MBSE Methodology for FM System Design
(Model Based System Engineering Methodology for Fault Management System Design)

Lui Wang, Michel Izygon*, Ph.D., Shira Okon*/ ER6
Spacecraft Software Engineering Branch, *Tietronix Software
JSC/NASA

Magdy Bareh, Castet, Jean-Francois, Nunes, Jeffery, Lorraine Fesq
JPL/NASA

January 29, 2015
MBSE Context

Model once and Use many times

Capability/Impact Assessment

Resource Management

Mission Operation Planning

Simulation

Electronic Procedure

ISHM and C/W

Safety Analysis

System Design

System Design Validation

System Displays

Training

Schedule MEL Cost

Activity Diagrams

Modelica SCXML

XTCE ATML

SCXML FMEA Connectivity

XTCE Connectivity

Fault Trees RBD FMEA

FMEA Connectivity MEL

FMEA Requirement Traceability RBD

SCXML XTCE FMEA Cost

SysML Models

Fault Trees RBD FMEA
MBFME Tool Suite Concept

Model based Fault Management Engineering (MBFME)
MBFME Meta-Model

Method utilizes SysML specifications and minimally invasive techniques to generate models.
Complexity is captured via interfaces in the physical architecture (IBD) and via transitions in the behavior models.
Applied MBFME Methodology to the Fan in the Can SysML model

- References a NASA spacecraft power architecture
- Contains 3 Subsystems (Power System, ECLSS, C&DH System)
- Common Cabin Air Assembly (CCAA) provides air circulation
Either MBSU1 or MBSU2 are required to provide power to PDU1. Each MBSU can be powered from either a Solar Array, 2 batteries, or from the cross-strap. 

Both Battery1 and Battery2 are required to provide power to the MBSU.

Fan in the Can SysML model:
- Demonstrates redundancy in the power system
- Demonstrates power cross-strapping
A Common Cabin Air Assembly (CCAA) function is to provide air circulation. Loss of the CCAA1’s function can result in loss of crew; Assigned a criticality level of 1.
Interactions Between PDU1 and CCAA1
FMECA (Failure Mode and Effects Criticality Analysis) Data Exchange

Magic Draw Plug-Ins

FMECA Output

<table>
<thead>
<tr>
<th>System</th>
<th>Subsystem</th>
<th>LRU/Assembly Type</th>
<th>LRU/Assembly Name</th>
<th>Item Function</th>
<th>Potential Failure Mode</th>
<th>Immediate Failure Effect</th>
<th>End Effect</th>
<th>Number of Independent Failures</th>
<th>Other Independent Failures</th>
<th>CRIT LEVEL</th>
<th>SEV</th>
<th>Potential Causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>FanInCan ECSS</td>
<td>CCAA</td>
<td>CCAA1</td>
<td>CCAA1 Circulates Air</td>
<td>Failed Off</td>
<td>Loss of CCAA1 air Circulation</td>
<td>Loss of CCAA1 air Circulation</td>
<td>1</td>
<td></td>
<td></td>
<td>Internal Mal</td>
<td></td>
<td>Internal Mal</td>
</tr>
<tr>
<td>FanInCan Power Subsystem</td>
<td>MBUSU</td>
<td>MBUSU1</td>
<td>MBUSU1 Distribute Power</td>
<td>Failed Off</td>
<td>Loss of MBUSU1 output power</td>
<td>Loss of CCAA1 air Circulation</td>
<td>2</td>
<td>MBUSU2 Failed Off</td>
<td>Internal Mal</td>
<td>Internal Mal</td>
<td></td>
<td>Internal Mal</td>
</tr>
<tr>
<td>FanInCan Power Subsystem</td>
<td>MBUSU</td>
<td>MBUSU1</td>
<td>MBUSU1 Distribute Power</td>
<td>Failed On</td>
<td>MBUSU1 Output Power On</td>
<td>Loss of MBUSU1 output power</td>
<td>2</td>
<td>MBUSU1 Failed Off</td>
<td>Internal Mal</td>
<td>Internal Mal</td>
<td></td>
<td>Internal Mal</td>
</tr>
<tr>
<td>FanInCan Power Subsystem</td>
<td>MBUSU</td>
<td>MBUSU2</td>
<td>MBUSU2 Distribute Power</td>
<td>Failed Off</td>
<td>Loss of ability to manage MBUSU2 loads</td>
<td>Loss of CCAA1 air Circulation</td>
<td>2</td>
<td>MBUSU1 Failed Off</td>
<td>Internal Mal</td>
<td>Internal Mal</td>
<td></td>
<td>Internal Mal</td>
</tr>
<tr>
<td>FanInCan Power Subsystem</td>
<td>MBUSU</td>
<td>MBUSU2</td>
<td>MBUSU2 Distribute Power</td>
<td>Failed On</td>
<td>MBUSU2 Output Power On</td>
<td>Loss of MBUSU2 output power</td>
<td>2</td>
<td>MBUSU1 Failed Off</td>
<td>Internal Mal</td>
<td>Internal Mal</td>
<td></td>
<td>Internal Mal</td>
</tr>
<tr>
<td>FanInCan Power Subsystem</td>
<td>PDU</td>
<td>PDU1</td>
<td>PDU Distribute Power</td>
<td>Failed Off</td>
<td>Loss of PDU output power</td>
<td>Loss of CCAA1 air Circulation</td>
<td>1</td>
<td></td>
<td></td>
<td>Internal Mal</td>
<td></td>
<td>Internal Mal</td>
</tr>
<tr>
<td>FanInCan Power Subsystem</td>
<td>PDU</td>
<td>PDU1</td>
<td>PDU Distribute Power</td>
<td>Failed On</td>
<td>PDU Output Power On</td>
<td>Loss of CCAA1 air Circulation</td>
<td>1</td>
<td></td>
<td></td>
<td>Internal Mal</td>
<td></td>
<td>Internal Mal</td>
</tr>
</tbody>
</table>
FMECA Analysis Results

- 10 Failure Modes Can Result in a Critical 1 Level Failure
- Due to redundancy (initial analysis without crosstie):
  - 6 potential failure modes are 2-fault tolerant
  - 2 potential failure modes are 1-fault tolerant
- The failure of the CCAA1 and PDU1 are critical failures requiring reliability measures

<table>
<thead>
<tr>
<th>System</th>
<th>Subsystem</th>
<th>LRU/Assembly Type</th>
<th>LRU/Assembly Name</th>
<th>Item Function</th>
<th>Potential Failure Mode</th>
<th>Immediate Failure Effect</th>
<th>End Effect</th>
<th>Number of Independent Failures</th>
<th>Other Independent Failures</th>
<th>CRIT LEVEL</th>
<th>SEV</th>
<th>Potential Causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>FaninCan</td>
<td>Power_Subsystem</td>
<td>AMPS_PDU</td>
<td>PDU1</td>
<td>PDU_Distribute_Power</td>
<td>FailedOff</td>
<td>Loss of PDU_output_power</td>
<td>Loss of CCAA1_air_Circulation (CO2 Poisoning)</td>
<td>1</td>
<td></td>
<td>1</td>
<td>1</td>
<td>pdus1s/external/1</td>
</tr>
<tr>
<td>FaninCan</td>
<td>ECSS</td>
<td>CCDA</td>
<td>CCDA1</td>
<td>CCDA1_Circulate_Air</td>
<td>FailedOff</td>
<td>Loss of CCDA1_air_Circulation (CO2 Poisoning)</td>
<td>Loss of CCDA1_air_Circulation (CO2 Poisoning)</td>
<td>1</td>
<td></td>
<td>1</td>
<td>1</td>
<td>ccda1s/external/Malf</td>
</tr>
<tr>
<td>FaninCan</td>
<td>Power_Subsystem</td>
<td>AMPS_MBUSU</td>
<td>MBSU1</td>
<td>MBSU1_Distribute_Power</td>
<td>FailedOff</td>
<td>Loss of MBSU1_output_power</td>
<td>Loss of CCDA1_air_Circulation (CO2 Poisoning)</td>
<td>2</td>
<td>MBSU2 FailedOff</td>
<td>1</td>
<td>1</td>
<td>mbsu1s/external/1</td>
</tr>
<tr>
<td>FaninCan</td>
<td>Power_Subsystem</td>
<td>AMPS_MBUSU</td>
<td>MBSU2</td>
<td>MBSU2_Distribute_Power</td>
<td>FailedOff</td>
<td>Loss of MBSU2_output_power</td>
<td>Loss of CCDA1_air_Circulation (CO2 Poisoning)</td>
<td>2</td>
<td>MBSU1 FailedOff</td>
<td>1</td>
<td>1</td>
<td>mbsu2s/external/1</td>
</tr>
<tr>
<td>FaninCan</td>
<td>Power_Subsystem</td>
<td>AMPS_Solar_Array</td>
<td>SolarArray1</td>
<td>SA1_Generate_Power_SA_B1_Generate_Power</td>
<td>FailedOff</td>
<td>Loss of SA1_output_power</td>
<td>Loss of CCAA1_air_Circulation (CO2 Poisoning)</td>
<td>3</td>
<td>Battery1 FailedOff OR Battery2 FailedOff MBSU2 FailedOff</td>
<td>1</td>
<td>1</td>
<td>solararray1s/external/1</td>
</tr>
<tr>
<td>FaninCan</td>
<td>Power_Subsystem</td>
<td>AMPS_Solar_Array</td>
<td>SolarArray2</td>
<td>SA2_Generate_Power_SA_B1_Generate_Power</td>
<td>FailedOff</td>
<td>Loss of SA2_output_power</td>
<td>Loss of CCAA1_air_Circulation (CO2 Poisoning)</td>
<td>3</td>
<td>Battery1 FailedOff OR Battery2 FailedOff MBSU1 FailedOff</td>
<td>1</td>
<td>1</td>
<td>solararray2s/external/1</td>
</tr>
<tr>
<td>FaninCan</td>
<td>Power_Subsystem</td>
<td>AMPS_Modular_Lithium_Battery</td>
<td>Battery1</td>
<td>Battery_Generate_Power</td>
<td>FailedOff</td>
<td>Loss of Battery1_output_power</td>
<td>Loss of CCAA1_air_Circulation (CO2 Poisoning)</td>
<td>3</td>
<td>SolarArray1 FailedOff MBSU1 FailedOff</td>
<td>1</td>
<td>1</td>
<td>battery1s/external/1</td>
</tr>
<tr>
<td>FaninCan</td>
<td>Power_Subsystem</td>
<td>AMPS_Modular_Lithium_Battery</td>
<td>Battery2</td>
<td>Battery_Generate_Power</td>
<td>FailedOff</td>
<td>Loss of Battery2_output_power</td>
<td>Loss of CCAA1_air_Circulation (CO2 Poisoning)</td>
<td>3</td>
<td>Battery2 FailedOff MBSU2 FailedOff</td>
<td>1</td>
<td>1</td>
<td>battery2s/external/1</td>
</tr>
<tr>
<td>FaninCan</td>
<td>Power_Subsystem</td>
<td>AMPS_Modular_Lithium_Battery</td>
<td>Battery3</td>
<td>Battery_Generate_Power</td>
<td>FailedOff</td>
<td>Loss of Battery3_output_power</td>
<td>Loss of CCAA1_air_Circulation (CO2 Poisoning)</td>
<td>3</td>
<td>Battery3 FailedOff MBSU3 FailedOff</td>
<td>1</td>
<td>1</td>
<td>battery3s/external/1</td>
</tr>
<tr>
<td>FaninCan</td>
<td>Power_Subsystem</td>
<td>AMPS_Modular_Lithium_Battery</td>
<td>Battery4</td>
<td>Battery_Generate_Power</td>
<td>FailedOff</td>
<td>Loss of Battery4_output_power</td>
<td>Loss of CCAA1_air_Circulation (CO2 Poisoning)</td>
<td>3</td>
<td>Battery4 FailedOff MBSU4 FailedOff</td>
<td>1</td>
<td>1</td>
<td>battery4s/external/1</td>
</tr>
<tr>
<td>FaninCan</td>
<td>Power_Subsystem</td>
<td>AMPS_MBUSU</td>
<td>MBSU1</td>
<td>MBSU_Distribute_Power</td>
<td>FailedOn</td>
<td>Loss of ability_to_manage_MBSU1_loads</td>
<td>Loss of CCAA1_air_Circulation (CO2 Poisoning)</td>
<td>3</td>
<td>MBSU1/external/1</td>
<td>1</td>
<td>2</td>
<td>mbsu1s/external/2M</td>
</tr>
<tr>
<td>FaninCan</td>
<td>Power_Subsystem</td>
<td>AMPS_MBUSU</td>
<td>MBSU2</td>
<td>MBSU_Distribute_Power</td>
<td>FailedOn</td>
<td>Loss of ability_to_manage_MBSU2_loads</td>
<td>Loss of CCAA1_air_Circulation (CO2 Poisoning)</td>
<td>3</td>
<td>MBSU2/external/2M</td>
<td>1</td>
<td>2</td>
<td>mbsu2s/external/2M</td>
</tr>
<tr>
<td>FaninCan</td>
<td>Power_Subsystem</td>
<td>AMPS_MBUSU</td>
<td>MBSU2</td>
<td>MBSU_Distribute_Power</td>
<td>FailedOn</td>
<td>Loss of ability_to_manage_MBSU3_loads</td>
<td>Loss of CCAA1_air_Circulation (CO2 Poisoning)</td>
<td>3</td>
<td>MBSU3/external/2M</td>
<td>1</td>
<td>2</td>
<td>mbsu3s/external/2M</td>
</tr>
<tr>
<td>FaninCan</td>
<td>Power_Subsystem</td>
<td>AMPS_MBUSU</td>
<td>MBSU2</td>
<td>MBSU_Distribute_Power</td>
<td>FailedOn</td>
<td>Loss of ability_to_manage_MBSU4_loads</td>
<td>Loss of CCAA1_air_Circulation (CO2 Poisoning)</td>
<td>3</td>
<td>MBSU4/external/2M</td>
<td>1</td>
<td>2</td>
<td>mbsu4s/external/2M</td>
</tr>
<tr>
<td>FaninCan</td>
<td>Power_Subsystem</td>
<td>AMPS_PDU</td>
<td>PDU1</td>
<td>PDU_Distribute_Power</td>
<td>FailedOn</td>
<td>Loss of PDU_output_power</td>
<td>Loss of CCAA1_air_Circulation (CO2 Poisoning)</td>
<td>3</td>
<td>MBSU1/external/1</td>
<td>1</td>
<td>2</td>
<td>pdus1s/external/1</td>
</tr>
</tbody>
</table>

[Table continues]
FTA (Fault Tree Analysis) Data Exchange

Magic Draw Plug-Ins

Select Top Level Event to Analyze

Fault Tree in Graphviz (FTA XML Generated)
Future Directions / Conclusions

- Expand the FM meta-models (model attributes) to support additional FM products
- Continue collaboration with additional FM analysis experts (e.g., QSI TEAMS)
- Demonstrate the tools on NASA systems of varying complexity (e.g., CDS 2.0)
- Support automated generation of simulations with failure injection
Uses of System Models

Model once and Use many times

- Capability/Impact Assessment
- Resource Management
- Mission Operation Planning
- Simulation
- Electronic Procedure
- ISHM and C/W
- System Displays
- Training
- Safety Analysis
- System Design
- System Design Validation
- Fault Trees
- RBD
- FMEA
- SCXML
- XTCE
- FMEA Cost
- Schedule MEL
- Activity Diagrams
- Modelica
- SCXML
- XTCE
- ATML
- FMEA Connectivity
- MEL Cost
- Requirement Traceability RBD
- Activity Diagrams
- XTCE Connectivity
- SCXML Connectivity
Backup Slides
Generate MEL from SysML

SysML Models

Magic Draw Plug-Ins

MEL

<table>
<thead>
<tr>
<th>Items</th>
<th>Item Type</th>
<th>Item Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDS-PMM-1</td>
<td>Pearl MM relay</td>
<td>C&amp;DH System/Facility C&amp;DH</td>
</tr>
<tr>
<td>CDS-PMM-2</td>
<td>Pearl MM relay</td>
<td>C&amp;DH System/Facility C&amp;DH</td>
</tr>
<tr>
<td>FAC-PMM-1</td>
<td>Pearl MM relay</td>
<td>C&amp;DH System/Facility C&amp;DH</td>
</tr>
<tr>
<td>CDS-SMS18-1</td>
<td>Sensoray 518</td>
<td>C&amp;DH System/Facility C&amp;DH</td>
</tr>
<tr>
<td>CDS-SMS18-2</td>
<td>Sensoray 518</td>
<td>C&amp;DH System/Facility C&amp;DH</td>
</tr>
<tr>
<td>CDS-SMS18-3</td>
<td>Sensoray 518</td>
<td>C&amp;DH System/Facility C&amp;DH</td>
</tr>
<tr>
<td>FAC-SMS18-1</td>
<td>Sensoray 518</td>
<td>C&amp;DH System/Facility C&amp;DH</td>
</tr>
<tr>
<td>CDS-D322AT-1</td>
<td>DMM-322-AT</td>
<td>C&amp;DH System/Facility C&amp;DH</td>
</tr>
<tr>
<td>CDS-D322AT-1</td>
<td>DMM-322-AT</td>
<td>C&amp;DH System/Facility C&amp;DH</td>
</tr>
<tr>
<td>CDS-JAN12-1</td>
<td>Power Supply Board</td>
<td>Facility C&amp;DH/C&amp;DH System</td>
</tr>
<tr>
<td>FAC-JAN12-1</td>
<td>Power Supply Board</td>
<td>Facility C&amp;DH/C&amp;DH System</td>
</tr>
<tr>
<td>CDS-MEP405-1</td>
<td>CPU</td>
<td>C&amp;DH System/Facility C&amp;DH</td>
</tr>
<tr>
<td>FAC-MEP405-1</td>
<td>CPU</td>
<td>Facility C&amp;DH/C&amp;DH System</td>
</tr>
<tr>
<td>CDS-T5-1</td>
<td>AC bus termination board</td>
<td>C&amp;DH System/Facility C&amp;DH</td>
</tr>
<tr>
<td>FAC-T5-1</td>
<td>AC bus termination board</td>
<td>C&amp;DH System/Facility C&amp;DH</td>
</tr>
<tr>
<td>CD-1</td>
<td>Cascade Distiller</td>
<td>Cascade Distillation System/Water Recovery...Assembly</td>
</tr>
<tr>
<td>THP3</td>
<td>Heat Pump</td>
<td>Cascade Distillation System/Water Recovery...Assembly</td>
</tr>
<tr>
<td>CDS UMC</td>
<td>Universal Micro Controller</td>
<td>C&amp;DH System</td>
</tr>
<tr>
<td>FAC UMC</td>
<td>Universal Micro Controller</td>
<td>Facility C&amp;DH/C&amp;DH System</td>
</tr>
<tr>
<td>E1</td>
<td>Conductivity Sensor</td>
<td>Cascade Distillation System/Water Recovery...Component</td>
</tr>
<tr>
<td>E2</td>
<td>Conductivity Sensor</td>
<td>Cascade Distillation System/Water Recovery...Component</td>
</tr>
</tbody>
</table>
XTCE Exchange

XML Telemetric and Command Exchange (XTCE) - OMG standard for Spacecraft T&C

```
<SpaceSystem name="RIU2">
  <AliasSet>
    <Alias alias="02" nameSpace="id"/>
    <Alias alias="020602" nameSpace="interface"/>
  </AliasSet>
  <Header classification="INTERFACE"/>
  <TelemetryMetaData>
    <ParameterSet>
      <Parameter parameterTypeRef="HUMIDITY_DEWPOINT_SENSOR" shortDescription="GEOLAB_GB_HUMIDITY1_DEWPOINTSENSOR"
        name="020602018001">
        <ParameterProperties dataSource="telemetry">
          <SystemName>CORE.GEOLAB.RIU2.HUMIDITY_DEWPOINT_SENSOR.1</SystemName>
        </ParameterProperties>
      </Parameter>
      <Parameter parameterTypeRef="VALIDITY" name="020602054001">
        <ParameterProperties dataSource="telemetry">
          <SystemName>CORE.GEOLAB.RIU2.VALIDITY.1</SystemName>
        </ParameterProperties>
      </Parameter>
    </ParameterSet>
  </TelemetryMetaData>
</SpaceSystem>
```
State Machine (SCXML)/FSM Exchange

SCXML: "State Chart extensible Markup Language". Provides a generic state-machine based execution environment based on Harel State Tables.
Concept of Operations