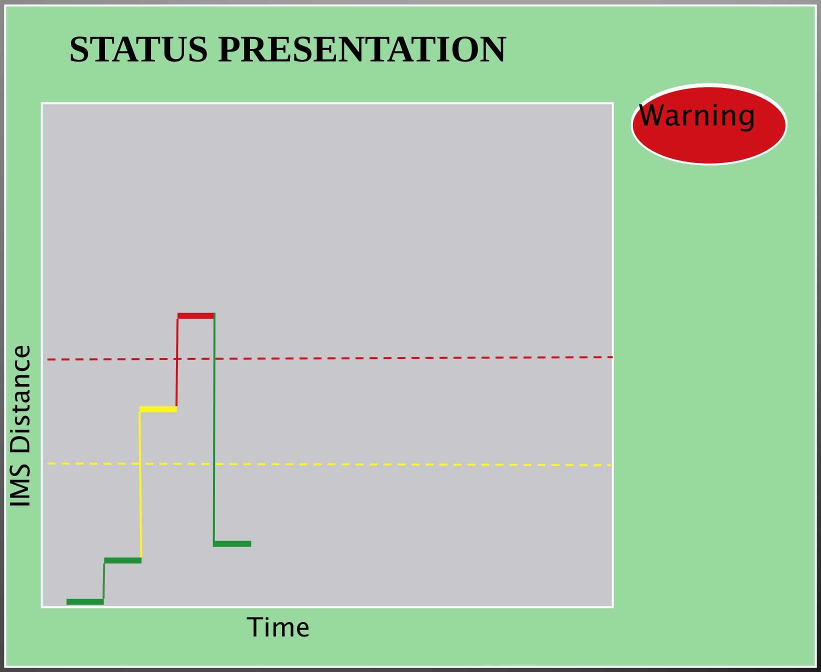


… As real time data is received, compare to nominal operations clusters…

Real-time data stream:

(2, 3)
(4, 6)
(11, 1)
(11, 8)
(5, 2)

… Plot distance from closest nominal cluster to incoming data and/or issue caution/warning alert.



Early Benefits of Integrated FDIR

- Anomaly Detection
  - Training of knowledge base using simulation will allow early evaluation of models compared to real hardware under test
  - Allows models and simulations to be updated to higher fidelity to support application software development and team training
- Fault Isolation
  - Model integration between Ground Support Equipment and Launch Vehicle will allow earlier discovery of technical and operational disconnects
  - Provides analysis of GSE subsystems for Fault Detection ability
    - Ambiguity group size
    - Number of undetectable Failure Modes
- Development
  - Reduces the amount of ILOA Requirements that need to be developed to meet the FDIR requirements.
    - Do not need Requirements for subsystem functional fault models.
    - Built off of Design Schematics, FMEA and other design documents.
    - Built by Modelers, reviewed and accredited by subject matter experts.

Expected Benefits

- Many expected benefits
  - Improves launch availability (reduces component of Mean Time To Repair)
    - Reduces integrated troubleshooting time (Isolation & Recovery Recommendation)
  - Reduces console operator cognitive workload
    - Helps considering the reduction in console operators and non-integrated architecture of Ares / Orion subsystems
    - Supports reduction of FR personnel by 50% compared to Shuttle
  - Reduces engineering support needs for Anomaly Detection and Recovery Recommendation
  - Speeds assessment of flying with failed condition through trace to suspect failure modes.
  - Improves time to develop flight rationale for anomalous conditions
  - Fault modeling can uncover gaps in the analysis and forces analysis of Ground / Vehicle integration early
  - Anomaly Detection can lead to early intervention, prevent further system damage, and reduce remediation cost and effort
  - Captures subsystem design knowledge
  - Provides a pathway for prognostic capabilities and Condition Based Maintenance V.S. Reactive Maintenance
- Benefits will be assessed through benchmarking, performance testing, etc.
  - Initial requirement is fault isolated <= 1 second after fault detected

Benefit Scenarios

- STS-88 12/3/1998
  - Scenario where additional information could have prevented a 24 hour scrub
    - At T-minus 4 minutes 24 seconds a master alarm in the crew cabin was noted and the countdown clock automatically stopped the clock at a built in hold at the T-minus 4 minute mark. The alarm was due to pressure on Hydraulic System #1 temporarily registering below 2800 psi during its startup transition from low to high.
    - The launch countdown was then held at the T-31 second mark to further assess the situation. *Shuttle system engineers attempted to quickly complete an assessment of the suspect hydraulic system and eventually gave an initial "go" to resume the countdown. With only seconds to respond, launch controllers were unable to resume the countdown clock in time to launch within the allotted remaining window*, which was limited due to liquid oxygen (Lox) drain-back constraints. Managers are discussing the 24-hour launch turn-around plans and are expected to make a final determination later this morning.
  - How would FDIR help in this scenario?
    - Additional information would be provided to the console operators, which components are suspect will reduce the time required to assess the situation and provide a recommendation
    - By capturing the system design knowledge during development, we will be less sensitive to variations in personnel experience and skill set.

Benefit Scenarios

- STS-99 2/9/2000
  - Scenario where additional information could have provided positive information to hold the launch for a failure
    - On Monday, January 31, 2000, The launch team also investigated a potential problem with the onboard Master Events Controller (MEC) #2 Built In Test Equipment (BITE). The problem did not reoccur during additional testing. At 1:58pm EST, (18:58 UTC) NTD gave the go to pickup the count and countdown to the T-minus 9 minute mark and hold pending weather. At 2:08pm EST, the *call was made to scrub due to weather constraints and enter into at 24 hour scrub turnaround*. The new launch date was tentatively set for Tuesday, February 1, 2000 at 12:44pm.EST. Over the night, engineering teams will evaluate data from the Master Events Controller.
    - On Tuesday, February 1, 2000, mission managers decided to *delay the launch until no earlier than February 9, 2000 to give the launch team time to swap out Endeavour's Enhanced Master Events Controller (EMEC) #2* located in the orbiter's aft compartment
  - How would FDIR help in this scenario?
    - A positive list of failure modes for the detected indication would allow operators to quickly build the case for halting the launch to replace the component (launch was scrubbed for weather)
    - By capturing the design information during development, a reduced set of support personnel are required to be present during launch operations. Today the support personnel are asked to answer design questions in response to anomalies and reconstitute the corporate design knowledge in real-time.

Additional Benefits (Ares View)

- Ares supplies an accredited vehicle model that has very useful information about how failures propagate within a vetted architecture model including sensors.
  - This is a non-trivial model with wide-ranging value (Including training uses)
  - It is not something that GS will need to create and fund
- Fault Detection and Isolation Metrics can be determined through the models
  - Testability Analysis / Non Detectable Failures
- Failure Effect propagation times can be verified against system response
- Improving FMEA and System Documentation through modeling

Summary

- Ground Ops updated the LCS baseline to include the Integrated FDIR capability and requested funding for development in 2011
- Integrated FDIR concept will continue beyond Constellation as an institutional KSC Ground Operations capability
- Transition from ETDP to LCS development is in work
  - FDIR Concept of Execution completes April 2010
  - Development of formal requirements begins May 2010
    - 45% requirements, Test Plan
    - Fault modeling conventions, model integration ICD, Fault Model Accreditation Process (with Ares)
    - Anomaly Knowledge Base Accreditation Process
- Technology development/maturation for recovery recommendations/prognostics to follow

Task Organization

- Ground Ops
  - FDIR Architect/Customer Rep: Bob Waterman/KSC
  - FDIR CSCI Lead (Interim): Barbara Brown/ARC @ KSC
- Exploration Technology Development Program (ETDP)
  - Program Manager: Frank Peri/LaRC
    - ISHM Project Manager: Dave Korsmeyer/ARC
      - ISHM FDIR Task Lead: Barbara Brown/ARC @ KSC
        - FDIR Center Team Leads: Ann Patterson-Hine/ARC
Jose Perotti/KSC
Ryan Mackey/JPL
    - ISHM PI: Ann Patterson-Hine/ARC