# Launch Vehicle Applications

**Dr. Michael D. Watson**
**Dr. Stephen B. Johnson**
**NASA MSFC EV43**
**Advanced Sensors and SHM Branch**

**27 April 2010**

# Presentation Goal / Agenda

- **Goal:**
  - Describe MSFC EV43 experience with Integrated System Health Management application to launch vehicles

- **Agenda:**
  - EV43 ISHM Philosophy
  - Launch Vehicle Application
  - Abort Conditions & Algorithms
  - Sensor Data Qualification
  - Caution & Warning
  - Redundancy Management
  - Functional Fault Analysis
  - Diagnostics
  - Fleet Supportability
  - Certification, Verification & Validation

# EV43 ISHM Philosophy

- **ISHM (also known as VHM, SHM, PHM, FM, FDIR, RM, etc.) is the capability of the system to contain, prevent, detect, isolate, diagnose, respond to and recover from conditions that may interfere with nominal system operations.**

- **The operational subset is Fault Management, emphasized here**
  - Will not emphasize fault prevention mechanisms such as Quality Assurance procedures

- **ISHM/FM activities and design mechanisms work in concert with systems engineering, SRQA, operations, and subsystem design and operational activities**

- **ISHM/FM design mechanisms must be optimized against cost, performance, safety, reliability, and availability goals**
  - The goal is NOT to add bunches of sensors or algorithms, but to deploy the minimum set needed to adequately protect system functionality and human safety

# Key ISHM/FM Concepts

- **ISHM/FM exists to protect functionality**
- **Operational ISHM/FM design mechanisms typically operate in a "meta-control loop" to protect or restore functionality**
  - Example: nominal control loop for GNC compromised because processor fails or TVC propellant leaks fails; FM votes out failed processor or closes valves to stop leak, returns system to state in which nominal control loop again functions
  - Example: passive control (through design margins) of structures fails, structural failure begins; FM detects loss of control or loss of electronic signals and initiates an abort to protect the crew (system goal change)
- **Time to criticality matters**
  - ISHM/FM mitigation mechanisms must operate faster than the propagation of failure effects they attempt to mitigate
- **ISHM/FM can be implemented by hardware, software, or humans, on the ground or the vehicle**

# Launch Vehicle Application

- **In-flight time to criticalities are generally very short**
  - 10s to 100s of milliseconds
- **System functions cannot generally be compromised**
  - Failure containment / failure masking essential for top-level system functions (GNC, propellant & propulsion control, etc.)
  - Safing is not generally an option (except pre-launch)
- **In-flight operational period very short (8-10 minutes)**
  - Deep space missions will require much longer durations on the order of days or weeks
  - Multiple failure tolerance generally not required
- **Pre-launch capabilities crucial for cost-effective operation**
  - Rapid fault isolation and identification through automated ground-based diagnostics, analysis of integration and launch sequence tests, launch commit criteria; logistics and maintenance procedures part of ISHM/FM
- **Fleet support capabilities crucial for long-term cost-effective operation**
  - Isolation and identification of faults between flights, fix manufacturing line

# Abort Conditions (ACs)

- **Intermediate failure effects, which if they occur and are not mitigated, will lead to loss of crew**
  - Specifically identifiable as a system state or behavior at a particular location or set of locations on the vehicle
- **Top-down analysis against relatively small number (tens) of situations in which the crew is at risk**
  - Examples:  different explosion or conflagration cases, different ways in which TVC thrust direction or magnitude is compromised, etc.
  - Each case must be analyzed against mission timeline with appropriate environmental conditions (around Max-Q, separation, high-altitude, etc.), typically via Monte Carlo analyses
  - Conditions vary significantly in probability of loss of crew
- **Bottom-up analysis to ensure that the full set of abort conditions ("crew-at-risk" situations) are identified, and to determine probabilities of occurrence of each situation**
  - Probabilities of AC occurrence depend on failure mode probabilities, and failure effect propagation paths (FEPPs) from those failure modes to the abort condition

# Abort

- **A goal change… mission can no longer be accomplished but crew must be kept safe**

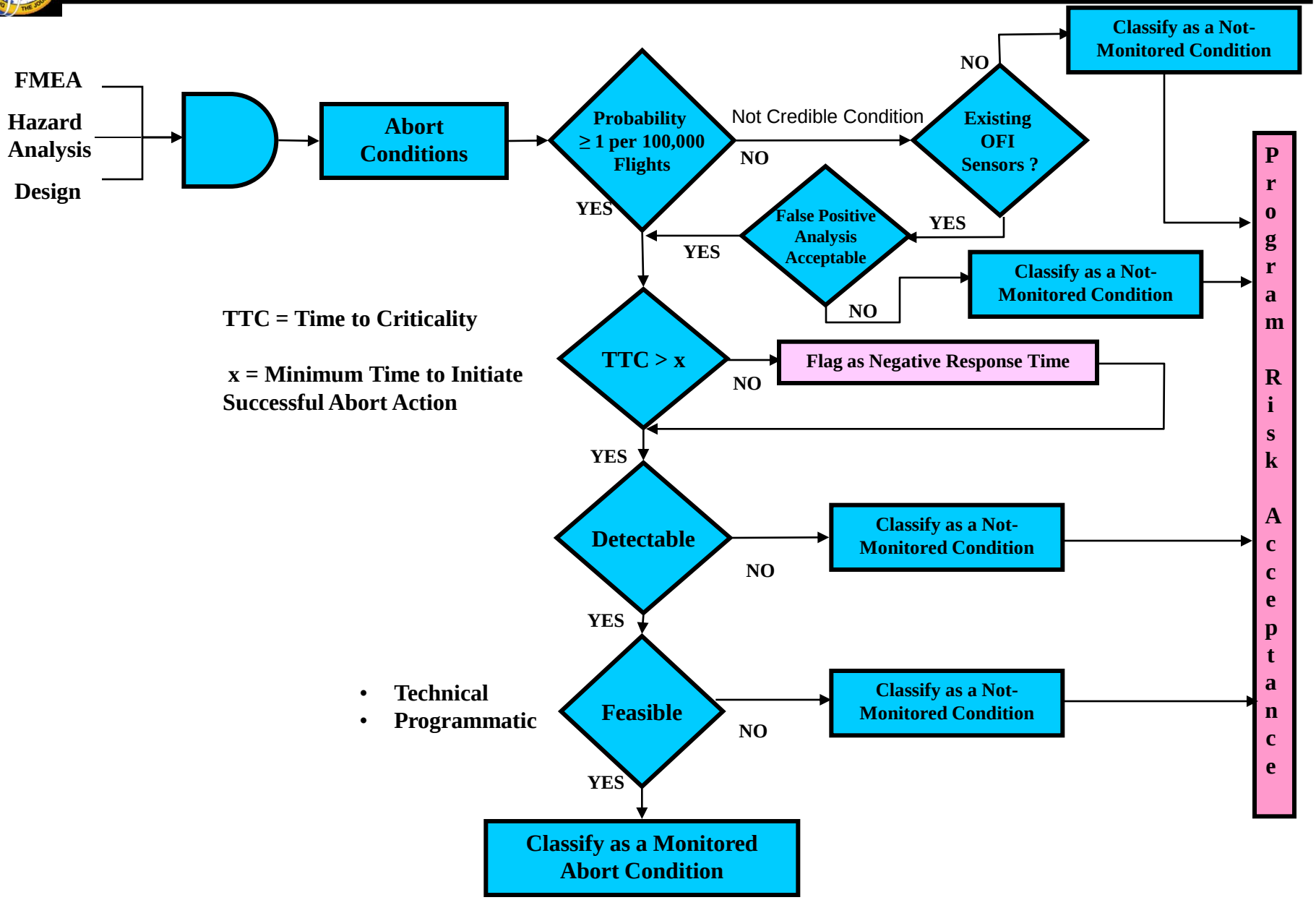
- **Classify abort conditions into monitored versus non-monitored**
  - Non-monitored = risk acceptance.
    - Always have crew detection and response as last-ditch abort detection and response mechanism, but they are not generally fast enough
  - Quantify probabilities of detection by candidate mechanisms, and how effective these mechanisms are at reducing risk to crew
    - Recognize and estimate very large uncertainties as part of decision process

- **Aborts implemented through hardware, software, and humans**
  - Crew always has the choice of whether to abort, or inhibit automatic abort
  - Vehicle can only recommend an abort, crew (or crew capsule) decides

- **3 Measurements necessary for each monitored abort condition: Detect, confirm, and 1 level of fault tolerance**
  - Similar or dissimilar measurements / SDQS (measurement validation)
  - Protect against False Positive / False Negative

- **Abort recommendation sent to crew capsule---crew / capsule decides to initiate abort**

# Abort Conditions Identification Process



# Abort Response

- **Analysis of abort response must consider:**
  - Performance characteristics of abort system (such as Orion LAS)
  - Abort Detection capabilities (false positive/false negative)
  - Response latencies (sensors, data transfers, processing, crew)
  - Failure effect propagation times and paths (internal and external)
  - Environmental conditions (next to tower, early ascent, Max-Q, separation, high-altitude, etc., wind, pressure, etc.)

- **Abort Warning Time**
  - How long does crew/capsule have before abort must be initiated
  - Race condition of abort response latencies versus failure effect propagation paths and times
  - Typically automatic abort if AWT < 15-30 seconds (crew inhibit possible), crew initiated abort if AWT > 15-30 seconds
  - AWT calculations are statistical, many failure modes detected by single detection mechanism

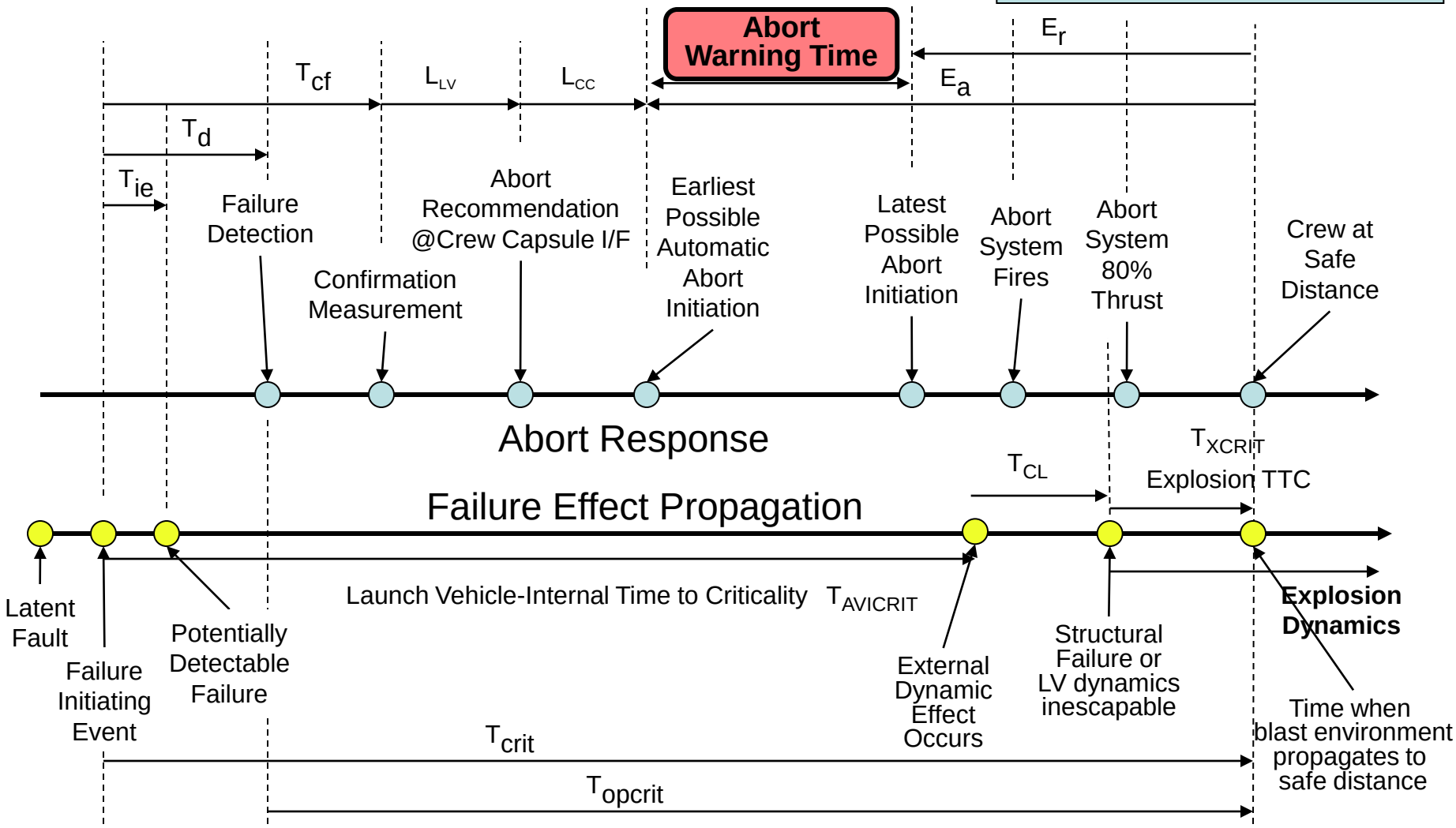
- **Special case:  liquid propellant engines, automatic shutdown to prevent catastrophic failure, abort required**

# Worst-Case (Auto Abort) Timing Analysis for Control Loss Case

$T_{ie}$ = Time to Initial Effect
$T_d$ = Time to Detect
$T_{cf}$ = Time to Confirm

Tcrit = Time to Criticality
Topcrit = Operational Time to Criticality
Txcrit = Explosion TTC
Tcl = Control Loss TTC

$E_a$ = Abort Escape Time Available
$E_r$ = Abort Escape Time Required
$L_{LV}$ = LV Abort Avionics Latency
$L_{CC}$ = Crew Capsule Abort Avionics Latency



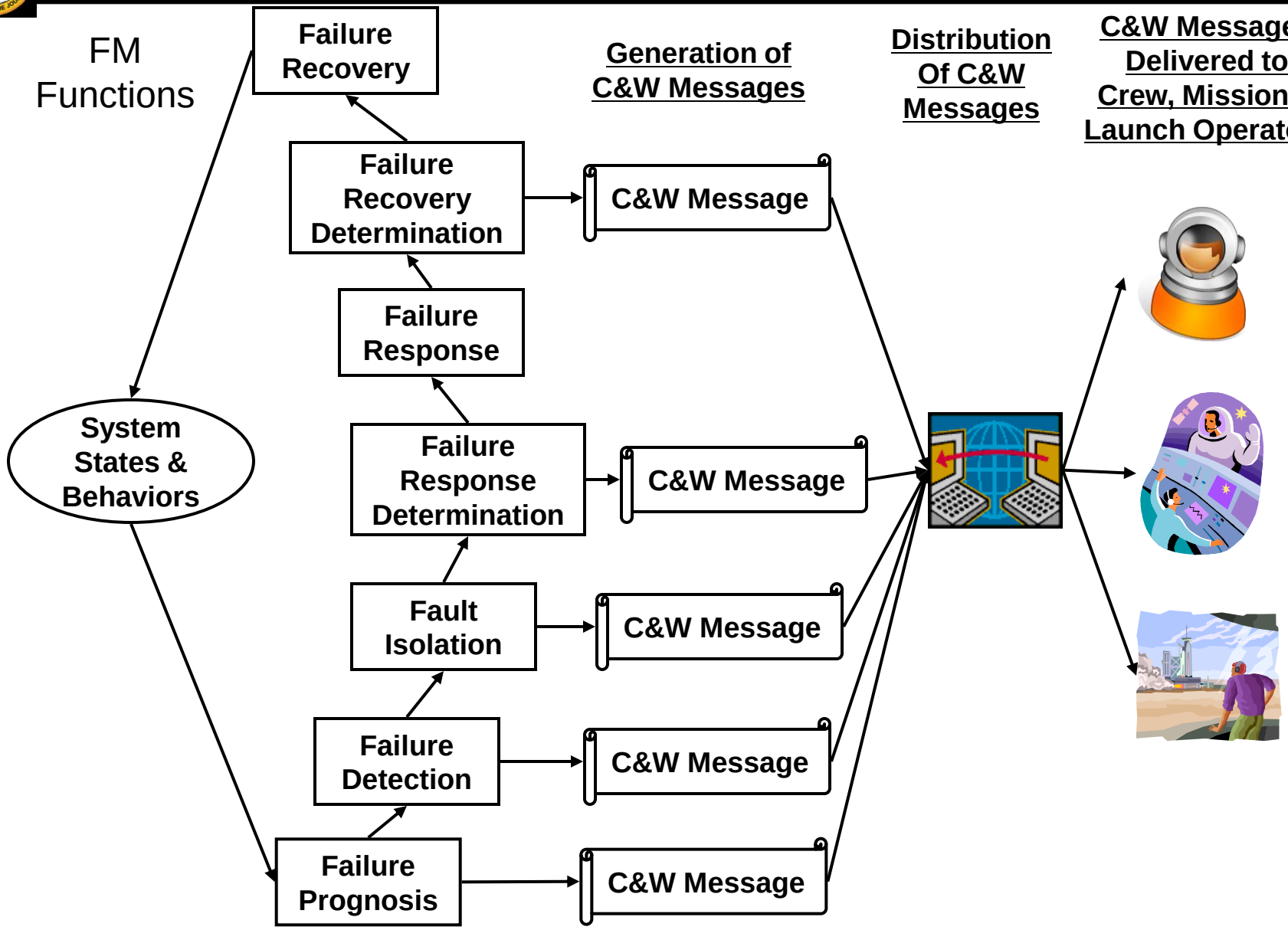
# Sensor Data Qualification

- **Monitor and detect faulty sensor data**
- **Types**
  - Limit checks
  - Rate of change checks
  - Hardware redundancy checks
  - Analytical Redundancy checks
- **Minimize False Positives / False Negatives**
- **Rapid processing essential**
- **Minimize code required**
- **Graceful degradation as redundancy lost**

# Caution & Warning

- **Notification to crew of critical vehicle situations**
  - Detection but not confirmation of abort condition
  - Loss of redundancy
  - Other situations to inform crew situational awareness
- **Notification based on a decision that a vehicle failure or failure response has occurred**
- **Sent to crew, Mission Control Center, Launch Control Center (for pre-launch cases)**
- **C&W Condition – the determination that one or more failures have occurred on the vehicle for which the Flight Crew, MS, or GS (pre-launch) need situational awareness.**
  - Bottom-up process to assess vehicle measurements and messages

# FM-C&W Relationship



# C&W Classes

- **Class 1:  Emergency Action / Abort Recommendation**

- **Class 2 C&W Condition (Warning): indicates a condition which may lead to an abort condition or loss of critical vehicle functionality, and may be related to manual or automated corrective or preventive action.**
  - Results from loss of non-safety critical vehicle function or loss of vehicle function that does not require an abort recommendation; indicates minimum safe level and/or system failure threshold (i.e., one failure away from need to abort or caution threshold violation indication for Class 1 C&W Condition).
  - Results from abort condition detection without confirmation or abort condition confirmation without a primary detection.
  - Can result due to association with redundancy management actions or sensor data disqualifications.

- **Class 3 C&W Condition (Caution): indicates that subsequent anomalies could lead to a Class 2 C&W Condition.**
  - Results from system deterioration or loss of redundancy level (i.e., caution threshold violation indication for Class 2 C&W Condition).
  - Can result due to association with redundancy management actions or sensor data disqualifications.

- **Class 4 C&W Condition (Advisory): requires no action by crew; used for troubleshooting purposes only by GS and/or MS.**
  - Results from loss of non-critical function or fault/failure of a non-critical device that poses no serious threat to continued operations.

# Redundancy Management

- **Fault Detection, Isolation, and Recovery, to manage vehicle redundancy, protecting functionality and hence preventing abort situations**
  - Includes degraded mode operations, functional redundancy, component redundancy
  - Recovery can utilize dissimilarity
- **Redundancy based on failure tolerance requirements**
  - But often determined from the bottom-up through historical designs and reliability data
- **Generally, electrical, mechanical, liquid propellant, and data systems**
  - Computers, avionics, sensors, power distribution, liquid propellant feedlines & valves, thrusters, sometimes engines
- **Distributed design, requires centralized coordination**
- **Pre-launch includes safing**

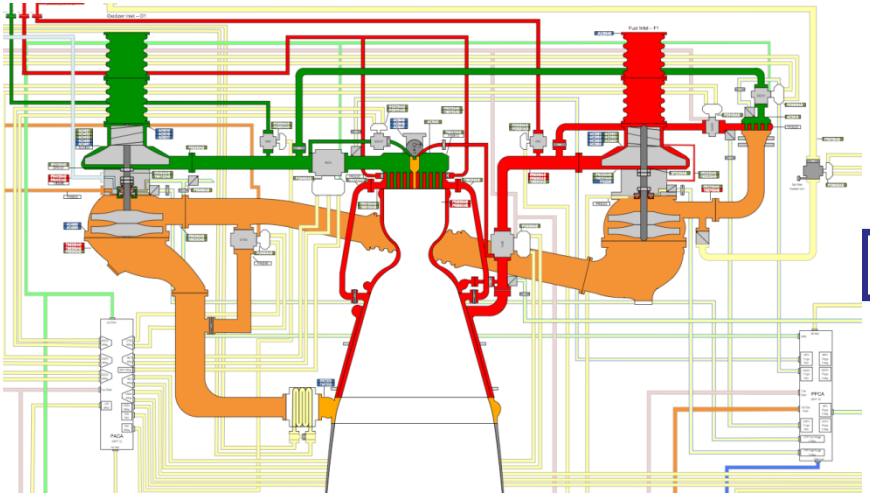
# Functional Fault Analysis

- **Early analysis of failure modes and effects in the system architecture, and ISHM control loops and mechanisms**
- **Early analysis = function, later analysis = mechanism**
- **Tools to efficiently perform functional analysis, and connect to systems engineering and SRQA tools for ISHM/FM are lacking**
- **Tools for analysis of failure effect propagation paths, vehicle instrumentation exist (TEAMS one example)**
  - Failure detection and fault isolation metrics
  - Support development of pre-launch troubleshooting procedures
  - Support development of launch commit criteria
  - Support development of caution and warning conditions
  - Support development of redundancy management conditions
  - Support development of abort conditions
  - Support probabilistic risk analysis, fault trees, hazard trees (an effective representation and tool to trace failure modes to failure effects)

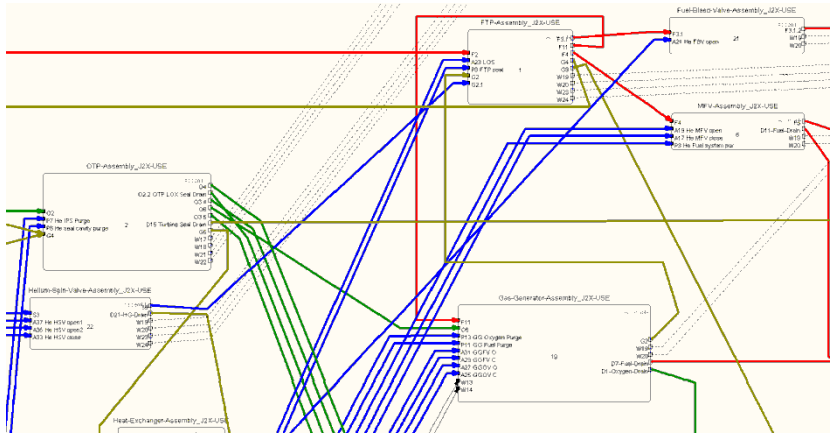
# Directed Graph Modeling

- **… is a fundamental, efficient representation of the failure effects**
  - More accurate and complete than fault trees or hazard analyses
  - Provides information that supports a variety of tasks and processes, including reliability & availability analyses; troubleshooting procedures; C&W, LCC, abort condition analysis

- **… but also difficult to accomplish early enough in design to have significant architectural impact**
  - Need improved functional analysis capabilities for early architecture studies
  - Need automation tools to connect to systems engineering functions, fault trees, FMEAs



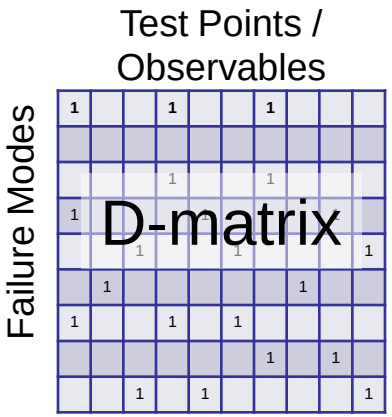
**Upper Stage Engine Schematic**

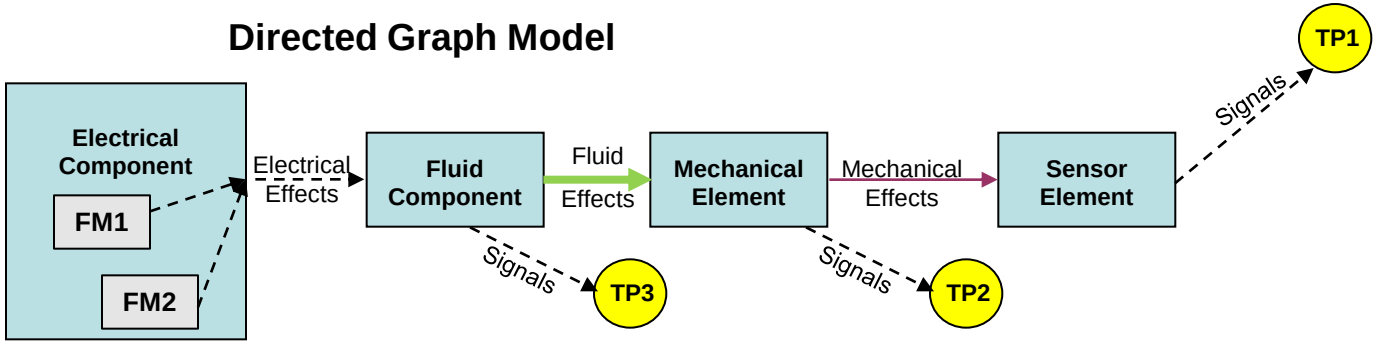


**Functional Model in TEAMS**

# Functional Fault Analysis
# Ares Vehicle Diagnostic Model

- **Built from schematics, IPCL, FMEAs, LRU list, ICDs, and Integrated Mission Timeline**
- **Built to level required to analyze and diagnose faults to the LRU**
  - Level defined by subsystem schematics + LRUs + FMEAs + IPCL
- **Exports the D-matrix to AGBD, which operates on it using TEAMS-RT to perform real-time diagnostics**



# Diagnostics
# (Fault Isolation + Fault Identification)

- **Can be on-board or ground-based**
  - Launchers = ground-based, deep space/orbital stages could be on-board
- **LVs usually ground-based because response times and response actions are limited**
- **Export the Functional Fault Analysis mechanism model to diagnostics task**
  - For launchers, ground-based
  - For deep-space systems could be on-board
- **Attach code to process vehicle telemetry through threshold and context-switching algorithms**
- **Use for operational diagnostics**
  - Pre-launch: automate fault isolation and identification
  - Fleet support:  support analysis of vehicle failures and anomalies
- **For Constellation, integrate Ares Ground-Based Diagnostics with Ground Operations Project FDIR system for combined diagnosis in the Launch Control Center**

# Fleet Supportability

- **Assessment of each vehicle's test, integration, and flight data to search for anomalies and identify failure modes**
  - Anomaly detection: search for unusual behavior in data
  - Relies on rigorous management and availability of data
- **Just as important to launch vehicles as on-board algorithms and pre-launch capabilities**
- **Root Cause Analysis: Assess anomalies and failures to determine causes**
- **Can be on-board or post-flight;**
  - LVs usually post-flight since response times and actions are limited
  - Actions are fixes to design and manufacturing processes

# Certification, Verification and Validation

- **Model certification for all models used for design decisions**
  - Functional Fault Analysis
  - Rigorous review of models with design experts, SRQA, and systems engineering
  - Reviews/accreditation process provides significant systems integration value by reconciliation of diverse documentation sources

- **Application V&V**
- **Verification**
  - Trace to ISHM/FM requirements (for CxP: TVRs---test and verification requirements)
  - Fault injection testing representing system failure space, in analysis, FM testing / simulation laboratory, subsystem, and system test labs

- **Validation**
  - Assessment of design with operational users
  - System and flight tests for on-board algorithms
  - Operational use testing for ground-based systems

# Advanced Sensors

- **All ISHM depends on ability to detect off-nominal phenomena**
  - Do not have all of the sensing capabilities we would like
- **Use control sensors whenever possible**
  - These already exist, tied to crucial functions
  - For Aborts, few sensors needed beyond control sensors
- **Sensor technologies in development**
  - Leak detection (H2, O2, Hydrazine)
  - Cryogenic FBG (non-threatening at pump inputs)
  - Structural health monitoring (detect damage prior to launch for detailed NDE)
  - Vehicle breakup detection in-flight
  - Embedded FBG, Piezoelectrics, Lamb-wave, SAW, acoustic emission
- **Smart sensors**
- **RF transmission (no wires)**