
Luis Trevino, Ph.D., Peter Berg, Dwight England, Stephen Johnson
Jacobs ESSSA Group – Marshall Space Flight Center
Mission & Fault Management (M&FM), EV43
Spacecraft and Vehicle Systems Department
Space 2016, 9/13/2016 – 9/16/2016
Long Beach, CA
Co-Authors

- **Peter Berg**
  SLS State Flow Lead, M&FM Team
  Stinger Ghaffarian Technologies, Inc.
  Intelligent Systems Division
  NASA Ames Research Center

- **Dwight England**
  Chief, Integrated Systems Health Management & Automation Branch, EV43
  NASA Marshall Space Flight Center

- **Stephen B. Johnson, Ph.D.**
  Analysis Lead, M&FM Team
  Dependable System Technologies, LLC
  Jacobs ESSSA Group
  University of Colorado, Colorado Springs
Mission & Fault Management - SLS

- Fault Management Software
  - Error Prone
  - Requirements and Design Phase
  - Other Factors

- Model Based Systems Engineering
  - Rich graphical constructs
  - Deterministic
  - Standards

- Previous NASA Stateflow® Applications
  - LADEE
  - Ares – Orion Command Abort
  - NESC – Toyota, Commercial Spacecraft
State Analysis Model (SAM)
function determine_if_failed_high_reg_is_only_remaining_source
    {functrac[determine_if_failed_high_reg_is_only_remaining_source]=true;}

    [redundancy_counter_for_valve==x]
    {redundancy_counter_for_valve--;
        deenergize_the_valve_supplying_over_pressure();
        set_loss_of_valve_control_event();
    }

    {set_above_limit_event();}

function deenergize_the_valve_supplying_over_pressure

function set_above_limit_event
SAM Testing

- Script Driven → Ground Operations Timeline →
- Nominal Sequence Generator → Fault Generator
- Rule Checker → Analysis Report Generator → Timeline & State Report scripts → SAM Test Report
- User GUI
- Test Cases: Nominal, Off-Nominal, VMET, MCaRT, SIL
- TRAC Trouble Ticket System Summaries
User GUI

Command

failure_bus_HIGH_CURRENT=true

Selected Scenario

failure_bus_HIGH_CURRENT=true

M&FM EVENTS

EVT_..GoFor..CMD_Received At time MET =
EVT_EPS_.Auto_LAUNCH_SEQUENCE At time MET =
EVT_EPS..1553_COMM At time MET =
EVT_EPS..1553_COMM At time MET =
EVT_EPS..1553_COMM At time MET =
EVT_EPS..1553_COMM At time MET =
EVT_EPS..1553_COMM At time MET =
EVT_EPS..1553_COMM At time MET =
EVT_MPS_Eva..1 LOSS_OF_FUNCTION At time MET =
EVT_MPS_Eva..1 LOSS_OF_FUNCTION At time MET =
EVT_MPS_Eva..1 LOSS_OF_FUNCTION At time MET =
EVT_E..Engine_Fail At time MET =
EVT_E..Launch_Halt At time MET =
EVT_E..Launch_Halt At time MET =
EVT_E..Launch_Halt At time MET =
EVT_E..Launch_Halt At time MET =
EVT_E..Pad_Safing Complete At time MET =
EVT_E..Pad_Safing_Received At time MET =

MISSING NOMINAL EVENTS

EVT_..Start_Enable_Command_Sent
EVT_A..Engine_Fail At time MET =
EVT_A..Launch_Halt At time MET =
EVT_A..Launch_Halt At time MET =
EVT_A..Launch_Halt At time MET =
EVT_A..Launch_Halt At time MET =
EVT_A..Pad_Safing Complete At time MET =
EVT_A..Pad_Safing_Received At time MET =

RULE VIOLATIONS

EVT_D..Engine_Commanded_Open Without failsafe will not

UNEXPECTED EVENTS

EVT_D..LOSS_OF_FUNCTION
EVT_D..Engine_Fail
EVT_D..Launch_Halt
EVT_D..Launch_Halt
EVT_D..Launch_Halt
EVT_D..Launch_Halt
EVT_D..Pad_Safing
EVT_D..Pad_Safing
EVT_D..Pad_Safing Complete

Halt/No Halt

LAUNCH HALT
VMET, MCaRT, SIL Test Cases for the SAM

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Test Objective</th>
<th>Success Criteria</th>
<th>Duration / Fault Injection</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Test failure of helium isolation valve</td>
<td>&quot;EVT_Booster_HeliumValve_REdundancy_Reduced&quot; becomes &quot;True&quot; at Mission_Elapsed_Time</td>
<td>Test duration is from Mission_Elapsed Time = - sec to - sec</td>
</tr>
</tbody>
</table>
|             |                                                                                | = - sec                                                                           | Fault injected at Mission_Elapsed Time = - sec by setting Helium_Energy = - & detected |}

<table>
<thead>
<tr>
<th>Element</th>
<th>System</th>
<th>Response</th>
<th>Monitored Condition Name</th>
<th>Monitored Condition Description</th>
<th>Start Monitoring</th>
<th>Stop Monitoring</th>
<th>Units</th>
<th>Lower Trigger Limit (TBD)</th>
<th>Upper Trigger Limit (TBD)</th>
<th>Number of Indicators Needed to Generate Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Booster</td>
<td>Igniter</td>
<td>Sealing</td>
<td>DualBoosterIgnitionFailure</td>
<td>Both Boosters fail to ignite after T reaches</td>
<td>T= - msec</td>
<td>T= - msec</td>
<td>psia</td>
<td></td>
<td></td>
<td>2012</td>
</tr>
</tbody>
</table>
Findings: VMET & SAM

**MCaRT & SIL**
- 19% of MCaRT entries tested
  - 85.5% passed
- 45% of SIL test cases executed
  - 27% passed

**Finding Types**
- Logic Interpretation: 30%
- Editorials: 55%
- Logic Update: 15%
SAM Forward Directions / Summaries

- Interactive Failures
- Prelaunch procedures → OMRs → LCCs → Rule Checker
- Hazardous State Identification
- Post Flight Analysis
- Other: EUS, crew habitat, payloads, proximity ops, rovers, robotic deep space missions, EDL ops
- MBE → M&FM Algorithms → FSW → Testing
- Challenges
- Questions