Integrating AADL-based Tool Chain into Existing Industrial Processes

Alexey Khoroshilov, Igor Koverninskiy, Alexander Petrenko, Alexander Ugnenko
Adoption of AFDX - Challenges

- Analysis of AFDX network configurations
  - Flow latency
  - Size of buffers
  - Fault analysis

- Generation of configurations for AFDX switches and end systems
Virtualization of Network

Avionics Full-Duplex Switched Ethernet

![Diagram of network components and switches]
Adoption of AFDX - Challenges

- Analysis of AFDX network configurations
  - Flow latency
  - Size of buffers
  - Fault analysis
- Generation of configurations for AFDX switches and end systems
- What is else?
System Design Process

Design Document

Detailed Specification

Model for safety analysis
Model for reliability analysis
Model for resource allocation analysis
Model for test stand configuration

No good traceability between elements of diagrams
System Design Process

- Design Document
- Detailed Specification
- Model for safety analysis
- Model for reliability analysis
- Model for resource allocation analysis
- Model for test stand configuration

Change Request Processing
- Manual propagation
- Manual review
  => time consuming & expensive
Adoption of AFDX - Challenges

- Analysis of AFDX networks
  - Flow latency
  - Size of buffers
- Generation of configurations for AFDX switches and end systems
- Unification of architecture models
  - Unified data source for analysis tools
  - Improved traceability between documents
System Design Process

- Design Document
- Detailed Specification
- Formalized Model
- Model for safety analysis
- Model for reliability analysis
- Model for resource allocation analysis
- Model for test stand configuration
ICD DB

- is a data source for test stand configuration and management
- contains network-centered model of system
  - buses and messages/signals
  - hardware components
  - software partitions
- supports process workflow
  - configuration management
  - branch management
  - access rights management
ICD DB (2)

- Extend ICD DB
  - Add attributes of AFDX networks, ARINC-653 partitions, hardware components
  - Develop required tools on top of it

and enjoy AFDX tools and unified model
ICD DB (2)

- Extend ICD DB
  - Add attributes of AFDX networks, ARINC-653 partitions, hardware components
  - Develop required tools on top of it and enjoy AFDX tools and unified model
- Or use one of standardized architecture description languages
  - AADL
  - MARTE
  - SysML
# AADL vs. SysML

<table>
<thead>
<tr>
<th>Feature</th>
<th>AADL</th>
<th>SysML</th>
</tr>
</thead>
<tbody>
<tr>
<td>Formal semantics</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Real world modeling</td>
<td>-</td>
<td>+</td>
</tr>
<tr>
<td>Requirements traceability</td>
<td>±</td>
<td>+</td>
</tr>
<tr>
<td>Avionic specific features</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Textual representation</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Commercial tool support</td>
<td>±</td>
<td>+</td>
</tr>
<tr>
<td>Open source tool support</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>
System Design Process

- Design Document
- Detailed Specification
- AADL Model
- Model for safety analysis
- Model for reliability analysis
- Model for resource allocation analysis
- Model for test stand configuration
Our Needs

- **AADL IDE**
  - AADL textual & graphical editor
  - AADL parser & semantic checker
  - AADL model
  - Analysis and generation tools integration
- Transformation AADL to other models
- System Design Process Integration
AADL Open Source Tools

- OSATE – Eclipse-based IDE
- ADELE – Eclipse-based graphical editor
- OCARINA – transformation tools
  - Emacs&vi
  - Dia
OSATE as AADL IDE

OSATE is a great Eclipse-based IDE except for:

- Textual AADL representation is a second class citizen
- Too highly coupled
- Some stability issues
- AADLv2 not yet supported
System Design Process Integration

- Configuration Management
  - Baseline, etc.
  - Change Requests associated with modifications in an architecture model
- Branch Management
  - Modifications of aircraft
  - Several variants to be analyzed simultaneously
- Access Rights Management
  - Restriction of modification rights
  - Subcontractors
- Traceability
- Tools Qualification
<table>
<thead>
<tr>
<th></th>
<th>AADL</th>
<th>Fine-grained SCM</th>
<th>Fine-grained SCM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration management</td>
<td>N / A</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Branch management</td>
<td>±</td>
<td>±</td>
<td>+</td>
</tr>
<tr>
<td>Access rights management</td>
<td>N / A</td>
<td>±</td>
<td>+</td>
</tr>
<tr>
<td>Tools qualification</td>
<td>N / A</td>
<td>±</td>
<td>–</td>
</tr>
</tbody>
</table>
System Design Process

Design Document → Detailed Specification → AADL Model → ICD DB

- Model for safety analysis
- Model for reliability analysis
- Model for resource allocation analysis
- Model for test stand configuration
MASIW Pluggable Components

- Scheduling algorithms
  - Early Deadline First
  - Rate Monotonic
  - Custom limitations
- CPM configuration generators
  - ARINC-653
  - WindRiver VxWorks-653
- Validation and analysis tools
  - AFDX network simulator
  - AFDX configuration generator
Pilot Project Results

- AADL is an appropriate platform for unification of architecture models
- Open source tools for AADL have limited flexibility
- Integration into existing development process
  - Configuration management
  - Branch management
  - Access rights management
  - Traceability
  - Qualification
Future Works

- Support for AADLv2 and ARINC-653 annex
- Graphical editor
- Integration with open-source tools such as OCARINA, CHEDDAR, MAST, REAL, AADL2Fiacrete, OSATE checks
- Support for requirements traceability
- More flexible AFDX simulation
- Multi-level AADL models
Thank you!

Alexey Khoroshilov
khoroshilov@ispras.ru