System Health Management Methodology/Handbook/Textbook

Dr. Stephen B. Johnson
NASA MSFC EV43

Advanced Sensors and SHM Branch
stephen.b.johnson@nasa.gov

27 April 2010

Presentation Goal / Agenda

- **Goal:**
  - Describe current status of SHM methodology development, and its incarnation in a Fault Management Handbook and SHM Reference Textbook

- **Agenda:**
  - History of SHM and FM methodology development
  - SHM/FM Conceptual Framework & Methodology Elements
  - CxP Status
  - FM Handbook Status
  - SHM Reference Textbook Status

SHM and FM

- **SHM (also known as VHM, ISHM, PHM, FM, FDIR, FP, 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.**
  - Includes fault prevention through design, manufacturing quality, etc.
- **The operational subset is Fault Management**
- **SHM/FM addresses all aspects of faults and failures, and hence encompasses (but does not aim to "take over") aspects of SRQA functions such as FMEAs, fault trees, reliability, hazards**
  - Safety is not identical to reliability/dependability, but significant overlaps
- **Within some parts of NASA CxP and HQ, FM now seen as directly synonymous with SHM/ISHM**
  - Be aware of this interpretation!

Brief History of SHM Methodology Development

- **1960s-1990s: Variety of concepts of fault tolerance and application-specific developments**
  - Computing and software conceptual leaders, terminology work, deep-space fault protection & autonomy, Byzantine Generals problem, safety & reliability methods
  - LaRC, JPL, Academia (UCLA, Toulouse, CMU, MIT), Industry (Bendix, Honeywell, IBM, Draper Labs, etc.)
- **1980s: DOD Integrated Diagnostics, Dependability Working Group (Aerospace Corp.)**
- **1991-92: VHM Methodology, JSC/NLS funding, Martin Marietta**
- **1994-95: Control loop representation, comparison of SHM methods & architectures across multiple applications (aircraft, launchers, spacecraft)**
  - Boeing Company / Dependable Systems International

SHM Methodology History continued

- **1990s: SHM technologies (specific insights, particularly in diagnostics), Reliability-Centered Maintenance, Open System Alliance – Condition-Based-Maintenance (OSA-CBM)**
- **2000s: 2008 Rasmussen paper on GNC Fault Protection, CAIB Report---culture connection**
- **2005: ISHEM Forum, FDDR methodology work begins**
- **2008: SMD FM Workshop, CxP Stands up FMAAT, SHM textbook contract signed with Wiley UK, PHM conferences begin**
- **2009: FMAAT Reviews, CW/FDIR group establishes FM team, FM Handbook proposal approved, International Journal of Prognostics & Health Management established**
- **2010: CxP FM team directed to look at clean sheet approach, Conceptual Framework paper**

Current NASA and "community" SHM/FM Methodology Development Locales

- **Constellation Program & Ares Project**
  - Ares: Failure Detection, Diagnostics, and Response Working Group (FDDR WG), since 2005
  - CxP: Software and Avionics Integration Office, Caution & Warning / Failure Detection, Isolation, and Recover WG, since 2009
  - CxP: Fault Management Assessment and Advisory Team (FMAAT), since 2008
- **Science Mission Directorate**
  - Fault Management Workshop April 2008
  - Support for Handbook
- **JPL Project Practices, and JPL Design Principles**
- **NASA HQ Chief Engineer's Office**
  - FM Handbook
- **NASA SHM (ISHM) Community**
  - ISHEM Forum, November 2005
- **Government, Academia, Industry: SHM Textbook**

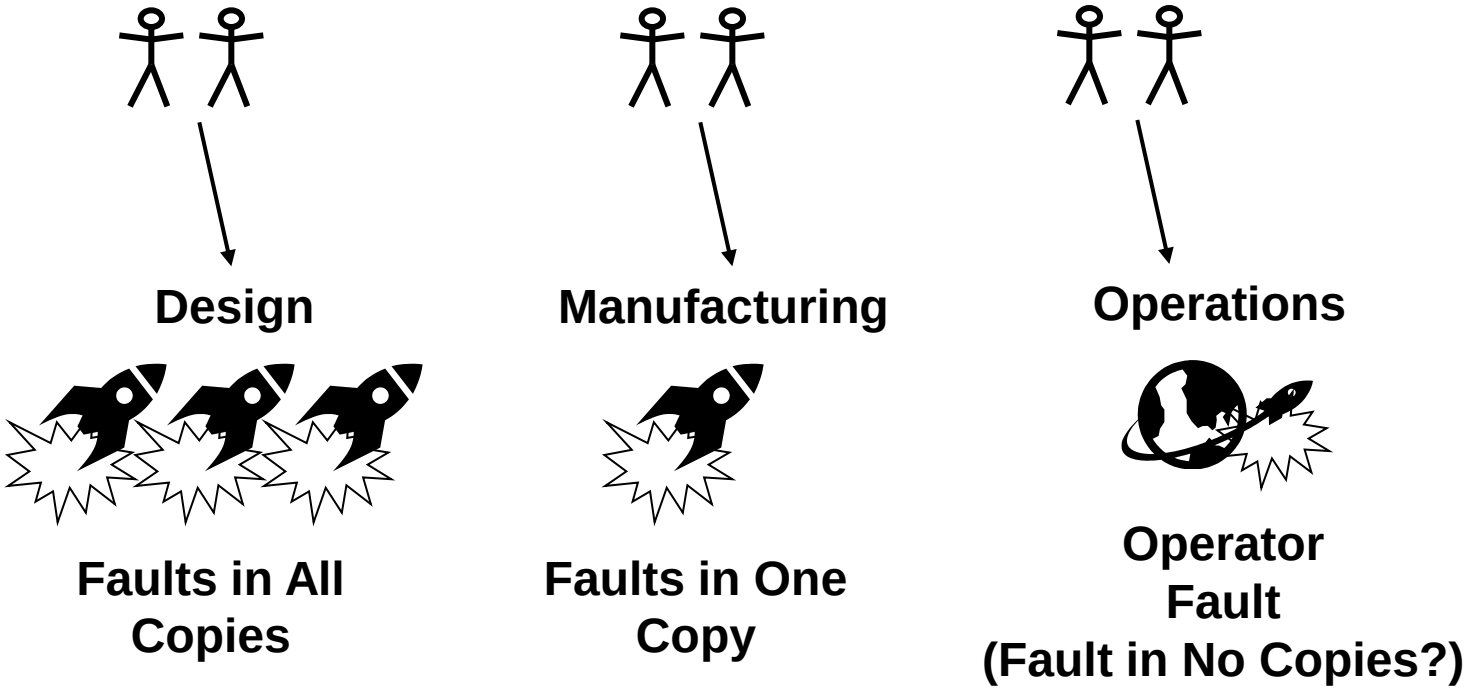
Why do we need an SHM Methodology?

- **Lack of a consistent conceptual basis, common terminology, and defined methodology hinders systems integration and analysis**
  - While often locally effective, the ad hoc methods used in SHM implementations result in gaps and inefficiencies in the overall SHM design (and is especially problematic for system-of-systems programs).
  - These methods are also unable to answer, or only partially address important questions relating to characteristics such as the completeness and effectiveness of the SHM design.
- **Lack of a standard hinders integration and interaction with Systems Engineering, SRQA, and subsystem / disciplinary experts**
- **Move away from the "SHM = technology" viewpoint**
  - This perception among design community hinders application and understanding of SHM

Key ISHM/FM Concepts

- **ISHM/FM exists to protect functionality** (Rasmussen 2008)
- **Operational ISHM/FM design mechanisms operate in a "meta-control loop" to protect or restore functionality** (Albert et al. 1995)
  - 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**
- **SHM/FM is an extension of systems and control theory**
  - Can use systems and control concepts and terminology

Fault Causes and Life Cycle Consequences



Implications: The raw rates of design, manufacturing, and operational faults are fundamentally the same, because they are all based on human failure ("mistake") rates, which are probably about 90-95% for well-trained humans.

SHM Terminology

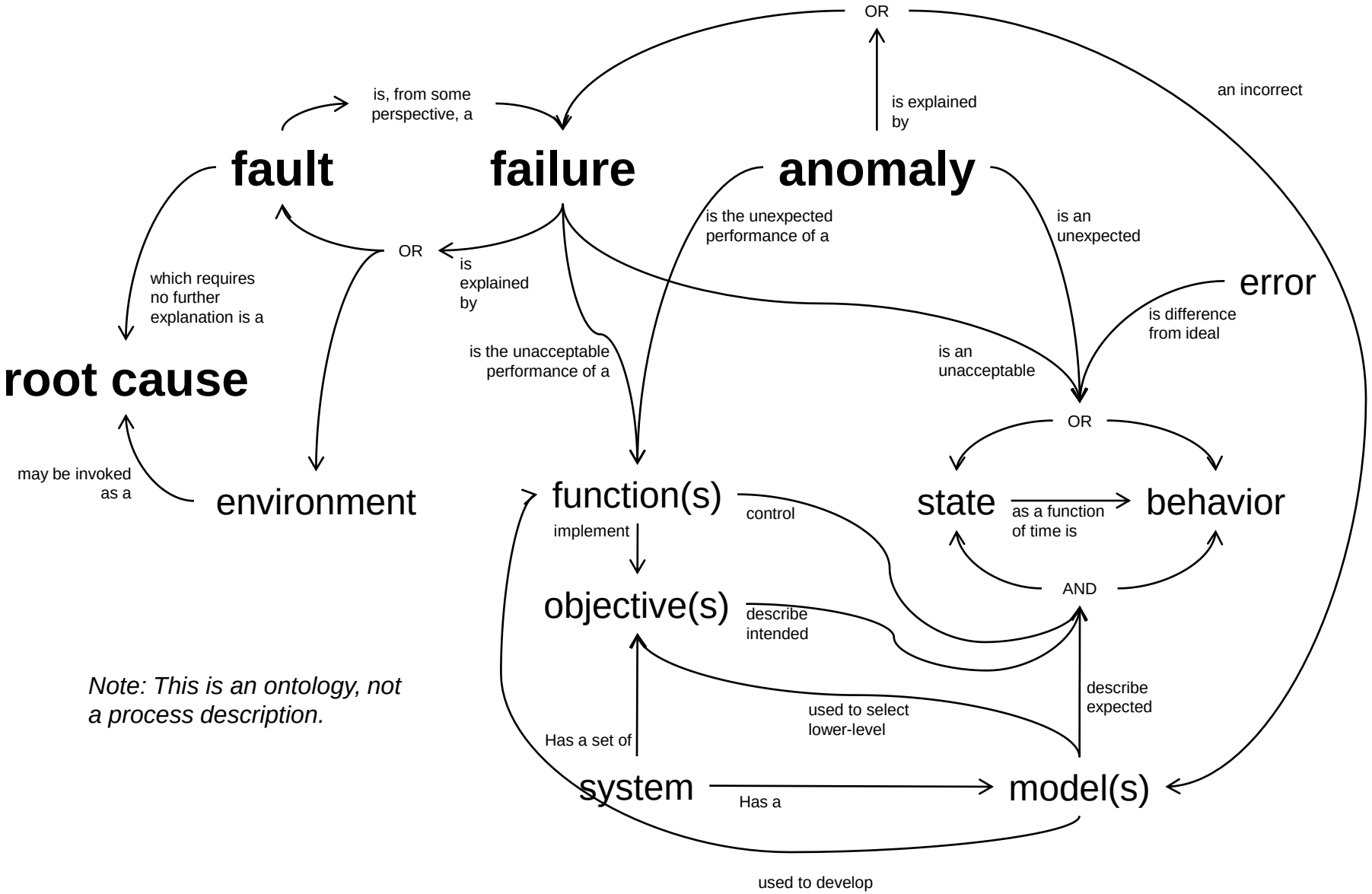
- **Draw from prior work**
  - Avizienis/Laprie[1] and Heimerdinger/Weinstock[2]
    - This work, in turn, traces back to the 1960s and 1970s in computer systems and software dependability theory.

- **Core Terms**
  - Anomaly: The unexpected performance of intended function.
  - Failure: The unacceptable performance of intended function.
  - Fault: A physical or logical cause, which explains a failure.
  - Root Cause: In the chain of events leading to a failure, the first fault or environmental cause used to explain the existence of the failure.

1 - Avizienis, A., Laprie, J-C, and Randell, B. "Fundamental Concepts of Dependability", 3rd Information Survivability Workshop, (ISW-2000), Boston, Massachusetts, October 24-26, 2000

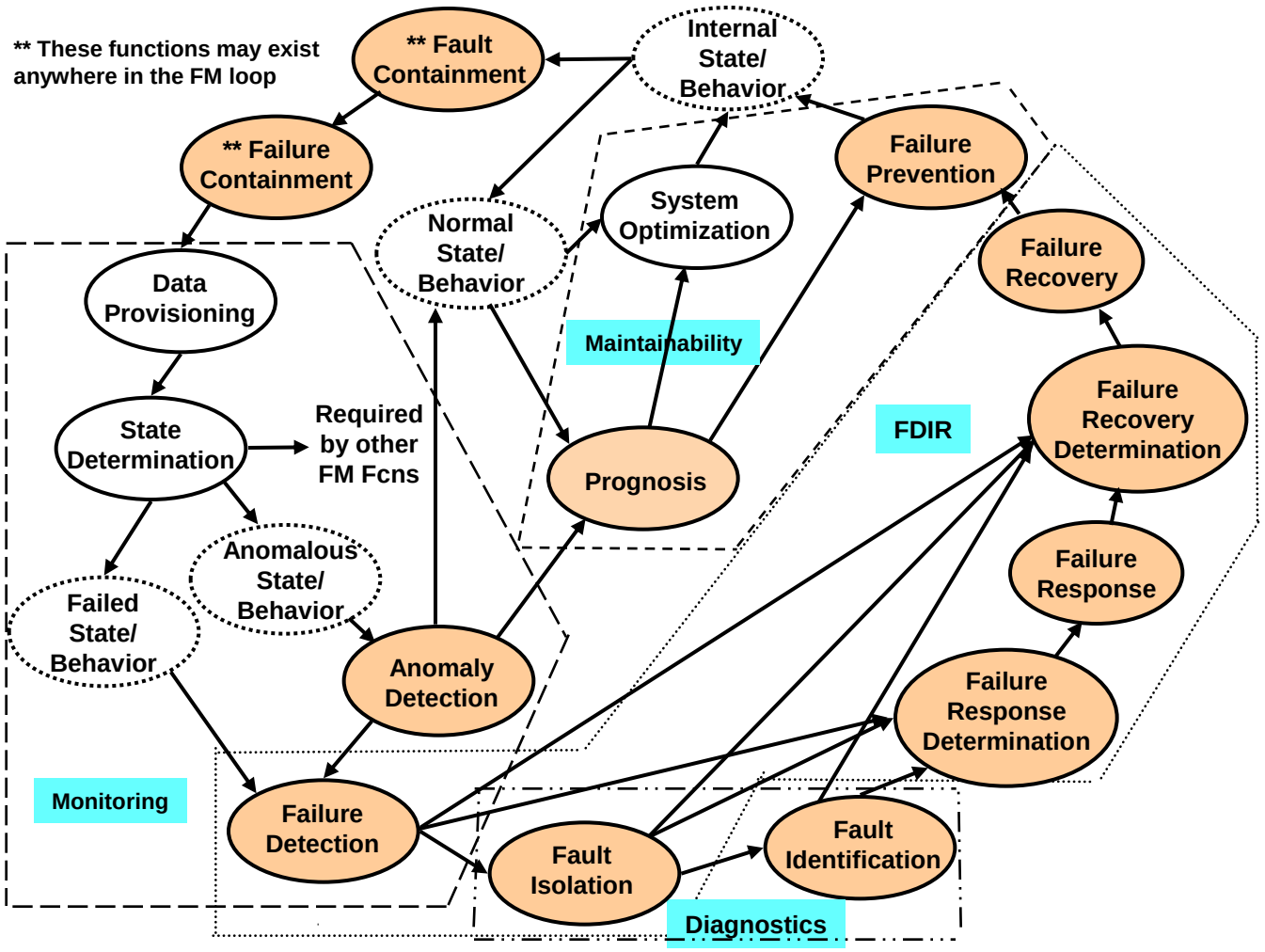
2 - Heimerdinger, W.J., and Weinstock, C.B., *A Conceptual Framework for System Fault Tolerance. Technical Report CMU/SEI- 92-TR-033. Software Engineering Institute, Carnegie Mellon University, October 1992*

FM Terminology: Conceptual Relationships



Note: This is an ontology, not a process description.

FM Operational Functions and Relationships



LEGEND: FM function; non-FM system function; system states

Based on, but evolved from Albert, J., Alyea, D., Cooper, L., Johnson, S., and Uhrich, D. "Vehicle Health Management (VHM) Architecture Process Development," Proceedings of SAE Aerospace Atlantic Conference, Dayton, Ohio, May 1995

FM Terminology: FM Functions

- **FM Functions and Definitions**
  - ***Anomaly Detection***: Deciding that an *anomaly* exists.
  - ***Failure Containment***: Preventing a *failure* from causing further *failures*.
  - ***Failure Detection***: Deciding that a *failure* exists.
  - ***Failure Prevention***: Preventing a *failure* from occurring.
  - ***Failure Recovery***: The actions taken to return the system to normal operations after a *failure*.
  - ***Failure Response***: An action taken to mitigate the effects of a *failure*.
  - ***Fault Containment***: Preventing a *fault* from causing further *faults*.
  - ***Fault Identification***: Determining the possible causes of a *failure*.
  - ***Fault Isolation***: Determining the possible locations of hypothesized *failure* causes, to a defined level of granularity.
  - ***Prognosis***: Prediction of future states or behaviors based upon recent observable states or behaviors.

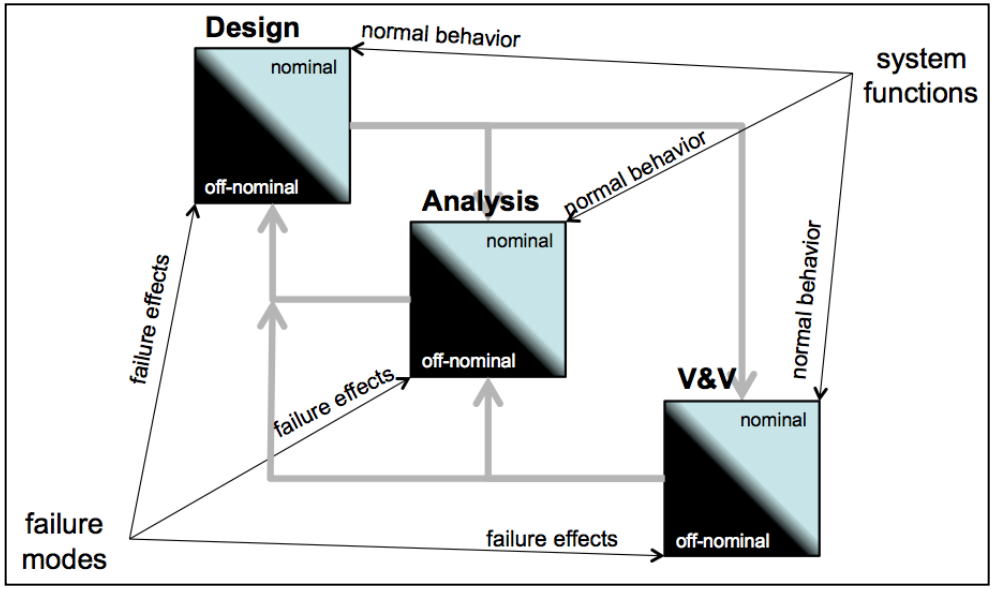
- **Additional Relevant FM Terms**
  - ***Failure Tolerance***: The ability to perform a function in the presence of any of a specified number of coincident, independent *failure causes* of specified types.
  - ***Failure Mitigation***: Active response, and recovery from a *failure* that has occurred.

Function Preservation

- **Standard systems engineering procedure: perform a functional breakdown of the system, which defines the functions the system must perform to achieve its goals**

- **Rasmussen's insight[1] that SHM acts to preserve function implies one of the primary ways in which SHM can be tied to the systems engineering process**

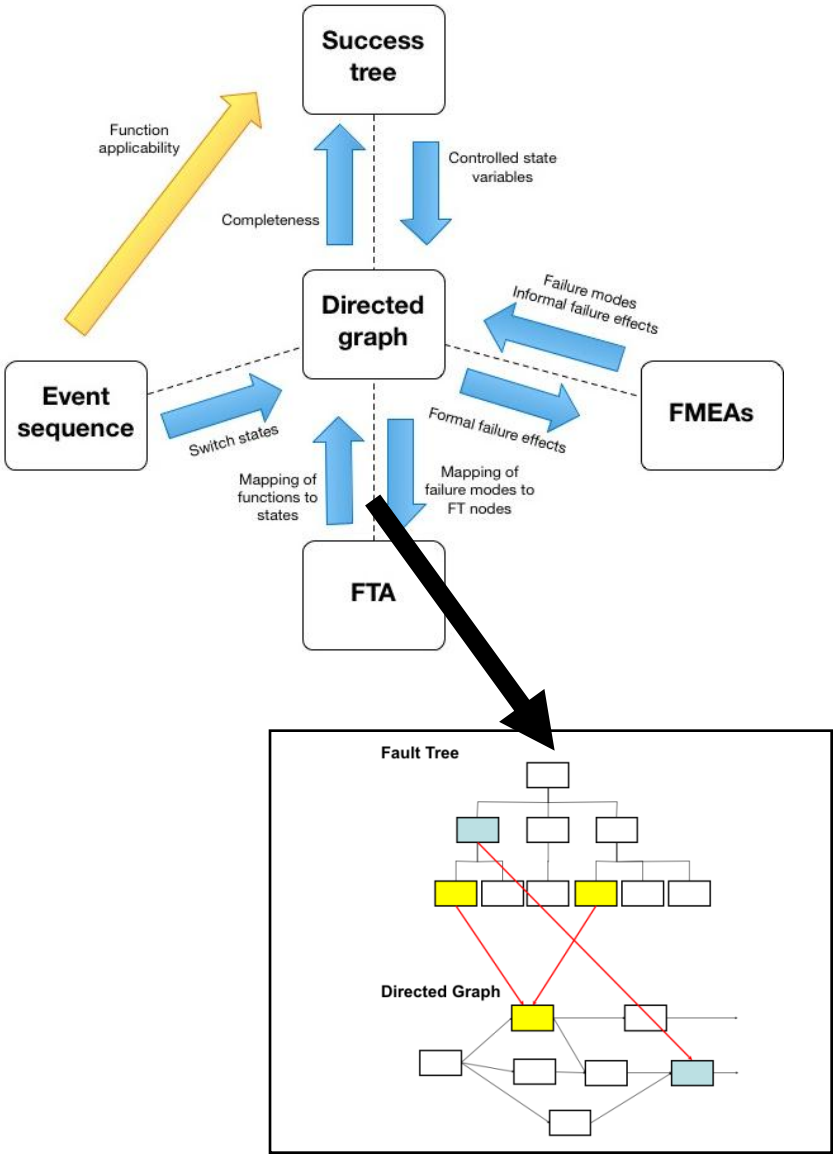
  - **Each system function has the possibility of failure, the "dark side" that must be addressed in design, analysis, and V&V.**
    - FM goal to preserve functionality in the face of impending or actual failure implies that each function can and should be assessed from the standpoint of how that function can be preserved or protected.
    - Function tree provides a mechanism to assess nominal design completeness, and also provides a mechanism to assess FM completeness.



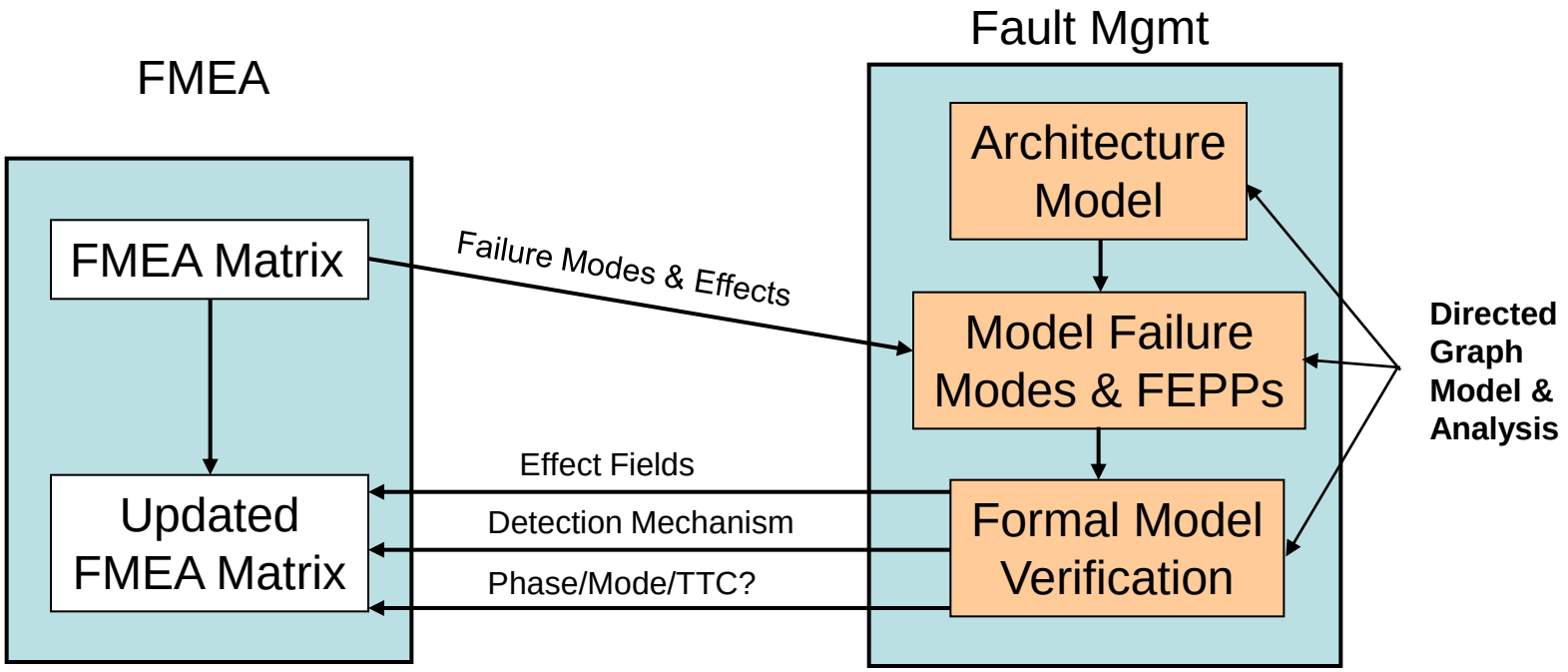
1 - Rasmussen, R.D., "GN&C Fault Protection Fundamentals," 31st Annual American Astronautical Society Guidance, Navigation, and Control Conference, AAS 08-031, Breckenridge, Colorado, February 1-6, 2008.

Representations and Relationships

- **Success Trees**
  - Represent system functions and functional decomposition
  - Conditions for success; "light" side
- **Fault Trees**
  - Represent system functions and paths to failure of top event
  - Conditions for failure; "dark" side
- **Directed graphs**
  - Represent components and connections/interfaces
  - Modeling of physical and logical connections enables formal modeling of failure effect propagation
- **Failure Modes and Effects Analyses (FMEA)**
  - Description of the failure modes (mechanisms) and the immediate failure effect
  - Modeled failure effect propagation enables formal and complete development of all failure effects
- **Event Sequences**
  - Describes system functionality as a function of time
  - Provides "triggers" to enable/disable elements of directed graph representation

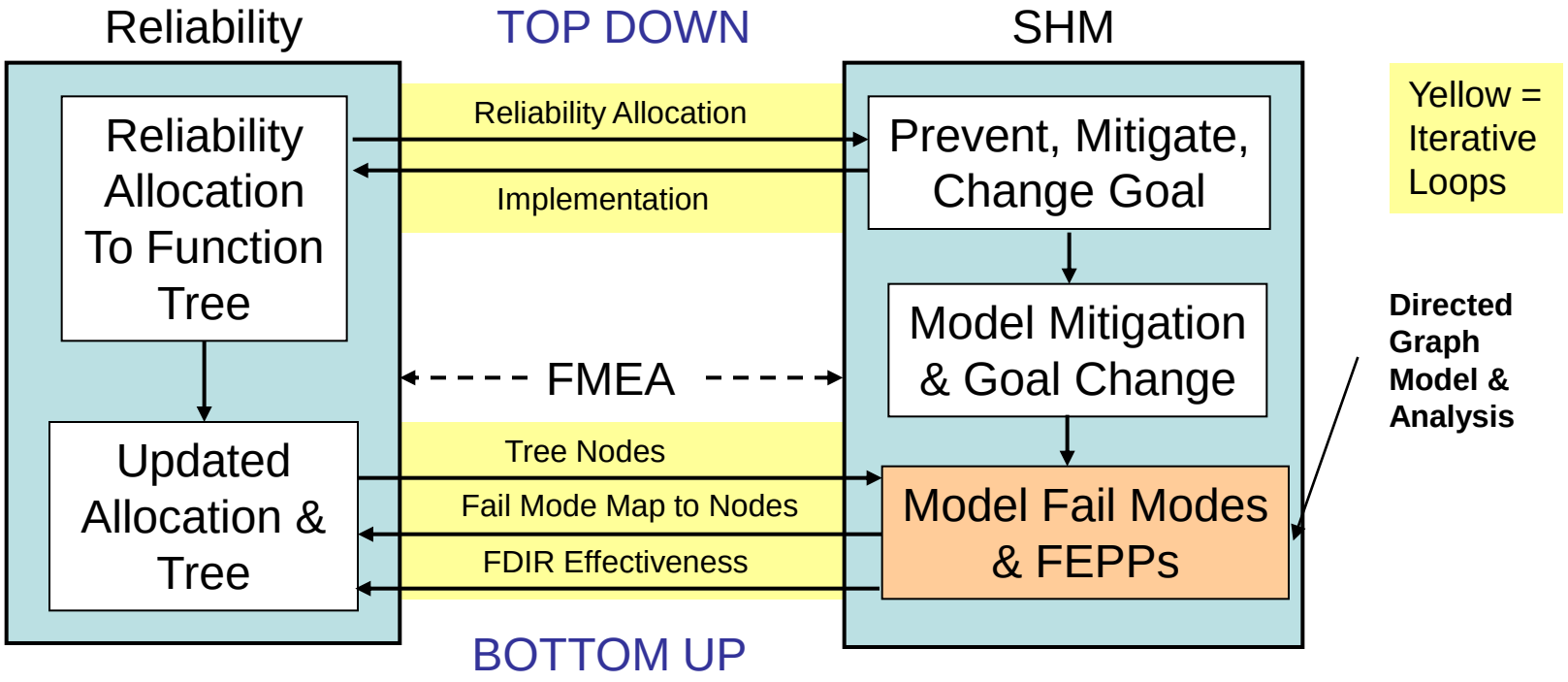


FMEA - SHM Relationships



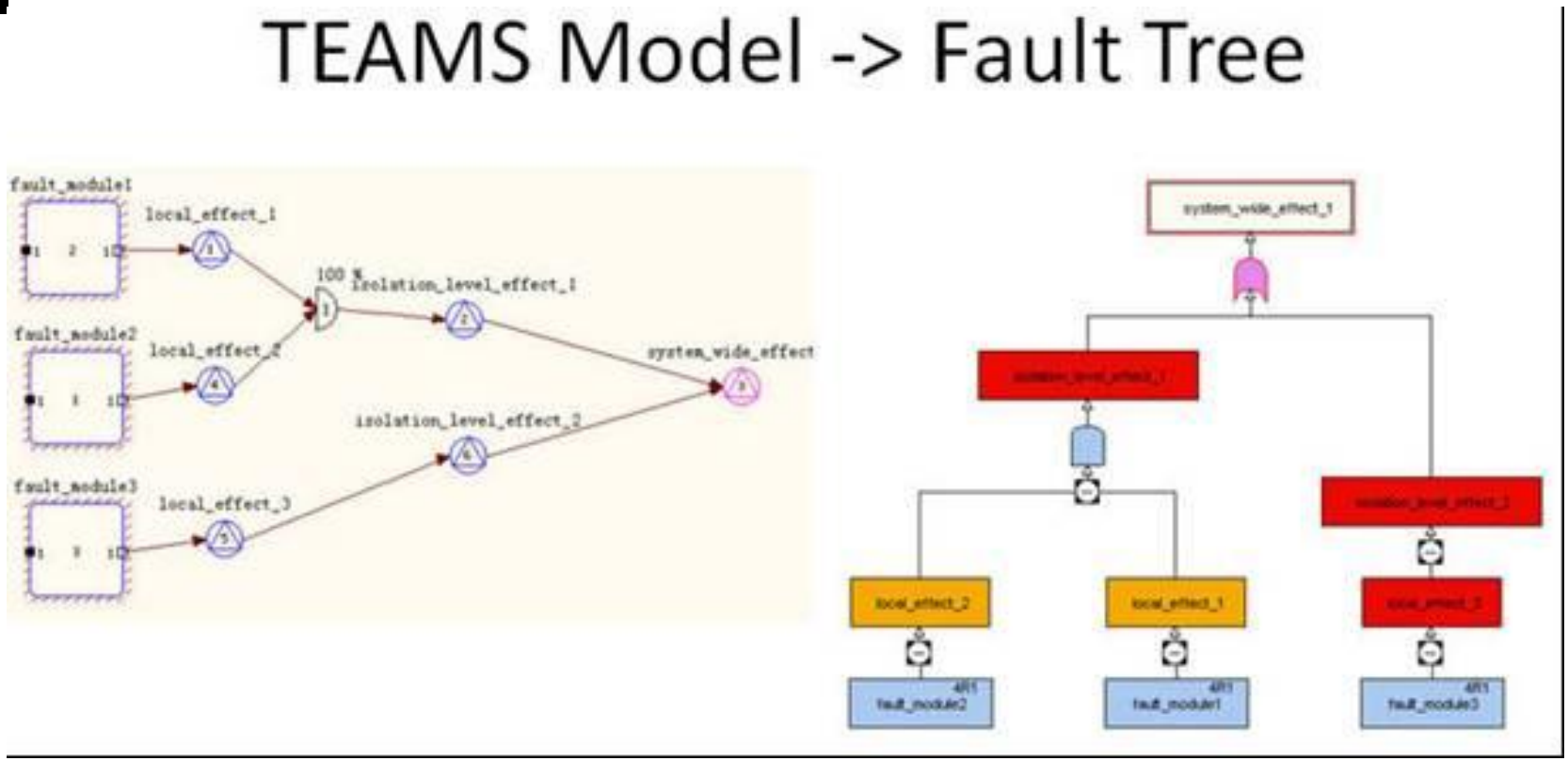
- **Formal model verified with designers & FMEA analysts**
  - Formal meeting ensures deeper communication and learning
- **Phase/mode and Time-to-Criticality info could be provided**
- **SW and human FMEA just as important as hardware**

Reliability-SHM Interaction



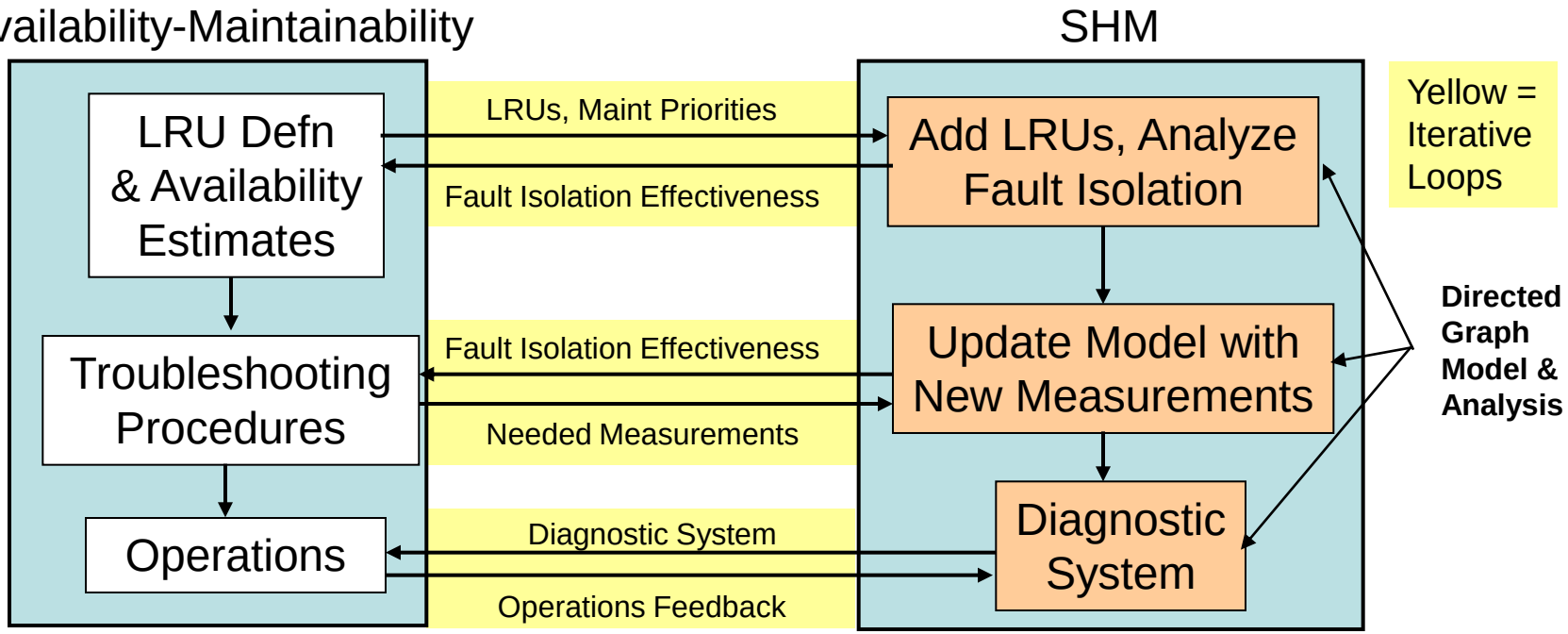
- **SHM design has been ad hoc, bottom-up process with subsystem designers determining their redundancy approach & FDIR, and SHM experts "patching up" the integration**
  - Change to an initial top-down process based on functions and reliability
- **SHM can provide formal map of failure modes to reliability nodes in architectural (not tree) model**
- **SHM provides metrics of failure detection, isolation, and response**

Directed Graph to Fault Tree



- **Fault tree developed to level of key intermediate failure effects and failure detections**
- **Directed graph provides mapping from intermediate failure effect to the failure modes**

SHM – Availability / Maintainability / Pre-Launch Operations



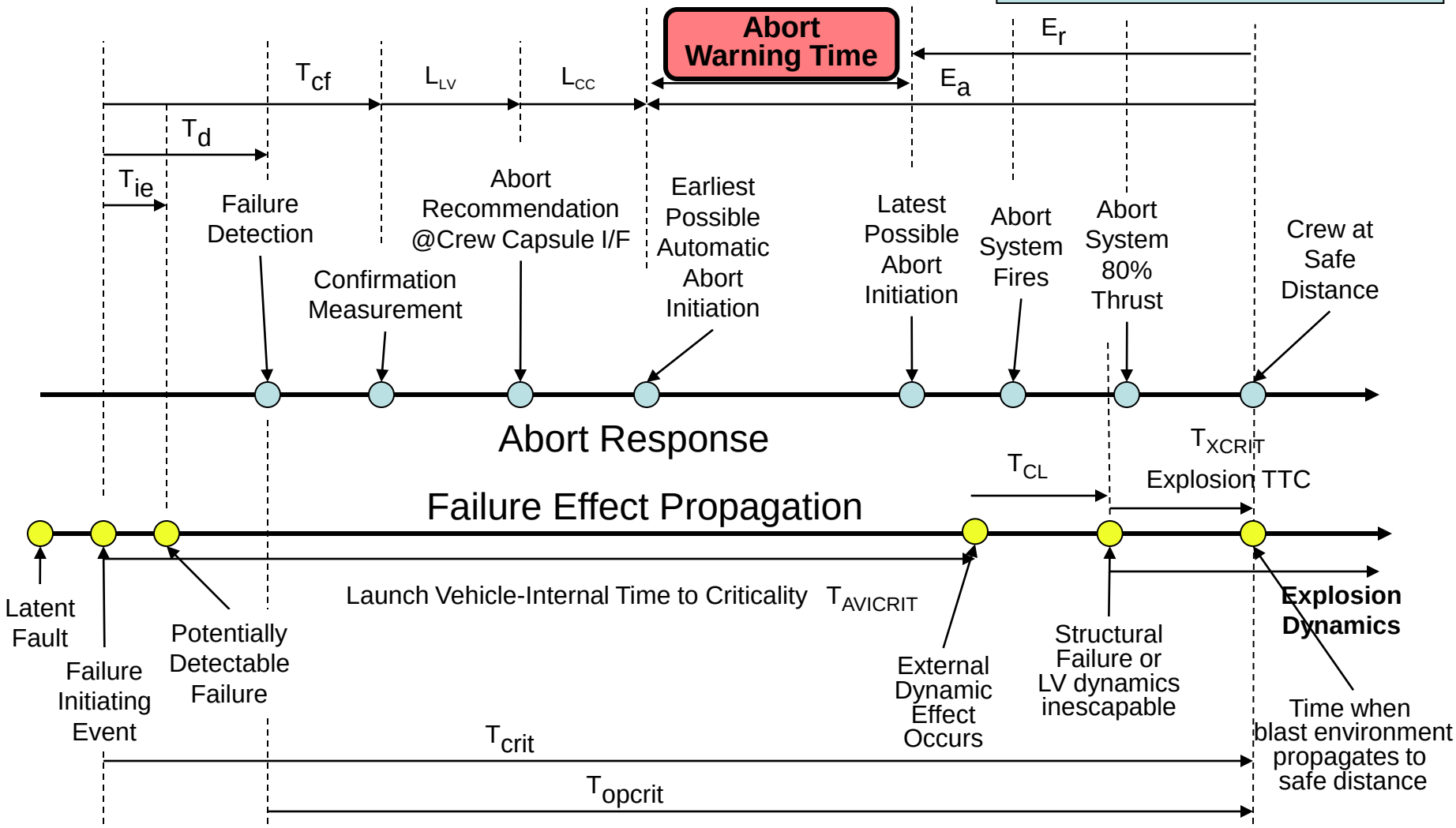
- **SHM Diagnostic Model can assess capability of vehicle and ground measurements to isolate faults**
  - A-M can use to support availability model and troubleshooting procedures
- **SHM Diagnostic Model forms core for Diagnostic System, which automates fault isolation**
  - Pre-launch for launchers, in-flight for crew capsule (though system could be on the ground with Mission Systems)

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



Status of CxP FM Team

- **Aiming to "wrap up" work by September 30**

- **Develop and document as far as possible in remaining time:**
  - Ideal FM requirements
  - FM Terminology
  - FM Methodology
  - Connection to Systems Engineering processes
  - FM Architectural representation(s)
  - "Ideal" FM Plan

Status of FM Handbook

- **Headed by Lorraine Fesq (JPL)**
- **Proposal in 2009 to Office of Chief Engineer, approved**
- **Project briefly canceled Jan 2010, then reinstated Mar 2010**
- **SMD FM Handbook now in planning, should start by May/June 2010**
- **NESC/OCE interested in providing funds, expand to agency-level**
- **Task team organized, funding and NASA institutional arrangements in work**

Status of SHM Reference Text

- **Based on papers from 2005 ISHEM Forum**
  - Forum organized so as to create the chapters for the book
  - Each paper a general overview
- **Contract signed with John Wiley UK in 2008**
- **Title: *System Health Management: With Aerospace Applications***
- **General Editor, Stephen Johnson**
- **32 of 41 chapters delivered, 27 have been reviewed by general editor**
  - Drafts exist for all others
  - Remainder to be delivered to general editor by early May
  - Final reviews in July/August
- **Manuscript delivery scheduled for 30 September 2010**
- **Publication 2011**

SHM Reference Text Outline

- **Part I: SHM and its Socio-Technical Context (*Mott*)**
- 1 SHM Theory (*Johnson*)
- 2 Multi-Model Communication (*Sauer & Tenney*)
- 3 High Reliability Organizations (*Wiedlea*)
- 4 Knowledge Management (*Rogers*)
- 5 Business Case for SHM (*Wilmering*)

- **Part II: SHM and the System Life Cycle (*Kessler*)**
- 6 Systems Engineering and Integration (*Wilmering, Mott*)
- 7 Architecture (*Kessler, Deal*)
- 8 Design Methods and Fault Management (*Tumer*)
- 9 Technical Readiness Assessment (*Mackey*)
- 10 Verification and Validation (*Markosian, Feather, Brinza*)
- 11 Certification and Standards (*Kessler*)

- **Part III: Analytical Methods (Patterson-Hine):**
- 12 Physics of Failure (*Jata*)
- 13 Failure Assessment (*Lutz, Nikora*)
- 14 Safety and Hazard Analysis (*Leveson*)
- 15 Reliability Analysis (*Meeker, Escobar*)
- 16 Probabilistic Risk Assessment (*Vesely*)
- 17 Diagnostics and Testability (*Patterson-Hine, Aaseng, Biswas, Narashimhan, Pattipati*)
- 18 Prognostics (*Roemer & Kacprzynski*)
-

- **Part IV: Operations (Reichard)**
- 19 Quality Assurance (*Hughitt*):
- 20 Maintainability (*O'Neill*):
- 21 Human Factors (*McCann, Spirkovska*):
- 22 Launch Operations (*Waterman*):
- 23 Mission Operations (*O'Hagan & Crocker*):
- 24 Logistics (*Crow*)

SHM Reference Textbook Outline

- **Part V: Subsystems Health Management (*Scandura*)**
- 25 Aircraft Propulsion Health Management (*Volponi, Wood*)
- 26 Intelligent Sensors for Health Management (*Hunter, Oberle, Baaklini, Perotti, Hong*)
- 27 Structural Health Management (*Chang, Markmiller, Yang, Kim*)
- 28 Electrical Power Health Management (*Button, Chicatelli*)
- 29 Avionics Health Management (*Watson, Varnavas, Patrick, Chau, Hodge, Baroth*)
- 30 Fault Tolerant Architectures for Health Management (*Siewiorek, Narasimhan*)
- 31 Flight Controls Health Management (*Zinchuk, Hammett, Zinfer*)
- 32 Life Support Health Management (*Kortenkamp, Biswas, Manders*)
- 33 Software (*Scandura*)

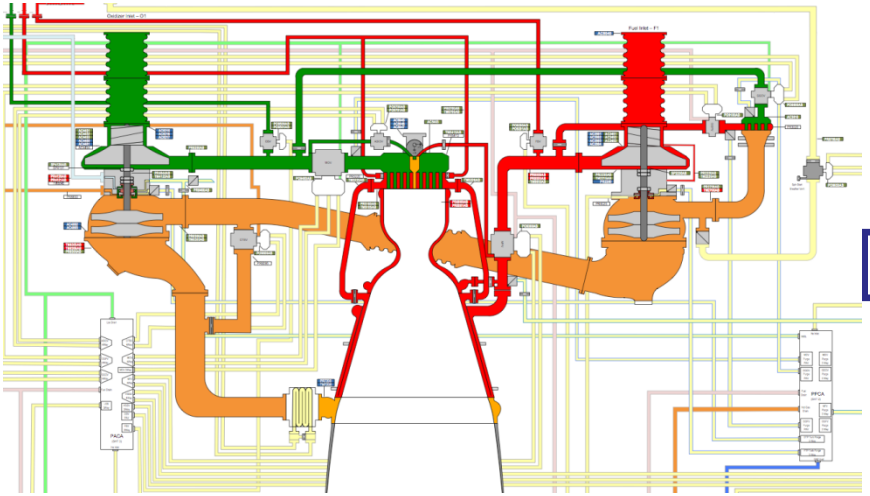
- **Part VI: Systems (Gormley)**
- 34 Launch Vehicle Health Management (*Brown & Kelley*)
- 35 Robotic Spacecraft Health Management (*Morgan*)
- 36 Tactical Missiles Health Management (*Kudiya & Marotta*)
- 37 Strategic Missiles Health Management (*Ruderman*)
- 38 Rotorcraft Health Management (*Dempsey & Zakrajsek*)
- 39 Commercial Aviation Health Management (*Scandura, Bird, Christensen, Lutz*)
- 40 Military Aircraft Health Management (*Derriso*)
- 41 System of Systems Health Management (*DiMario, Gormley*)

Backup Slides

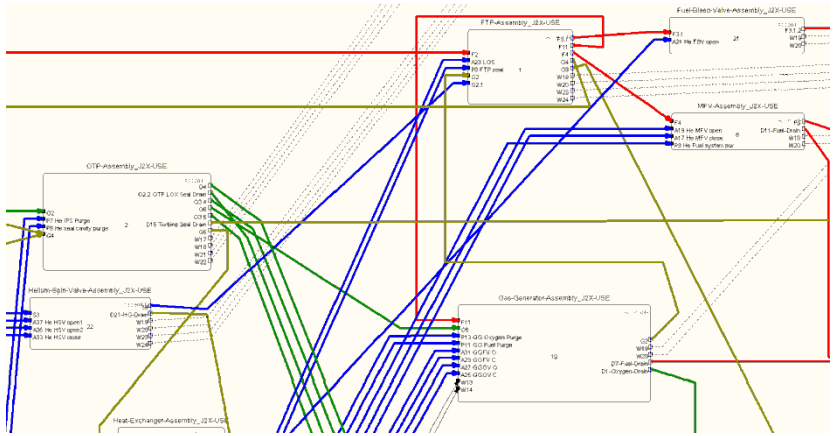
Directed Graph Modeling

- **… 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

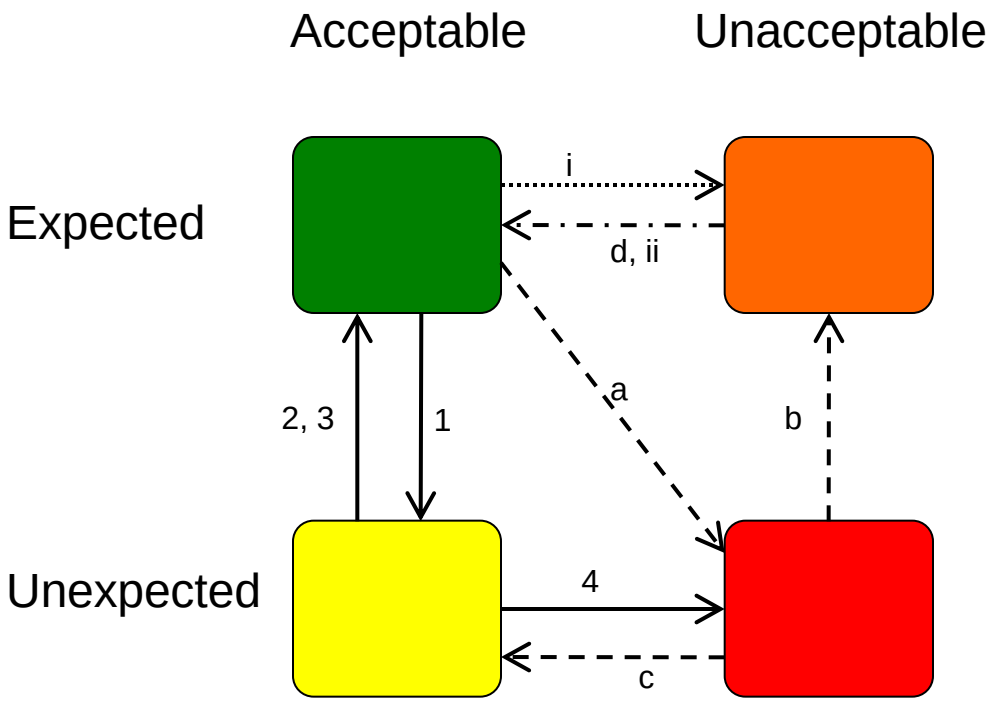


Upper Stage Engine Schematic



Functional Model in TEAMS

Progression of Anomalous/Failed States



Anomaly, no Failure

1) current value of state reaches an unexpected value
2) review of system data indicates that model/expectation is invalid, and state is expected (expectations changed) [e.g., noise in RF link due to un-modeled effect]

- model reviewed and parameters adjusted until model predicts current behavior (e.g., if RWA unhealthy, will have larger attitude errors)
- review of system data indicates that this is an unacceptable value (indicative of a failure; the goal is adjusted)

Anomaly, with Failure

a) current value of state unexpectedly reaches an unacceptable value
b) model reviewed and parameters adjusted until model predicts current behavior (e.g., if IMU1 unhealthy, will have attitude failure)

- review of system data indicates that model/expectation is invalid, and state is acceptable (expectations changed)
- recover intended functionality by restoring state to acceptable value and/or changing functional goal

Failure, no Anomaly

i. expected condition results in failure
ii. recover intended functionality by restoring state to acceptable value and/or changing functional goal