



Modeling Failure Modes with SysML

Lui Wang and Shira Okon/ ER6

lui.wang-1@nasa.gov

shira.okon@nasa.gov

Spacecraft Software Engineering Branch

JSC

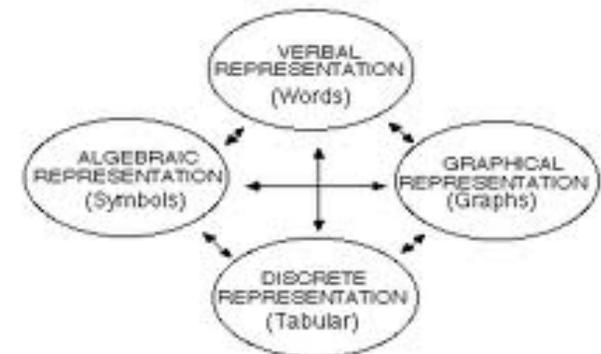
April 10, 2012



Problem



- ◆ **Spacecraft design and operation stakeholders are creating models/artifacts of the same system with different processes, tools, and representations.**
- ◆ **These oft uncoordinated approaches create locally successful products but also create a communication barrier among the various stakeholders (the “Tower of Babel” Effect).**
- ◆ **The same information is captured multiple times, in multiple places, with multiple representations, creating a maintenance challenge.**

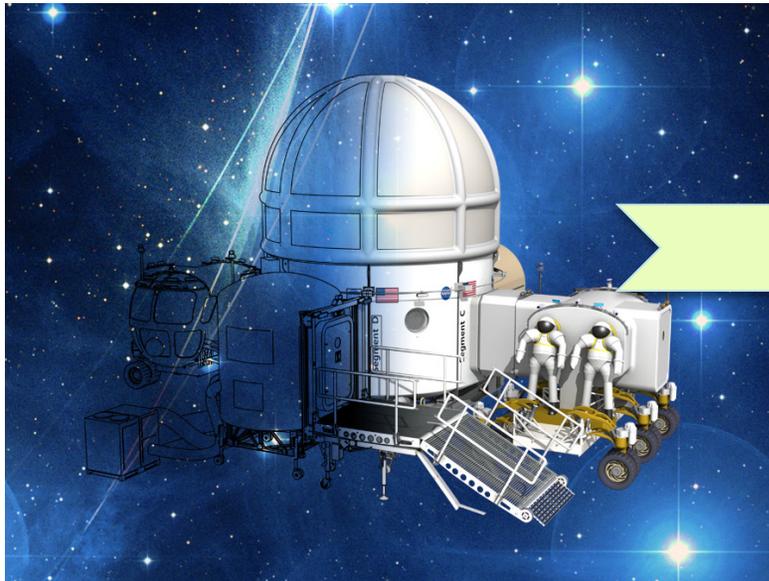




Habitat Demonstration Unit (HDU) Project Description



- ◆ **Multi-center Technology Investment Project started in 2009.**
- ◆ **Objectives:**
 - Evaluate and validate Lunar Surface System (LSS) Habitat Concept efficiency and effectiveness
 - Build, integrate, test, and evaluate the vertical habitat configuration utilizing developmental hardware & software





HDU-DSH Technology & Innovations Demonstrations & Evaluations – 2011



- 1. Inflatable Loft (X-Hab Competition)**
- 2. Logistics-to-Living**
- 3. Autonomous Ops: “Intelligent” Habitat System Management Software**
 - A. Advanced Caution & Warning System and Procedure Execution**
- 4. iHab Digital Double (D²)**
- 5. Power management systems**
- 6. Environmental Protection Technologies**
 - A. Dust Mitigation Technologies**
 - a. Electrodynamic Dust Screen to repel dust from surfaces**
 - b. Lotus Coating**
 - c. Vent Hood at the General Maintenance Workstation**
 - d. Operational Concept for End-to-End Dust Contamination Management**
 - e. Vacuum Cleaner**
 - B. Micrometeoroid Mitigation Technologies**
 - a. Micrometeoroid Detection**
 - C. Radiation**
 - a. Operational Demonstration of Cargo Transfer Bags to deployable blankets for Radiation Protection**
- 7. HDU Core Computing, Wireless Communication and RFID**
- 8. Standards-based Modular Instrumentation System: Wireless Sensor Nodes**
- 9. Flat Surface Damage Detection system**
- 10. MMOD Hab impact monitoring system**
- 11. Telerobotic Workstation**
- 12. General Maintenance/EVA Workstation**
- 13. Medical Ops/Life Science Workstation**
- 14. Geo-Science Lab Glovebox/Workstation**
- 15. Material Handling**
- 16. Food Production: Atrium concept**
- 17. LED Lighting**
- 18. 3-D Layered Damage Detection System for Surfaces**
- 19. Habitability / Habitation**
- 20. Hygiene Module**

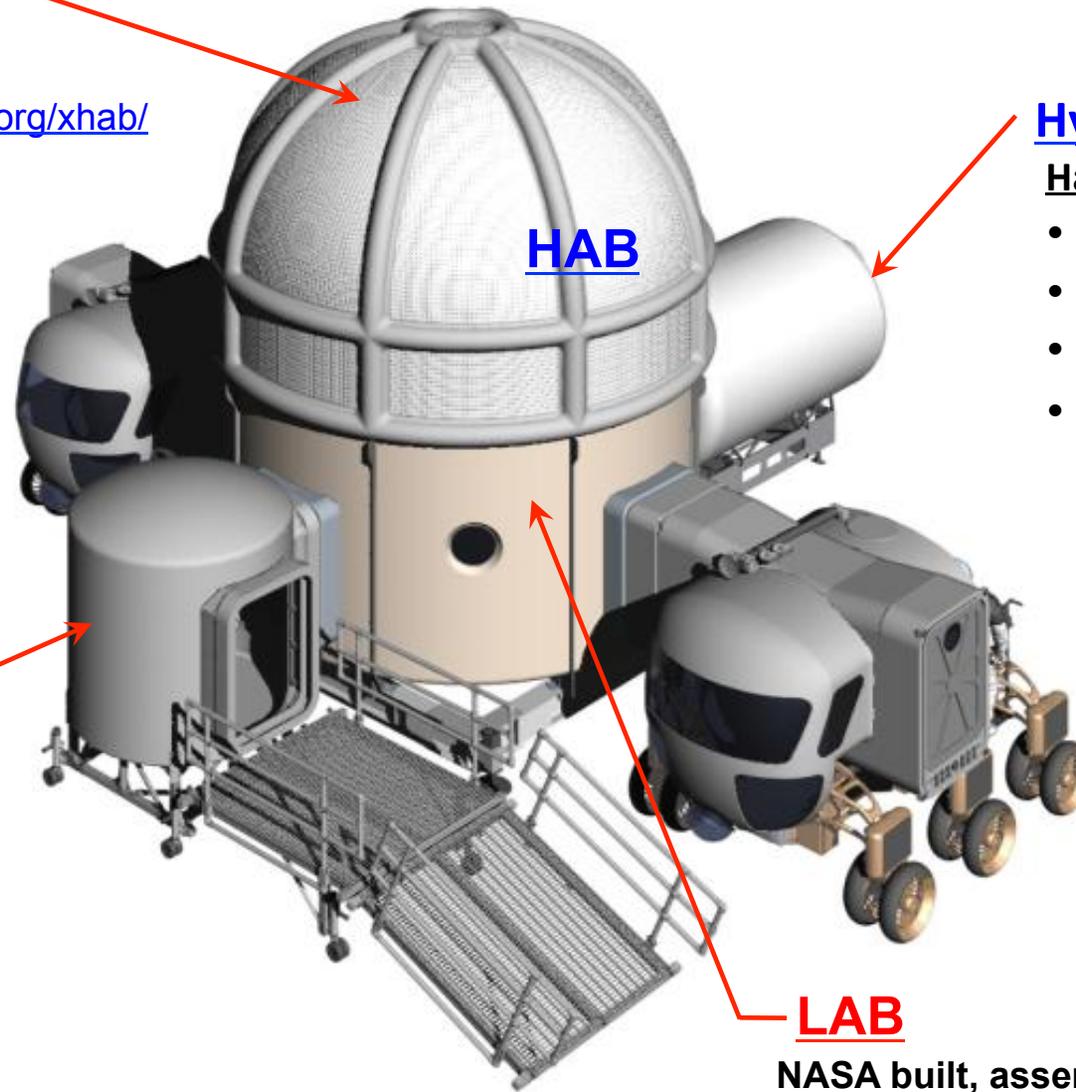


FY11 HDU-DSH Configuration



X-Hab Challenge
Inflatable “Loft”

<http://www.spacegrant.org/xhab/>



Hygiene Module
Habitat Innovation

- Toilet
- Hand Wash
- Whole Body Wash
- Reuses shell from JPL MicroHab

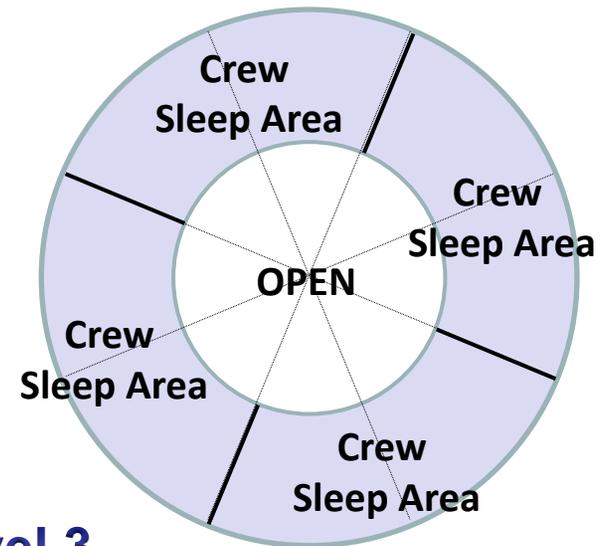
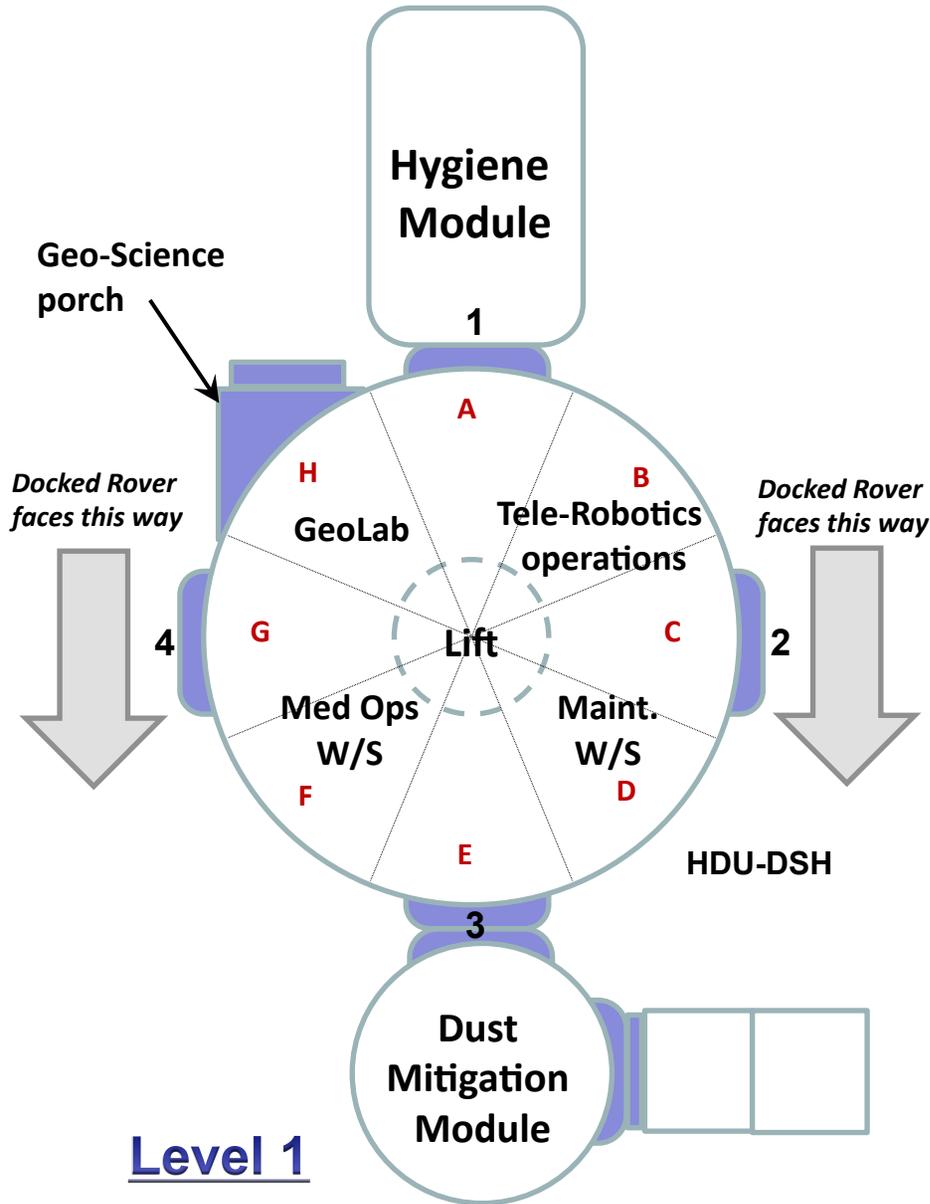
Airlock / Dust Mitigation module

LAB

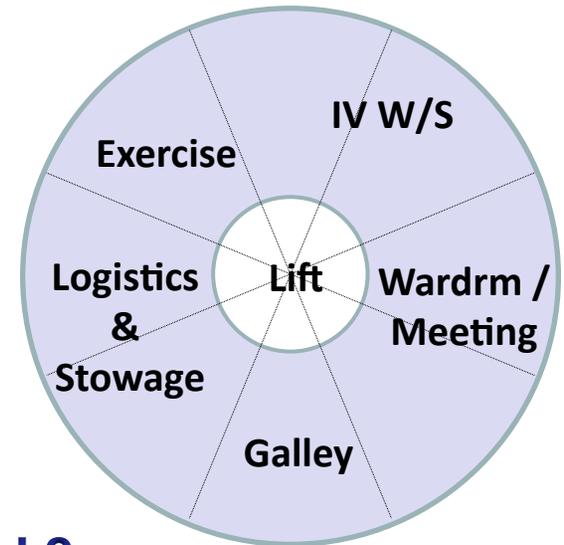
NASA built, assembled, and outfitted a 4-port 1-story vertical Lab in FY10



HDU-DSH Functional Views



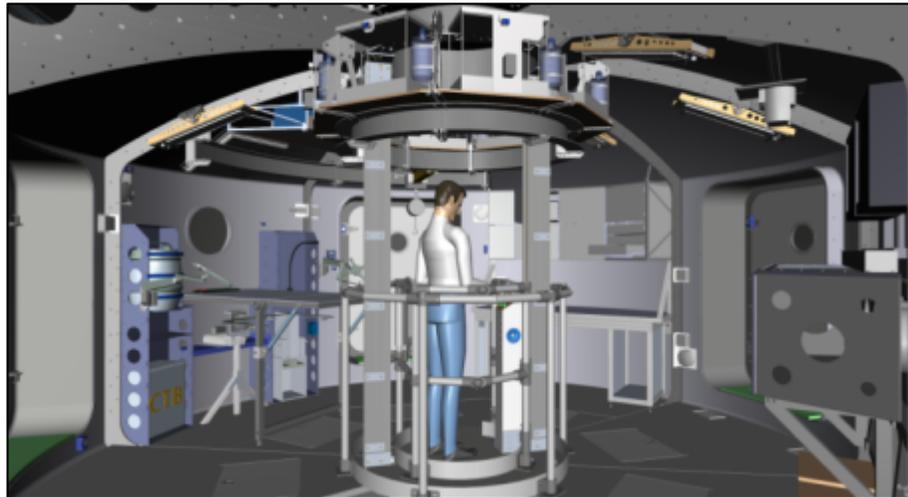
Level 3



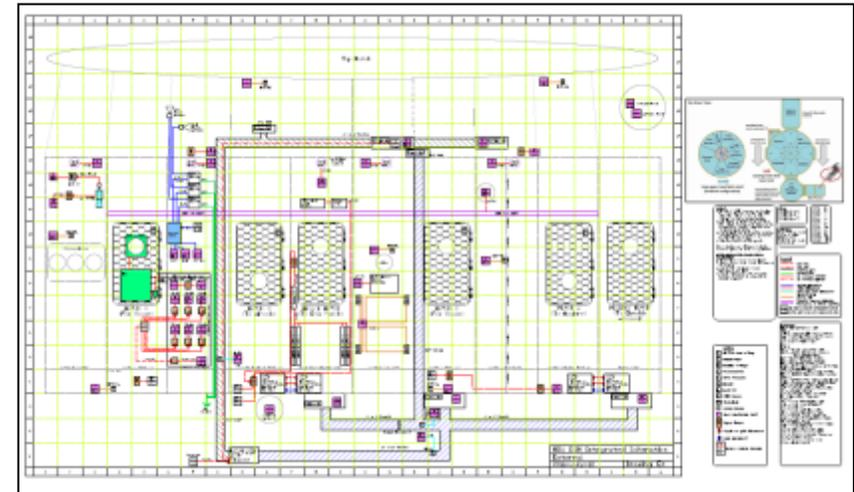
Level 2



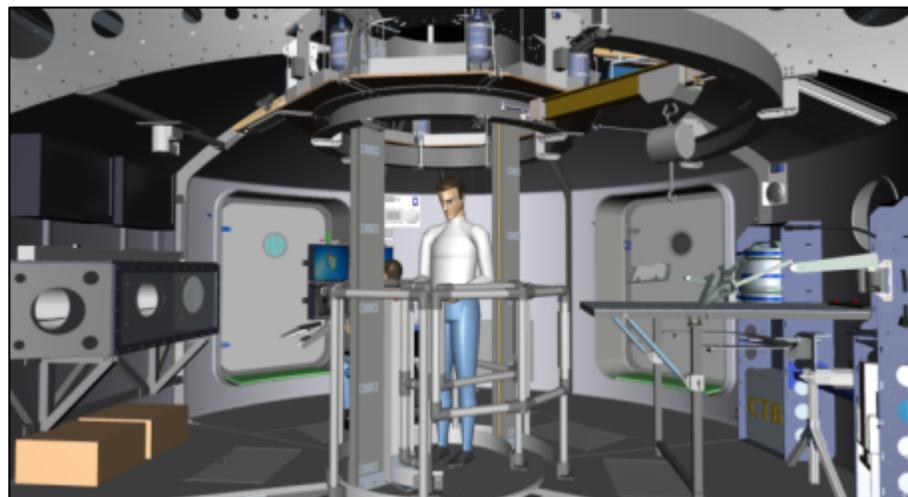
HDU-DSH Systems Integration



CAD Integration invaluable in integrating lift platform with material handling system, lighting, atrium, existing hardware, and access between the two levels



Integrated Schematics invaluable in developing Digital Double Representations of DSH systems and interfaces

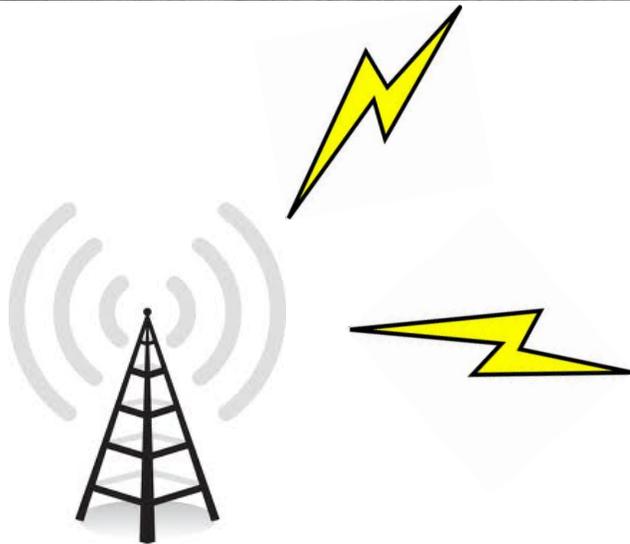




Test Operations



- Desert RaTS 2011 was successfully completed 8/25/11-9/14/11.

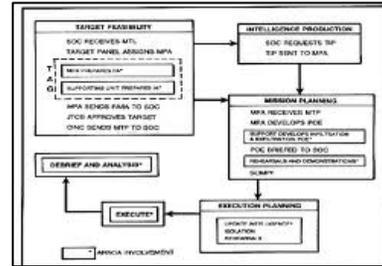




HDU Artifacts by Multiple Stakeholders



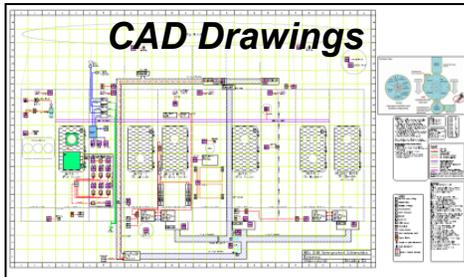
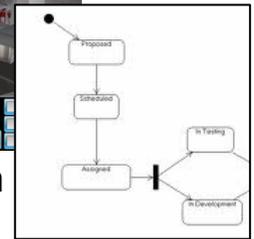
Telemetry and Command



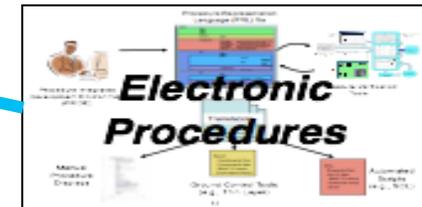
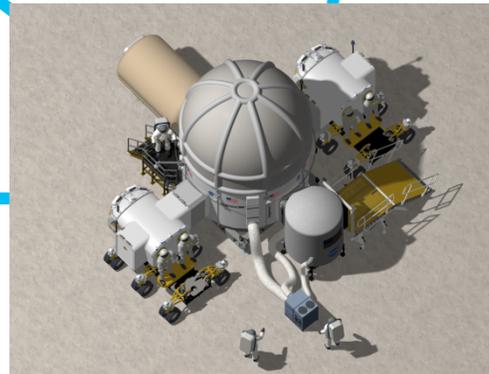
Mission Operation Planning



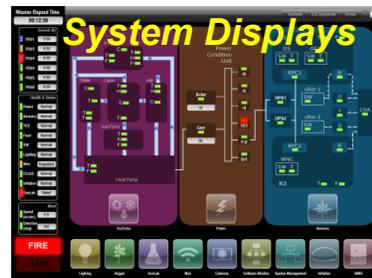
Simulation



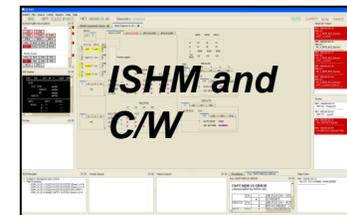
CAD Drawings



Electronic Procedures



System Displays



ISHM and C/W



Proposed HDU Solution



◆ **Build HDU/Deep Space Habitat (DSH) SysML Model**

- Detailed SysML models of all subsystems including the full set of structural and behavioral models from HDU paper artifacts

◆ **Derive Models**

- System connectivity representation in a database
- XTCE capturing Telemetry and Commands for electronic Procedure software
- Fault Management Artifacts (FMEAs, RBDs, TEAMS model, etc)

◆ **Develop Exchange Mechanisms Software**

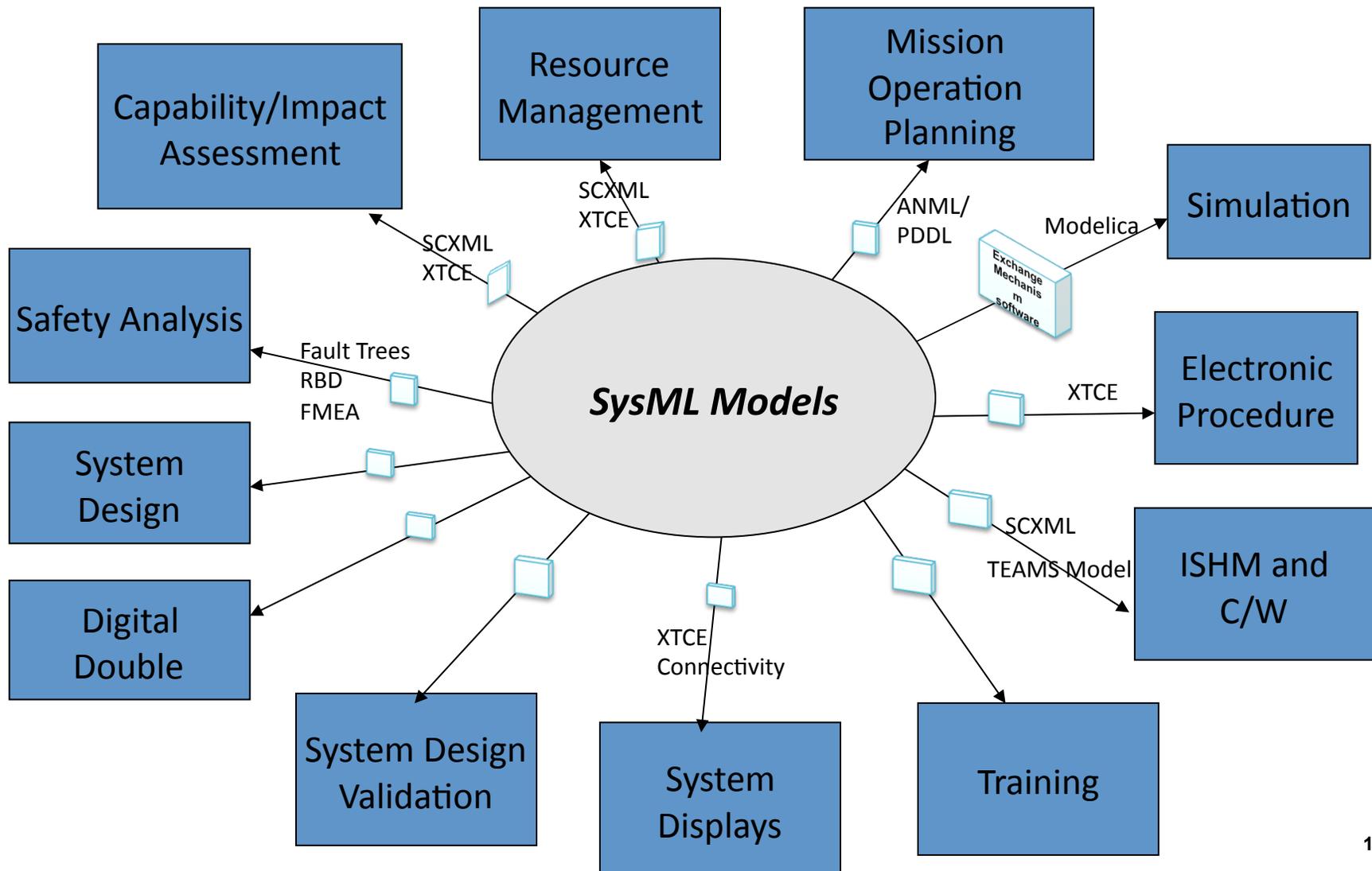
- Initial set of software that translate the models from SysML to other languages/models such as XTCE for Command and Telemetry, Modelica for Simulation, TEAMS models, FMEA, etc...



Uses of System Models



Model once and Use many times





Current HDU SysML Modeling Status



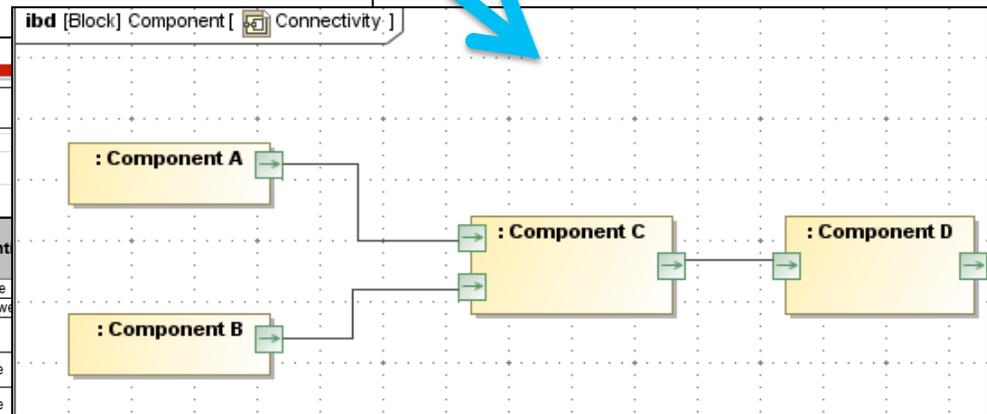
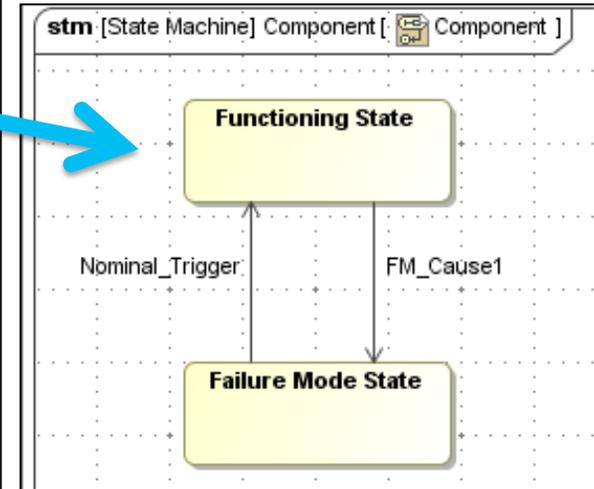
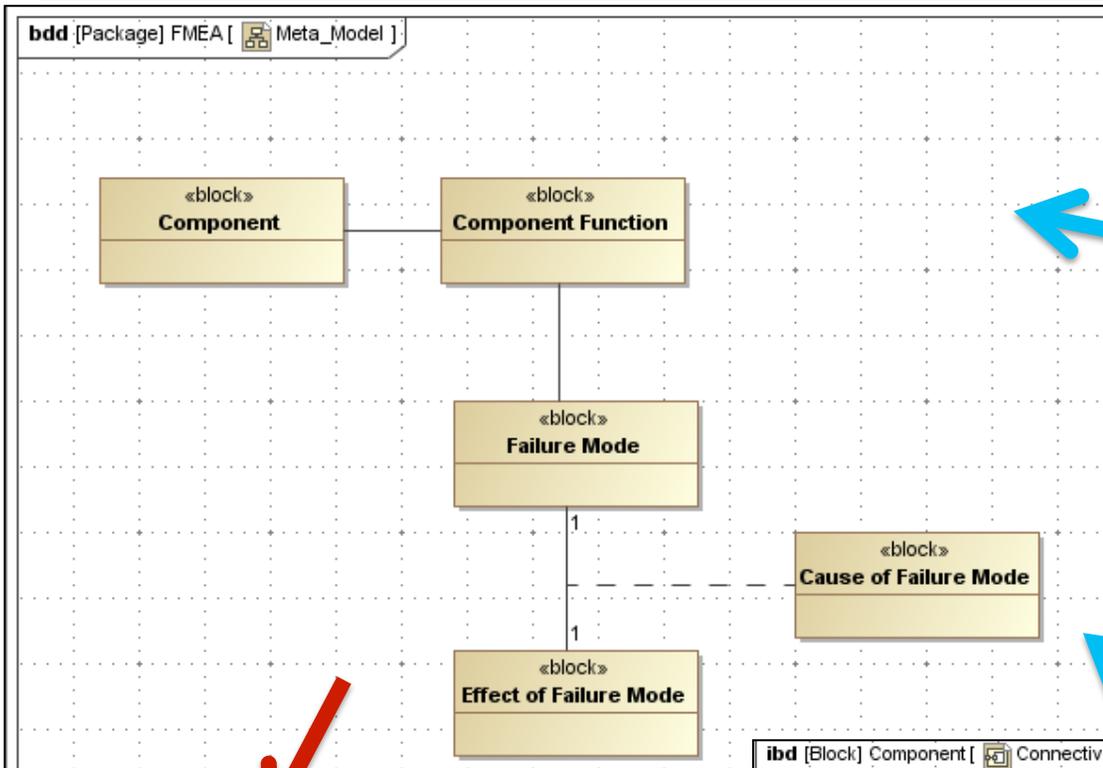
- ◆ Modeled the following HDU elements:
 - Subsystems (Power, ECLSS, Cameras, Lights, WSN, Avionics, etc)
 - System connectivity (power, data, and control)
 - commands and telemetry
 - state machines
 - component function and associated failure mode, cause, and effect

- ◆ Initiated library of re-usable component models

- ◆ Created plug-ins to generate artifacts from SysML models (MagicDraw):
 - Component/master equipment list from Subsystems
 - connectivity information (CSV)
 - XTCE
 - SCXML
 - FMEA artifacts



SysML Meta-Model for FM Artifacts

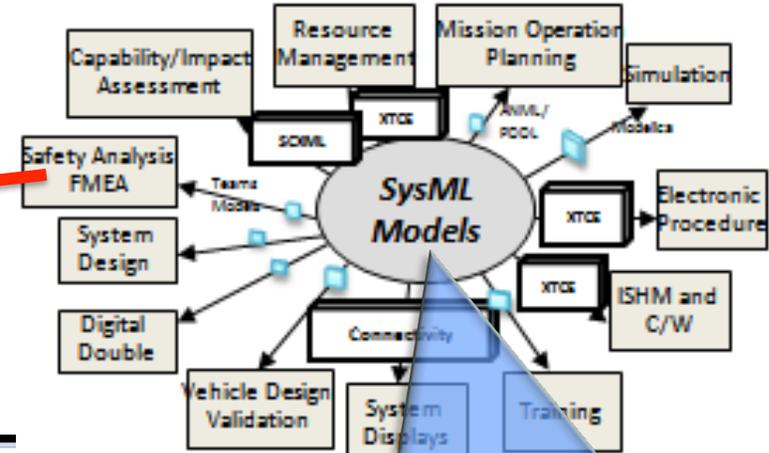
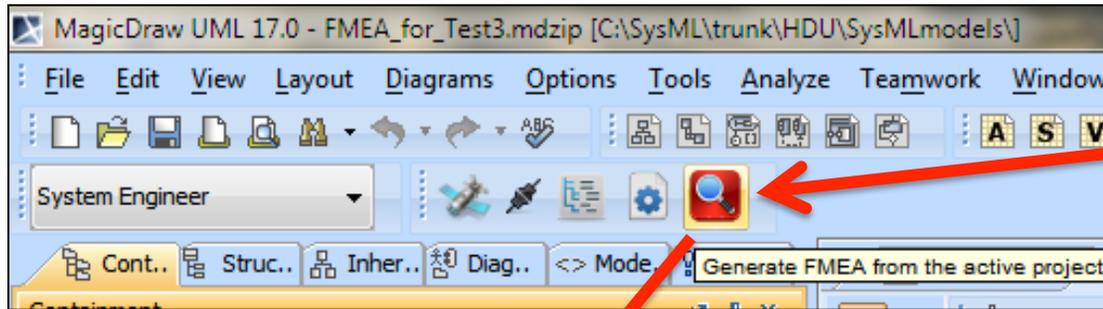


Failure Modes and Effect Analysis (FMEA)

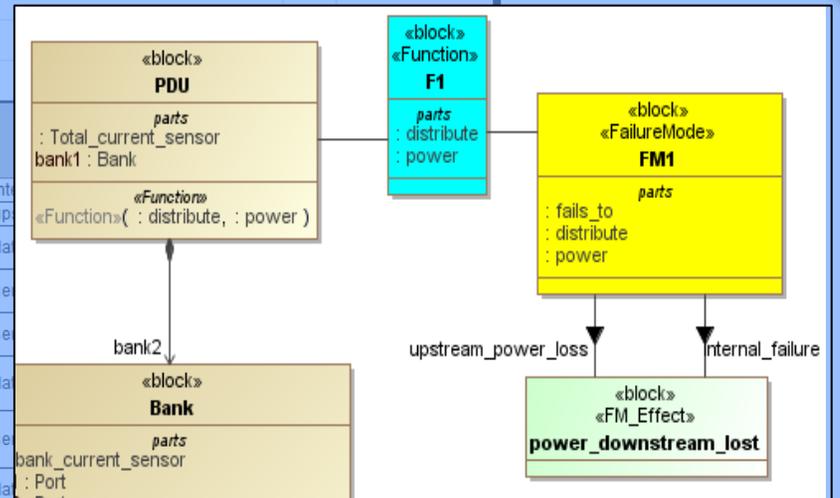
Project Name:		PDU			
Component	Item Function	Potential Failure Mode	Potential Effect(s) of Failure	SEV	Potent
PDU	distribute power	fails_to distribute power	power_downstream_lost		internal_failure
PDU	distribute power	fails_to distribute power	power_downstream_lost		upstream_power
PDU_Bank_bank_current_sensor	monitor current	fails_to monitor current	loss_of_warnings_and_alarms		data_failure
PDU_Bank_bank_current_sensor	monitor current	fails_to monitor current	loss_of_warnings_and_alarms		sensor_failure
PDU_Bank_bank_current_sensor	monitor current	fails_to monitor current	not_monitoring		sensor_failure
PDU_Bank_bank_current_sensor	monitor current	fails_to monitor current	not_monitoring		data_failure
PDU_Bank_bank_current_sensor	monitor current	fails_to monitor current	reduced_ability_to_monitor_current		sensor_failure



Fault Management Exchange

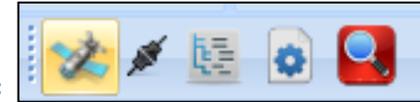


Failure Modes and Effect Analysis (FMEA)				
Project Name:		PDU		
Component	Item Function	Potential Failure Mode	Potential Effect(s) of Failure	SEV
PDU	distribute power	fails_to distribute power	power_downstream_lost	int
PDU	distribute power	fails_to distribute power	power_downstream_lost	up
PDU_Bank_bank_current_sensor	monitor current	fails_to monitor current	loss_of_warnings_and_alarms	da
PDU_Bank_bank_current_sensor	monitor current	fails_to monitor current	loss_of_warnings_and_alarms	se
PDU_Bank_bank_current_sensor	monitor current	fails_to monitor current	not_monitoring	se
PDU_Bank_bank_current_sensor	monitor current	fails_to monitor current	not_monitoring	da
PDU_Bank_bank_current_sensor	monitor current	fails_to monitor current	reduced_ability_to_monitor_current	se
PDU_Bank_bank_current_sensor	monitor current	fails_to monitor current	reduced_ability_to_monitor_current	da
PDU_Bank_bank_current_sensor	monitor current	fails_to monitor current	reduced_ability_to_monitor_current	sensor_degradation
PDU_Bank_bank_current_sensor	monitor current	current_sensor_reads_high_current	loss_of_warnings_and_alarms	data_failure
PDU_Bank_bank_current_sensor	monitor current	current_sensor_reads_high_current	loss_of_warnings_and_alarms	sensor_failure

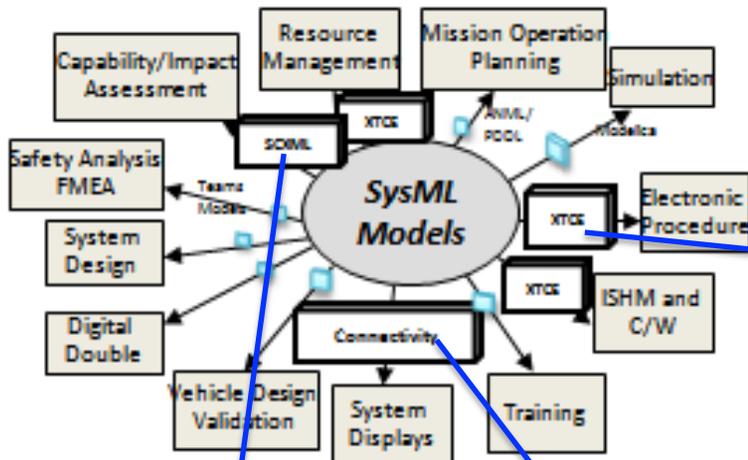




Other Exchange Examples



Magic Draw Plug-Ins:



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

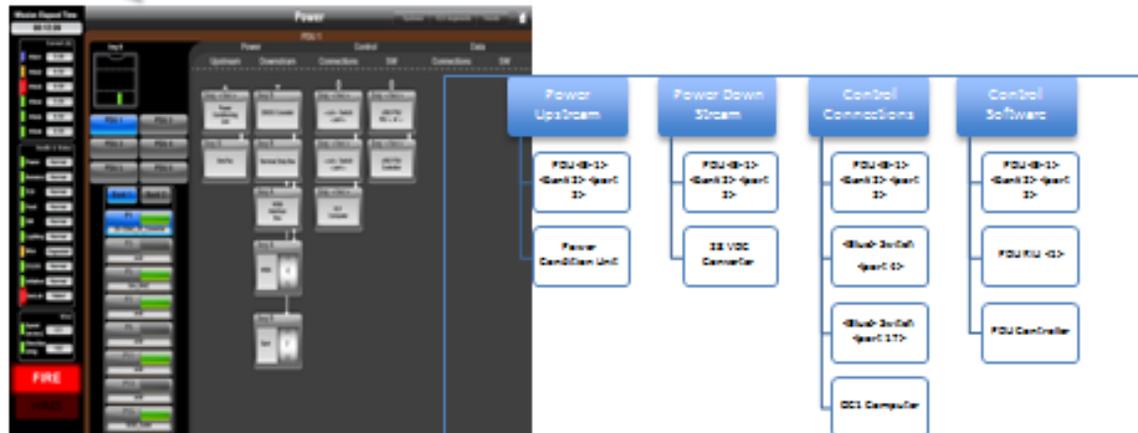
```

<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_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>
      <Parameter parameterTypeRef="HUMIDITY_PRESSURE_SENSOR" </Parameter>
    </ParameterSet>
  </TelemetryMetaData>
</SpaceSystem>
  
```

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

```

<state id="S" initial="s1">
  <state id="s1" initial="s11">
    <onexit> <log expr="leaving s1"/> </onexit>
    <state id="s11">
      <onexit> <log expr="leaving s11"/> </onexit>
    </state>
    <transition event="e" target="s21">
      <log expr="executing transition"/>
    </transition>
  </state>
  
```





Future Work



- ◆ **Further develop SysML to FMEA Generation and FMEA to SysML Import**
- ◆ **Generate RT-TEAMS model (caution and warning system)**
- ◆ **Explore the use of ModelicaML as an extension to the SysML models**
- ◆ **Explore generation of GUNNS (General Use Nodal Network Solver)/Trick manager**
- ◆ **Explore generation of ATML from SysML model**
- ◆ **Maturation of the NASA SysML Foundation profiles by**
 - Extending the habitation models to includes additional stakeholders such as SMA, Mission Operation Training, V&V
 - Selecting new exemplar project domains to ensure coverage of different domains
 - Spacecraft human/unmanned
 - Robotics
 - Develop more exchange mechanisms software to translate from SysML to many stakeholders models/information format
- ◆ **Delivery Processes, Tools to enable support for “significant” GFE project development**



HDU SysML Demo



EXTRA SLIDES



HDU-DSH Views

