System Health Management Theory and Design Strategies

Stephen B. Johnson,
NASA MSFC and University of Colorado at Colorado Springs
and
John C. Day,
Jet Propulsion Laboratory, California Institute of Technology

Agenda

- Context
- System Health Management Principles
- Fault Management Functions
- SHM in the Early Design Process
- Conclusion

Context

- **System Health Management (Reliability, Fault Tolerance, Fault Protection, VH Monitoring, VH Mgmt, Dependability, ISHM, PHM, Fault Mgmt, etc.)**
  - Has evolved from the 1940s until now to address the analysis, design, testing, and operation of complex systems under current or predicted failure conditions
  - We draw from much of this work, particularly the Fault Protection, SHM, and Dependability heritage from the 1980s – 2000s---sophisticated work in terminology and control concepts
    - Avizienis & Laprie, Rasmussen, earlier work by Johnson et al.

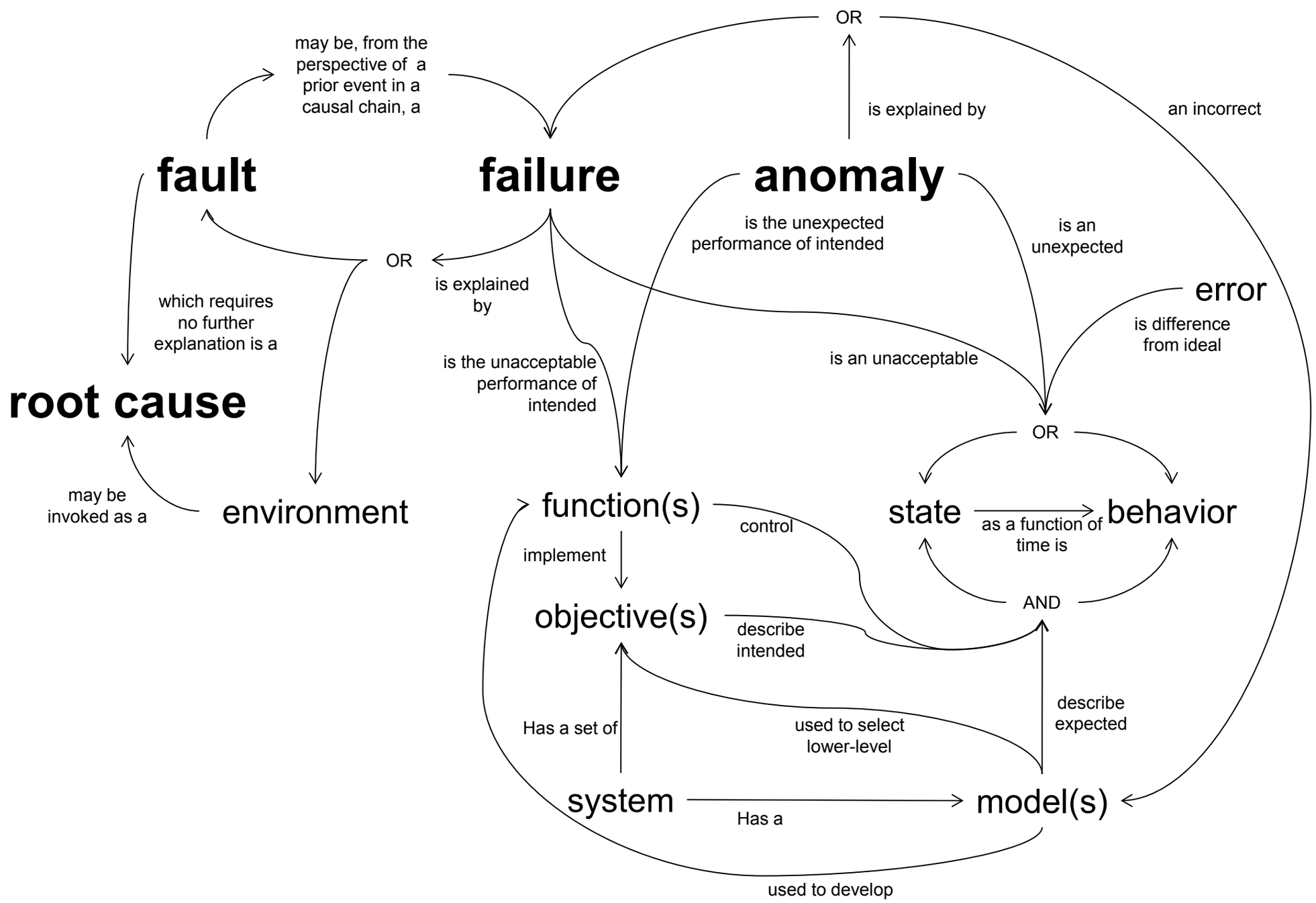
- **A "critical mass" seems to have developed in the late 2000s**
  - SHM Textbook, NASA FM Handbook, ESA SHM Standard
  - PHM Society & Journal
  - Several dedicated conferences & major blocks of other conferences
  - Recognition of ISHM / FM / SHM / diagnostics in DoD and NASA
  - NASA CAIB and DoD Oversight / Insight Issues
  - NASA Science Mission Directorate Issues

- **Institutional Context**
  - Ares I (M. Watson) and (now) Space Launch System FDDR (M. Bodiford)
  - System Health Management: with Aerospace Applications (reference text---thru MSFC EV43)
  - Constellation SE&I/SAVIO (SW&Avionics Integration Office, R. Morillo)
  - NASA SMD FM Handbook (L. Fesq)

Disciplinary Definitions

- **System Health Management =** *the capabilities of a system that preserve the system's ability to function as intended*.
- **Dependability =** *the ability of a system to function as intended.*
- **Therefore, SHM =** *the capabilities of a system that provide dependability***.**
- **Fault Management:** *the <u>operational</u> capabilities of a system that provide dependability*.
- **FM = operational subset of SHM**
  - Alternative: FM as a synonym of SHM… we will not use this interpretation here
- **SHM includes design-time prevention of failures through design margins and quality assurance, as well as operational prevention and mitigation (FM)**

Terminology Concept Diagram

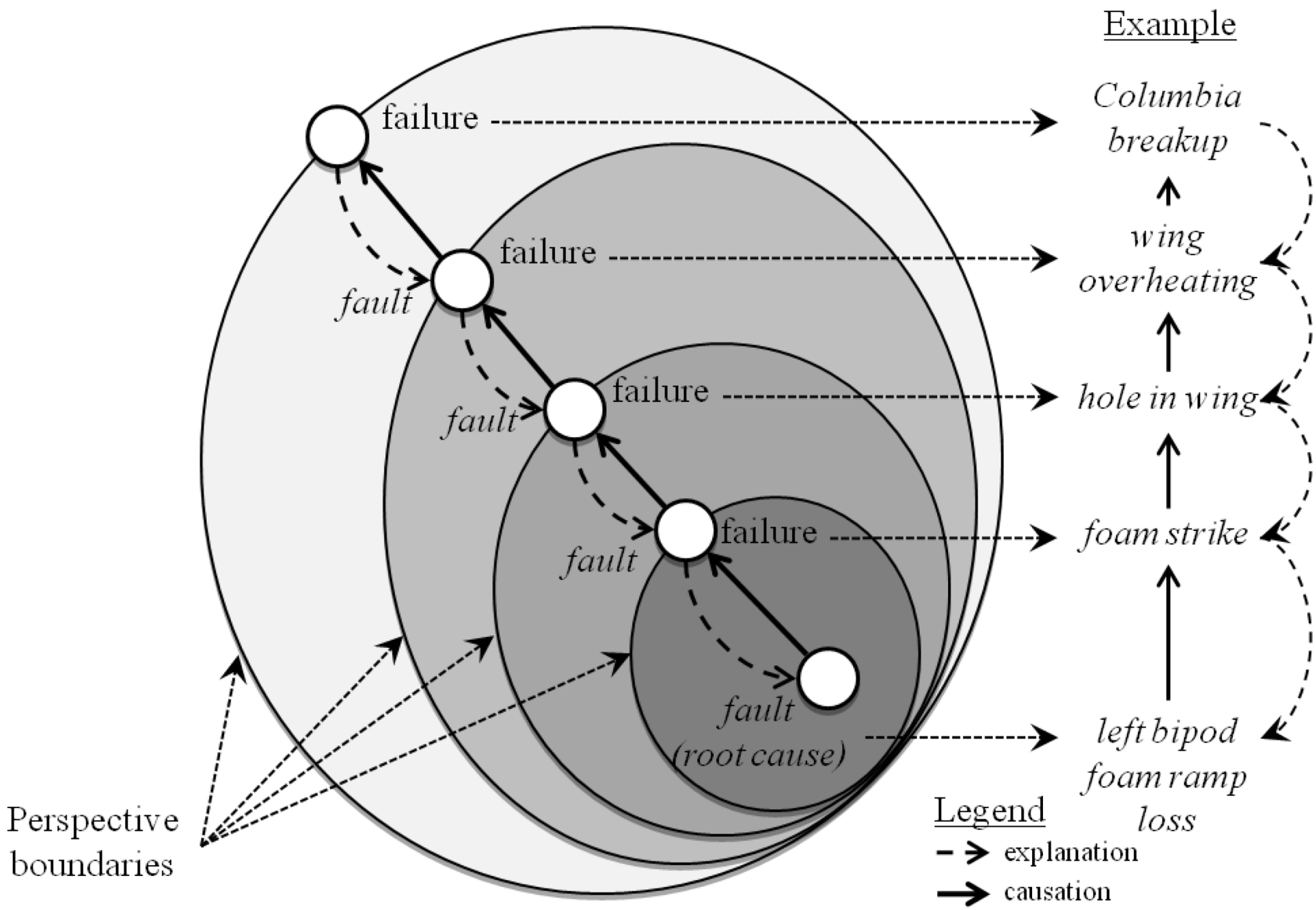


Core and System Terms

- **Core Terms**
  - ***Degradation:*** The decreased performance of intended *function*.
  - ***Anomaly***: The unexpected performance of intended *function*.
  - ***Failure***: The unacceptable performance of intended *function*.
  - ***Fault***: A physical or logical cause internal to the system, 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*

- **System Terms**
  - **System:** A combination of interacting elements organized to achieve one or more stated purposes.
  - **State:** The value of a set of physical or logical state variables at a specified point in time.
  - **Behavior:** The temporal evolution of a *state*.
  - **Function:** The process that transforms an input *state* to an intended output *state*.
  - **Control Error**: The deviation between the *estimated state* and the ideal intended *state*.
  - **Nominal**: The *state* of the *system* when the output *state* vector matches the intentions of the designer and/or operator.
  - **Expectation**: The most likely predicted *state* or *behavior*.

Fault – Failure Recursion



SHM Principles (1)

- SHM utilizes basic concepts of systems theory, including the system boundary, hierarchical decomposition, and recursion.

- SHM exists to preserve system functionality.
  - $\boldsymbol{y} = f(\boldsymbol{x})$, the function f transforms the input state vector $\boldsymbol{x}$ into the output state vector $\boldsymbol{y}$
  - SHM ensures the transformation f occurs properly

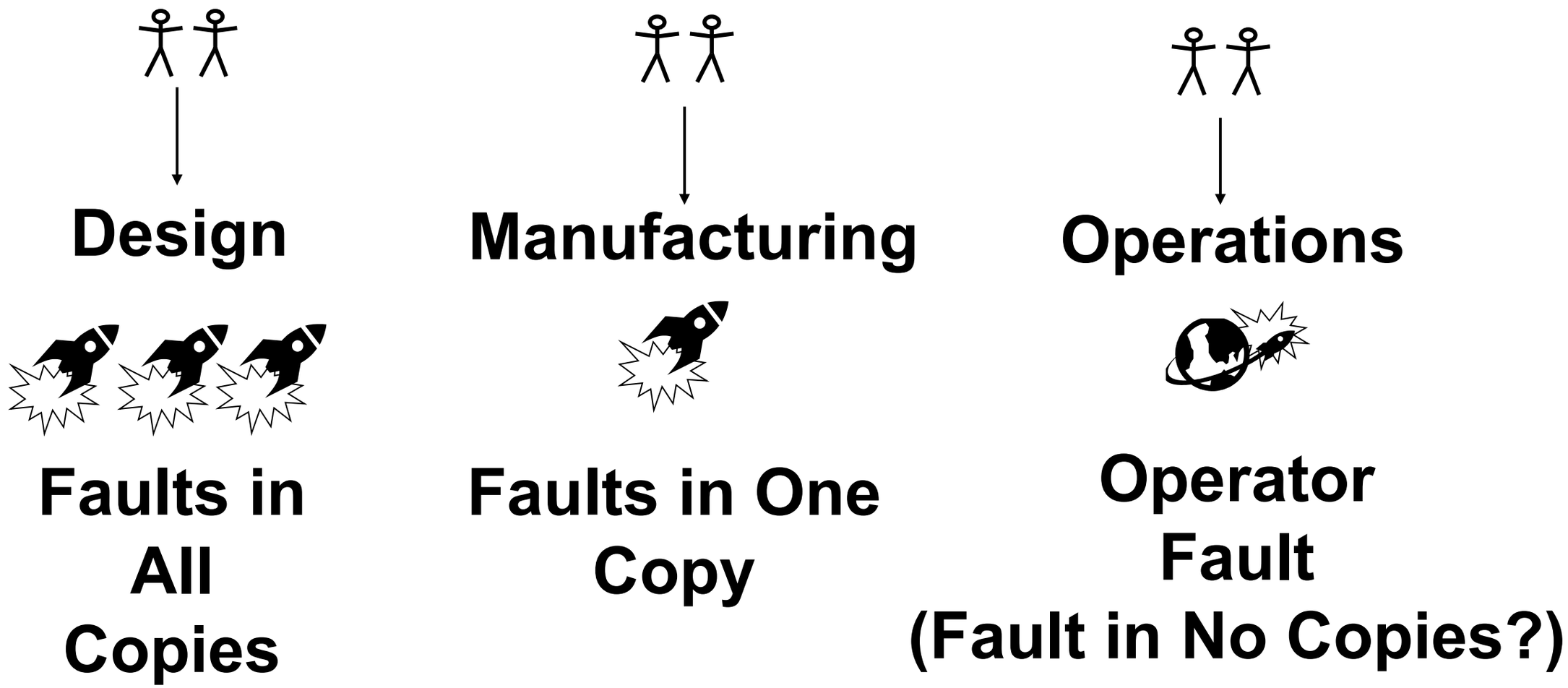
- Classification of states is based on models that define individual and group expectations of system behavior. Reclassification of a state is based on modification of the model(s) that define behavioral expectations.
  - “Normalization of deviance” (Vaughan) is a “normal” activity

- There are three categories of off-nominal states: anomalies, degradations, and failures. Anomalies refer to knowledge errors, and failures and degradations refer to control errors.

- Faults are causes of (explanations of) failure internal to the system. Fault and failure are recursive concepts.

SHM Principles (2)

- The root causes of the vast majority of failures are human communicative and cognitive faults.
  - SHM must account for design, manufacturing, and operations faults
  - Rates of fault occurrence roughly equal, based on amount of human touch-labor with the system
  - Human fault rates are roughly 1-10% for well-trained humans
  - The remaining failures caused by system wear-out and environmental causes

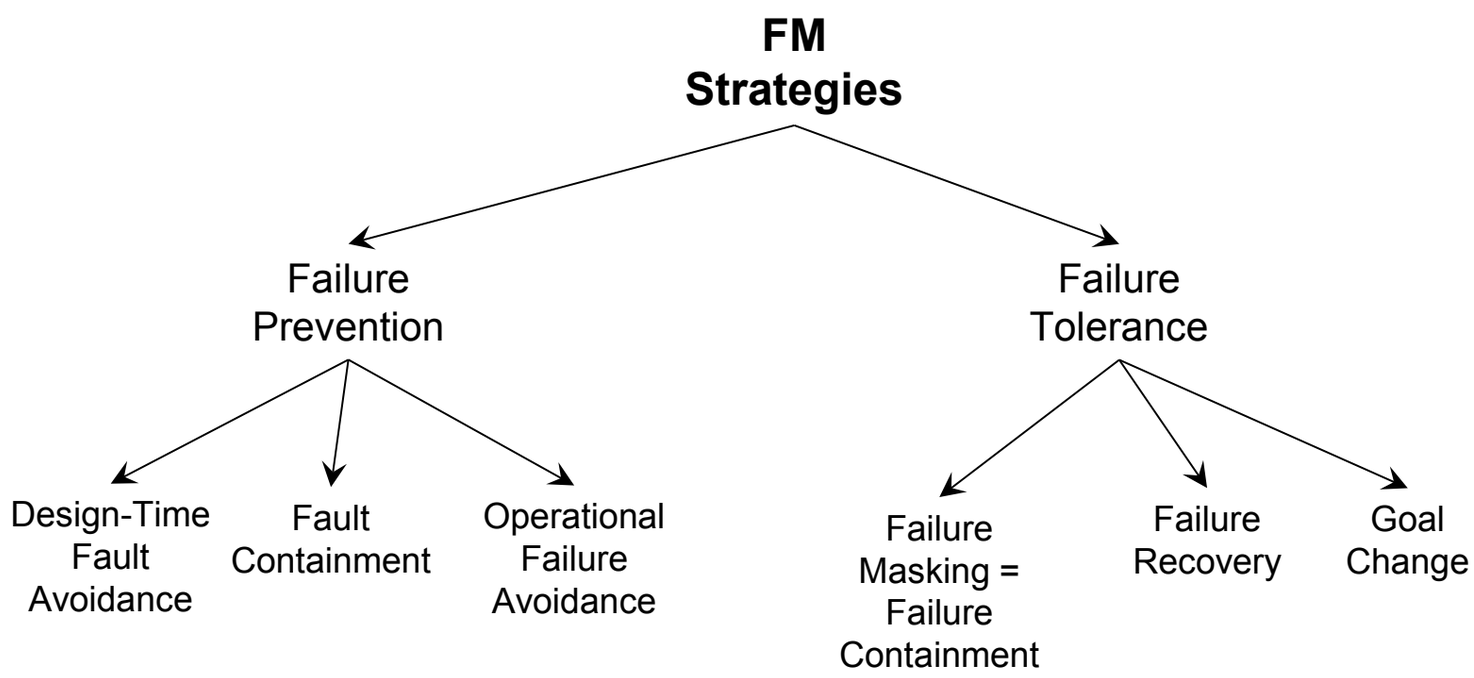


SHM Principles (3)

- Humans build complex systems that they cannot fully understand. SHM must address failures due to unpredicted causes.

- SHM is deployed based on assessment of the risk to the system should a system function fail.
  - See the early design process description later in this presentation

- SHM strategies to preserve system function are: design-time fault avoidance, fault containment, operational failure avoidance, failure masking, failure recovery, and goal change.



SHM Principles (4)

- Operational Fault Management is an extension of control theory, in that it provides control regimes to enable system function in the presence of failures that are, or are predicted to become, beyond the ability of the normal (passive or active) control system to successfully maintain function.

- Control theory ideas such as characteristic times (FM Control Loop (FMCL) latency versus failure effect propagation times to the Critical Failure Effect (CFE)), knowledge and control errors, and state estimation versus control functions extend directly to Fault Management.
  - Failure detection, diagnosis, and response—the FMCL latency must complete before failure effects reach the CFE when mission objectives are compromised.

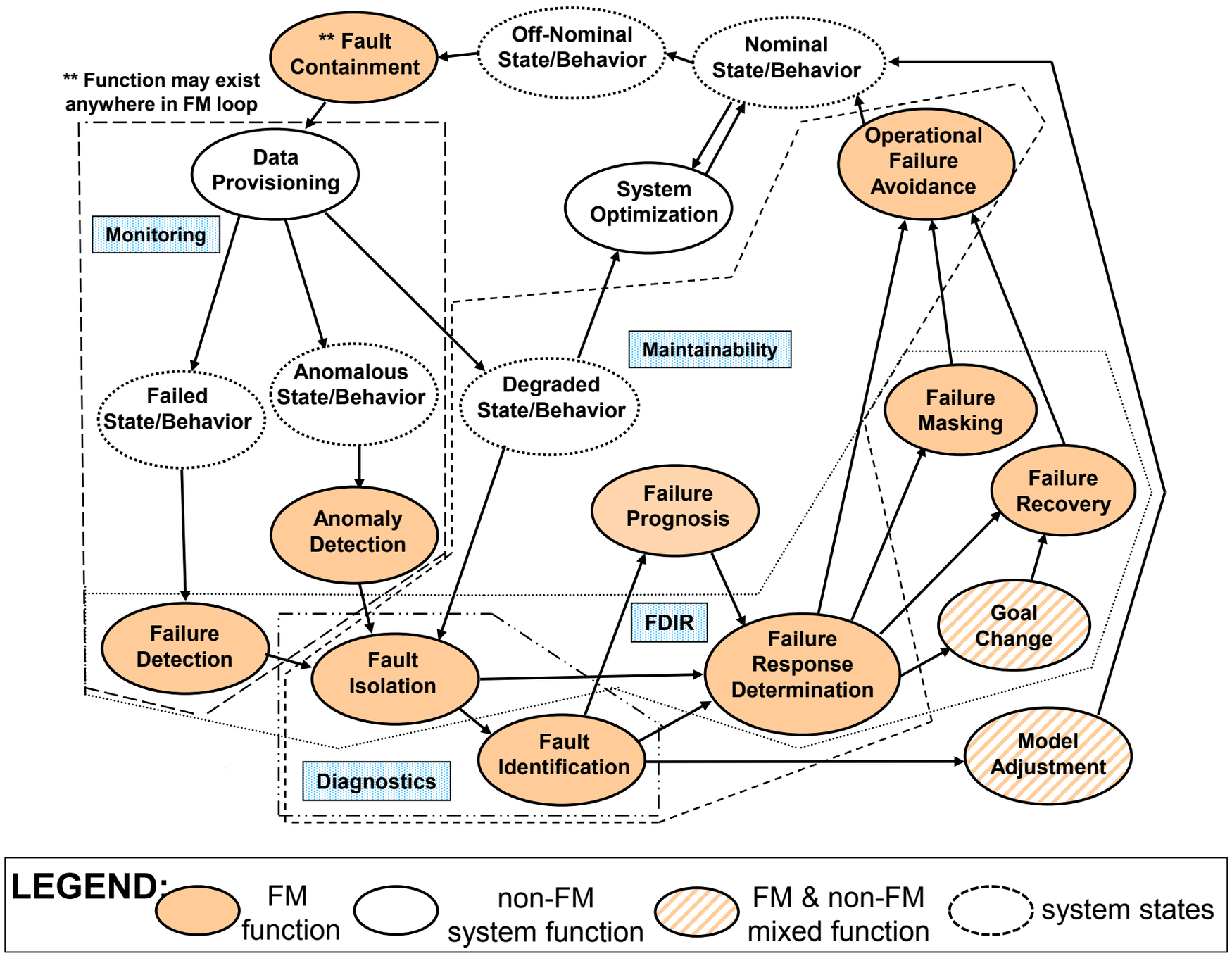
- ***All*** operational Fault Management implementations use some form of redundancy.
  - Identical redundancy
  - Functional (analytic, dissimilar) redundancy
  - Information redundancy (e.g.: EDAC)
  - Temporal redundancy (e.g.: multiple commanding, checkpoint-rollback)
  - Knowledge redundancy (e.g.: thresholds set based on physics-based analysis---alternate knowledge about the system, separate from the system itself)

FM as an Extension of Control Theory

- **The control system perspective brings with it several important concepts of relevance to FM**
  - Key terminology and the concepts embedded in this terminology.
    - e.g., specifying system boundaries, and delineating between the control system and the system under control
  - Importance of time in the ability of any control system to control the relevant state variables.
    - Every state variable to be controlled has a “characteristic time” associated with how quickly the phenomenon it represents can change, based on the physics related to that state variable.
      - The control system must operate on a time scale that is similar or faster than the variable to be controlled.

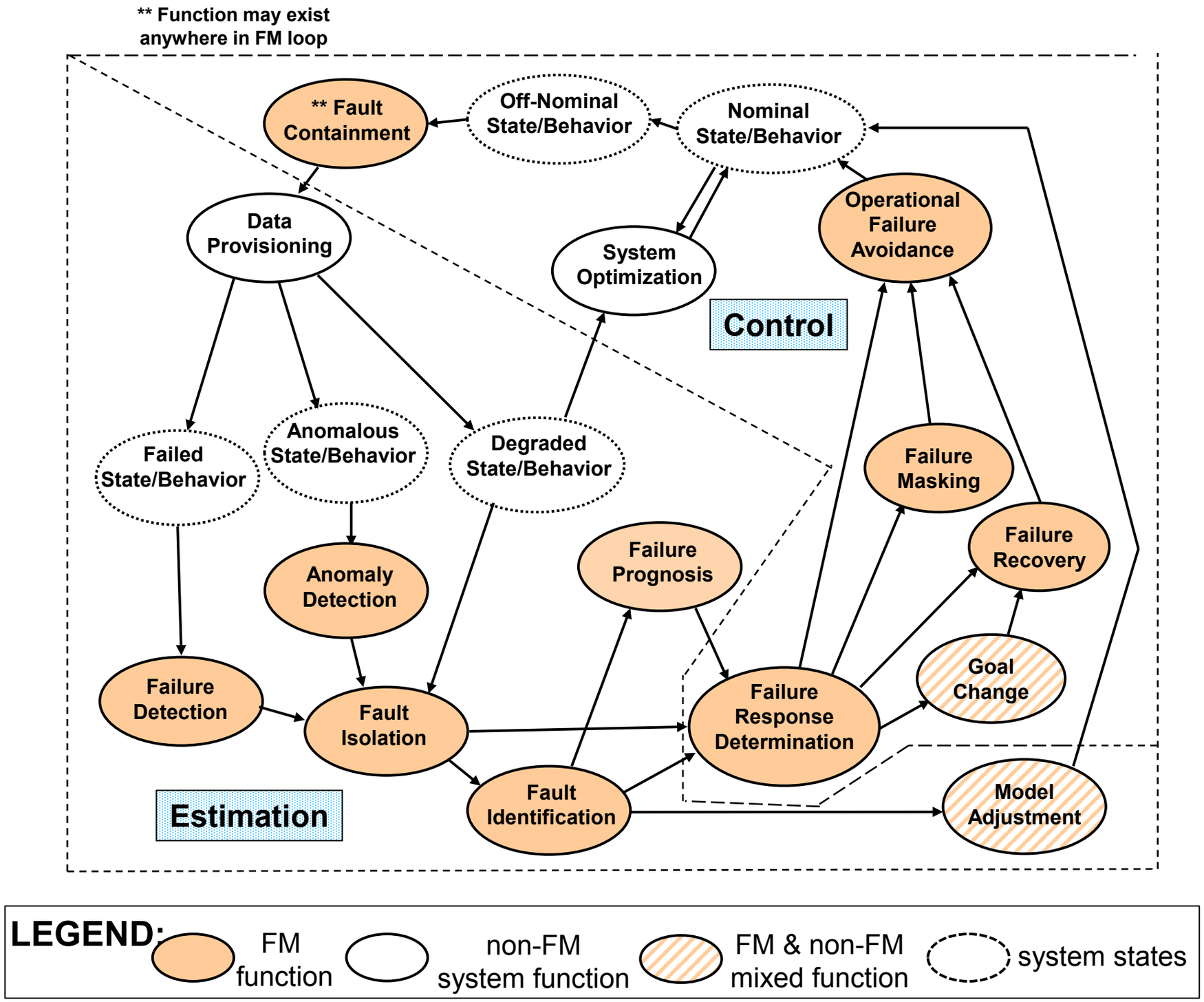
- **The insight that FM operates via control loops provides a path to clarify certain problematic FM design issues**
  - There is always a race condition in time between the propagation of failure effects, and the mitigation function that is attempting to fix the problem.
    - For the mitigation to work, the mitigation must operate faster than the failure effect
    - Mitigation mechanisms must use physical laws faster than the physical laws propagating the failure effects.
  - Unexpected, hazardous interactions of FM responses - the so-called "deadly embrace" - occur when two or more control loops intersect
    - Modeling the loops and intersections identifies the locations

Fault Management Functions



Updated since Johnson & Day 2010

Fault Management Functions as State Estimation and Control



Updated since Johnson & Day 2010

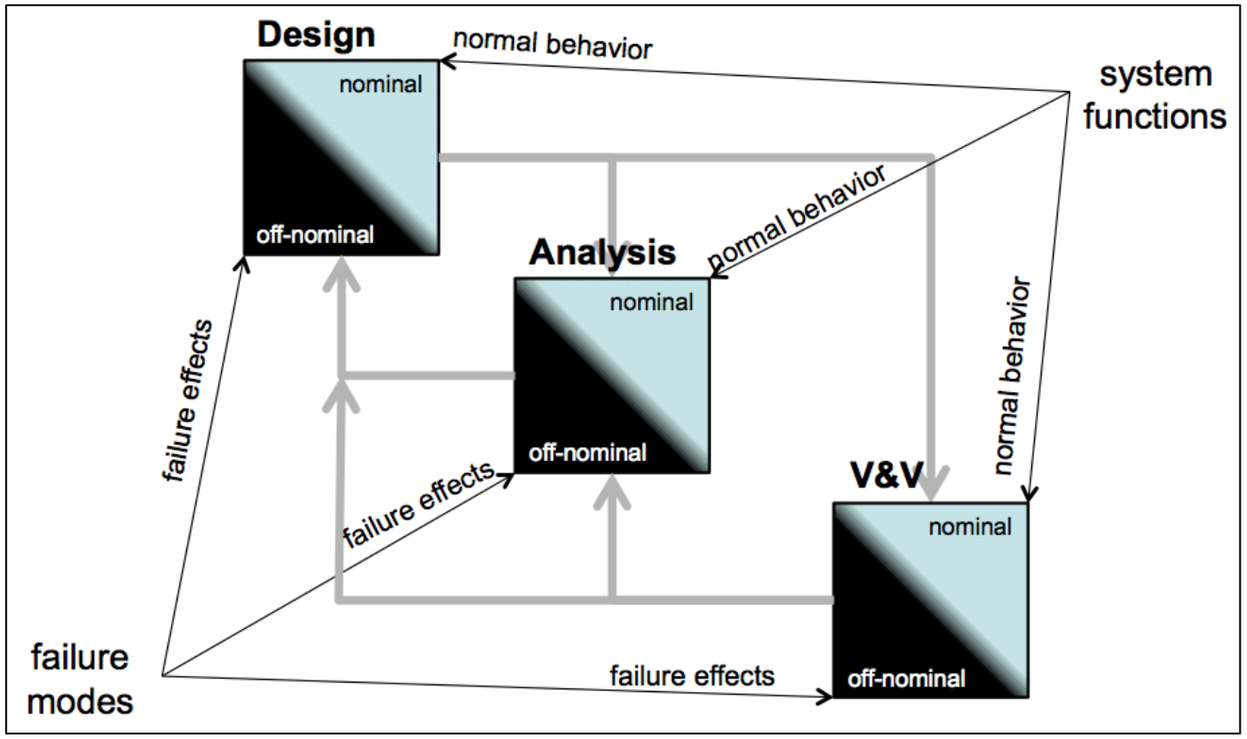
FM Function Definitions

- ***Anomaly Detection***: Deciding that an *anomaly* exists.
- ***Failure Containment***: Preventing a *failure* from causing further *failures*.
- ***Failure Detection***: Deciding that a *failure* exists.
- ***Failure Masking***: An action to maintain intended *function* in the presence of *failure*.
- ***Failure Prognosis***: Predicting the time at which a component will *fail*.
- ***Failure Recovery***: An action taken to restore *functions* necessary to achieve existing or redefined system *goals* after a *failure*.
- ***Failure Response Determination***: Selecting actions to mitigate a current or future *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.
- ***Goal Change***: An action that alters the system's current set of *objectives*.
- ***Model Adjustment***: Modifying the model of the *system* upon which *expectations* of future *states* and *behaviors* are based.
- ***Operational Failure Avoidance***: An action to prevent a *failure* from occurring.

Function Preservation

- **Standard systems engineering procedure is to perform a functional decomposition of the system, which defines the functions the system must perform to achieve its goals**
- **Rasmussen's insight[1] that FM acts to preserve function implies one of the primary ways in which FM can be tied to the systems engineering process**

- **Each system function has the possibility of failure, which is the "dark side" of each function that must be addressed in design, analysis, and verification and validation.**
  - Fault management's 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.
  - Just as the function tree provides a mechanism to assess nominal design completeness, it 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.

SHM Design Process (1)

- **Build a function/success/goal tree of the system**
  - Each major operating mode/phase is an “activity” of a functional flow block diagram or event sequence.
  - Each mode/phase/activity generates its own success tree of functions.
  - Model the state variables, and associate with each function.
    - Each function transforms an input state vector into an output state vector. The output state vector is the set of controlled state variables.
  - Construct the success tree so that connection to the architecture, and to physics-based models is simple.
    - Use the state variable inputs and outputs as a guide to proper selection of serial versus parallel paths in the tree branches.

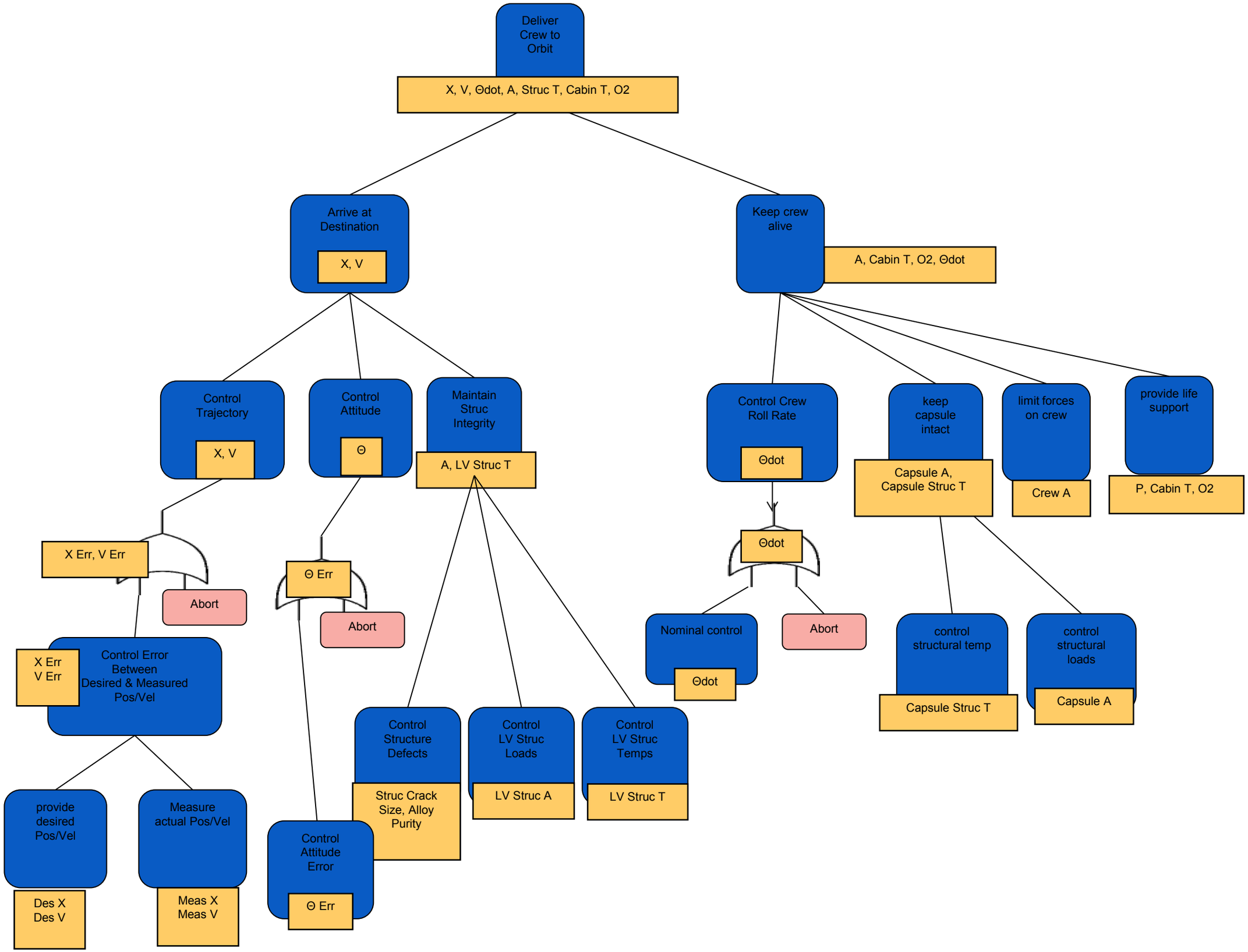
- **Determine which success tree nodes require reliability / availability / safety (RAS)---dependability, improvements**
  - Compare required dependability (top down) to estimated dependability (bottom up) for each node of the tree, assuming single string design
  - If estimated dependability < required dependability, estimated dependability must be improved for that node ➔ deploy improved SHM capabilities

SHM Design Process (2)

- **Select SHM Design Strategy**
  - Default when required dependability < estimated dependability = design-time fault avoidance
    - Design margins and quality assurance are sufficient
  - If required dependability > estimated dependability, select strategy(ies) for improvement. These appear as OR gates in the success tree, providing alternate paths to perform the function (or a portion of the function for goal changes).
    - Design-time fault avoidance (passive SHM)
    - Operational failure avoidance (operational FM)
    - Failure masking (operational FM)
    - Failure recovery (operational FM)
    - Goal change (e.g. safing, abort, reduced mission objectives) (operational FM)

- **Map Design Strategies to Architecture / Design**
  - In modeling terms, map from tree and event sequence representations to directed graph and schematics

Generic Function/Goal Tree for Crewed Launcher



SHM Design Process (3)

- **Analyze SHM Strategy effectiveness**
  - For design-time fault avoidance, estimate dependability (RAS) as probability of the function failing, a “simple” assessment based on component reliabilities
  - For all others, FMCL effectiveness must be calculated.
    - (Detection effectiveness) x (diagnostic effectiveness) x (response effectiveness) = FMCL effectiveness, per failure scenario
    - FMCL effectiveness x probability of condition occurring = probability of success for that scenario
    - Probabilistically “sum” success probabilities for all failure scenarios to get system success probability
    - For operational failure avoidance, substitute prognostic effectiveness for detection effectiveness.
  - Response effectiveness must sum up FMCL latencies & compare to failure effect propagation times to the CFE
  - Number of failure scenarios in practice should not be overly large
    - For a system with 6k failure modes, should have 200-600 failure scenarios to assess
- **Iterate until design is sufficiently effective**
- **V&V (not discussed in this paper)**
- **Operations (not discussed in this paper)**

Conclusion

- **A self-consistent theory and lexicon for SHM has been developed**
  - Connections to systems theory and control theory---extends both into off-nominal realm
  - Terminology / lexicon draw from systems and control theory, and fault tolerance / dependability taxonomy developed over several decades

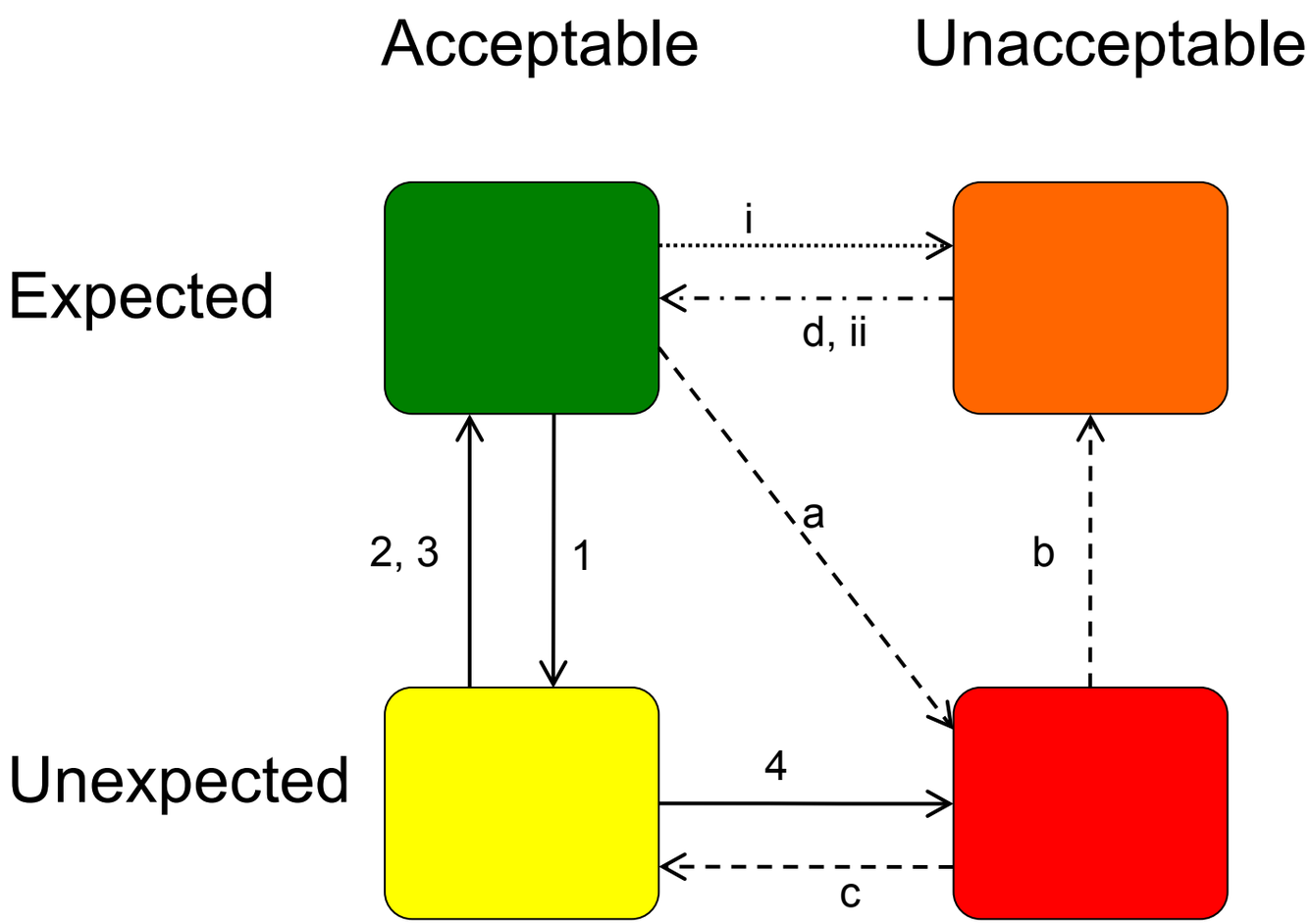
- **Operational FM constructed from the basis of control theory, to detect, assess, decide, and act (military---OODA loop) on current or predicted failures, and anomalies**
  - FM functions defined, and their relationships represented, assessed, and understood
  - Each FM Control Loop must operate faster than the failure effects they mitigate

- **Initial design process for SHM has been developed**
  - Draws from systems engineering event sequences and functional decompositions
  - Connects directly to fault trees and probabilistic risk assessments, and utilizes data from these analyses to make design decisions
  - Identification of state variables in the success / fault trees enables direct connection to the system architecture represented by schematics and directed graphs
  - Analysis process to factor FM Control Loop effectiveness into overall dependability / RAS calculations has been developed

- **Contact information:**
  - Stephen B. Johnson – Stephen.B.Johnson@nasa.gov, 719.487.9833
  - John C. Day – jday@inspacesystems.com, 510.339.0333 (soon, at JPL: john.c.day@jpl.nasa.gov)

Backup

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

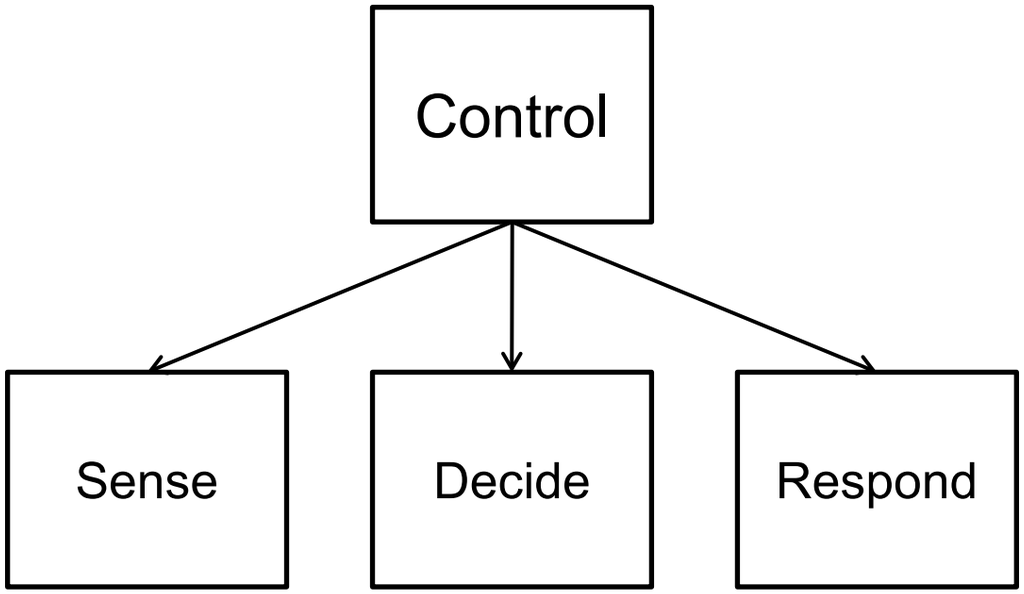
a) current value of state unexpectedly reaches an unacceptable value
b) model reviewed and parameters adjusted until model predicts current behavior (e.g., if IMU1 unhealthy, will have attitude failure)

- 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

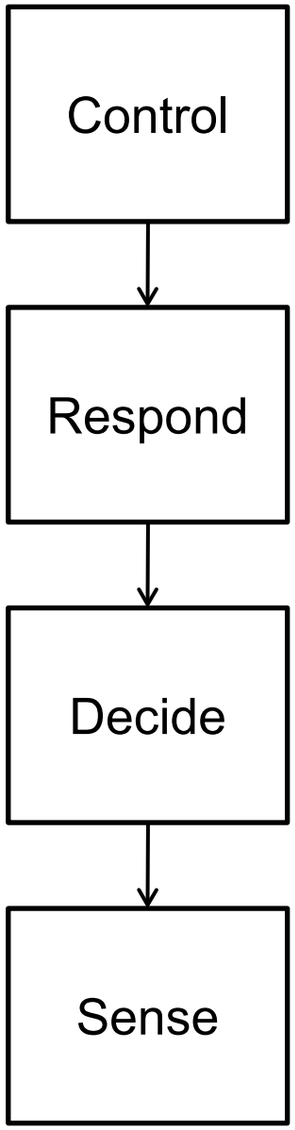
Failure, no Anomaly

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

Model Structure



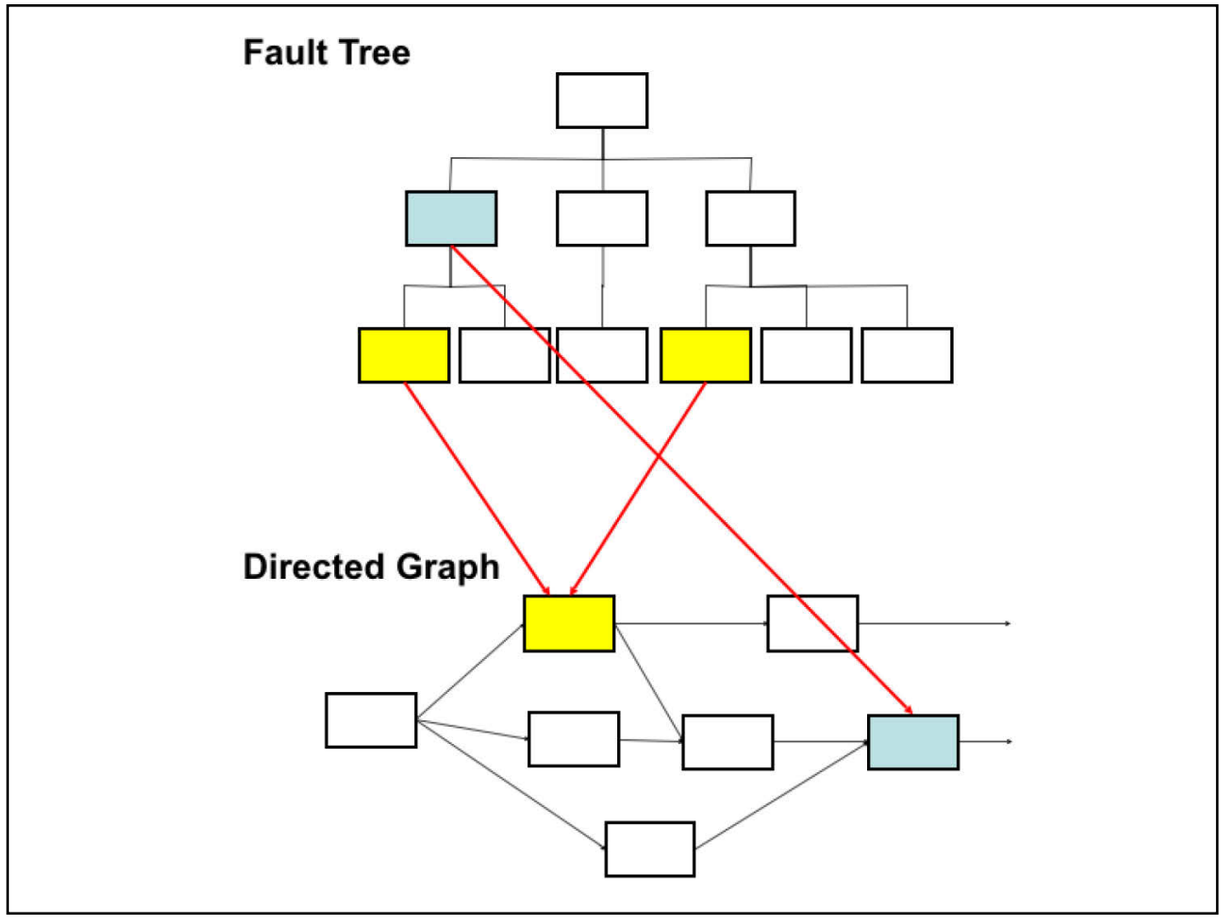
= ?

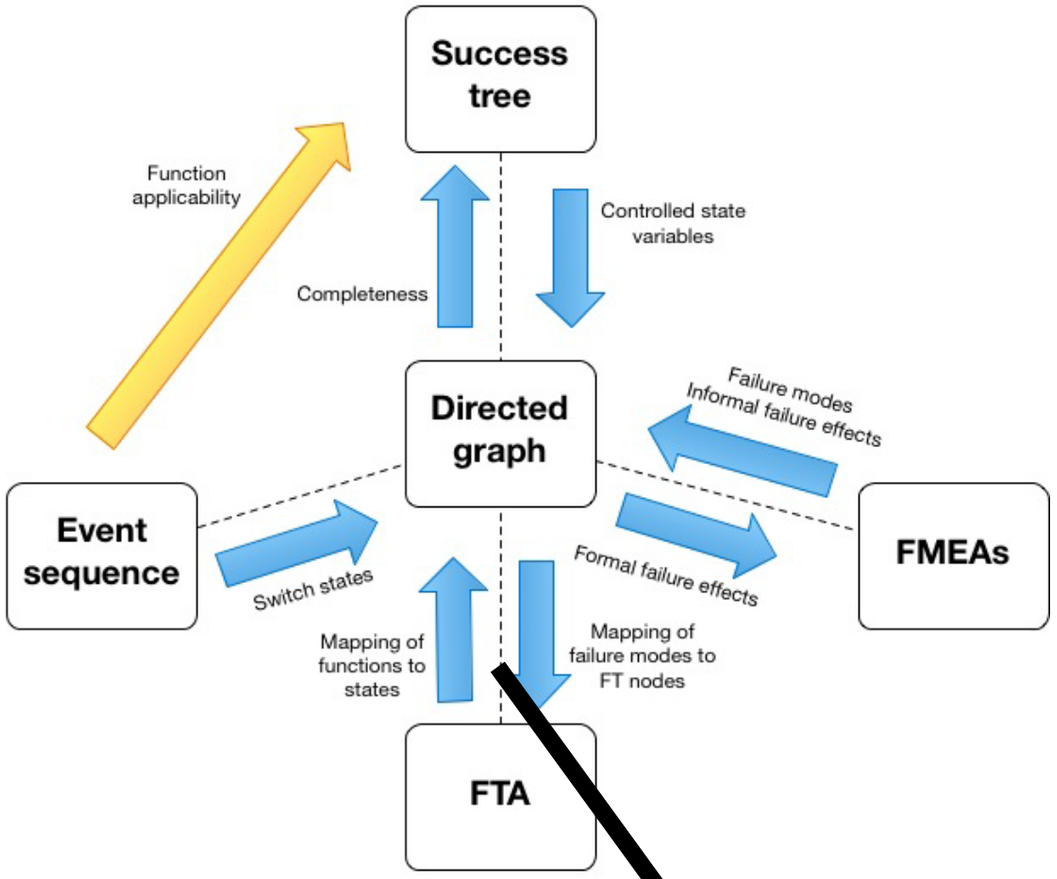
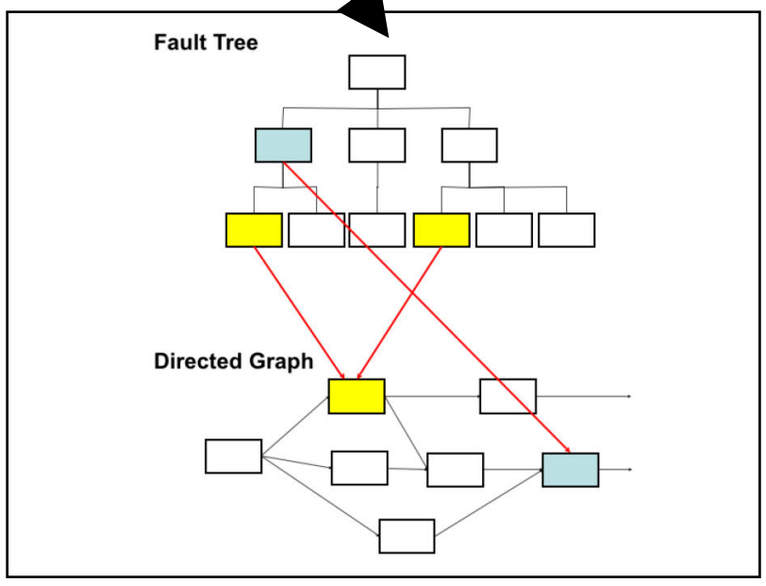


The choice MUST match physical / logical system architecture, or else subsystem and element designers' physics-based models and associated probabilities will not fit into the tree!

Mapping from Success or Fault Tree to Directed Graph (Architecture)

- **Each tree node associated with state variables to be controlled**
- **The same state variables often appear in several branches of the tree**
- **Directed graph (DG) is a physical model of the system architecture**
- **State variables in general appear at a single location (or along a single serial path) in the DG**
- **Therefore many-to-one mapping from tree to DG is common**
  - Each mapping from tree node to DG node represents a requirement on a system component



Relevant 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
- **State Machines** (Not Shown)
  - Necessary to assess sequencing of system states, both nominal and off-nominal