A Tool Set for Integrated Software and Hardware Dependability Analysis Using the Architecture Analysis and Design Language (AADL) and Error Model Annex

Myron Hecht, Alex Lam, Chris Vogl,

Presented to
2011 UML/AADL Workshop
Las Vegas, NV

April, 2011
Outline

• AADL vs. UML for Stochastic Analysis of Risk and Reliability
• AADL Error Annex
• Tool Set for Analyzing Risk and Reliability/Availability
• Satellite Example
• FMEA Generation
• Conclusions
AADL vs. UML for Stochastic Analysis of Risk and Reliability

• Advantages
  – Objects directly represent real-time system hardware and software
  – Standard method for incorporation of quantitative attributes
    • Failure and Recovery Probabilistic Distributions
    • Parameters of those distributions
    • Probabilities and rates for individual transitions
  – Standard methods for representing propagation of failures across multiple components
    • Event ports for failure propagations
    • Guards to enable conditional propagations (important for abstractions and reuse)

• Drawbacks
  – No commercial quality tools
    • Public domain tools are available and usable – but not bug free
AADL Error Annex

• AADL annex that supports stochastic analysis
• Defines error model
  – *State transition diagram that represents normal and failed states*
  – *Error models can be associated with hardware components, software components, connections, and “system” (composite) components*
• Error model consists of
  – *State definitions*
  – *Propagations from and to other components*
  – *Probability distribution and parameter definitions*
  – *Allowed state transitions and probabilities*
AADL Error Model Example

**error model example features**
ErrorFree: initial error state;
Failed: error state;
Fail: error event {Occurrence => poisson lambda};
Repair: error event {Occurrence => poisson mu};
Failvisible: in out error propagation {Occurrence => fixed p};
end example;

**error model implementation example.general transitions**
ErrorFree-[Fail]-Failed;
Failed-[Repair]-ErrorFree;
ErrorFree-[in Failvisible]-Failed;
Failed-[out Failvisible]-Failed;
end example.general;
AADL Tool Set

- Eclipse Development Environment (Ganymede) and Eclipse Modeling Framework (EMF)
- Component plug-ins
  - **TopCASED** graphical editor to create AADL architecture diagrams (SEI, Aerospace modifications)
  - **Error Model Editor** graphical editor to create AADL error model diagrams (Aerospace)
  - **OSATE** AADL generator (SEI, Aerospace modifications)
  - **ADAPT-M** Stochastic Petri net to MoBIUS stochastic analysis network tool ((SEI/LAAS Toulouse and Aerospace)
  - **MoBIUS** Quantitative Dependability modeling and prediction tool (University of Illinois, Champaign Urbana)
  - **FMEAGEN** FMEA Generator (Aerospace)
AADL Modeling Tool Set Data Flow

TopCASED → OSATE

AADL Architectural Model

ADAPT

AADL Error Model

Error Model Editor → OSATE

FMEAGEN → FMEA → MS Excel → Qualitative Results

Generalized Stochastic Petri Net

ADAPT-M → SAN file → MoBIUS → Quantitative Results
Tool Set Screen Shot
AADL Components (graphical representation)
Simple Satellite Hardware/Software Architecture Representation

Bus Control Software

Payload Control Software

Vehicle Network

Inter-BCP Bus

Inter-PCP Bus
Simple Satellite MDDA Representation

• Bus and Payload Computers
  – Object names:
    • SBCU (Spacecraft Bus Computer Unit)
    • SPCU (Spacecraft Payload Computer Unit)
  – Payload relies on the Bus, thus whenever the Bus is in Standby, the Payload goes to Standby.
Spacecraft Bus Control Unit (SBCU)

• Architecture Description
  – Dual redundant Bus Control Processors (BCP)
  – Each runs identical copy of bus control software (BCS)

• Failure Behavior
  – Permanent Failures (primarily hardware)
    • A hardware failure results in loss of a processor
    • Two permanent failures result in a mission loss
  – Transient Failures (primarily software)
    • Once BCP is active, when it fails control immediately switches to other processor (hot standby)
    • Switching is not always successful (“imperfect switching”)
      – If successful, then a short (“minor failure”) occurs
      – If not successful, then a longer (“major failure”) occurs
SBCU AADL Architecture Graphical Representation

SBCU Top Level Diagram

Next Lower level:
flight software running on one of two replicated processors
Reusable AADL Representation of SBCU
Stochastic Analysis Representation (product of ADAPT-M conversion)
Results: Uptime vs. Recovery Time

On Orbit Operating Time (Thousands of Hours)

Software Recovery Time (Hours)

Bus Computer Uptime

Payload Computer Uptime
Results: Mission Duration vs. Processor Reliability
Automatically Generated FMEA Features

• Automatically Generated
  – *Utilizes information in petri nets and error models*
  – *Automation enables analyses to be performed repeatedly*
    • Manual analyses are constrained because of cost (typically done only once)

• No limit to number of effect levels
  – *Conventional manually generated FMEAs are done to 3 levels (immediate, next level, end effect)*
  – *Propagations are traced across components*

• Editable
  – *Output Generated in MS Excel*
Example: Supplemental Restraint System
Generation of FMEA from Petri Net of Error Models
Results: Automatically Generated FMEA

<table>
<thead>
<tr>
<th>Item</th>
<th>Initial Failure Mode</th>
<th>1st Level Effect</th>
<th>Failure Mode</th>
<th>2nd Level Effect</th>
<th>Failure Mode</th>
<th>3rd Level Effect</th>
<th>Security</th>
<th>Mitigation</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accelerometer</td>
<td>Failure</td>
<td>Sensor,Accelerometer Failed</td>
<td>Sensor Fail from Accelerometer to ControlUnit</td>
<td>CPU, ControlUnit Failed</td>
<td>CPU Fail from ControlUnit to Airbag</td>
<td>Actuator, Airbag Not Ready</td>
<td>[State Property]</td>
<td>[Designer Input]</td>
<td>[Analyst Input]</td>
</tr>
<tr>
<td>ControlUnit</td>
<td>Failure</td>
<td>CPU, ControlUnit Failed</td>
<td>CPU Fail from ControlUnit to Airbag</td>
<td>Actuator, Airbag Not Ready</td>
<td>[State Property]</td>
<td>[Designer Input]</td>
<td>[Analyst Input]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Actuator</td>
<td>Failure</td>
<td>Actuator, Airbag Not Ready</td>
<td>[State Property]</td>
<td>[Designer Input]</td>
<td>[Analyst Input]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Enhanced formatting for presentation purposes
## Excerpt of Automatically Generated FMEA for 10-state error model

<table>
<thead>
<tr>
<th>ID</th>
<th>Item</th>
<th>Initial Failure</th>
<th>1st Level Effect</th>
<th>Transition</th>
<th>2nd Level Effect</th>
<th>Transition</th>
<th>3rd Level Effect</th>
<th>Transition</th>
<th>4th Level Effect</th>
<th>Transition</th>
<th>5th Level Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>SBCU.Primary_SU Failure</td>
<td>SU.SBCU_Primary ReportDown</td>
<td>SBCU.Sdown from SBCU.Primary_SU to SBCU.Primary_SU</td>
<td>SU.SBCU_Primary Down</td>
<td>SU.SBCU_Primary ReportRecover</td>
<td>SBCU.Srecover from SBCU.Primary_SU to SBCU.Primary_SU</td>
<td>SU.SBCU_Primary HotStandby</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2</td>
<td>SBCU.Primary_SU Failure</td>
<td>SU.SBCU_Primary Down</td>
<td>SU.SBCU_Primary ReportRecover</td>
<td>SBCU.Srecover from SBCU.Primary_SU to SBCU.Primary_SU</td>
<td>SU.SBCU_Primary HotStandby</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3</td>
<td>SBCU.FMS guardin PrimaryDown</td>
<td>FMS.SBCU UsingPrimary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>SBCU.Backup_SU Failure</td>
<td>SU.SBCU_Backup ReportDown</td>
<td>SBCUSdown from SBCU.Backup_SU to SBCU.Backup_SU</td>
<td>SU.SBCU_Backup RecoverMajor</td>
<td>SBCU.Srecover from SBCU.Backup_SU to SBCU.Backup_SU</td>
<td>SU.SBCU_Backup HotStandby</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2</td>
<td>SBCU.Backup_SU Failure</td>
<td>SU.SBCU_Backup ReportRecover</td>
<td>SBCU.Srecover from SBCU.Backup_SU to SBCU.FMS FMS.SBCU UsingBackup</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1</td>
<td>SBCU.Primary_PU Failure</td>
<td>PU.SBCU Terminated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.2</td>
<td>SBCU.FMS guardin PrimaryTerminated</td>
<td>FMS.SBCU PrimaryisTerminated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1</td>
<td>SBCU.Backup_PU Failure</td>
<td>PU.SBCU Terminated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.2</td>
<td>SBCU.FMS guardin BackupTerminated</td>
<td>FMS.SBCU Down</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1</td>
<td>SPCU.Primary_SU Failure</td>
<td>SU.SPCU_Primary ReportDown</td>
<td>SPCUSdown from SPCU.Primary_SU to SPCU.Primary_SU</td>
<td>SU.SPCU_Primary Down</td>
<td>SU.SPCU_Primary ReportRecover</td>
<td>SPCU.Srecover from SPCU.Primary_SU to SPCU.Primary_SU</td>
<td>SU.SPCU_Primary HotStandby</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.2</td>
<td>SPCU.Primary_SU Failure</td>
<td>SU.SPCU_Primary Down</td>
<td>SU.SPCU_Primary ReportRecover</td>
<td>SPCU.Srecover from SPCU.Primary_SU to SPCU.FMS FMS.SPCU UsingPrimary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>SPCU.Backup_SU Failure</td>
<td>SU.SPCU_Backup ReportDown</td>
<td>SPCUSdown from SPCU.Backup_SU to SPCU.Backup_SU</td>
<td>SU.SPCU_Backup Down</td>
<td>SU.SPCU_Backup ReportRecover</td>
<td>SPCU.Srecover from SPCU.Backup_SU to SPCU.FMS FMS.SPCU UsingBackup</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>SPCU.FMS guardin PrimaryDown</td>
<td>FMS.SPCU Down</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.1</td>
<td>SPCU.Primary_PU Failure</td>
<td>PU.SPCU Terminated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.2</td>
<td>SPCU.FMS guardin PrimaryTerminated</td>
<td>FMS.SPCU PrimaryisTerminated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.1</td>
<td>SPCU.Backup_PU Failure</td>
<td>PU.SPCU Terminated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.2</td>
<td>SPCU.FMS guardin BackupTerminated</td>
<td>FMS.SPCU Down</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>SPCU.Primary_SU Failure</td>
<td>SU.SPCU_Primary ReportDown</td>
<td>SPCUSdown from SPCU.Primary_SU to SPCU.Primary_SU</td>
<td>SU.SPCU_Primary Down</td>
<td>SU.SPCU_Primary ReportRecover</td>
<td>SPCU.Srecover from SPCU.Primary_SU to SPCU.Primary_SU</td>
<td>SU.SPCU_Primary HotStandby</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>SPCU.Primary_SU Failure</td>
<td>SU.SPCU_Primary Down</td>
<td>SU.SPCU_Primary ReportRecover</td>
<td>SPCU.Srecover from SPCU.Primary_SU to SPCU.FMS FMS.SPCU UsingPrimary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>SPCU.FMS guardin PrimaryDown</td>
<td>FMS.SPCU Down</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>SPCU.FMS guardin BackupDown</td>
<td>FMS.SPCU Down</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>SPCU.Primary_SU Failure</td>
<td>SU.SPCU_Primary ReportDown</td>
<td>SPCUSdown from SPCU.Primary_SU to SPCU.Primary_SU</td>
<td>SU.SPCU_Primary Down</td>
<td>SU.SPCU_Primary ReportRecover</td>
<td>SPCU.Srecover from SPCU.Primary_SU to SPCU.Primary_SU</td>
<td>SU.SPCU_Primary HotStandby</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>SPCU.Primary_SU Failure</td>
<td>SU.SPCU_Primary Down</td>
<td>SU.SPCU_Primary ReportRecover</td>
<td>SPCU.Srecover from SPCU.Primary_SU to SPCU.FMS FMS.SPCU UsingPrimary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>SPCU.FMS guardin PrimaryDown</td>
<td>FMS.SPCU Down</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Conclusions

• A new generation tool set for quantitative stochastic analysis and qualitative Failure Modes and Effects Analysis (FMEAs) for space systems is under development
  – Based on use of the Architecture Analysis and Design Language (AADL)
  – Graphically oriented
  – Modularized with reusable components

• Results will be able to support decisions from concept development through detailed design
  – Extent and type of redundancy
  – Tradeoffs of reliability vs. Weight, power, and functional capability
  – Failure rate and recovery time requirements
  – Strategies for recovering from computing disruptions
  – Handling failure propagation and common mode failures