Automated Generation of Failure Modes and Effects Analyses from AADL Architectural and Error Models

Myron Hecht, Alexander Lam, Russell Howes, and Christopher Vogl, The Aerospace Corporation

Presented to
Systems and Software Technology Conference
Salt Lake, City, UT
April, 2010
Outline

• Motivation
• Background on FMEAs
• Introduction to AADL
• AADL Error Model Annex
• Tool Set for Analyzing Risk and Reliability/Availability
• Automated FMEA Generation Example
• Additional Discussion
• Conclusions
Motivation

• Failure Modes and Effects Analyses (and related Criticality Analyses) are rigorous and comprehensive reliability and safety design evaluations
  – Generally required either by industry standards or Government policies
  – A fundamental element of defense in many product liability lawsuits

• When performed manually, FMEAs are usually done only once during the detailed design phase because of cost and schedule constraints
  – Labor intensive
  – Require senior level; analysts

• If automated, FMEAs would have significant benefits
  – Multiple iterations from conceptual to detailed design
  – Enables early identification of potential problems
    • Single points of failure
    • Unanticipated effects
  – Facilitates tradeoff studies and evaluations of alternatives
Failure Modes and Effects Analysis (FMEA)

• Purpose
  – To determine the effect of hardware and software failures upon the system and equipment failures.
    • Classify effects by impact on mission success and personnel/equipment safety.
    • Identify single points of failure

• History
  – First defined as Military Procedure MIL-P-1629, “Procedures for Performing a Failure Mode, Effects and Criticality Analysis”, November 1949.
  – Further developed and applied by NASA in the 1960’s to improve and verify reliability of space program hardware.
  – Since the 1980s, a standard of practice in a wide variety of industries
    • DoD: MIL-STD-1629A
    • Industrial: IEC 60812 (1985)
    • Aviation: SAE ARP 5580 (2001)
    • Automotive: SAE J1739 (2002)
    • Space: ECSS-Q-30-02A
# FMEA Methodology

<table>
<thead>
<tr>
<th>Conventional</th>
<th>Automated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define Ground Rules and Assumptions</td>
<td>• Ground rules and assumptions defined by component properties</td>
</tr>
<tr>
<td>Levels of indenture</td>
<td>• Components and failure modes defined in models</td>
</tr>
<tr>
<td>Components to be considered</td>
<td>• Effects identified through graph tracing</td>
</tr>
<tr>
<td>Failure modes by component category</td>
<td></td>
</tr>
<tr>
<td>Severity Level Definitions</td>
<td></td>
</tr>
<tr>
<td>Rules for recovery mechanisms and compensating provisions</td>
<td></td>
</tr>
<tr>
<td>For Each Component</td>
<td></td>
</tr>
<tr>
<td>Postulate failure and failure mode</td>
<td></td>
</tr>
<tr>
<td>Identify immediate effect of failure</td>
<td></td>
</tr>
<tr>
<td>Identify next higher level effects and “end effects”</td>
<td></td>
</tr>
<tr>
<td>Identify compensating provisions</td>
<td></td>
</tr>
<tr>
<td>Evaluate severity level at end effect</td>
<td></td>
</tr>
</tbody>
</table>
FMEA Output

*In Either Worksheet or Tabular Format…*

- Identification: Failure Mode identification.
- Item: For software, a process in its context.
- Failure Mode:
  - **Immediate Effect:**
  - **Intermediate Effect: Second level effect.**
    - Operator
    - External networks
    - Database
    - Recovery
  - **End Effect:**
    - System Level (e.g., Individual satellites or the constellation through TT&C functions)
    - Payload performance
    - Data to outside users through terrestrial interfaces
- Existing Mitigations: Any existing mitigations present in the architecture or design were identified.
- Severity level:
  - *Set under assumption that existing mitigations assumed to work*
- Comments:
  - Additional comments documenting assumptions and uncertainties.
Introduction to the Architecture Analysis & Design Language (AADL)

• Society of Automotive Engineers (SAE) Aerospace Standard AS5506 (2004)
  – Preceded by more than a decade of development under the DARPA Meta-H program
• Provides a standardized textual and graphical notation for describing software and hardware system architectures and their functional interfaces
  – architectures (using standard language).
  – expected program behavior (using behavior annex)
  – Failure and recovery behavior (using error annex)
AADL vs. other OMG Languages 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 Components (graphical representation)

- text and xml representations also defined
AADL Error Model 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*
Enabling Features of AADL

• Standard representation of architecture and error models
• Representation of failure propagation through system components
  – Event Ports
  – Guards
  – Propagations
• Error Model properties
  – Working status of states
  – Descriptive information for initial states, effects (subsequent states), and failure modes (transitions)
  – Initial states
  – Terminal States
AADL Error Model Example

**Error model example features**
ErrorFree: initial error state;
Failed: error state;
Fail: error event \{Occurrence $\Rightarrow$ poisson lambda\};
Repair: error event \{Occurrence $\Rightarrow$ poisson mu\};
Failvisible: in out error propagation \{Occurrence $\Rightarrow$ 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 (The Aerospace Corporation newly developed)
  – **OSATE** AADL generator (SEI, The Aerospace Corporation modifications)
  – **ADAPT-M** Stochastic Petri net to MoBIUS stochastic analysis network tool ((SEI/LAAS Toulouse and The Aerospace Corporation)
  – **MoBIUS** Quantitative Dependability modeling and prediction tool (University of Illinois, Champaign Urbana)
  – **FMEAGEN** FMEA Generator (The Aerospace Corporation newly developed)
AADL Modeling Tool Chain Data Flow

Qualitative Analysis Chain
- FMEAGEN
- FMEA
- MS Excel
- Qualitative Results

Quantitative Analysis Chain
- ADAPT-M
- SAN file
- MoBIUS
- Quantitative Results

TopCASED → OSATE → AADL Architectural Model → ADAPT → Generalized Stochastic Petri Net

AADL Error Model → Error Model Editor → OSATE
Tool Set Screen Shot
FMEA Generation Algorithm Features

• Automatically traces from all working states to failure states
  – *Terminates when trace detects a restoration condition or a failure condition*
• Not limited to only 3 levels of effects
• Checks to prevent repeated visits to same states
  – *Ensures termination*
  – *Of particular importance for recoverable systems*
Example: Supplemental Restraint System

Architectural Model

Error Models
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>Severity</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 Control Unit</td>
<td>CPU,ControlUnit Failed</td>
<td>CPU Fail from Control Unit to Airbag</td>
<td>Actuator,Airbag NotReady</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ControlUnit</td>
<td>Failure</td>
<td>CPU,ControlUnit Failed</td>
<td>CPU Fail from Control Unit to Airbag</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Actuator</td>
<td>Failure</td>
<td>Actuator,Airbag NotReady</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
More Complex Error Model
<table>
<thead>
<tr>
<th>ID</th>
<th>Item Name</th>
<th>Device</th>
<th>Failure Mode</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>
<th>Transition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SBCU.Primary_SU</td>
<td>Node</td>
<td>Failure</td>
<td>SU.SBCU_Primary ReportDown</td>
<td>SBCU.Primary SU to SBCU.Primary_SU</td>
<td>SU.SBCU_Primary HotStandby</td>
<td>SBCU.Primary SU to SBCU.FMS FMS.SBCU UsingPrimary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>SBCU.Backup_BU</td>
<td>Node</td>
<td>Failure</td>
<td>SBCU_backup BU to SBCU.Backup_SU</td>
<td>SBCU.Backup_BU to SBCU.Backup_SU</td>
<td>SBCU.Backup_BU to SBCU.FMS FMS.SBCU UsingBackup</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>SPCU.Primary_SU</td>
<td>Node</td>
<td>Failure</td>
<td>SPCU_Primary_ReportDown</td>
<td>SPCU_Primary SU to SPCU.Primary_SU</td>
<td>SPCU_Primary HotStandby</td>
<td>SPCU_Primary SU to SPCU.FMS FMS.SPCU UsingPrimary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>SPCU.Backup_BU</td>
<td>Node</td>
<td>Failure</td>
<td>SPCU_backup BU to SPCU.Backup_SU</td>
<td>SPCU_Backup_BU to SPCU.Backup_SU</td>
<td>SPCU_Backup_BU to SPCU.FMS FMS.SPCU UsingBackup</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>SPCU.Primary_PU</td>
<td>Node</td>
<td>Failure</td>
<td>SPCU_Primary_PU</td>
<td>SPCU_Primary SU to SPCU.Primary_SU</td>
<td>SPCU_Primary HotStandby</td>
<td>SPCU_Primary SU to SPCU.FMS FMS.SPCU UsingPrimary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>SPCU.Backup_PU</td>
<td>Node</td>
<td>Failure</td>
<td>SPCU_Backup_PU</td>
<td>SPCU_Backup_SU to SPCU.Backup_SU</td>
<td>SPCU_Backup_SU to SPCU.FMS FMS.SPCU UsingBackup</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Results:** Automatically Generated FMEA
Tool Set Capabilities for Quantitative Evaluation

AADL Architecture and Error Models

Mobius Stochastic Analysis Network Model

Results
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

• Automated Generation of FMEA/CA enables multiple iterations analyses throughout all stages of the design
  – Allows design alternatives to be evaluated
    • Strategies for recovering from computing disruptions
    • Handling failure propagation and common mode failures
  – Enables safety and reliability problems to be identified early
    • Of critical importance to all users and stakeholders
    • Significant economic value where products liability is an issue because of conforming and exceeding standard of care
Acronyms

ADAPT: AADL Architectural models to stochastic Petri nets through model Transformation,
AADL: Architecture Analysis & Design Language
FMEA: Failure Mode and Effects Analysis
FMEA/CA: FMEA /Criticality Analysis
OSATE: Open Source AADL Tool Environment (Software tool integrated into Eclipse)
SAE: Society of Automotive Engineers
SAN: Stochastic Analysis Network
TOPCASED: Toolkit In OPen source for Critical Applications & SystEms Development
References

• IEC 60812 (1985) Analysis techniques for system reliability - Procedures for failure mode and effect analysis (FMEA), International Electrotechnical Commission,
• SAE J1739 (2002) Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA) and Effects Analysis for Machinery (Machinery FMEA), Society of Automotive Engineers, available online from www.sae.org

All trademarks, service marks, and trade names are the property of their respective owners