Joint Common Architecture (JCA) Demonstration - Architecture Centric Virtual Integration Process (ACVIP) Shadow Effort

Presented by:
Alex Boydston, Electronics Engineer
US Army Aviation Development Directorate

Presented to:
2015 Safe & Secure Systems Symposium (S5)

Date:
11 June 2015
Opportunity for Rework Cost Reduction

Software Interaction Complexity Drives System Cost

Post-unit test software rework cost 50% of total system cost and growing

Software as % of total system cost
1997: 45% → 2010: 66% → 2024: 88%
SAE standard Architecture Analysis & Design Language (AADL) for hardware, software and system modeling and analysis

- Supports incremental development and predictive analysis
- Leads to early discovery of issues in operational quality attributes

**Automation and auto-generation from verified models**

- Results in major certification related rework cost reduction
- Increases assurance confidence by complementing system testing

AADL is designed to support:
1) Predictive Architecture Analysis
2) Incremental development
3) Standardized strong semantics
4) Analysis driven synthesis
Single Annotated Architecture Model Addresses Impact Across Operational Attributes

Safety & Reliability
- MTBF
- FMEA
- Hazard analysis

Data Quality
- Data precision/accuracy
- Temporal correctness
- Confidence

Security
- Intrusion
- Integrity
- Confidentiality

Real-time Performance
- Execution time/Deadline
- Deadlock/starvation
- Latency

Resource Consumption
- Bandwidth
- CPU time
- Power consumption

Auto-generated analytical models
Multi-Dimensional Cross-Domain Analysis

Single Annotated Architecture Model Addresses Impact Across Operational Attributes

**Safety & Reliability**
- MTBF
- FMEA
- Hazard analysis

**Data Quality**
- Data precision/accuracy
- Temporal correctness
- Confidence

**Real-time Performance**
- Execution time/Deadline
- Deadlock/starvation
- Latency

**Security**
- Intrusion
- Integrity
- Confidentiality

**Resource Consumption**
- Bandwidth
- CPU time
- Power consumption
- Change of Encryption from 128 bit to 256 bit
  - Higher CPU demand

**Auto-generated analytical models**

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited
Multi-Dimensional Cross-Domain Analysis

Single Annotated Architecture Model Addresses Impact Across Operational Attributes

Safety & Reliability
- MTBF
- FMEA
- Hazard analysis

Data Quality
- Data precision/accuracy
- Temporal correctness
- Confidence

Real-time Performance
- Execution time/Deadline
- Deadlock/starvation
- Latency

Security
- Intrusion
- Integrity
- Confidentiality

Resource Consumption
- Bandwidth
- CPU time
- Power consumption

Auto-generated analytical models

Change of Encryption from 128 bit to 256 bit

Increased latency

Higher CPU demand

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited
Multi-Dimensional Cross-Domain Analysis

Single Annotated Architecture Model Addresses Impact Across Operational Attributes

Safety & Reliability
- MTBF
- FMEA
- Hazard analysis

Security
- Intrusion
- Integrity
- Confidentiality

Data Quality
- Data precision/accuracy
- Temporal correctness
- Confidence

Real-time Performance
- Execution time/Deadline
- Deadlock/starvation
- Latency

Resource Consumption
- Bandwidth
- CPU time
- Power consumption

Change of Encryption from 128 bit to 256 bit

- Higher CPU demand
- Increased latency

Affects temporal correctness

- Change of Encryption from 128 bit to 256 bit
- Higher CPU demand
- Increased latency

- Safety & Reliability
- Security
- Resource Consumption
- Data Quality
- Real-time Performance

Auto-generated analytical models
Multi-Dimensional Cross-Domain Analysis

Single Annotated Architecture Model Addresses Impact Across Operational Attributes

Safety & Reliability
- MTBF
- FMEA
- Hazard analysis

Security
- Intrusion
- Integrity
- Confidentiality

Resource Consumption
- Bandwidth
- CPU time
- Power consumption

Potential new hazard

Data Quality
- Data precision/accuracy
- Temporal correctness
- Confidence

Auto-generated analytical models

Real-time Performance
- Execution time/Deadline
- Deadlock/starvation
- Latency

Increased latency

Architecture Model

Change of Encryption from 128 bit to 256 bit

Higher CPU demand

Affects temporal correctness

JMR

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited
Early Discovery Reduces High Rework Cost and Increases Confidence
Incremental System Development and Assurance through ACVIP

Early Discovery Reduces High Rework Cost and Increases Confidence
Incremental System Development and Assurance through ACVIP

Incremental Architecture & Requirement Evolution

Incremental Evolution and Execution of Assurance Plans

Early Discovery Reduces High Rework Cost and Increases Confidence
Incremental System Development and Assurance through ACVIP

Early Discovery Reduces High Rework Cost and Increases Confidence
Early Discovery Reduces High Rework Cost and Increases Confidence
Attributes of ACVIP

- Architecture centricity using SAE Standard 5506 AADL
- Virtual integration
- Early and iterative modeling throughout the lifecycle
- Semantic precision
- Single source of truth
- Software AND Hardware Architecture modeling
- Model Based Analyses across domains
  - Requirements
  - Security
  - etc.
  - Timing
  - Assurance
  - Safety
  - Resource
- Generative capabilities
- Model evolution over the life of a system
- Integral part of the acquisition process

**Designed for software intensive safety and security critical real-time systems**
• Future Airborne Capability Environment (FACE™)

• Open standard established between DoD and Industry via OpenGroup©

• The FACE™ architecture comprises points where variance occurs (i.e., layered architectural segments)

• A SOFTWARE computing environment to enable product lines for military aviation

• Eliminates barriers to software portability, prevents lock-in and improves competition

• Not only a technical standard but also includes a business strategy

• Includes:
  • Development Ecosystem
  • Conformance Test Suite
  • Verification & Certification
  • Repository

Learn more @ http://www.opengroup.org/face/face101
What is Joint Common Architecture (JCA)?

JCA is a Reference Architecture (not a system architecture) for FVL Family of Systems

**JCA Guides and constrains** architecture implementations by providing:
- a common lexicon and taxonomy
- a common (architectural) vision
- modularization and the complementary context

JCA v1.0 describes conceptual avionics capabilities with specific focus on the Mission Computer (MC) subsystem

JCA includes:

**Functional Model**
- Decomposed Mission Level Capabilities allocated to the MC subsystem and their top level organization and interactions

**Semantic Model**
- Conceptual level
- Linked to Functional Model

**Model Analysis**
- Model representation in AADL allowing ACVIP type analysis

**Documentation**
- Development Plan
- Implementation Plan

**Tools/Ecosystem**
- Translation of the JCA v1.0 conceptual model into FACE v3.x conformant conceptual and logical models
- JCA conformance
JCA Demo BLUF

Goals/Objectives

- Validate the JCA & FACE approaches
- Demonstrate portability, modularity and interoperability using JCA and FACE
- Mature JCA, FACE Standard & Ecosystem tools & business practices reducing risks
- Gain experience implementing a model based approach (learn by doing)

Approach

- Procure single software component from multiple vendors built to same specification
- Integrate component on two undisclosed Operating Environments (OEs)
- Follow a representative model-based acquisition approach
- Use FACE Ecosystem for development & test
- Exercise FACE Verification Authority process
- Develop a Reusable Verification Component
- Exercise ACVIP as a parallel shadow effort
- Limit interaction between developer and integrator and ACVIP researchers

* Refer to Proceedings of 71st AHS Forum Papers for more info

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited
• Analysis performed in parallel with the DCFM component development

• ACVIP Shadow analysis included:
  – Requirements – discovered missing, erroneous, and conflicting requirements
  – Safety – evaluated potential hazards and identified safety requirements.
  – Timing – analyzed end-to-end latency, jitter, scheduling, partitioning effects, etc.

• Analyses proved effective even in less than optimum implementation
  – Low complexity of system integration (e.g., 7 textual rqmts, limited DCFM interaction)
  – Immaturity of tools (previously unreleased and still under development)
  – Architecture was not previously modeled in AADL (MIS was modeled in UML)

• Only a limited ACVIP process was demonstrated on JCA Demo
  – Pre-solicitation requirements analysis would have uncovered issues
  – ACVIP was not part of the acquisition process
  – Incremental modeling and analysis was not performed
  – Three separate AADL models were developed
  – AADL models were not integrated nor shared amongst participates

• AADL/ACVIP training attended by government and industry personnel

Objective was to obtain AADL analysis experience and verify advertised benefits. The ACVIP Shadow succeeded on both counts!
ACVIP Process on
JCA Demo

- DCFM Supplemental Requirements
- DCFM EA UML Data Model
- MIS Stakeholder Requirements
- MIS System Requirements
- MIS Rhapsody UML Model
- MIS Build 2 Plan (system description)

Assumptions

AADL Model Construction In OSATE

Conceptual Integration Model

- Architecture Led Requirements Specification (ALRS) Analysis
- Architecture Led Safety Analysis (ALSA)
- Architecture Led Timing Analysis

Run-time Integration Model

Assumptions

DCFM
EA UML Data Model
MIS Stakeholder Requirements
MIS System Requirements
MIS Rhapsody UML Model
MIS Build 2 Plan (system description)
• Textual requirements result in:
  − Ambiguous, missing, incomplete and inconsistent requirements
  − Cost and schedule impacts due to error injected in the design

• Solution:
  − Represent verifiable requirements in an architecture model

• ALRS Analysis Process:
  1. Every element of a system specification must be addressed by requirements
  2. Non-functional requirements are driven by utility trees as output of an ATAM*
  3. Resulting annotated model is basis for Architecture-led Safety Analysis (ALSA)

* Architecture Tradeoff Analysis Method™
Aircraft Survivability Situational Awareness System (ASSA) = MIS + DCFM

Collection, Correlation, Fusion, Assessment of observations

EGI

ASSA

Situation Assessment

Data Correlation Fusion

Data Correlation

Sensor Track Format

Source Track set

Correlated Track set

Assessed Track set

Data Correlation

ASSA presentation

Pilot

ASSA command & control

SensorTrack set

Sensor Track Format

Data Correlation

Correlated Track set

Alert

Assessed Track set

Hostile fire

Threat

Missile

Radar

Obstacle

Terrain

Adjacent Aircraft

Common Operating Picture (COP)

Weather

Own Aircraft Position

Collection, Correlation, Fusion, Assessment of observations

Aircraft Position

Aircraft Survivability Situational Awareness System (ASSA) = MIS + DCFM
Aircraft Survivability Situational Awareness System (ASSA) = MIS + DCFM

Collection, Correlation, Fusion, Assessment of observations

ASSA

Response time, jitter, staleness in partitioned system

Potential Integration Issues

ASSA

Situation Assessment

Data Correlation

Correlated Track set

ASSA presentation

Data Correlation

Assessed Track set

Alert

Pilot

ASSA command & control

Sensor Te

Sensor Ob

Sensor T1

Sensor T2

Data Correlation

Sensor Track Format

Source Track set

Hostile fire

Missile

Radar

 Terrain

Obstacle

Adjacent Aircraft

Common Operating Picture (COP)

Weather

Response time, jitter, staleness in partitioned system
Potential Integration Issues

Aircraft Survivability Situational Awareness System (ASSA) = MIS + DCFM

Collection, Correlation, Fusion, Assessment of observations

Response time, jitter, staleness in partitioned system

Hostile fire
Missile
Radar
Obstacle
Terrain
Adjacent Aircraft
Common Operating Picture (COP)
Weather

Response time, jitter, staleness in partitioned system

Assessment

Pilot

ASSA presentation

ASSA annunciation

ASSA command & control
Aircraft Survivability Situational Awareness System (ASSA) = MIS + DCFM

Potential Integration Issues

ASSA

Collection, Correlation, Fusion, Assessment of observations

Scope / Boundary of System

Data Correlation

Data Correlation

SensorT1

SensorT2

SensorOb

SensorTe

Own Aircraft Position

EGI

Hostile fire

Missile

Radar

Obstacle

Terrain

Adjacent Aircraft

Common Operating Picture (COP)

Weather

SA Data Conversion

Response time, jitter, staleness in partitioned system

Situation Assessment

Assessed Track set

Correlated Track set

Source Track set

Std Track Format

Sensor Format

Pilot

Assessment

Presented

Announced

Command & Control

ASSA command & control

ASSA Presentation

ASSA Annunciation

t > 1.6 sec

MIS + DCFM

Aircraft Survivability Situational Awareness System (ASSA) = MIS + DCFM

Weather

Scope / Boundary of System

Common Operating Picture (COP)

Terrain

Adjacent Aircraft

Obstacle

Radar

Missile

Hostile fire

Response time, jitter, staleness in partitioned system

Data Correlation

Data Correlation

SensorT1

SensorT2

SensorOb

SensorTe

Own Aircraft Position

EGI

Presentation

Annunciation

Command & Control

Pilot

Situation Assessment

Assessed Track set

Correlated Track set

Source Track set

Std Track Format

Sensor Format
Potential Integration Issues

Aircraft Survivability Situational Awareness System (ASSA) = MIS + DCFM

Collection, Correlation, Fusion, Assessment of observations

ASSA

Scope / Boundary of System

Own Aircraft Position

Hostile fire

Missile

Radar

Obstacle

Terrain

Adjacent Aircraft

Common Operating Picture (COP)

Weather

Situation Assessment

Data Correlation

Data Correlation

Data Fusion

Assessed Track set

Correlated Track set

Source Track set

Sensor Track Format

ASSA SensorT1

ASSA SensorT2

ASSA SensorOb

ASSA SensorTe

Data Correlation

SA Data Conversion

SA Data Service

Response time, jitter, staleness in partitioned system

t > 1.6 sec

Pilot

ASSA Command & Control

Assessed Track set

Alert

ASSA Annunciation

ASSA Presentation

Weather

Scope / Boundary of System

Response time, jitter, staleness in partitioned system
Aircraft Survivability Situational Awareness System (ASSA) = MIS + DCFM

- **Collection, Correlation, Fusion, Assessment of observations**
- **ASSA Health Monitor**
- **Scope / Boundary of System**
- **Own Aircraft Position**
- **EGI**
- **ASSA**
- **ASSA Health Monitor**
- **Data Correlation Fusion**
- **Situation Assessment**
- **ASSA presentation**
- **ASSA annunciation**
- **Pilot**
- **ASSA command & control**
- **Response time, jitter, staleness in partitioned system**

**Potential Integration Issues**

**Potential Integration Issues**

**ASSA**

- **Hostile fire**
- **Missile**
- **Radar**
- **Obstacle**
- **Terrain**
- **Adjacent Aircraft**
- **Common Operating Picture (COP)**
- **Weather**

**ASSA Sensor T1**

**ASSA Sensor T2**

**ASSA Sensor Ob**

**ASSA Sensor Te**

**Source Track set**

**Correlator Track set**

**Sensor Track Format**

**Std Track Format**

**Alert**

**SA Data Conversion**

**SA Data Service**

**Response time, jitter, staleness in partitioned system**

**t > 1.6 sec**

**Aircraft Survivability Situational Awareness System (ASSA) = MIS + DCFM**

**Weather Scope / Boundary of System**

**ASSA Health Monitor**

**ASSA**

**ASSA presentation**

**ASSA annunciation**

**Pilot**

**ASSA command & control**

**Response time, jitter, staleness in partitioned system**

**Potential Integration Issues**

**ASSA**

**Hostile fire**

**Missile**

**Radar**

**Obstacle**

**Terrain**

**Adjacent Aircraft**

**Common Operating Picture (COP)**

**Weather**

**SA Data Conversion**

**SA Data Service**

**Response time, jitter, staleness in partitioned system**

**Potential Integration Issues**

**ASSA**

**Hostile fire**

**Missile**

**Radar**

**Obstacle**

**Terrain**

**Adjacent Aircraft**

**Common Operating Picture (COP)**

**Weather**

**SA Data Conversion**

**SA Data Service**

**Response time, jitter, staleness in partitioned system**

**Potential Integration Issues**
• AADL Error Model Annex supports ARP 4761
  - Automated fault impact analysis improves labor-intensive process

• Pre-assigned Design Assurance Level (DAL) E but:
  - Aircraft are lost to operational threats, obstacles, and terrain
  - Embedded software is a major hazard source

• SEI demonstrated the value of ALSA to assure ASSA to higher DAL
  - Annotated architectural model from ALRS used to conduct safety analysis
  - Error propagation ontology guided identification of hazards
  - Awareness of false positives, false negatives, untimely information
  - Derived health monitoring system requirements
  - Safety hazards introduced by health monitor
• Challenge: analysis of end-to-end timing for distributed, multidisciplinary, heterogeneous computer systems
  – Different scheduling on different network and processing nodes
  – Co-existence of sampled and event-driven processing of time sensitive information
• Two approaches for timing: simulation and schedulability analysis.
  – ACVIP Shadow focused on schedulability analysis
• Adventium developed and used Framework of Schedulability, Timing and Resources (FASTAR)
  – Integration of variable scheduled subsystems and end-to-end analysis
  – SPICA: Separation Platform for Integrating Complex Avionics for Partitioning analysis
• 16 Timing Issues identified for JCA Demo
• ACVIP analyses identified more than 85 issues on JCA Demo

• Performing ACVIP analysis prior to the release of JCA Demo BAA would have been beneficial to overall program execution.

• Modeling in an iterative and hierarchical fashion from a high to a low level provides early predictive results

• ACVIP analyses could reduce error perpetuation from requirements phase to system integration & test

• Many of the ACVIP tools are currently immature

• AADL training proved beneficial
  – Provided government personnel with insight into AADL modeling
  – Created interest with industry

JCA Demo ACVIP Shadow was successful in providing the Government with experience and validating the ACVIP concept.
• Roadmap for maturation of ACVIP has been developed
  – Additional resources are required to meet JMR / FVL timeline

• ACVIP to be exercised in future JMR Demonstrations
  – Improve tools for practical and viable engineering use
  – Demonstrate rapid prototyping and code generation capabilities
  – Test the scalability for complex system level analyses
  – Integration of ACVIP into acquisition process

• JMR is helping transition ACVIP from R&D into practice
  – ACVIP development and acquisition guidance handbooks
  – ACVIP Training
  – Hands-on use of ACVIP tools and processes (Learn by doing!)
  – Establish an ACVIP Community of Practice

**ACVIP has the potential of making a significant and strategic impact for helping FVL achieve success in rapid integration and affordability!**
<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>AADL</td>
<td>Architecture Analysis and Design Language</td>
</tr>
<tr>
<td>AAM</td>
<td>ACVIP Acquisition Management Handbook</td>
</tr>
<tr>
<td>ACVIP</td>
<td>Architecture Centric Virtual Integration Process</td>
</tr>
<tr>
<td>ALRS</td>
<td>Architecture Led Requirements Specification</td>
</tr>
<tr>
<td>ALSA</td>
<td>Architecture Led Safety Analysis</td>
</tr>
<tr>
<td>ALTA</td>
<td>Architecture Led Timing Analysis</td>
</tr>
<tr>
<td>AMA</td>
<td>ACVIP Modeling Analysis Handbook</td>
</tr>
<tr>
<td>AMRDEC</td>
<td>Aviation &amp; Missile Research, Development and Engineering Center</td>
</tr>
<tr>
<td>ASSA</td>
<td>Aircraft Survivability Situational Awareness System</td>
</tr>
<tr>
<td>ATAM</td>
<td>Architecture Trade-Off Analysis Method</td>
</tr>
<tr>
<td>AVSI</td>
<td>Aerospace Vehicle Systems Institute</td>
</tr>
<tr>
<td>BAA</td>
<td>Broad Agency Announcement</td>
</tr>
<tr>
<td>CMU</td>
<td>Carnegie Mellon University</td>
</tr>
<tr>
<td>COCOMO</td>
<td>Constructive Cost Model</td>
</tr>
<tr>
<td>CPU</td>
<td>Computer Processing Unit</td>
</tr>
<tr>
<td>DCFM</td>
<td>Data Correlation and Fusion Manager</td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DD</td>
<td>Dependability Diagram</td>
</tr>
<tr>
<td>DAL</td>
<td>Design Assurance Level</td>
</tr>
<tr>
<td>EGI</td>
<td>Embedded GPS / INS</td>
</tr>
<tr>
<td>EMV2</td>
<td>Error Model Version 2</td>
</tr>
<tr>
<td>FMEA</td>
<td>Failure Modes Effects Analysis</td>
</tr>
<tr>
<td>FTA</td>
<td>Fault Tree Analysis</td>
</tr>
<tr>
<td>FHA</td>
<td>Functional Hazard Analysis</td>
</tr>
<tr>
<td>FACE™</td>
<td>Future Airborne Capability Environment</td>
</tr>
<tr>
<td>FASTAR</td>
<td>Framework of Schedulability, Timing and Resources</td>
</tr>
<tr>
<td>FVL</td>
<td>Future Vertical Lift</td>
</tr>
<tr>
<td>GME</td>
<td>Generic Modeling Environment</td>
</tr>
<tr>
<td>GPP</td>
<td>General Purpose Processor</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>INS</td>
<td>Inertial Navigation System</td>
</tr>
<tr>
<td>JCA</td>
<td>Joint Common Architecture</td>
</tr>
<tr>
<td>JMR</td>
<td>Joint Multi Role</td>
</tr>
<tr>
<td>MAST</td>
<td>Modeling &amp; Analysis Suite for Real-Time Systems</td>
</tr>
<tr>
<td>MFD</td>
<td>Multi Function Display</td>
</tr>
<tr>
<td>MIS</td>
<td>Modular Integrated Survivability</td>
</tr>
<tr>
<td>OSATE</td>
<td>Open Source AADL Tool Environment</td>
</tr>
<tr>
<td>OE</td>
<td>Operating Environment</td>
</tr>
<tr>
<td>ACRONYM</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>PM</td>
<td>Program Manager or Program Management</td>
</tr>
<tr>
<td>QAW</td>
<td>Quality Attribute Workshop</td>
</tr>
<tr>
<td>RDECOM</td>
<td>Research, Development and Engineering Command</td>
</tr>
<tr>
<td>RS</td>
<td>Requirements Specification</td>
</tr>
<tr>
<td>RT</td>
<td>Real Time</td>
</tr>
<tr>
<td>SA</td>
<td>Situational Awareness</td>
</tr>
<tr>
<td>SADM</td>
<td>Situational Awareness Data Manager</td>
</tr>
<tr>
<td>SPICA</td>
<td>Separation Platform for Integrating Complex Avionics</td>
</tr>
<tr>
<td>SED</td>
<td>US Army AMRDEC Software Engineering Directorate</td>
</tr>
<tr>
<td>SEI</td>
<td>Software Engineering Institute</td>
</tr>
<tr>
<td>SLOC</td>
<td>Software Lines of Code</td>
</tr>
<tr>
<td>SAVI</td>
<td>Systems Architecture Virtual Integration</td>
</tr>
<tr>
<td>TRL</td>
<td>Technology Readiness Level</td>
</tr>
<tr>
<td>TS</td>
<td>Transport Services</td>
</tr>
<tr>
<td>UoP</td>
<td>Unit of Portability</td>
</tr>
<tr>
<td>UML</td>
<td>Unified Modeling Language</td>
</tr>
<tr>
<td>VA</td>
<td>Verification Action</td>
</tr>
<tr>
<td>WCET</td>
<td>Worst Case Execution Time</td>
</tr>
</tbody>
</table>