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
Model once and Use many times

MBSE Context

- 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

SysML Models

- Modelica
- SCXML
- XTCE
- ATML
- FMEA Connectivity
- Activity Diagrams
- Schedule MEL Cost
- Fault Trees
- RBD
- FMEA
- FMEA Requirement Traceability
- RBD
- MEL Cost
- SCXML Connectivity
- XTCE Connectivity
- XTCE Connectivity
- Modelica SCXML
Model based Fault Management Engineering (MBFME)
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.
Power Subsystem Internal Block Diagram (IBD)

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
Power Subsystem Internal Block Diagram (IBD)

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

Each MBSU can be powered from either a Solar Array, 2 batteries, or from the cross-strap.

Either MBSU1 or MBSU2 are required to provide power to PDU1.

Fan in the Can SysML model
- Demonstrates redundancy in the power system
- Demonstrates power cross-strapping
State Machine Diagram for CCAA1

- 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.

CCAA1 can transition to “On” if (PDU1 is On) or (PDU1 is Failed On).
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>Effects</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>ECSS</td>
<td>CCAA</td>
<td>CCAA1</td>
<td>CCAA1</td>
<td>Failed Off</td>
<td>Loss of CCAA1 air Circulation.</td>
<td>1</td>
<td></td>
<td>1</td>
<td>1</td>
<td>Internal Malfunction</td>
</tr>
<tr>
<td>FanInCan</td>
<td>Power Subsystem</td>
<td>MBSU</td>
<td>MBSU1</td>
<td>MBSU1</td>
<td>Failed Off</td>
<td>Loss of MBSU1_output_power</td>
<td>2</td>
<td>MBSU1 Failed Off</td>
<td>1</td>
<td>1</td>
<td>Internal Malfunction</td>
</tr>
<tr>
<td>FanInCan</td>
<td>Power Subsystem</td>
<td>MBSU</td>
<td>MBSU1</td>
<td>MBSU1</td>
<td>Failed On</td>
<td>MBSU1_Output_Power_On</td>
<td>1</td>
<td></td>
<td>1</td>
<td>1</td>
<td>Internal Malfunction</td>
</tr>
<tr>
<td>FanInCan</td>
<td>Power Subsystem</td>
<td>MBSU</td>
<td>MBSU2</td>
<td>MBSU2</td>
<td>Failed On</td>
<td>Loss of ability_to_manage_</td>
<td>1</td>
<td></td>
<td>1</td>
<td>1</td>
<td>Internal Malfunction</td>
</tr>
<tr>
<td>FanInCan</td>
<td>Power Subsystem</td>
<td>MBSU</td>
<td>MBSU2</td>
<td>MBSU2</td>
<td>Failed On</td>
<td>Loss of ability_to_manage_</td>
<td>1</td>
<td></td>
<td>1</td>
<td>1</td>
<td>Internal Malfunction</td>
</tr>
<tr>
<td>FanInCan</td>
<td>Power Subsystem</td>
<td>PDU</td>
<td>PDU1</td>
<td>PDU1</td>
<td>Failed Off</td>
<td>Loss of PDU_output_power</td>
<td>1</td>
<td></td>
<td>1</td>
<td>1</td>
<td>Internal Malfunction</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>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>MiPS_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></td>
<td>pdu1 internal Malffer</td>
</tr>
<tr>
<td>FanInCan</td>
<td>ECLSS</td>
<td>CCAA</td>
<td>CCAA1</td>
<td>CCAA1_Circle_Air</td>
<td>FailedOff</td>
<td>Loss_of_CCAA1_air_Circulation_CO2_Poisoning</td>
<td>Loss_of_CCAA1_air_Circulation_CO2_Poisoning</td>
<td>1</td>
<td></td>
<td>1</td>
<td></td>
<td>ccaa1 internal Malffer</td>
</tr>
<tr>
<td>FanInCan</td>
<td>Power_Subsystem</td>
<td>MiPS_MBUSU</td>
<td>MBUSU1</td>
<td>MBUSU_Distribute_Power</td>
<td>FailedOff</td>
<td>Loss_of_MBUSU1_output_power</td>
<td>Loss_of_CCAA1_air_Circulation_CO2_Poisoning</td>
<td>2</td>
<td>MBUSU2 FailedOff</td>
<td>1</td>
<td></td>
<td>mbusu1 internal Malffer</td>
</tr>
<tr>
<td>FanInCan</td>
<td>Power_Subsystem</td>
<td>MiPS_MBUSU</td>
<td>MBUSU2</td>
<td>MBUSU_Distribute_Power</td>
<td>FailedOff</td>
<td>Loss_of_MBUSU2_output_power</td>
<td>Loss_of_CCAA1_air_Circulation_CO2_Poisoning</td>
<td>2</td>
<td>MBUSU1 FailedOff</td>
<td>1</td>
<td></td>
<td>mbusu2 internal Malffer</td>
</tr>
<tr>
<td>FanInCan</td>
<td>Power_Subsystem</td>
<td>MiPS_Solar_Array</td>
<td>SolarArray1</td>
<td>SA1_Generate_Power_SA_B1_Gen</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) MBUSU1 FailedOff</td>
<td>1</td>
<td></td>
<td>solararray1 internal Malffer</td>
</tr>
<tr>
<td>FanInCan</td>
<td>Power_Subsystem</td>
<td>MiPS_Solar_Array</td>
<td>SolarArray2</td>
<td>SA2_Generate_Power_SA_B1_Gen</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 Battery4 FailedOff) MBUSU1 FailedOff</td>
<td>1</td>
<td></td>
<td>solararray2 internal Malffer</td>
</tr>
<tr>
<td>FanInCan</td>
<td>Power_Subsystem</td>
<td>MiPS_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 MBUSU1 FailedOff</td>
<td>1</td>
<td></td>
<td>battery1 internal Malffer</td>
</tr>
<tr>
<td>FanInCan</td>
<td>Power_Subsystem</td>
<td>MiPS_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>SolarArray1 FailedOff MBUSU2 FailedOff</td>
<td>1</td>
<td></td>
<td>battery2 internal Malffer</td>
</tr>
<tr>
<td>FanInCan</td>
<td>Power_Subsystem</td>
<td>MiPS_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>SolarArray1 FailedOff MBUSU1 FailedOff</td>
<td>1</td>
<td></td>
<td>battery3 internal Malffer</td>
</tr>
<tr>
<td>FanInCan</td>
<td>Power_Subsystem</td>
<td>MiPS_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>SolarArray2 FailedOff MBUSU1 FailedOff</td>
<td>1</td>
<td></td>
<td>battery4 internal Malffer</td>
</tr>
</tbody>
</table>
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
- System Design Validation
- Safety Analysis
- System Design

SysML Models

- FMEA
- Connectivity
- MEL
- Electronic Procedure
- System Design
- Validation
- Schedule MEL Cost
- Activity Diagrams
- XTCE Connectivity
- SCXML Connectivity
- Modelica Connectivity
- Modelica ATML
- Fault Trees RBD FMEA
- SCXML XTCE FMEAs Cost
- Activity Diagrams
- XTCE ATML
Backup Slides
Generate MEL from SysML

Magic Draw Plug-Ins

SysML Models

MEL
Connectivity Data Exchange

SysML Models

Magic Draw Plug-Ins

Connectivity

Utilized in Connectivity Applications
XML Telemetric and Command Exchange (XTCE): OMG standard for Spacecraft T&C

```xml
<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_DEWPOINT_SENSOR" 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