Safety Evaluation with AADLv2

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Julien Delange
09/24/2013
Agenda

Overview of AADL Error-Model Annex

Approach for Safety Evaluation

Support of Safety Evaluation with AADL

Case-Study

On-Going Work

Discussion
Agenda

Overview of AADL Error-Model Annex

Approach for Safety Evaluation

Support of Safety Evaluation with AADL

Case-Study

On-Going Work

Discussion
Error-Model Annex within the AADL ecosystem
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 → ValueError → Processing
Sink for ValueError & source for NoData
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”
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

Approach for Safety Evaluation

Analysis of System Safety with AADL

Case-Study

On-Going Work

Discussion
Safety Analyses

Aircraft-Level FHA
  Define aircraft 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
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

ARP4761, section 3
Fault-Tree Analysis

Relationship of failure effects and failure modes

Reference to system hierarchy

Support with Open-Source and Commercial Tools

Initial Failure Mode

Fault Occurrence

Failure Mode

ARP4761, section 4.1
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 Vout</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>+5V 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>
Agenda

Overview of AADL Error-Model Annex

Approach for 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)

Validation Materials (FHA, FTA)

Check PSSA and SSA consistencies

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

Component implementation

System Safety Assessment

Refinement & development evolution
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
https://wiki.sei.cmu.edu/aadl/index.php/ARP4761_-_Wheel_Brake_System_%28WBS%29_Example

Use of Error-Model and ARINC annexes
  Relevance for the avionics community

Reuse for SAVI
  Provide support for the AFE61 demo

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

| A | B                          | C                          | D                      | E                      | F                  | G                  | H                  | I                  | J                  | K                  | L                  | M                  | N                  | O                  |
|---|---------------------------|---------------------------|-------------------------|------------------------|----------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|
| 2 | Root system               | AsymmetricLoss            | AIR3110 page 36 figure 17 | Partial Sy Landing or RTO | Asymmetric Catastrophic | Extremophile        | Decrease in braking performance. Tendency to veer off the runway. |
| 3 | Root system               | InadvertentBrake          | AIR3110 page 37 figure 17 | Inadvertent Takeoff    | Undetectable Catastrophic | Extremophile        | Crew cannot detect the failure by the asymmetry which is very small. Brakes are essentially normal. |
| 4 | Root system               | AnnunciatedBrakingLoss    | AIR3110 page 35 figure 17 | Crew Det: Landing or RTO | Total Loss Hazardous | Extremophile        | Reference to crew procedures for loss of normal and reserve modes |
| 5 | Root system               | UnannunciatedBrakingLoss  | AIR3110 page 35 figure 17 | Crew Det: Landing or RTO | Total Loss Hazardous | Extremophile        | Reference to crew procedures for loss of normal and reserve modes |
| 6 | Root system               | PartialBrakingLoss        | AIR3110 page 35 figure 17 | Crew Det: Landing or RTO | Partial Sy Hazardous | Extremophile        | Additional study required to determine classification |
| 7 | Announcement              | LossAnnunciation          | AIR3110 and ARP4761 - see ARP4 | Loss of Air all | General Catastrophic | Extremophile        | The system is not operational. |
| 8 | pedal1                    | NoService on signal1     | TBD                     | No signal               | No signal            | Would be critical if both power supplies are lost |
| 9 | pedal2                    | NoService on signal2     | TBD                     | No signal               | No signal            | Would be critical if both power supplies are lost |
| 10 | power/battery1            | Depleted                  | TBD                     | Battery E: all          | Battery E: all       | Major hazard if both power are lost and redundant battery is not lost |
| 11 | power/battery1            | Explode                   | TBD                     | Battery E: all          | Battery E: Catastrophic | Major hazard if both power are lost and redundant battery is not lost |
| 12 | power/battery1            | NoPower on socket        | ARP4761 page 277 figure 9 | Loss of or Landing/RTO | Loss of E: Major    | Probable            | Can be an issue if redundant battery is not lost |
| 13 | power/battery2            | Depleted                  | TBD                     | Battery E: all          | No more Major        | Probable            | Can be an issue if redundant battery is not lost |
| 14 | power/battery2            | Explode                   | TBD                     | Battery E: all          | Battery E: Catastrophic | Major hazard if both power are lost and redundant battery is not lost |
| 15 | power/battery2            | NoPower on socket        | ARP4761 page 277 figure 9 | Loss of or Landing/RTO | Loss of E: Major    | Probable            | Major hazard if both power are lost and redundant battery is not lost |
| 16 | blue_pump                 | HydraulicError           | ARP4761 page 275 figure L9 | Hydraulic TDB          | Loss of or Major    | Probable            | Major hazard if both pumps are lost |
| 17 | green_pump                | HydraulicError           | ARP4761 page 275 figure L9 | Hydraulic TDB          | Loss of or Major    | Probable            | Major hazard if both pumps are lost |
| 18 | accumulator               | HydraulicError           | ARP4761 page 275 figure L9 | Hydraulic TDB          | Loss of or Major    | Probable            | 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 defective |
| 20 | sub1/mon                  | InvalidReport            | TBD                     | Invalid Ref: TBD       | Report from 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 defective |
| 22 | sub2/mon                  | InvalidReport            | TBD                     | Invalid Ref: TBD       | Report from Minor    | Probable            | Minor Hazard |
| 23 | platform/cpu              | HardwareFailure          | TBD                     | all                    | Hardware Major      | Probable            | Impact all software components associated to the hardware |
| 24 | cpu/partition1            | SoftwareFailure          | TBD                     | all                    | Software Major      | Probable            | Impact all components that are controlled by this software |
| 25 | cpu/partition2            | SoftwareFailure          | TBD                     | all                    | Software Major      | Probable            | Impact all components that are controlled by this software |
| 26 | cpu/partition3            | SoftwareFailure          | TBD                     | all                    | Software Major      | Probable            | Impact all components that are controlled by this software |
| 27 | cpu/partition4            | SoftwareFailure          | TBD                     | all                    | Software Major      | Probable            | Impact all components that are controlled by this software |
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>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>

Current State

Out propagation

Propagation path

Out propagation or error containment

Component 1

Component 2
Agenda

Overview of AADL Error-Model Annex

Approach for Safety Evaluation

Support of Safety Evaluation with AADL

Case-Study

On-Going Work

Discussion
Consistency Checks

Consistency at integration time
   Consistency between models from different suppliers
   Strengthen the Virtual Integration promoted by SAVI

Consistency of the internal model
   ex: Can I propagate this error according to my actual state?

Consistency across error models specifications
   Component Error Behavior with Composite Error Behavior
   Correctness of a state according to subcomponents

Error information with Behavior information
Providing Modeling Guidance

Improve tooling aspects
  Help engineers to use the toolset
  Enhance tool support & functions

Release documentation
  Technical report, webinar or other media
  Modeling best practices & AADL patterns
  Guidance for using tools
  To be published in 2013

Customer training, consulting services for specific needs
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