

Fault Management on Manned Spacecraft From Design to Operations



Carlos Garcia-Galan

5/5/09



Agenda



- Fault Management dimensions
- Fault Management analysis
- Real-time Fault Management
- Learning from Real Failures
- Evolution of on-board Fault Management Approach



Fault Management Dimensions



- Fault Management is accomplished in several dimensions:
 - Spacecraft Robustness, redundancy and margins
 - Subsystem Hardware, **Firmware and Software capabilities for Failure Detection Isolation and Recovery (FDIR)**
 - System-Level FDIR
 - Role of the Spacecraft Crew and Mission Control Center (MCC) in Fault Management



Spacecraft Robustness



- How much system degradation can you take, and still accomplish your mission or bring the crew safely home?
 - Independent Strings of HW/FSW for critical functions
 - Power – Generation, storage and distribution.
 - Avionics – Command & Control Computers, On-board Data Network
 - Environmental Control – Cabin Air Revitalization, Pressure Control
 - Guidance, Navigation & Control – Attitude Control, State Determination
 - Thermal Control – Cooling Loops, and Heaters.
 - Communications – Telemetry/Commands & Voice.
 - Mechanisms – Mechanisms for Critical Equipment/Functions
 - Deployment of Solar Arrays, Radiator, Antennas, parachutes, etc
 - Propulsion – Propellant Management, Engines



Spacecraft Robustness



- How much system degradation can you take, and still accomplish your mission or bring the crew safely home?
 - Margins of Critical Consumables
 - Power – Ability to accomplish the mission or preserve crew safety with half of power available
 - Thermal –
 - Ability to accomplish the mission or preserve crew safety with half of cooling loops + maximize thermal clocks upon the loss of heating/cooling
 - Ability to survive at different attitudes for some period of time
 - Air –
 - CO₂ removal capability
 - O₂ generation, humidity removal, etc
 - Propellant – Maximizing the options to get to and return from destination (burns)



Subsystem FDIR Responsibilities



- **Expectations for Each Subsystem**

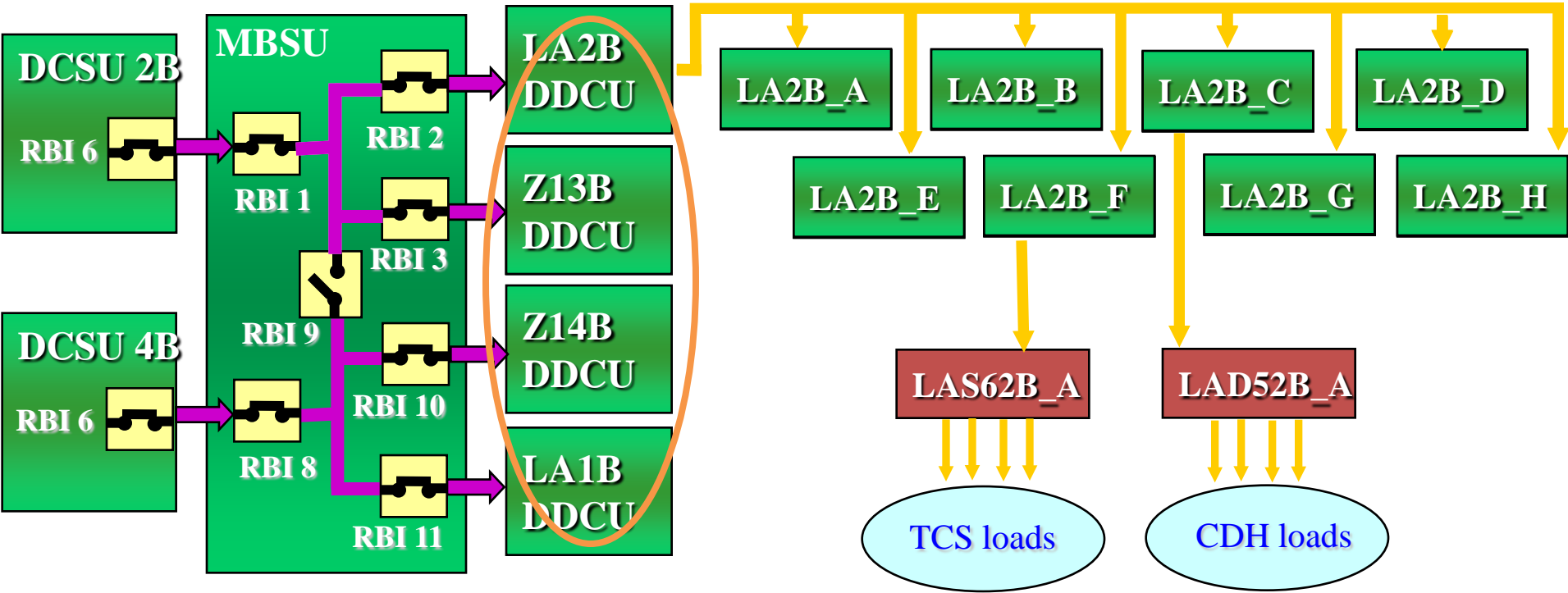
- Provide the necessary level of Subsystem FDIR over all components within Subsystem boundary
- Report all faults and health status
- Evaluate sensor inputs to determine their validity and infer sensor health
- Evaluate data inputs from subsystem components to determine validity and respond accordingly

- **Key Objectives of Subsystem FDIR**

- To ensure safe operation of the Subsystem
- To maintain functionality through available local redundancy
- To prevent fault propagation beyond the subsystem boundary
- Provide the necessary monitoring and functional tests as determined by safety analysis to identify and report latent faults or hazardous conditions and support:
 - Situational awareness for crew and ground
 - Initiation of system-level and/or higher level recovery actions



DDCU Example



DC-to-DC Converter Unit

Converts Power from Primary Voltage $\sim 150-160$ Vdc to 123Vdc

DDCU has several FDIR capabilities due to it's function, and the lack of such up-stream and down-stream



Subsystem FDIR Example- HW



DDCU Z14B Trip Status

Input Undervoltage Trip
Trip
Trip Function M
Enable
Arm
Enable
Inhibit
Arm
Inhibit

125% Current Output
Trip
Trip Function M
Enable
Arm
Enable
Inhibit
Arm
Inhibit

Thermal
Trip
Trip Function M
Enable
Arm
Enable
Inhibit
Arm
Inhibit

Input Overvoltage Trip
Trip
Trip Function M
Enable
Arm
Enable
Inhibit
Arm
Inhibit

150% Current Output
Trip
Trip Function M
Enable
Arm
Enable
Inhibit
Arm
Inhibit

Temp Setpoint deg C
Temp Setpoint Set
Temp Setpoint deg C
Set
Trip Time Setpoint ms
Trip Time Setpoint Set
Time Setpoint ms
Set

Current Limit Indicator
Backup Current Trip
DCE Overvoltage

- ### DDCU HW FDIR
- Current Limit = The DDCU will limit the amount of current available to the load (I_{out} = 78-82 A) rather than regulate the secondary bus voltage.
 - Backup Current Trip = I_{out} > 65A for 95-105 ms or current limit > 50-55ms
 - DCE Overvoltage = 153 ± 2 Vdc for 10 μs
 - HW FDIR has no functional inhibits



Subsystem FDIR Example- FW



DDCU Z14B Trip Status

Input Undervoltage Trip 125% Current Output Thermal

Trip Trip Trip

Trip Function M Trip Function M Trip Function M

Enable Enable Enable

Arm Arm Arm

Enable Enable Enable

Inhibit Inhibit Inhibit

Arm Arm Arm

Inhibit Inhibit Inhibit

Input Overvoltage Trip 150% Current Output Temp Setpoint 87.80 deg C

Trip Trip Temp Setpoint Set

Trip Function M Trip Function M Arm

Enable Enable Set

Arm Arm Temp Setpoint deg C

Enable Enable Set

Inhibit Inhibit Trip Time Setpoint 60000 ms

Arm Arm Trip Time Setpoint Set

Inhibit Inhibit Arm

Current Limit Indicator Time Setpoint ms

Backup Current Trip Set

DCE Overvoltage

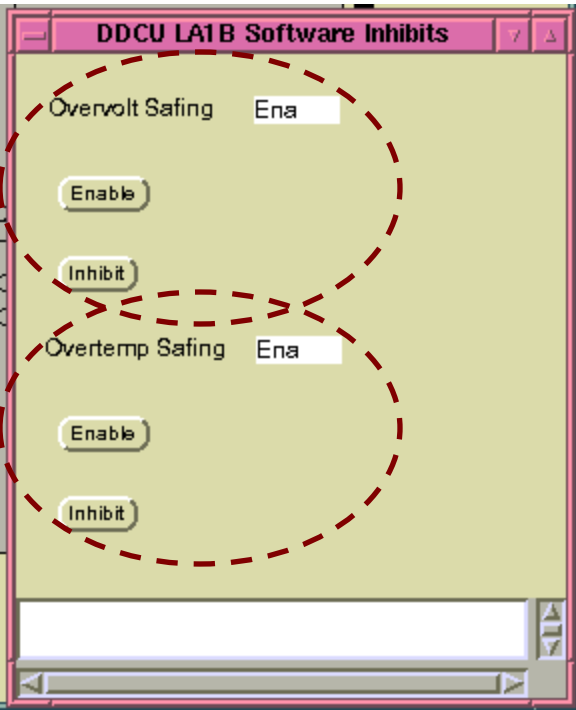
DDCU FW FDIR

DDCU Converter Trips off when:

- Primary (input) under voltage trip= 90 - 115 Vdc for 115 ms \pm 4 ms
- Primary (input) Overvoltage trip= 173 - 182 Vdc for 3 ms
- Secondary (output) 125% Overcurrent trip= 57.5A < I_{out} < 65A for 99 \pm 5 ms
- Secondary (output) 150% Overcurrent trip= 78A < I_{out} < 82A for 52.5 \pm 2.5 ms



Subsystem FDIR Example- FSW



DDCU FSW FDIR

- Secondary (output) Overvoltage trip: 129 Vdc for 6 sec = Converter Off
 - This FDIR action is designed to protect downstream loads sensitive to higher voltage, i.e. computers, electronics
- Overtemperature trip:
 - Conv Temp >190 deg F = Converter Off
 - PS Temp >175 deg F = Converter Off
 - Baseplate Temp >185 deg F = Converter Off
 - FSW Overtemp trip values are changeable
- Both FDIR actions (Voltage and Temperature protection) can be inhibited - see display.



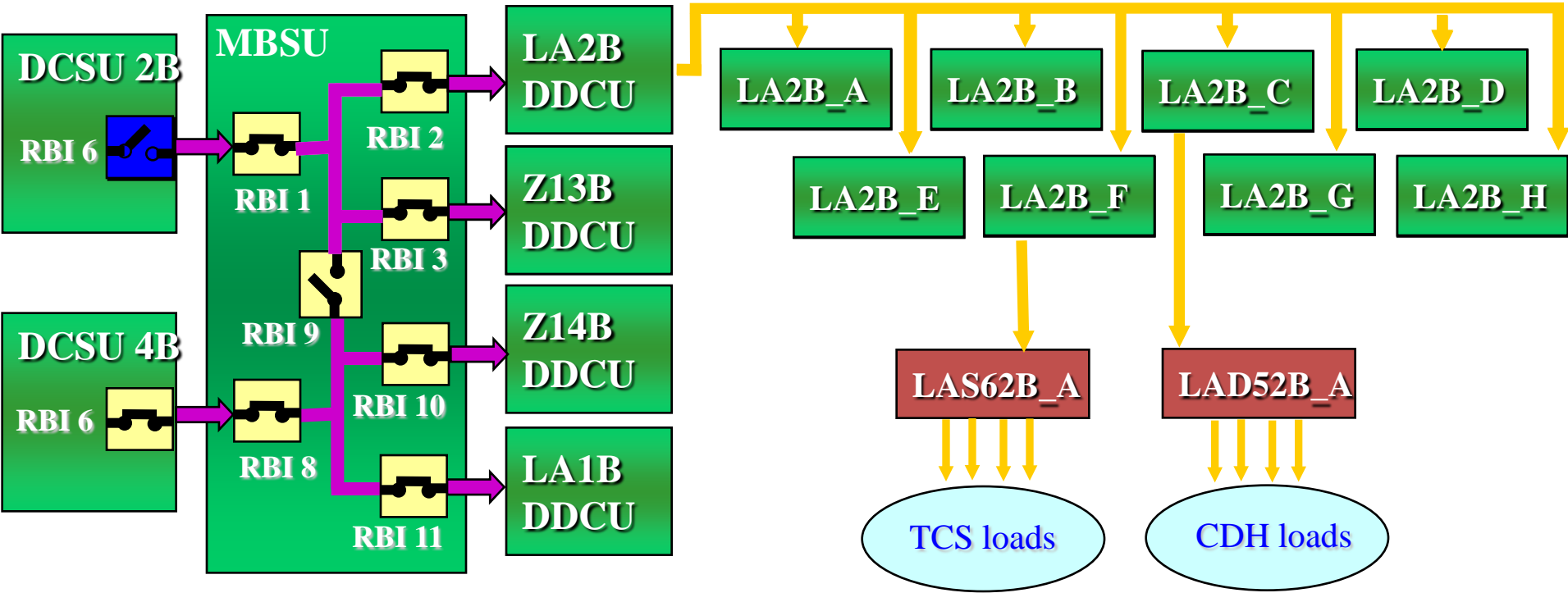
System-Level FDIR



- Correlate subsystem-level information to detect faults that propagate across several subsystems (FDIR)
- Isolate to source subsystem, LRU or LRU component (lowest possible), from multiple subsystem fault indications (FDIR)
- Perform multi-system recovery actions required to mitigate the effects of a fault that affects multiple subsystems (FDIR)



System-Level FDIR scenario



Scenario 1

EPS failure –Primary Power switch 6- causes the loss of power to half of the critical US LAB systems. The nature and location of the failure allows system reconfiguration to recover the lost functionality.



Resulting C&W



Caution & Warning Summary				
STAT	CL	ACK SYS	Message Text	Time of Event
*Alrm	C	CDH	Primary PMCU MDM Detected Local BUS EPS Node 2 Z3 Fail-LAB	22Jun00/09:59:48
*Alrm	C	TCS	Lab MTL PPA Pump Failure-LAB	22Jun00/09:58:06
*Alrm	C	TCS	Lab MTL Pump Efficiency Degradation-LAB	22Jun00/09:58:02
*Alrm	C	TCS	Lab Rack LAB1P6 Overtemp-LAB	22Jun00/09:57:38
*Alrm	C	CDH	Backup INT MDM Fail-LAB	22Jun00/09:57:09
*Alrm	C	CDH	Primary Int MDM Detected Static Frame Count for Lab 3 MDM-LAB	22Jun00/09:57:05
*Alrm	C	CDH	Primary Int MDM Detected Static Frame Count for Node 1-2 MDM-LAB	22Jun00/09:57:05
*Alrm	C	CDH	Primary Int MDM Detected Static Frame Count for Lab 2 MDM-LAB	22Jun00/09:57:05
*Alrm	C	EPS	RPCM LA2B_E Loss of Comm-LAB	22Jun00/09:57:05
*Alrm	C	EPS	RPCM LAD52B_A Loss of Comm-LAB	22Jun00/09:57:05
*Alrm	C	EPS	RPCM LA2B_D Loss of Comm-LAB	22Jun00/09:57:05
*Alrm	C	EPS	RPCM LAD62B_A Loss of Comm-LAB	22Jun00/09:57:05
*Alrm	C	TCS	Lab MTL PPA Pump In Press Sensor Failure and NIA Inhibited-LAB	22Jun00/09:57:05
*Alrm	C	EPS	RPCM LA2B_F Loss of Comm-LAB	22Jun00/09:57:05
*Alrm	C	EPS	RPCM LA2B_G Loss of Comm-LAB	22Jun00/09:57:05
*Alrm	C	EPS	RPCM LAS62B_A Loss of Comm-LAB	22Jun00/09:57:05
*Alrm	C	EPS	RPCM N13B_C Loss of Comm-Node 1	22Jun00/09:57:05
*Alrm	C	EPS	RPCM N13B_B Loss of Comm-Node 1	22Jun00/09:57:05
*Alrm	C	EPS	RPCM N13B_A Loss of Comm-Node 1	22Jun00/09:57:05
*Alrm	C	EPS	RPCM LA2B_C Loss of Comm-LAB	22Jun00/09:57:05
*Alrm	C	EPS	RPCM LA2B_B Loss of Comm-LAB	22Jun00/09:57:05
*Alrm	C	TCS	Lab MTL PPA Pump In Press Low-LAB	22Jun00/09:57:05
*Alrm	C	CDH	Node 1-1 MDM Detected User Bus Orb N1-1 Fail-PMA1	22Jun00/09:57:03
*Alrm	C	CDH	Primary Node 1 MDM Detected RT Fail of OIU-PMA1	22Jun00/09:57:03
*Alrm	C	EPS	PCU Z14B Failure-Z1	22Jun00/09:54:54
*Alrm	C	EPS	PCU Z13B Failure-Z1	22Jun00/09:54:54
*Norm	C	CDH	Node 1-1 MDM Detected RT Fail of Node 1-2 MDM-PMA1	22Jun00/09:49:54
*Norm	C	MCS	RS Auto Recovery Initiated	22Jun00/09:49:01
*Norm	W	CDH	Primary CC Detected Primary Node 1 MDM Failure - PMA1	22Jun00/09:48:57
*Alrm	W	CDH	Backup CC MDM Retry Fail-LAB	22Jun00/09:48:57
*Norm	W	CDH	Primary PMCU MDM Fail-LAB	22Jun00/09:48:56
*Norm	W	CDH	Primary GNC MDM Fail-LAB	22Jun00/09:48:56
*Alrm	W	CDH	Backup CC MDM Fail-LAB	22Jun00/09:48:56
*Alrm	W	CDH	CC MDM Recovery Fail-LAB	22Jun00/09:48:56
*Norm	W	CDH	Primary INT MDM Fail-LAB	22Jun00/09:48:55
*Alrm	C	EPS	DDCU LA2B Loss of Comm-LAB	22Jun00/09:48:54

C&W Toolbox

Sort On
Time:Newest

Filter On
ALL EWC

Advisories
Off

Robotics
Off

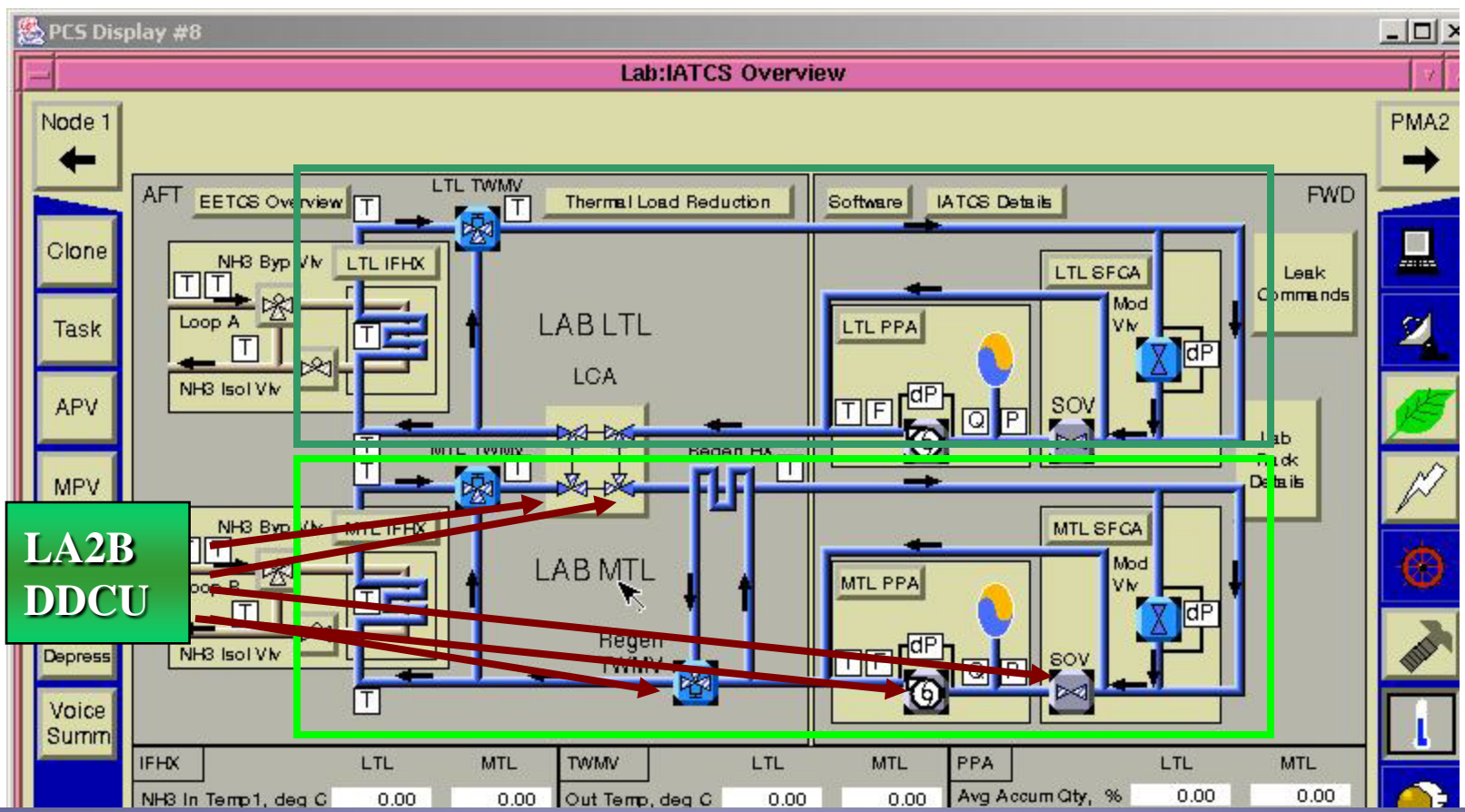
Alarm Trace
Master On
Master Off

Event Code
Tools
Enable
Suppress
Inhibit
Get Status

Log Tools
Log Menu



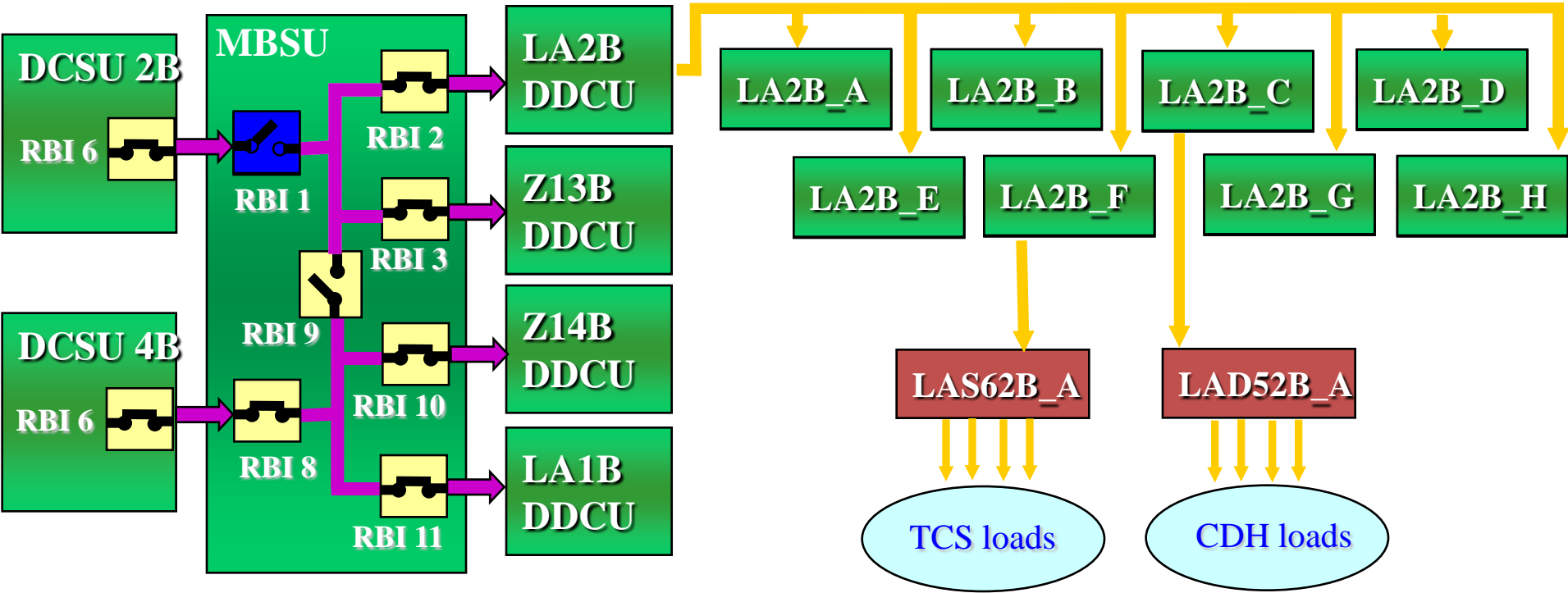
Subsystem vs. System-level Response



- DDCU Powers the Loop Pump, but also half of the valves required for subsystem FDIR to perform a proper reconfiguration
- Subsystem FDIR does not understand the nature of the fault (Pump failure) and tries to reconfigure = reconfiguration fails



System-Level FDIR scenario 2



Scenario 2

EPS failure –Primary Power switch 1- causes the loss of power to half of the critical US LAB systems. This failure prevents full system reconfiguration to regain lost functionality. Root cause, affected components and operator actions identified.



Fault Management Design



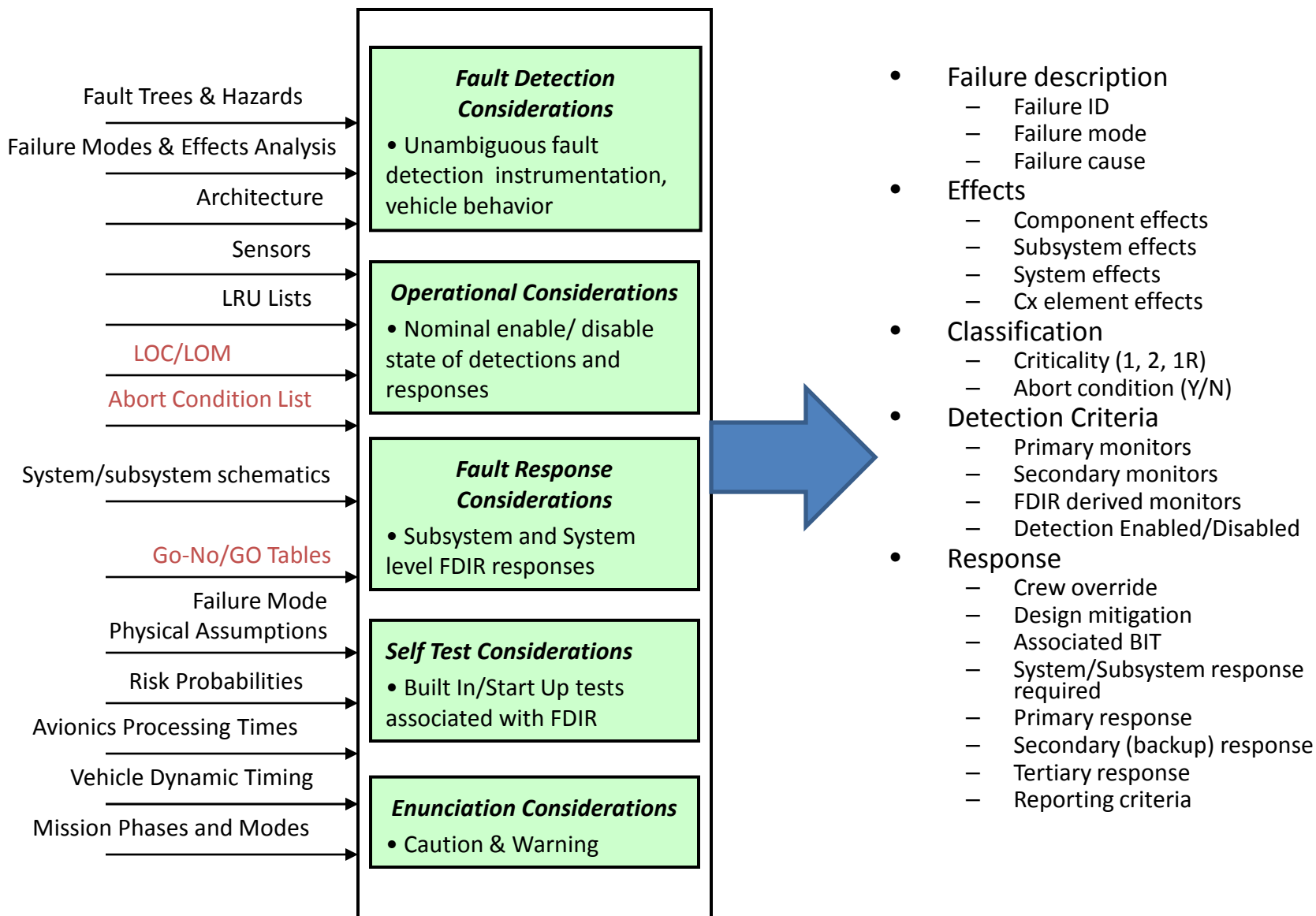
Integrated FDIR Design



- Integrated FDIR analysis includes three main activities:
 - Bottoms up analysis: Identify all failure modes at subsystem level
 - Functional Fault Analysis
 - Top-down analysis: Identify critical functions and impact of their loss
 - Loss of Crew/Loss of Mission (LOC/LOM) analysis
 - Go/No-Go Tables
 - Operational Functionality Assessment
 - Requirement Allocation: Decomposition of FDIR requirements to:
 - Subsystem-level (HW/FSW/FW)
 - System-Level
 - Crew
 - MCC
- FFA is “Functional Fault Analysis” captures **fault detection** and **response** analysis from the subsystem level to system level FDIR
- Instrumentation Assessment ensures proper fault coverage in design



FFA Ins/Outs





FFA – FMEA Input

Imported from FMEA

	A	B	C	D	E	F	G
1							
2	FAILURE DESCRIPTION				EFFECTS		
3	FAILURE ID	Failure Mode	Failure Cause	Phase	Component Effects	Subsystem Effects	System Effects
	Failure Mode ID unique to each failure mode: MODULE_SUBSYSTEM_C COMPONENT_FAILURE TYPE_ FAILURE CAUSE_PHASE Format is AA-BB-CCC-000-000-00	Brief description of what function has failed.		For what mission phase is this failure mode being analyzed? FMEA 'Mission	Component failure effects observable at component boundaries.	Subsystem failure effects observable at subsystem boundaries.	Observable system failure effects. Is the Mission still supported?
4	FMEA= Failure ID	FMEA= Failure Mode	FMEA= Failure Cause	Phase	FMEA= Immediate Effect	FMEA= Next Effect	FMEA= End Effect
5	This failure set is relevant to failures from the RCS pod isolation valves to the engines	Line failure resulting in propellant leakage	MMOD damage, weldment failure, waterhammer transients (internal pressure spikes, lateral reaction forces if not adequately supported)		Propellant leakage	Loss of Propellant	IAW baseline, loss of redundancy is LOM (inability to fulfill all mission objectives)
6		Pod iso valve fails open	No command or failed motor/coil		Loss of one inhibit in that string (A or B) Still have two inhibits	Feedline branch is still one fault tolerant to uncontrolled propellant leakage to space	Lost ability to perform leak detection on failed leg downstream of iso valve
7		Pod iso valve leaks internally	Contamination or damage to the seal		Loss of one inhibit in that string (A or B) Still have two inhibits	Feedline branch is still one fault tolerant to uncontrolled propellant leakage to space	Lost ability to perform leak detection on failed leg downstream of iso valve



FFA - Detection & Responses

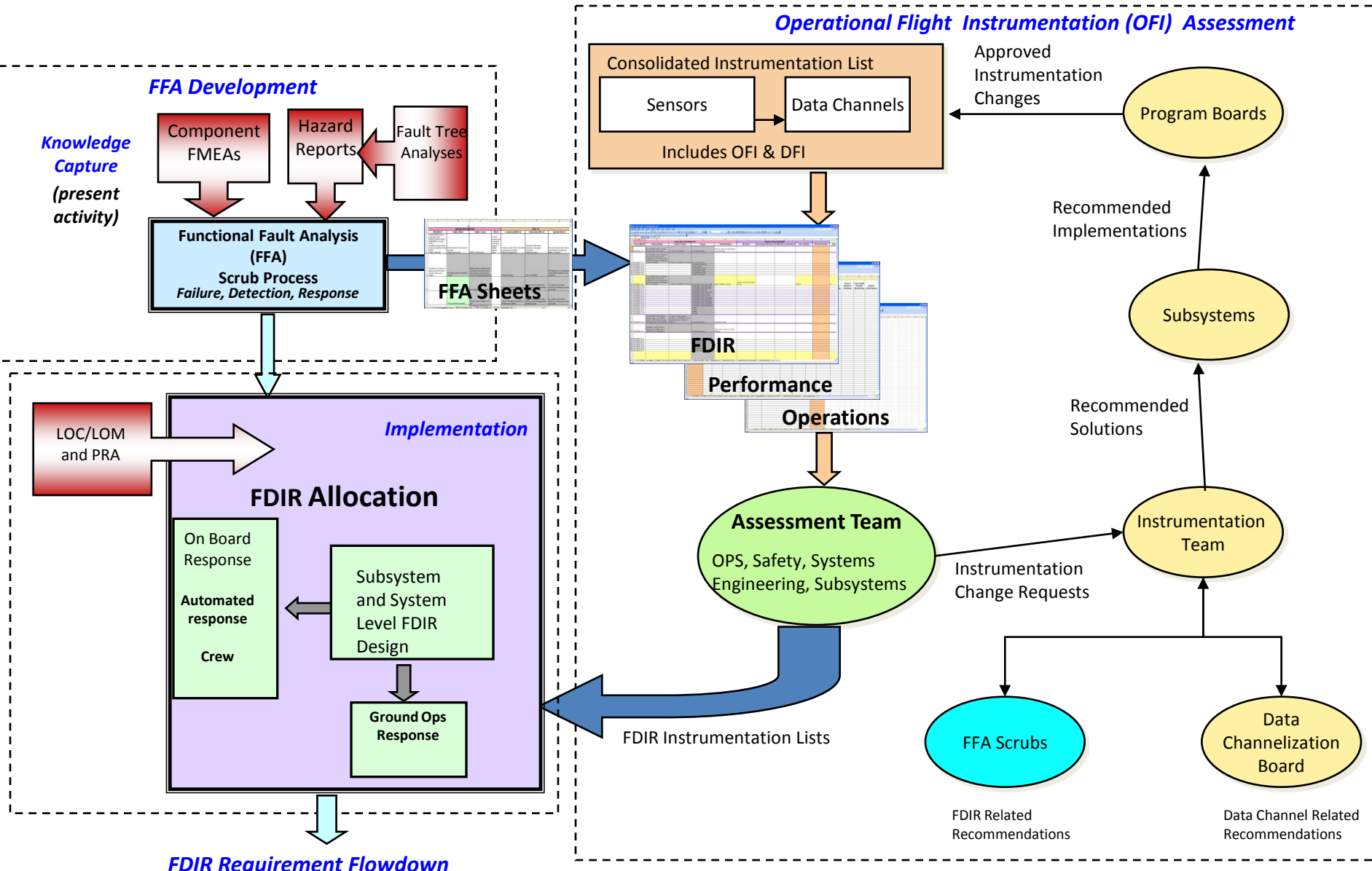


Derived Data from FFA Scrub Sessions

	A	B	O	P	Q	R	S	T
1								
2	FAILURE DESCRIPTION			DETECTION CRITERIA				
3	FAILURE ID	Failure Mode	Monitors	Secondary Monitors	FDIR Derived Monitors	Design Mitigation	Response	Backup Resp
4	Failure Mode ID unique to each failure mode: MODULE_SUBSYSTEM_COMPONENT_FAILURE_TYPE_FAILURE CAUSE_PHASE Format is AA-BB-CCC-000-000-00 FMEA = 'Failure ID'	Brief description of what function has failed. FMEA: 'Failure Mode'	Primary symptom of a fault. Most unambiguous indication of the fault condition. FMEA: 'Detection Method'	Telemetry used to confirm fault. Corroborating evidence of a fault condition	Are any algorithms needed to diagnose a fault condition? For example: M1-M2/I2 or middle select for three measurements	FMEA=Corrective Action	What hardware/software response is most likely to restore capability? FMEA= 'Software Response'	What response should be used if the first response fails on both the initial 're-try' attempts.
5	This failure set is relevant to failures from the RCS pod isolation valves to the engines	Line failure resulting in propellant leakage	Baseline is 1/day close pod iso valves to verify no leaks. PVT calculations used for gross leaks	Thermal or vehicle dynamics			Close pod iso valves	Early Return
6		Pod iso valve fails open	Valve position indicator Manifested at 1/day leak check				Troubleshooting	
7		Pod iso valve leaks internally	Valve position indicator shows "closed" Manifested at 1/day leak check				Switch to fully functional redundant branch	Early Return

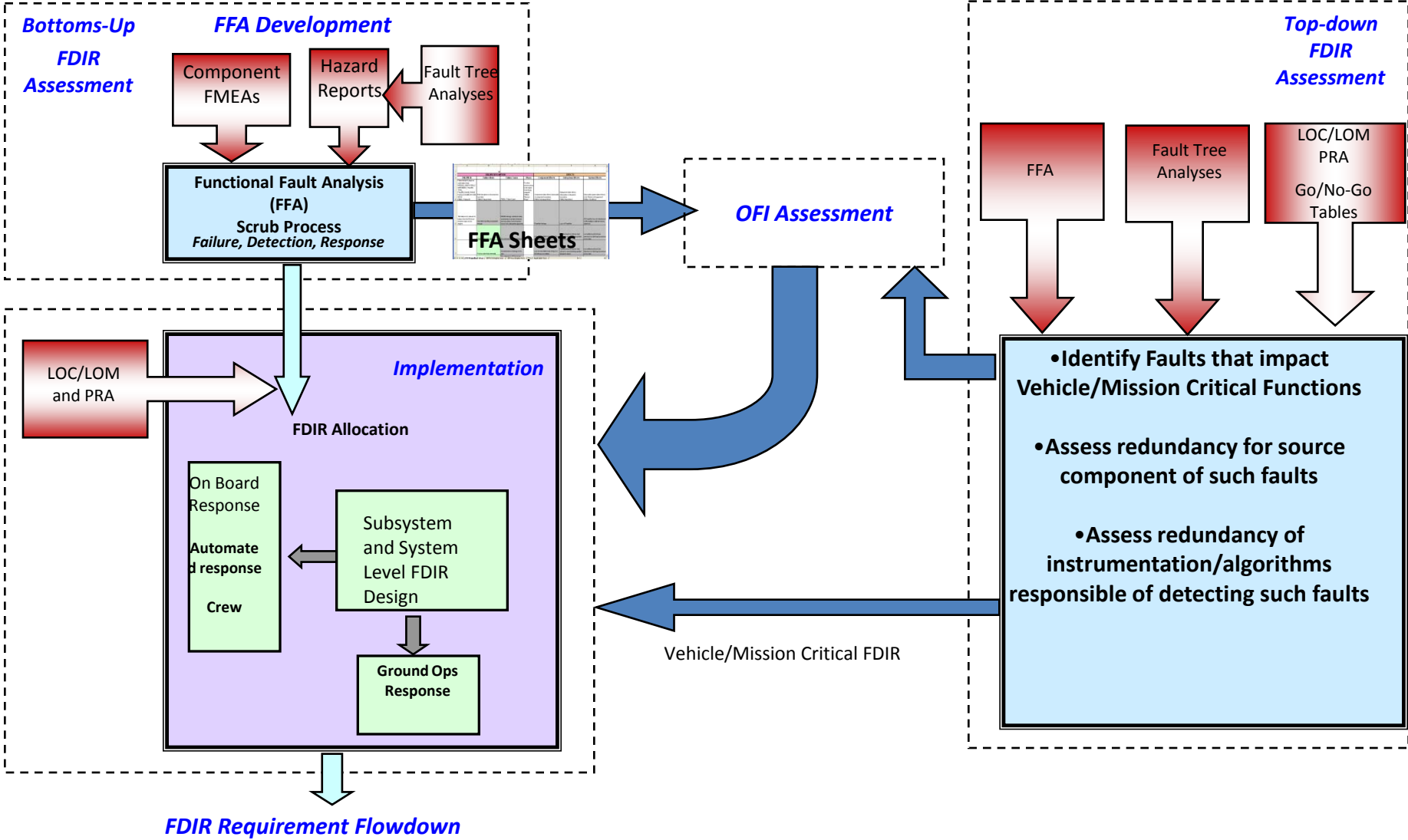


Relationship between FFA and OFI TDS





FDIR Design Integration





FMEA/CIL Criticality Definition



- 1 - Single failure that could result in loss of life or vehicle.
- 2 - Single failure that could result in loss of mission.
- 1R# - Redundant hardware which, if all failed, could cause loss of life or vehicle. A number is used to indicate the number of redundant paths or strings.
- 1S - Failure in a safety or hazard monitoring hardware item that could cause the system to fail to detect, combat, or operate when needed during a hazardous conditionk potentially resulting in loss of life or vehicle.
- 2R - Redundant hardware item which, if all failed, could cause a loss of mission.
- 3 - All other failures (3A, 3B, 3C)



Alternate Methods for FDIR Analysis



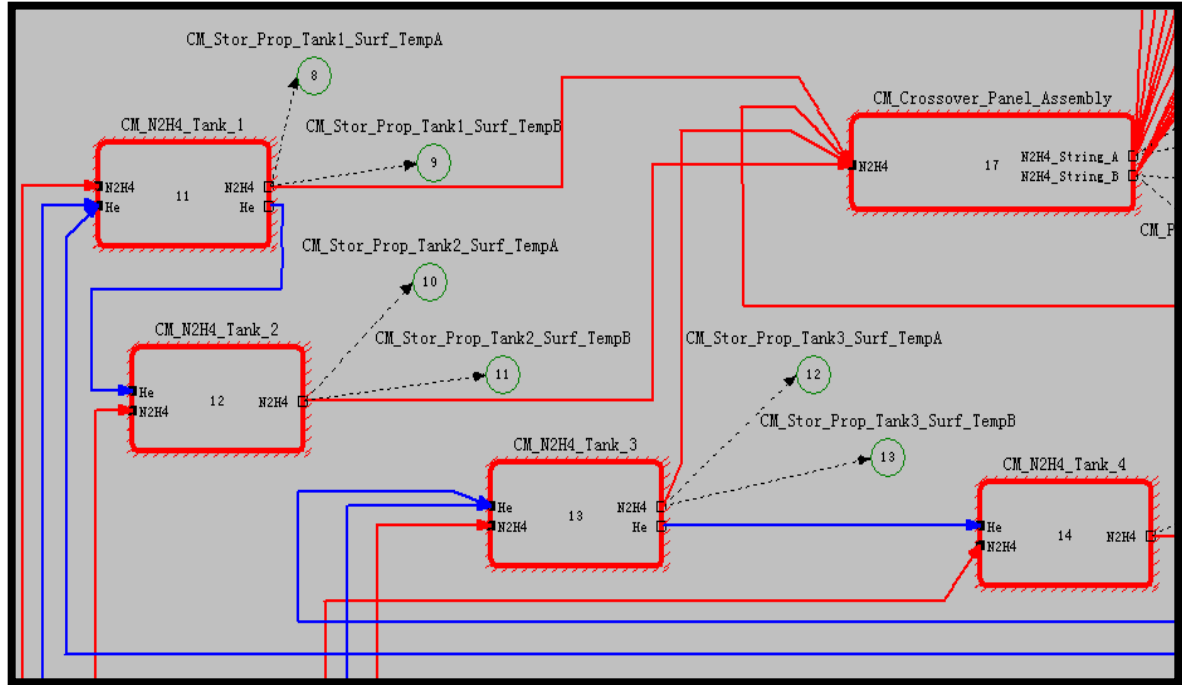
- Diagnostic/Testability Analysis tools (just to name two...)
 - QSI TEAMS
 - DSI eXpress
- Description/Benefits:
 - Cause and Effect, Multi-Functional Model of the Failure Behavior of the System
 - Graphical, Understandable way of representing the RM&T aspects of the design for the Life Cycle
 - Testability features enable fault detection, isolation, and diagnosis capabilities
 - Provide metrics of fault detection and fault isolation capabilities, various cases
 - Models can be “recycled” for use in real-time diagnostic systems




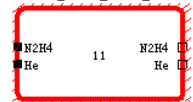
TEAMS Modeling Approach






Sample TEAMS Model for Propulsion Subsystem



 = **Test point (TEAMS)**
= **Sensor**

 = **Module (TEAMS)**
= **LRU**

 = **Link (TEAMS)**
 = **Fault Propagation Path**

 = **Module (TEAMS)**
= **Failure Mode**

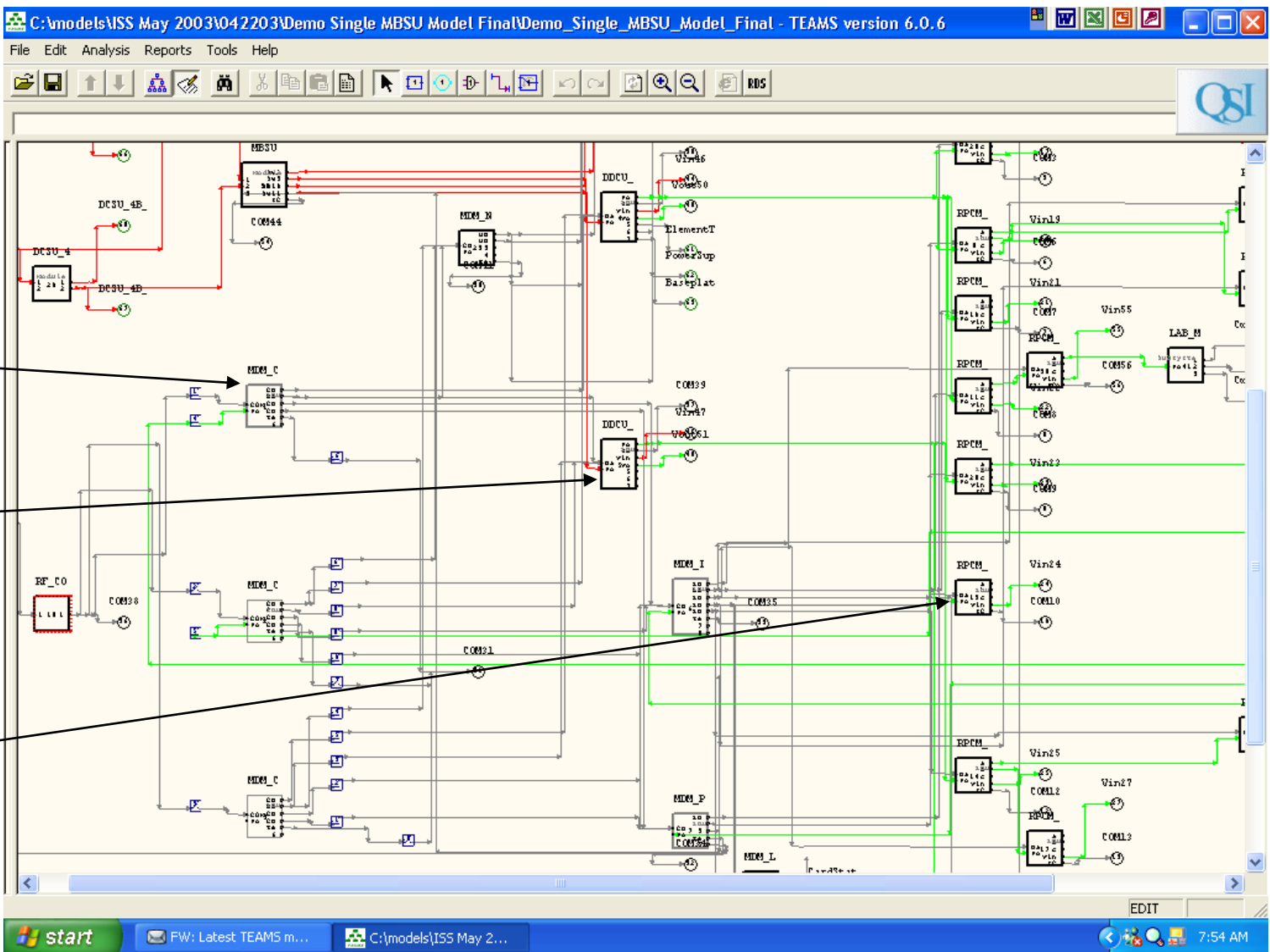
- Each **module** within a subsystem model is designated its own unique color
- Each **test point** is designated a color based on the source of document used to verify its existence
- Each **link** is designated its own unique color to differentiate between fluids, power, and data paths
- Each **failure mode** is designated a “hatched” color pattern



Multi-signal Dependency Modeling



Screen Shot of the Model used in the ISS Demonstration



MDM

DDCU

RPCM

Developing FDIR Modules - Fault Detection and Fault Isolation with TEAMS

Fault Isolation Example

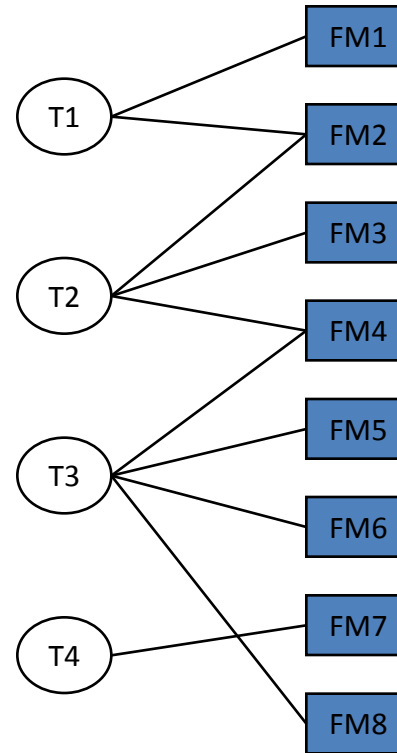
D-matrix

Failure Modes (causes)

Tests (observables)

	T1	T2	T3	T4
FM1	1			
FM2	1	1		
FM3		1		
FM4		1	1	
FM5			1	
FM6			1	
FM7				1
FM8			1	

1 = test can detect failure mode



Dependency matrix (D-matrix) is generated from the TEAMS Designer subsystem model

Developing FDIR Modules - Fault Detection and Fault Isolation with TEAMS

Fault Isolation Example (cont.)

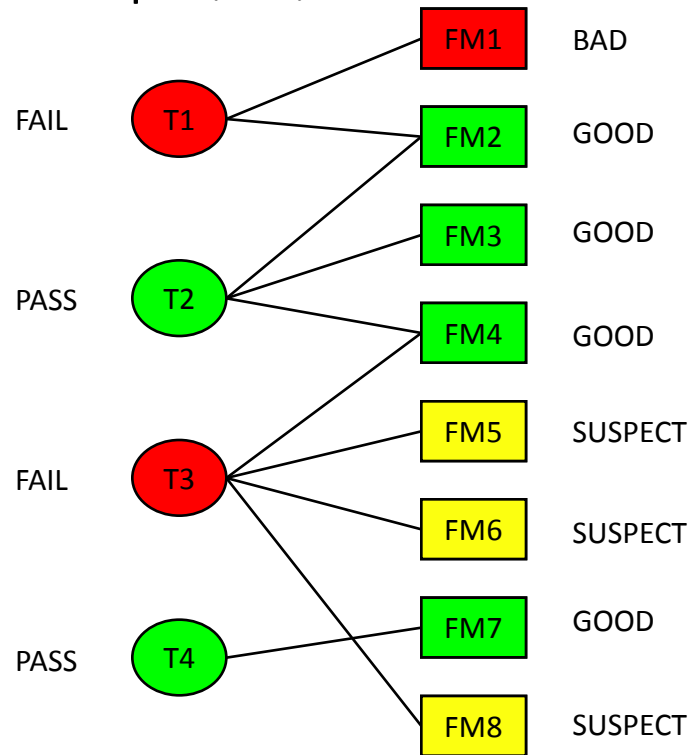
D-matrix

Tests (observables)

Failure Modes (causes)

	T1	T2	T3	T4
FM1	1			
FM2	1	1		
FM3		1		
FM4		1	1	
FM5			1	
FM6			1	
FM7				1
FM8			1	

1 = test can detect failure mode



Compute *GOOD* failure modes: Every failure mode connected to a *PASS* test is *GOOD*.

Compute *BAD* failure modes: Every test that is *FAIL* has **at least one** failure mode that is *BAD*.

If there is more than one failure mode that leads to a *FAIL* test, then all failure modes not labeled as *GOOD* are labeled as *SUSPECT*.

All remaining failure modes are labeled *UNKNOWN*: they are connected to tests for which we have no test information.



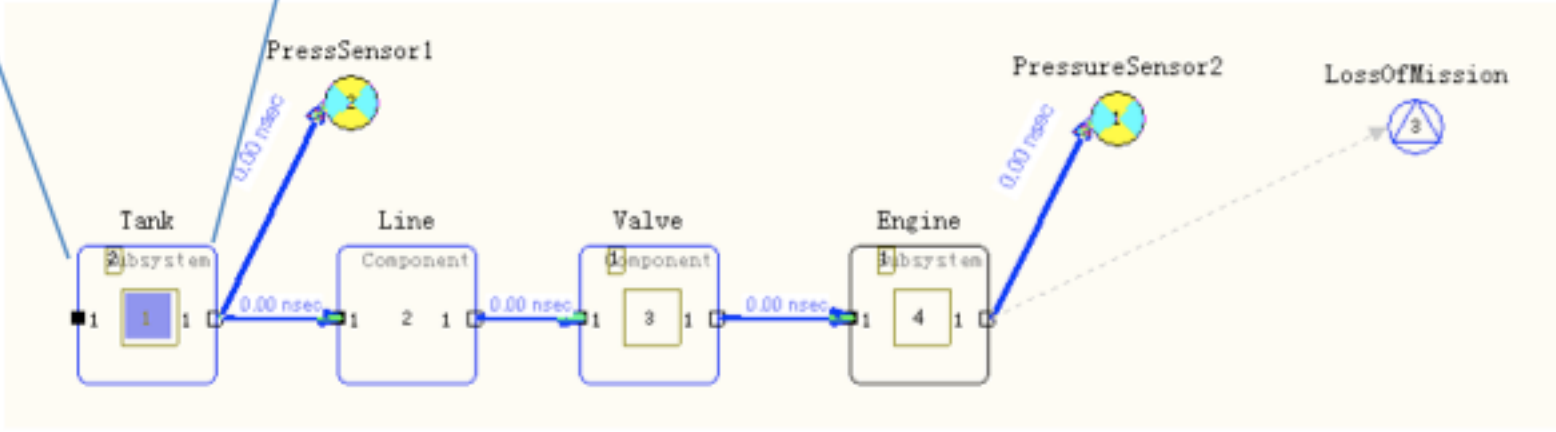
TEAMS Modeling



ExternalLeak-FM01



Failure Mode FM01 "External Leak"
for a generic tank component





Testability Analysis



TESTABILITY REPORT FOR Vehicle_Model_05

TEST OPTIONS

Test Algorithm NEAR OPTIMAL (Breadth=1, Depth=1)
Test cost weightage = 50.00 %
Test time weightage = 50.00 %
Test dollars per hour = 10.00
Fault Isolated to Failure Modes
System OK probability: 1 %
Mean time to first failure : 4425 (hours)

SYSTEM STATISTICS

Number of failure sources = 188
Number of tests = 85
Number of dependencies = 509
Number of modules at level 1 = 4
Level 2 = 26; Level 3 = 53; Level 4 = 126;
Level 5 = 9;

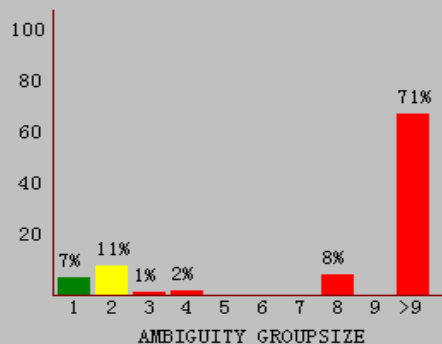
TEST ALGORITHM STATISTICS

Number of tests not used = 54
Number of nodes in tree = 69
Efficiency of test sequence = 26.15 %

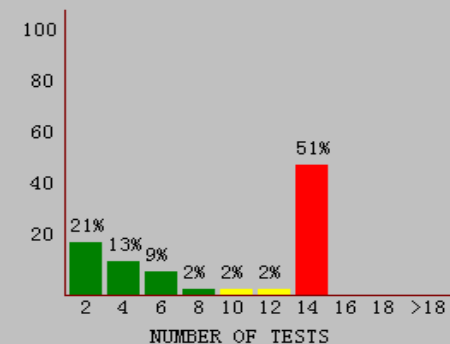
TESTABILITY FIGURES OF MERIT

Percentage Fault Detection	=	44.25 %	(UW: 51.06 %)
Percentage Fault Isolation	=	7.01 %	(UW: 8.47 %)
Percentage Retest OK's	=	84.36 %	
Ambiguity Group Size	=	57.78	
Mean Weighted Cost To Isolate	=	0.00	
Dollar Cost	=	0.00	Time = 0.00
Mean Cost To Detect	=	0.00	
Mean Time To Detect	=	0.00	

HISTOGRAM OF AMBIGUITY SIZE



HISTOGRAM OF TEST USAGE



- Determine % Fault Detection & Isolation – if low, can redesign to add more sensors or others detection or inference means
- Identify General System's metrics – Failure modes, Test points, etc



Expanded Benefits



- Element and Vehicle FMEAs improved
 - Formal modeling of failure effect propagation eliminates ambiguities of FMEA failure effect columns
 - Many comments fed back to element FMEAs, almost all of them incorporated into next FMEA revisions
 - Provides concrete and more precise time-to-effect information
 - Ties FMEAs concretely to design (FMEAs the basis for failure effect models, which are incorporated into Ares architectural model)
- Vehicle and element documentation problems found and fixed
 - Could become design problems or become much more expensive to fix later
 - Formal modeling of element and subsystem architectures uncovers a variety of documentation inconsistencies (missing IDs, mismatches between schematics and other documents that refer to those items)
 - Some concrete design issues, such as mismatches between number of interfaces between different subsystems (this uncovered a couple times in Upper Stage)
 - Modeling entails detailed review of interfaces / ICDs



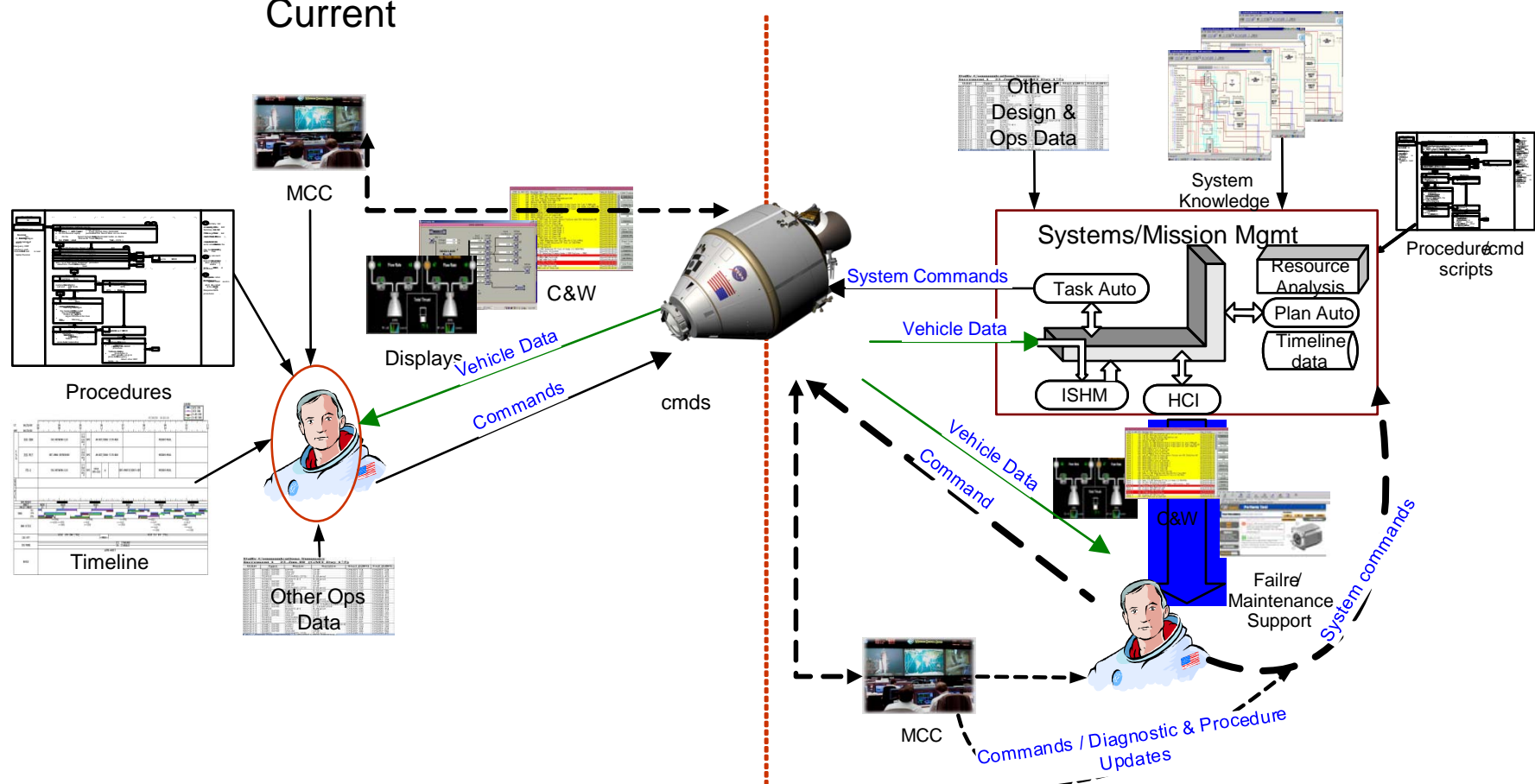
Real-Time Fault Management



Evolution of Systems/Fault Mgmt on-board



Current



Situational Awareness /System Cognizance	<div style="width: 30%; background-color: #90EE90; border: 1px solid black;"></div>	<div style="width: 70%; background-color: #00FF00; border: 1px solid black;"></div>	Enhance cockpit Situational Awareness
Crew Workload for Systems Mgmt	<div style="width: 60%; background-color: #FFFF00; border: 1px solid black;"></div>	<div style="width: 10%; background-color: #00FF00; border: 1px solid black;"></div>	Reduced Crew/MCC requirements for systems management actions
Tactical/real-time MCC dependency	<div style="width: 50%; background-color: #FFA500; border: 1px solid black;"></div>	<div style="width: 15%; background-color: #00FF00; border: 1px solid black;"></div>	Reduced real-time MCC support requirements
Task-Specific Training Requirements	<div style="width: 50%; background-color: #FFA500; border: 1px solid black;"></div>	<div style="width: 10%; background-color: #00FF00; border: 1px solid black;"></div>	Reduced Crew task training for nominal and off-nominal systems management



On-board Fault Management relevance to Ops



- **Mission Control Center (MCC)** - Level of dependency of the spacecraft and crew on tactical/real-time MCC support during nominal and off-nominal operations.
 - This includes the size of the team required for real-time operations, as well as mission preparation and planning.
- **Crew Training** - Training requirements associated with necessary crew involvement for nominal/routine system management, and response to off-nominal conditions.
 - If the crew is required to actively perform health monitoring, FDIR, and nominal routine system control = significant task and skill training is required.
- **Flight Product development** - Development of flight procedures and other products required by the crew and Flight Control Team (FCT) to manage the system and operate the spacecraft during nominal and off-nominal operations.



On-board Fault Management relevance to Ops



- **Engineering support** - Dependency on engineering teams, outside of the FCT, to provide system expertise during nominal operations and support anomaly troubleshooting.
- **Mission Planning** - Detail required in pre-mission planning to support the execution of a nominal mission and provide sufficient margins for contingency operations.
 - This includes resource analysis, and timeline development, thus on-board capabilities for resource management, or greater availability of resources, reduces granularity required in pre-mission planning.



Key Fault Management Elements



- **Vehicle Instrumentation & Displays**
 - Provide Crew and MCC insight into system performance, anomalies and current system status
 - Enables identification and response to failures
 - Provides sufficient insight to perform the mission specified for the spacecraft
- **Flight Data File**
 - Contains nominal, malfunction and reference procedures for the Crew to conduct their mission.
 - Malfunction procedures support Fault detection, Isolation and Recovery when this actions are not performed by on-board systems
- **Caution & Warning**
 - Alerts the crew to system failures that require their attention
 - Information provided by aural tones, lights, and displayed information
 - Level of information provided by the C&W system determines the crew response to the information.

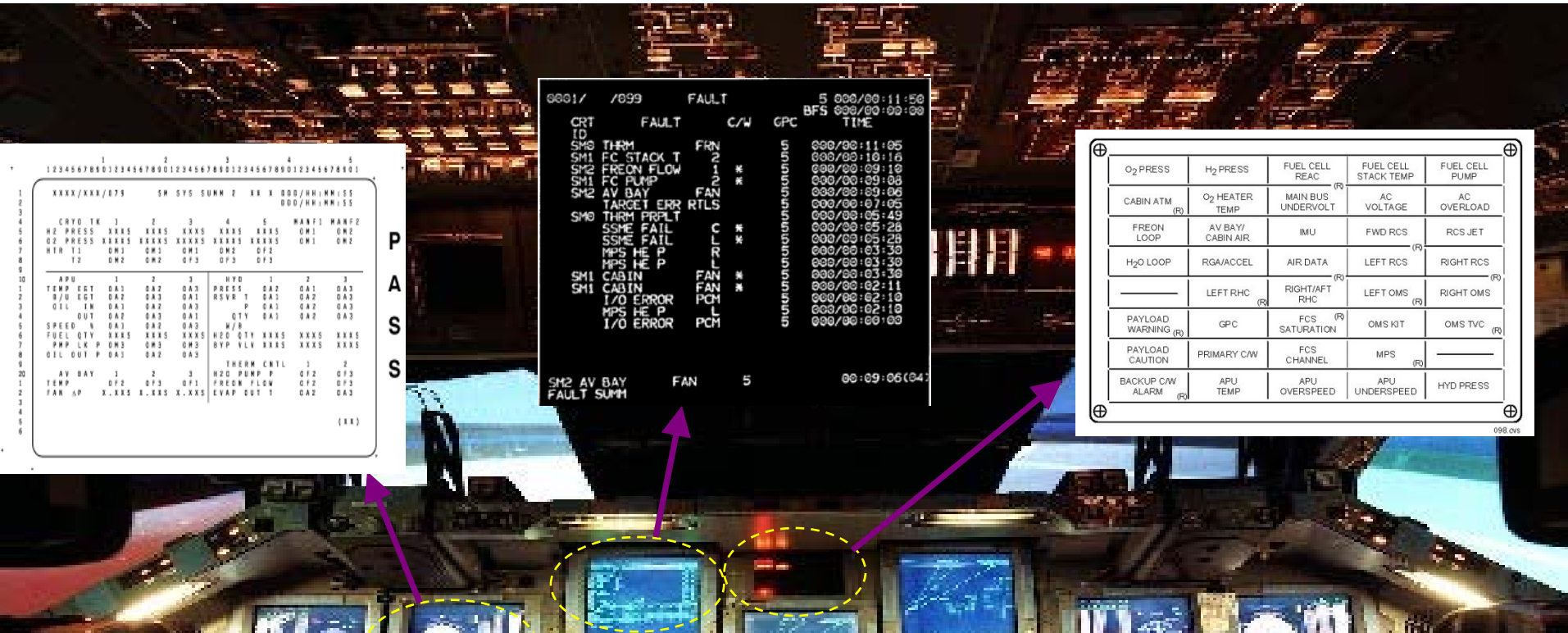


C&W Message Classification



Caution and Warning	Alert notification system for flight crew and ground that includes Emergencies, Cautions, Warnings, and Advisories.
Emergency (Class 1 event)	Any condition that threatens the life of the crew or vehicle and requires immediate action. Three specific conditions (event types) define the emergency class; fire/smoke, rapid change in cabin pressure and toxic atmosphere.
Warning (Class 2 event)	Any event that requires immediate correction to avoid loss of or major impact to the vehicle or potential loss of crew.
Caution (Class 3 event)	Any event that is not time critical in nature but further degradation has the potential to threaten the loss of crew, or the loss of redundant equipment such that subsequent failure could result in a Warning condition.
Advisory (Class 4 event)	A non Caution and Warning message which provides information about systems status and processes.

Fault Management on-board Orbiter



P
A
S
S

- Annunciator Matrix and On-board Fault Summary data based on individual conditions or pre-defined “hard-coded” rules = **no dynamic correlation**
- Failures that impact multiple components result in the generation of many seemingly unrelated messages that the crew needs to isolate = **cryptic C&W**
- Generated alerts are often not indicative of the real failure. E.g. ‘EPS bus ‘undervolt’ failure generated ‘Fuel cell Ph low’ = **crew diagnosis required**



Key FM Elements– Decision Support



- Decision Support Information
 - Generation of actionable information for the Crew or Flight Controllers
 - Required information to make a failure response decision
 - Typical information required:
 - **Affected Components** - System components that have lost partial or all functionality as a consequence of the root cause failure.
 - Power failure that also affects thermal control: all components that have lost power + all components that start getting hot.
 - **System-level impact** - Components or functionality that performs critical functions and has been affected by, or is the root-cause failure.
 - A power failure cuts power to 4 loads: light 1, light 2, light 3, and main air conditioning unit. Affected components are all four and system-level impact is the loss of air conditioning.
 - **Redundancy of Critical Components** – Level of redundancy degradation of critical components
 - In the Internal Measurement Unit (IMU) in the Shuttle, for example, the system is 2-fault tolerant, since there are 3 IMUs, and only one is necessary to perform the IMU system functions. Upon the loss of one IMU, the system would be 1-fault tolerant.
 - **Critical-to Information** - A system is “Critical to” any component that if failed, will prevent the system from performing its functions.
 - The IMU system is two-fault tolerant for individual IMU failures. If two IMUs have failed, then the IMU system is critical to the non-redundant components that keep the last IMU functioning.



Learning from System Anomalies - STS



- STS 93 Electrical Short During ascent
 - Seven seconds after lift-off, the Orbiter suffered a transient AC electrical short circuit
 - Failure Indications Onboard: ‘Fuel Cell pH’ message generated by the computer. This message occasionally occurs during ascent as a transient condition.
 - Root-cause: electrical short had momentarily dropped the AC bus voltage and a built-in self-check of the pH sensor had caused the message when the power was restored.
 - The crew was unaware of the real issue and the impact to the the health of critical systems for ascent.
 - **Affected Components** – equipment powered by shorted AC bus
 - **System impact** – none
 - **Redundancy of critical components** – 2 main engine controllers 0 Fault Tolerant to MEC, power and data
 - **Critical to:** MEC, Power and data components for affect MECs
 - Crew Situational awareness based on sysem indications - none



Learning from System Anomalies - ISS



- ISS US C&C Failure
 - STS-100/ISS 6A assembly mission in April 2001, the ISS suffered failures within the hard drive mass storage system of each of the 3 Command and Control (C&C) flight computers over several days.
 - Result: no command & control capability, no insight in system telemetry
 - Factors that contributed to recovery:
 - The ISS architecture comprised of US and RS segments – RS maintained critical capabilities
 - The Space Shuttle was docked to ISS – providing additional comm capabilities and ATT control
 - Systems Management functions in the ISS architecture are distributed
 - power generation, atmosphere control, attitude control, thermal control) are allocated within the subsystem control, between HW, firmware, tier 2 and local tier 3 computers.



Learning from System Anomalies - ISS



- ISS RS C&C Failure
 - At GMT 164:14:57, during ISS Assembly flight 13A, all six Russian computers (TsVMs & TVMs) became unavailable.
 - Both sets of RS computers TsVM & TVM, are triplex systems, but a single design feature caused all six computers to fail
 - The following functions provided by RS segment became un-available:
 - Oxygen generation (Elektron),
 - CO2 removal (Vozdukh)
 - Propulsive attitude control, necessary in the event US MM is unavailable or unable to maintain control.
 - Power to SOYUZ severely limited, since US to RS power converters were off at the time of failure
 - Factors that contributed to recovery:
 - The ISS architecture comprised of US and RS segments – RS maintained critical capabilities
 - The Space Shuttle was docked to ISS – providing additional communications capabilities and ATT control
 - Systems Management functions in the ISS architecture are distributed



Questions/comments?



carlos.garcia-galan-1@nasa.gov

NASA-Johnson Space Center