Supporting Safety Evaluation Process using AADL

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Julien Delange and Peter Feiler
12/09/2013
Safety Analysis issues (aka the problem)

**Manual process, inaccurate with system implementation**

Some errors are **not captured/caught during analysis**

**Long and error-prone evaluation process**

Different understanding of System Specifications

Manual Process

Inconsistent Development and Introduction of Errors

Implementation + Tests

Certification documents

Safety Evaluation Report
Automate/Improve Evaluation (aka the solution)

Derives materials from existing artifacts (i.e. architecture models)

Avoid manual process traps and pitfalls

Automate evaluation, reduce analysis time
Combine existing methods (aka the approach)

Add safety-information to existing models

Automate the evaluation process, avoid manual efforts

Generate materials required by safety standards (ARP4761)
Agenda

Overview of AADL & Error-Model Annex

Overview of ARP4761 and Safety Evaluation

Support of Safety Evaluation with AADL

Case-Study

On-Going Work

Discussion
Agenda

Overview of AADL/Error-Model Annex

Overview of ARP4761 & Safety Evaluation

Support of Safety Evaluation with AADL

Case-Study

On-Going Work

Discussion
Architecture Analysis Design Language

Modeling language standardized by SAE
  Inherit MetaH concepts
  Initiated in 2003; revised in 2008

Design of hardware and software
  Analysis of different criteria (performance, safety, security, etc.)
  Tool support: OSATE, Ocarina, MASIW

Evaluation during research projects
  SAVI: avionics community
  ASSERT: aerospace community
Overview of Error-Model Annex

Extension of AADL for fault description: error events, propagations, etc.

Integration with current models by extending existing components

Draft document to be proposed as a standard annex

Support for Safety Evaluation and Analysis
Error Types and propagations

Error types: error classification

Extensions and renaming

Error propagations across components
Associate errors with system connections
Define error sources, sinks and containment

Error Source of ValueError
Sensor

Sink for ValueError & source for NoData
ValueError
Processing

Error Sink for NoData
NoData
Actuator
Error behavior

States machines
- Error-related transitions
- Propagation rules
- Use of error types

Composite behavior
- Define system states according to its parts
  - ex: “I am failing if one of my component is failing”

Subsystem 1 (Normal)  Subsystem 2 (Normal)  Subsystem 1 (Normal)  Subsystem 2 (Failing)
Support of AADL textual syntax

Error types mechanism w/ extensions

Error propagations

Sensor → Processing

ValueError

Composite error state Machine

Sensor (Operational) → Processing (Operational) → Actuator (Operational)

Operational
Specific Error-Model Properties

Severity, likelihood, error description

Support for generating validation documentation

Tailoring for safety standards (ARP4761, MIL-STD-882)
Agenda

Overview of AADL & Error-Model Annex

Overview of ARP4761 & Safety Evaluation

Analysis of System Safety with AADL

Case-Study

On-Going Work

Discussion
ARP4761 Safety Standard

SAE standard for Safety Assessment
  Avionics Community mostly (relation with DO178B)
  Assurance of System Safety

Define Safety Evaluation Process Materials & Methodology
  Iterative process, follow development workflow
  Inter-connection between documents (cross checks)

Use in the SAE AIR6110 standard
  Example of safety evaluation process
  Wheel-Brake System Example
Safety Analysis Workflow

Aircraft-level (functions)
- Define failure conditions
- Allocate failure to system functions

Preliminary System Safety Assessment
- System Functional Hazard Analysis (FHA)
- System Fault-Tree Analysis (FTA)

System Safety Assessment
- Failure Mode and Effect Analysis
- Refined FTA with Quantitative Failures Rates

System Development Cycle
Functional Hazard Analysis

Identify and classify functions failure conditions

Aircraft or System Level

Aircraft, High-Level View

Refinement at System Level

Input for safety requirements specification

Description and specification in FTA, DD or MA

Reference of Aircraft Low-Level to System FHA

Spreadsheet with reference to functions failures description
Fault-Tree Analysis

Relationship of failure effects and failure modes

Reference to system hierarchy

Support with Open-Source and Commercial Tools

Fault Occurrence
Failure Mode

Initial Failure Mode
Markov Chain

Evaluation of system behavior over time

Probability of being in particular states

Analysis and evaluation of fault states

Support with Commercial and Open-Source Tools
Failure Mode and Effect Analysis

Impact of Fault at a Higher Levels

Start from Function Level to System/Aircraft Level

Spreadsheet/textual document

<table>
<thead>
<tr>
<th>Function Name</th>
<th>Failure Mode</th>
<th>Failure Rate (E-6)</th>
<th>Flight Phase</th>
<th>Failure Effect</th>
<th>Detection Method</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>+5 Vott</td>
<td>+5V out of spec.</td>
<td>0.2143</td>
<td>All</td>
<td>Possible P/S shutdown</td>
<td>Power Supply Monitor trips, shuts down supply and passes “invalid power supply (P/S)” to other BSCU system</td>
<td>BSCU channel fails</td>
</tr>
<tr>
<td>+5V short to ground</td>
<td>0.2857</td>
<td>All</td>
<td>P/S shutdown</td>
<td>Power supply monitor passes invalid P/S to other BSCU system</td>
<td>BSCU channel fails</td>
<td></td>
</tr>
<tr>
<td>Loss of / reduced filtering</td>
<td>0.3571</td>
<td>All</td>
<td>Increase Ripple</td>
<td>May pass out of spec voltage to rest of BSCU if ripple is such that it is not detected by the P/S monitor</td>
<td>May cause spurious P/S monitor trip</td>
<td></td>
</tr>
<tr>
<td>+5 V open</td>
<td>0.5714</td>
<td>All</td>
<td>P/S shutdown</td>
<td>Power supply monitor passes invalid P/S to other BSCU system</td>
<td>BSCU channel fails</td>
<td></td>
</tr>
<tr>
<td>No Effect</td>
<td>0.1429</td>
<td>All</td>
<td>No Effect</td>
<td>None/No Effect</td>
<td>No Effect</td>
<td></td>
</tr>
</tbody>
</table>

Total Failure Rate of +5V Supply: 1.5714
Agenda

Overview of AADL & Error-Model Annex

Overview of ARP4761 & Safety Evaluation

Support of Safety Evaluation with AADL

Case-Study

On-Going Work

Discussion
AADL & Safety Evaluation – Tool Overview

FHA
- Spreadsheet
- Use error propagations

FTA
- CAFTA
- Use composite behavior
- Error flows

Markov Chain
- PRISM
- Use error flow
- Error behavior

FMEA
- Spreadsheet
- Error behavior
- Propagations
Safety Analysis & AADL

Preliminary System Safety Assessment (PSSA) support
- High-level component, interfaces from the OEM
- Automatic generation of validation materials (FHA, FTA)

System Safety Assessment (SSA) support
- Use refined models from suppliers
- Enhancement of error specifications
- Support of quantitative safety analysis (FTA, FMEA, MA)
Evolution of Safety Analysis process with AADL

Preliminary System Safety Assessment

Component types (system interfaces)

Component implementation

Validation Materials (FHA, FTA)

Check PSSA and SSA consistencies

Validation with quantitative fault rates (FMEA, FTA, DD, MA)

System Safety Assessment

Refinement & development evolution
Safety Analyses on Refined Architecture

Aircraft-Level Safety Analysis
Define aircraft failure conditions
Allocate failure to system functions
Perform PSSA and SSA

Avionics Subsystem Level Safety Analysis
Perform PSSA and SSA at subsystem level
Ensure consistency with aircraft level analysis

Navigation Sub-Subsystem Level Safety Analysis
Perform PSSA and SSA at sub-subsystem level
Ensure consistency with aircraft level analysis
Evolution of the AADL model

Component extension, refinement & implementation

AADL model Version n  →  AADL model Version n + 1

Development Process
Evolution of Safety Assessment with AADL

**Development Process**

**Automatic Fault-Tree Generation**

AADL model version n

FTA Version n

FTA refinement & improvement

AADL model version n + 1

Automatic Fault-Tree Generation

FTA Version n + 1
Functional Hazard Analysis Support

Use of **component error behavior**
- Error propagations rules
- Internal error events

Specify initial failure mode

Define error description and related information

Create spreadsheet containing FHA elements
- To be reused by commercial or open-source tools
Fault-Tree Analysis Support

Use of composite error behavior
FTA nodes

Use of component error behavior
Incoming error events

Walk through the components hierarchy
Generate the complete fault-tree
Focus on specific AADL subcomponents

Export to several tools
Commercial: CAFTA
Open-Source: OpenFTA – http://www.openfta.com
Markov-Chain Support

Use of component error behavior
   Error propagations rules
   Error transitions

Map states and error types into specific values
   Tool-specific approach

Ability to evaluate system state over time
   What is the probability my system is failing within 30 days?

Export to open-source tools, PRISM http://www.prismmodelchecker.org/
Failure Mode and Effects Support

Use of **component error behavior**
- Error propagations rules (source, sink, etc.)
- Internal error events

Traverse all error paths
- Record impact over the components hierarchy

Use error description and related information

Create spreadsheet containing FHA elements
- To be reused by commercial or open-source tools
Reliability Block Diagram
aka ARP4761 Dependence Diagram (DD)

Use of composite error behavior
- Error propagations rules (source, sink, etc.)
- Internal error events

Compute reliability of the Dependence Diagram
- Use of recover and failure events
- Overall probability of system failure

Support in OSATE (built-in)
Agenda

Overview of AADL & Error-Model Annex

Approach for Safety Evaluation

Support of Safety Evaluation with AADL

Case-Study

On-Going Work

Discussion
Wheel Brake System

Development of a **public model**
Available on AADL public wiki

Use of core and additions of AADL
Error-Model (safety) + ARINC653 annexes (specific architecture)

Demonstration for the System Architecture Virtual Integration consortium
Relevance for the avionics domain

Apply the technology/toolset on a known example
Generation of FHA, FTA, MA & FMEA
AADL model root system

NoService

NoPower

NoPressure

InvalidReport

Software and/or RuntimeError
AADL model, BSCU variations
## FHA of the root system

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 1 | Component | AsymmetricLoss | AIRS110 page 36 figure 17 | Partial Sy Landing or RTO | Asymmetric Catastrop Extremeh | Decrease in braking performance. Tendency to veer off the runway. |
| 2 | Root system | Root system | InadvertentBrake | AIRS110 page 37 figure 17 | Inadvertent Takeoff | Undetect Catastrop Extremeh | Crew cannot detect the failure by the asymmetry which is very small. Bra |
| 3 | Root system | Root system | AnnunciatedBrakingLoss | AIRS110 page 35 figure 17 | Crew det: Landing or RTO | Total Loss Hazardou Extremeh | Reference to crew procedures for loss of normal and reserve modes |
| 4 | Root system | Root system | UnannunciatedBrakingLoss | AIRS110 page 35 figure 17 | Crew det: Landing or RTO | Total Loss Hazardou Extremeh | Reference to crew procedures for loss of normal and reserve modes |
| 5 | Root system | Root system | PartialBrakingLoss | AIRS110 page 35 figure 17 | Crew det: Landing or RTO | Partial Sy Hazardou Extremeh | Additional study required to determine classification |
| 6 | Root system | Root system | LossAnnunciation | AIRS110 and ARP4761 - see ARP4 | Loss of Av all | The syste Catastrop Extremeh |
| 7 |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 8 | pedails | NoService on signal1 | TBO | No signal TBO | No signal | Would be critical if both power supplies are lost |
| 9 | pedails | NoService on signal2 | TBO | No signal TBO | No signal | Would be critical if both power supplies are lost |
| 10 | power/battery1 | Depleted | TBO | Battery all TBO | No more Major Probable | Can be an issue if redundant battery is failing also |
| 11 | power/battery1 | Explode | TBO | Battery all TBO | Battery all TBO | Major hazard if both power are lost |
| 12 | power/battery1 | NoPower on socket | ARP4761 page 277 figure 9 | Loss of or Landing/ RTO | Loss of El: Major Probable | Major hazard if both power are lost |
| 13 | power/battery1 | Depleted | TBO | Battery all TBO | No more Major Probable | Can be an issue if redundant battery is failing also |
| 14 | power/battery1 | Explode | TBO | Battery all TBO | Battery all TBO | Major hazard if both power are lost |
| 15 | power/battery1 | NoPower on socket | ARP4761 page 277 figure 9 | Loss of or Landing/ RTO | Loss of El: Major Probable | Major hazard if both power are lost |
| 16 | blue_pump | HydraulicError | ARP4761 page 275 figure L9 | Hydraulic TBO | Hydraulic TBO | Major hazard if both pumps are lost |
| 17 | green_pump | HydraulicError | ARP4761 page 275 figure L9 | Hydraulic TBO | Hydraulic TBO | Major hazard if both pumps are lost |
| 18 | accumulator | HydraulicError | ARP4761 page 275 figure L9 | Hydraulic TBO | Hydraulic TBO | Major hazard if both pumps are lost |
| 19 | bscu/sub1 | Failed | ARP4761 figure L4 page 215 | Failure of all | Failure of Major Probable | Would be critical if two subsystem (primary and redundant) are deficient |
| 20 | sub1/mon | InvalidReport | TBO | Invalid Re TBO | Report fr Minor Probable | Minor Hazard |
| 21 | bscu/sub2 | Failed | ARP4761 figure L4 page 215 | Failure of all | Failure of Major Probable | Would be critical if two subsystem (primary and redundant) are deficient |
| 22 | sub2/mon | InvalidReport | TBO | Invalid Re TBO | Report fr Minor Probable | Minor Hazard |
| 23 | platform/cpu | HardwareFailure | ARP4761 figure L4 page 215 | all | BSCU val: Hazardou Extremeh |
| 24 | cpu/partition1 | SoftwareFailure | TBO | all | Hardware Major Probable |
| 25 | cpu/partition2 | SoftwareFailure | TBO | all | Software Major Probable |
| 26 | cpu/partition3 | SoftwareFailure | TBO | all | Software Major Probable |
| 27 | cpu/partition4 | SoftwareFailure | TBO | all | Software Major Probable |

**Footnotes:**

- FHA: Fault and Hazard Analysis

**References:**

- AIRS110: Artificial Intelligence Research Systems
- ARP4761: Avionics Software Standards and Processes

**Important Notes:**

- Major/Minor: Criticality of the failure
- Probable/Probable: Probability of occurrence
- TBO: Time to failure

**Conclusion:**

The FHA analysis highlights critical failures in the root system, including asymmetric loss, inadvertent braking, and partial braking. These failures can lead to catastrophic outcomes, such as loss of control, if not properly mitigated. The analysis also identifies secondary failures, such as power and battery failures, which can impact overall system integrity. The integration of hardware and software components is crucial for ensuring system reliability and safety.
FTA of the root system

Focus on a specific AADL subcomponent
FTA of the BSCU subcomponent
### FMEA of the root system

<table>
<thead>
<tr>
<th>Component</th>
<th>Initial Failure Mode</th>
<th>1st Level Effect</th>
<th>Failure Mode</th>
<th>second Level Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>pedals</td>
<td>{NoService}</td>
<td>pedals.signal1:{NoService}</td>
<td>pedals{NoService}-&gt;{sub1/cmd}</td>
<td>sub1/cmd: {NoService} Masked</td>
</tr>
<tr>
<td>pedals</td>
<td>{NoService}</td>
<td>pedals.signal2:{NoService}</td>
<td>pedals{NoService}-&gt;{sub2/cmd}</td>
<td>sub2/cmd: {NoService} Masked</td>
</tr>
<tr>
<td>pedals</td>
<td>internal event InternalFault</td>
<td>pedals.signal2:{NoService}</td>
<td>pedals{NoService}-&gt;{sub2/cmd}</td>
<td>sub2/cmd: {NoService} Masked</td>
</tr>
<tr>
<td>pedals</td>
<td>internal event InternalFault</td>
<td>pedals.signal1:{NoService}</td>
<td>pedals{NoService}-&gt;{sub1/cmd}</td>
<td>sub1/cmd: {NoService} Masked</td>
</tr>
<tr>
<td>power/battery1</td>
<td>{NoPower}</td>
<td>power/battery1.socket:{NoPower}</td>
<td>power/battery1{NoPower}-&gt;{bscu/sub1}</td>
<td>bscu/sub1: {NoPower} Masked</td>
</tr>
<tr>
<td>power/battery1</td>
<td>internal event Depleted</td>
<td>power/battery1.socket:{NoPower}</td>
<td>power/battery1{NoPower}-&gt;{bscu/sub1}</td>
<td>bscu/sub1: {NoPower} Masked</td>
</tr>
<tr>
<td>power/battery1</td>
<td>internal event Explode</td>
<td>power/battery1.socket:{NoPower}</td>
<td>power/battery1{NoPower}-&gt;{bscu/sub1}</td>
<td>bscu/sub1: {NoPower} Masked</td>
</tr>
<tr>
<td>power/battery2</td>
<td>{NoPower}</td>
<td>power/battery2.socket:{NoPower}</td>
<td>power/battery2{NoPower}-&gt;{bscu/sub2}</td>
<td>bscu/sub2: {NoPower} Masked</td>
</tr>
<tr>
<td>power/battery2</td>
<td>internal event Depleted</td>
<td>power/battery2.socket:{NoPower}</td>
<td>power/battery2{NoPower}-&gt;{bscu/sub2}</td>
<td>bscu/sub2: {NoPower} Masked</td>
</tr>
<tr>
<td>power/battery2</td>
<td>internal event Explode</td>
<td>power/battery2.socket:{NoPower}</td>
<td>power/battery2{NoPower}-&gt;{bscu/sub2}</td>
<td>bscu/sub2: {NoPower} Masked</td>
</tr>
</tbody>
</table>

### Diagram

Current State → Out propagation → Propagation path → Out propagation or error containment

Component 1 → Component 2
Agenda

Overview of AADL & Error-Model Annex

Overview of ARP4761 & Safety Evaluation

Support of Safety Evaluation with AADL

Case-Study

Conclusion

Discussion
Conclusion

Facilitate Safety Evaluation

- Derives safety materials from existing assets
- Automate evaluation & check architecture consistency
- Improve evaluation reliability & robustness
- Support for incremental evaluation

Investigate interaction with other system characteristics

- Behavior specification
Agenda

Overview of AADL & Error-Model Annex

Approach for Safety Evaluation

Support of Safety Evaluation with AADL

Case-Study

Case-Study

Discussion
Contact

Presenter / Point of Contact
Dr. Julien Delange
Telephone: +1 412-268-9652
Email: jdelange@sei.cmu.edu

U.S. Mail
Software Engineering Institute
Customer Relations
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
USA

Web
www.aadl.info
www.sei.cmu.edu
www.sei.cmu.edu/contact.cfm

Customer Relations
Email: info@sei.cmu.edu
Telephone: +1 412-268-5800
SEI Phone: +1 412-268-5800
SEI Fax: +1 412-268-6257