Space Launch System (SLS

Analytical Approaches to Guide SLS Fault Management (FM) Development

Jon Patterson
SLS Mission and Fault Management (M&FM) Lead
MSFC

April 10, 2012

SLS M&FM Scope

- Subset of the SLS Vehicle Management (VM) functions
  - Guidance, Navigation, and Control (GN&C)
  - Mission and Fault Management (M&FM)
- Manages SLS element and subsystem operations implemented in the SLS Flight Computer (FC) software
  - Nominal operations for:
    - Management of Core Stage (CS) subsystems (Avionics, MPS, CS TVC)
    - Interaction with the two Boosters for ignition, Booster TVC, and separation
    - Interaction with the four CS Engines for engine start and shutdown
  - Fault management for:
    - Detection and notification of SLS abort conditions, with autosafing where required
    - Notification of Caution and Warning (C&W) events
    - Redundancy Management (RM) to maintain critical functionality
    - Abort Trigger Sensor Data Qualification (SDQ)
- Nominal and FM teams were separate for Ares I, but have been combined for SLS
  - More efficient design---both functions address vehicle configurations, states & modes
  - Reduced overlap between groups (gray areas of off-nominal)
  - Reduced impact to element and subsystem
  - Better flow of understanding and potential improvements between the functions
- Current focus is on on-board FM capabilities
  - Trades are being conducted for allocation of functions between on-board and ground-based
  - FM for SLS ground systems being led by KSC and supported by VM/M&FM team

Nominal Operations vs. Fault Management

- Development of nominal capabilities is based on defining how the system and subsystems must be operated to perform the intended functions
  - May be discussions to determine how best to operate nominal functions, but little debate
  - Significant effort to assess the design specifications

- Fault management requires
  - Extensive effort to define the faults, failures, and consequences (severity)
    - Failure Mode and Effects Analysis (FMEA)
    - Hazards Analysis
    - Fault Trees and Probabilistic Risk Assessments
    - Abort Conditions
  - Determination of how to address these faults and failures
    - Design change or increased design margin
    - Redundancy
    - Dynamic monitoring and response
  - Dynamically monitored failures and faults require
    - Determination of how to detect and confirm the failure (triggers)
    - Definition of the proper response based on defined constraints, such as mission phase
      - Fail-over action
      - C&W message
      - Abort recommendation
      - Autosafing action
    - Assessment of response effectiveness

- Since FM-related actions for crewed vehicles can result in a loss of mission, associated topics may be hotly and passionately debated, and require strong supporting analysis
  - May result in increased cost due to increased quality and redundancy constraints on associated sensors
  - Require more stringent requirements to prevent False Positive (FP) indications (sensor data qualification, confirmation requirements, persistence checking, etc.)

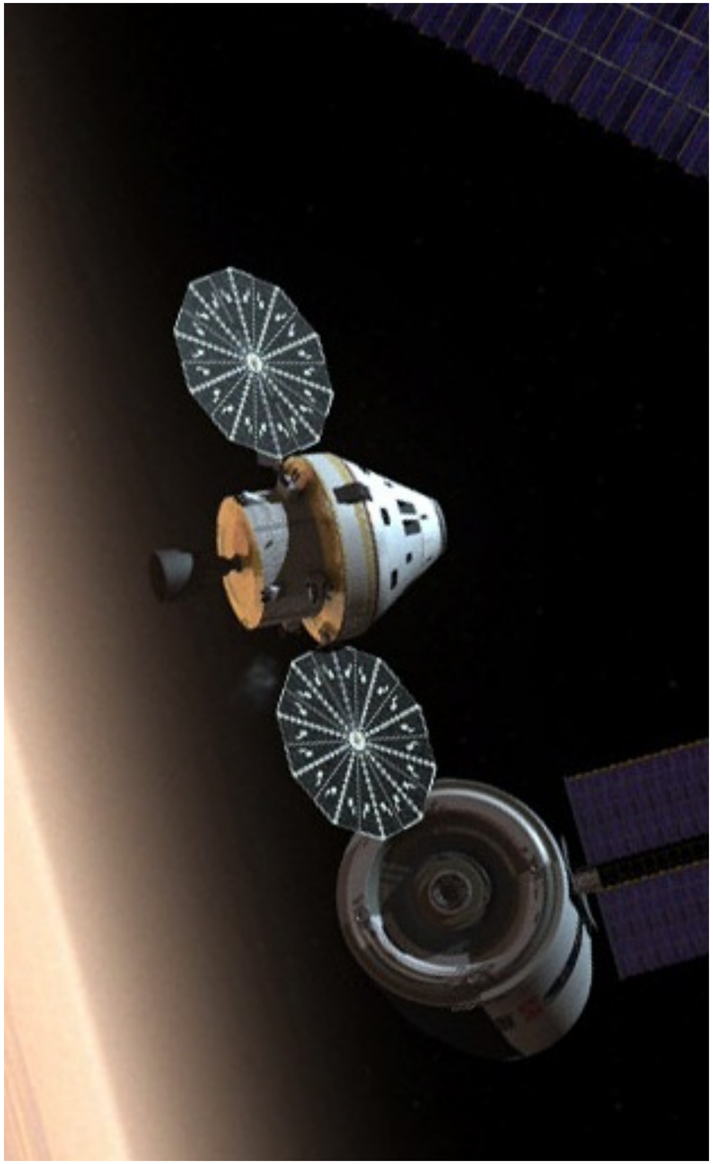
Development of SLS FM Capabilities

- Objective: Provide the right set of Fault Management capabilities for the SLS system
- Relies on strong collaboration with key stakeholders
- Steps:
  1. Identify system (vehicle), element, subsystem, and component faults and failures
  2. Select faults and failures requiring on-board detection and response
  3. Select detection triggers for each monitored fault/failure
  4. Define proper responses for each monitored fault/failure
  5. Assess design, trigger suite, and responses for effectiveness
  6. Implement FM algorithms
  7. Verify implemented FM capabilities

SLS FM Development Collaboration

- Safety and Mission Assurance (S&MA)
  - Define safety and reliability constraints for the system
  - Provide failure assessments (FMEA, Hazards, Probabilistic Risk Assessment, Fault Trees, Failure and Abort Scenarios)
  - SLS Loss of Mission (LOM) and contribution to Loss of Crew (LOC) estimates
- Systems Engineering and Integration (SE&I)
  - Define SLS FM-related requirements
  - Vehicle Functional Analysis Model (VFAM)
  - Interfacing with MPCV
  - Integrated aborts analysis
- Elements (Stages, Boosters, Engines, payloads) and Subsystems (MPS, RCS, TVC, etc.)
  - Element and subsystem operational scenarios and schematics
  - FMEA insight
  - Failure probability data
  - Response assessment support
- SLS Disciplines
  - Integrated Avionics and Software
  - VM/GN&C
  - Structures and Environments
  - Propulsion
  - Operations

SLS FM Development Collaboration



- Multi-Purpose Crew Vehicle (MPCV)/Orion
  - Abort Decision Logic (ADL) interface
  - MPCV/SLS Integrated Aborts analysis
  - Integrated failure definition
  - SLS abort conditions MPCV must detect
  - Required MPCV response capabilities on SLS
    - Retargetting
    - Manual steering
    - Engine shutdown and FTS discretes
- Crew Office – Most vested interest
  - Expertise and response preferences
  - C&W preferences
  - Automatic function inhibit definition
    - Automatic aborts
    - Engine redline shutdowns

Tools and Sources for Failure/Fault Identification

- Goal Tree/Success Tree
  - A top-down, design independent functional decomposition approach for early identification of potential monitored failure conditions for aborts or redundancy management
  - Identifies critical functions that must be protected
  - Precisely defines abort conditions and triggers in terms of state variables
  - Identifies hierarchical relationships between abort conditions & triggers

- Hazards Analysis
  - Top-down identification of threats to the vehicle/system, which can lead to failure
  - Require a “control” to mitigate the hazard through design margins, procedural actions, or automated monitoring and response

- Failure Scenarios/Abort Scenarios
  - Initial set provided by S&MA and managed by SE&I, developed collaboratively with M&FM and STE to determine which qualify as abort scenarios
  - Strong association between abort scenarios and abort conditions

- Failure Modes and Effects Analysis (FMEA)
  - A bottom-up breakout of the failures on the vehicle and the subsequent consequences
  - Used as the basis for M&FM to establish initial abort conditions on Ares I
  - Abort conditions to FMEA mapping ultimately required to ensure coverage and calculate scenario probabilities

- Heritage conditions defined on previous programs
  - Conditions were previously identified or employed for Ares I and shuttle
  - Conditions must be reassessed on SLS because of different configurations, interactions, and failure outcomes

Selection of On-board Monitoring Capabilities

For Abort Conditions:

- Calculate probability of occurrence
  - For abort conditions, a 1/100,000 probability threshold is used as a guide for identifying credible failures and filtering non-credible failures
  - Probabilities are developed by S&MA
- Assess detectability
  - Availability of reliable, feasible, affordable triggers/sensors
- Determine highest level of failure which absolutely requires abort, but provides sufficient Abort Warning Time (AWT)
  - MPS example
  - Requires detailed assessment of avionics to determine
    - The criticality of the provided function,
    - The combinations of avionics failures which exceed redundancy and result in loss of function,
    - The ability to clearly distinguish between when you can continue to fly safely and when you MUST abort

For C&W Conditions:

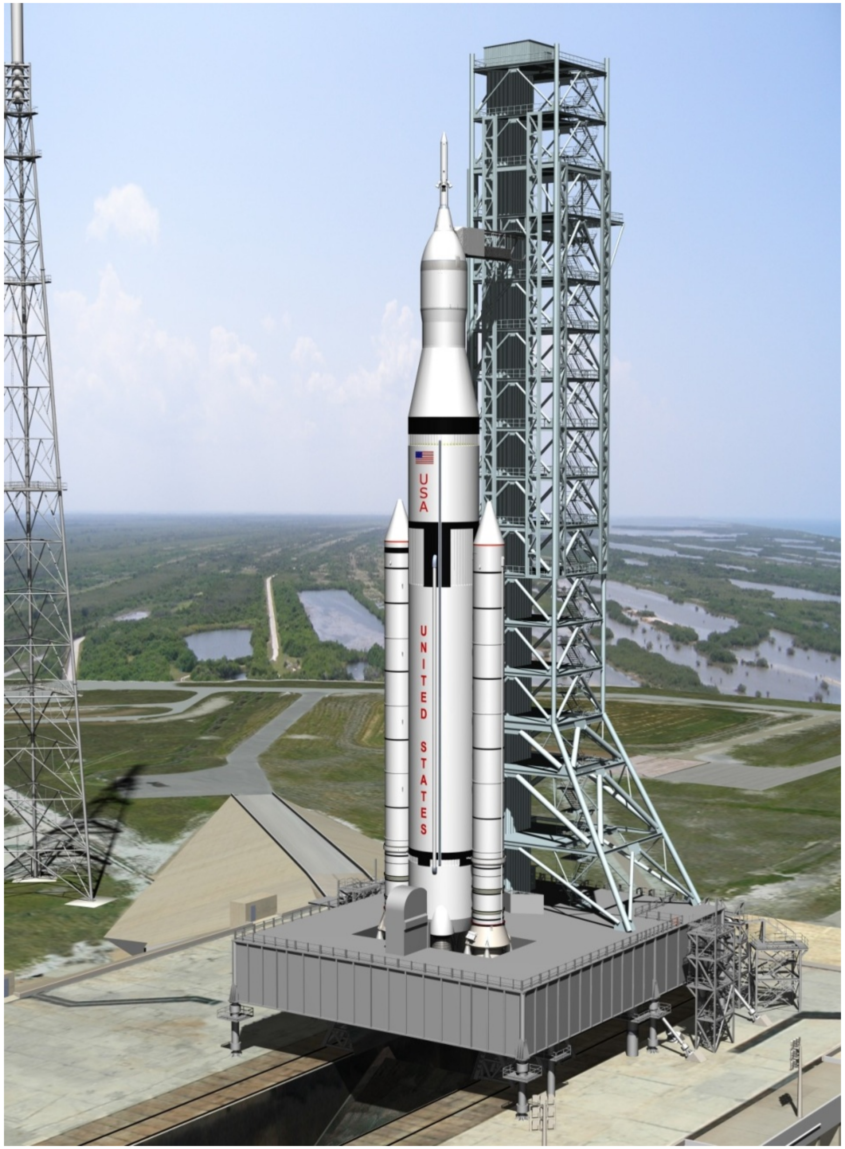
- Some candidate abort conditions for monitoring may be monitored as C&W instead due to reliability constraints that “disqualify” them for abort monitoring
- Some monitored abort conditions have “yellow line” thresholds
- For other conditions, generally as simple as
  - Working through FMEAs and associated measurements to determine what can be detected
  - Talking with the Crew Office, Mission Support, and Ground Support to identify what conditions they need to be made aware of that cannot be detected on the ground and MUST be detected on board

Selection and Assessment of Triggers

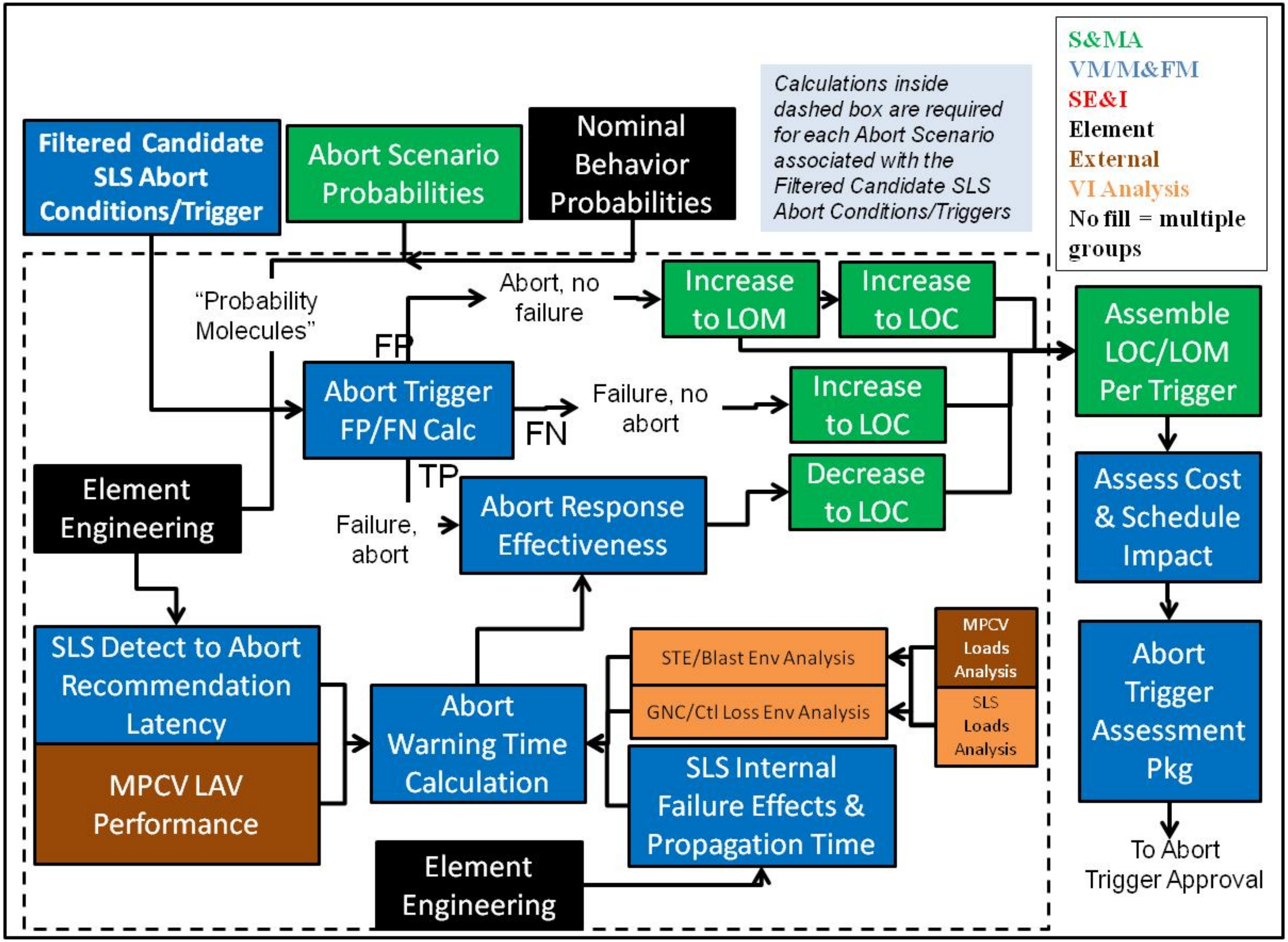
Identify and assess abort trigger "safety net" for qualitative coverage of top-level functions

Then, for each credible abort condition:

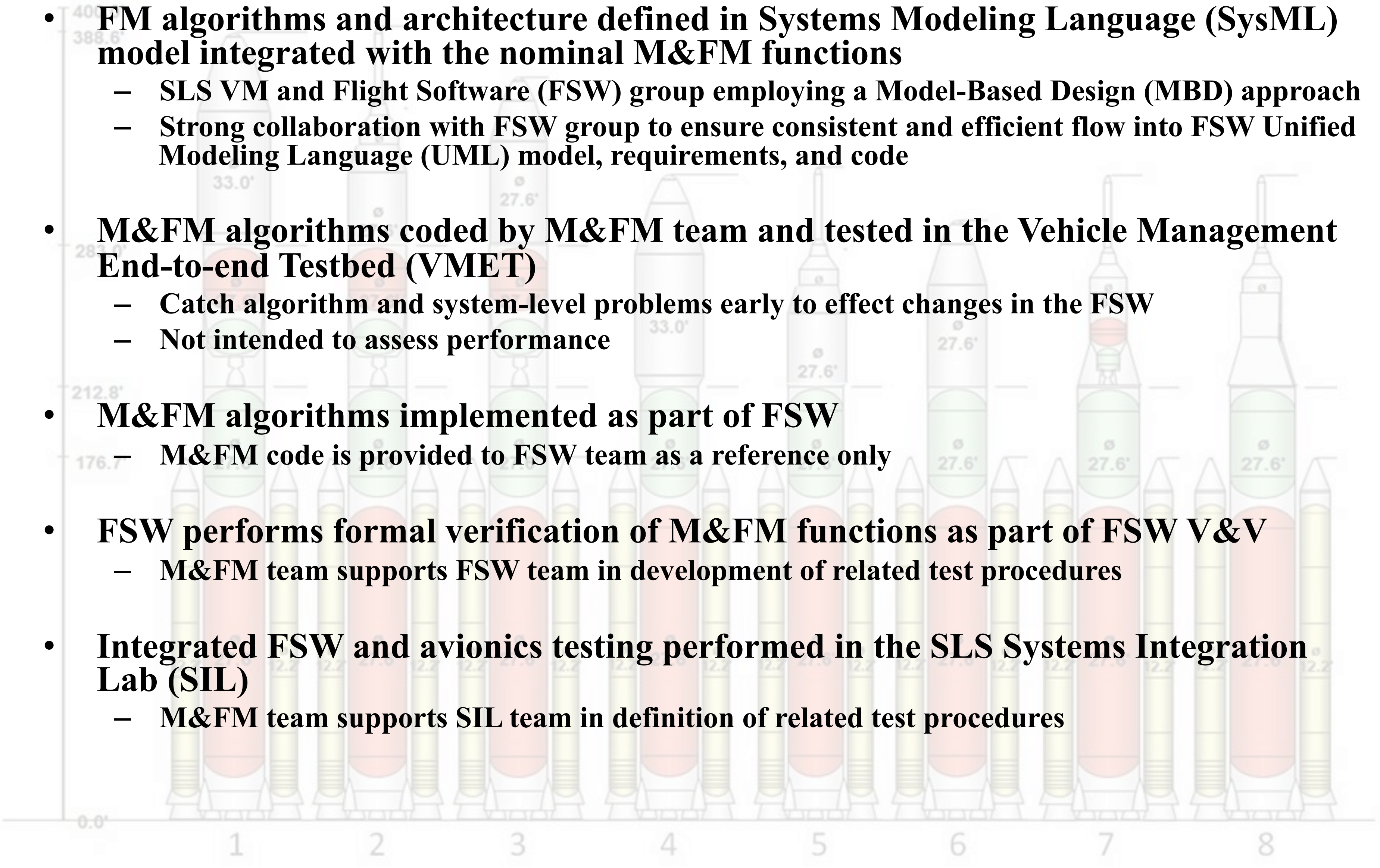
- **Identify candidate triggers for each abort condition**
  - **Example: TVC failures may be detected by:**
    - **Actuator position sensors**
    - **Loss of turbine speed**
    - **Loss of hydraulic or pneumatic pressure**
    - **Failure of TVC avionics**
    - **Violation of vehicle rate limits**
- **Assess False Positive (FP)/False Negative (FN) probabilities associated with each trigger**
  - **Assessment process factors in physics, sensors, avionics architecture, sensor data qualification logic, and detection algorithms**
  - **Completing the False Positive/False Negative Handbook begun at the end of Ares I to document the FP/FN assessment process**
- **Assess related Abort Effectiveness (including associated AWT) of each trigger (*reference the following slide*)**



SLS FM Design, Triggers, and Response Effectiveness Assessment


S&MA
VM/M&FM
SE&I
Element
External
VI Analysis
No fill = multiple groups
Calculations inside dashed box are required for each Abort Scenario associated with the Filtered Candidate SLS Abort Conditions/Triggers
Filtered Candidate SLS Abort Conditions/Trigger
Abort Scenario Probabilities
Nominal Behavior Probabilities
"Probability Molecules"
FP
Abort, no failure
Increase to LOM
Increase to LOC
Assemble LOC/LOM Per Trigger
Abort Trigger FP/FN Calc
FN
Failure, no abort
Increase to LOC
TP
Failure, abort
Abort Response Effectiveness
Decrease to LOC
Element Engineering
Assess Cost & Schedule Impact
SLS Detect to Abort Recommendation Latency
MPCV LAV Performance
Abort Warning Time Calculation
STE/Blast Env Analysis
GNC/Ctl Loss Env Analysis
MPCV Loads Analysis
SLS Loads Analysis
SLS Internal Failure Effects & Propagation Time
Element Engineering
Abort Trigger Assessment Pkg
To Abort Trigger Approval

SLS FM On-Board System Implementation and Verification



- FM algorithms and architecture defined in Systems Modeling Language (SysML) model integrated with the nominal M&FM functions
  - SLS VM and Flight Software (FSW) group employing a Model-Based Design (MBD) approach
  - Strong collaboration with FSW group to ensure consistent and efficient flow into FSW Unified Modeling Language (UML) model, requirements, and code

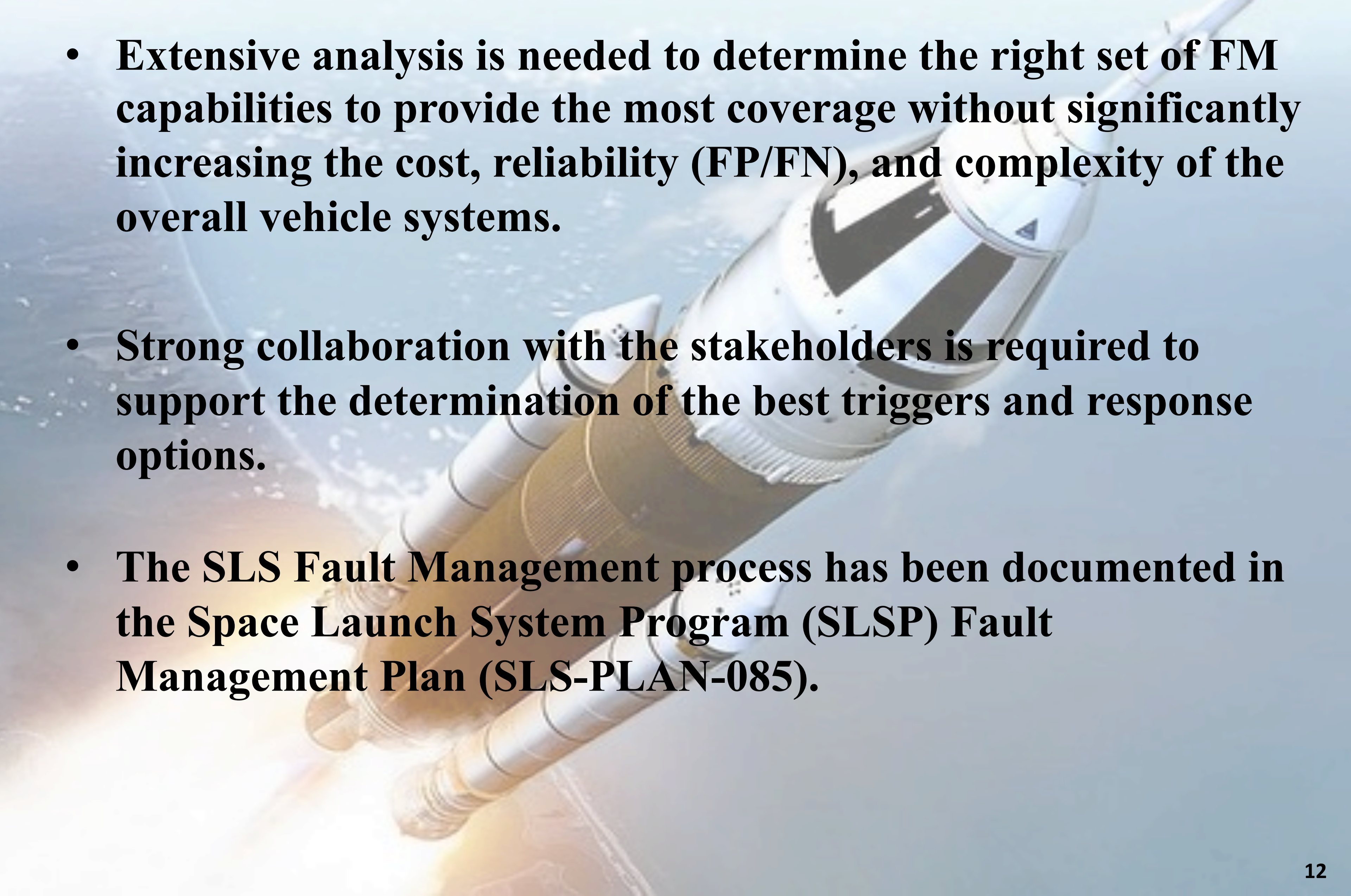
- M&FM algorithms coded by M&FM team and tested in the Vehicle Management End-to-end Testbed (VMET)
  - Catch algorithm and system-level problems early to effect changes in the FSW
  - Not intended to assess performance

- M&FM algorithms implemented as part of FSW
  - M&FM code is provided to FSW team as a reference only

- FSW performs formal verification of M&FM functions as part of FSW V&V
  - M&FM team supports FSW team in development of related test procedures

- Integrated FSW and avionics testing performed in the SLS Systems Integration Lab (SIL)
  - M&FM team supports SIL team in definition of related test procedures

Conclusion



- Extensive analysis is needed to determine the right set of FM capabilities to provide the most coverage without significantly increasing the cost, reliability (FP/FN), and complexity of the overall vehicle systems.

- Strong collaboration with the stakeholders is required to support the determination of the best triggers and response options.

- The SLS Fault Management process has been documented in the Space Launch System Program (SLSP) Fault Management Plan (SLS-PLAN-085).