The Boeing Team Perspective on Mixed Criticality Architecture Requirements

a briefing at the

AFRL Safe & Secure Systems & Software Symposium (S5)

04 June 2009
Dayton, Ohio
Outline

• Overview of Boeing Team Approach to MCAR
• Formal Architecture Requirements Processes leveraged in Boeing Effort
• MCAR Key Concepts Summary
• Interesting Research Areas
• Summary
MCAR in Boeing Context

ScanEagle

Components within each layer may vary

Applications
Middleware
Host RTOS

Applications
Middleware
Guest RTOS

Conventional Layers
Multiple Partitioned Layers

Partition 2
Partition n

Host Separation Kernel/Hypervisor
Hardware or Hardware Interface Abstraction

MCAR Embedded Software Stack
Boeing Team Organization

Boeing Research & Technology

Program Manager
Patrick Stokes
Boeing Phantom Works

PI – Baseline MCAR Program
Dr. James L. Paunicka
Technical Fellow
Boeing Phantom Works

PI – HCRTOS Option
James Barhorst
Associate Technical Fellow
Boeing Phantom Works

PI – Middleware Option
Dr. Douglas A. Stuart
Boeing Phantom Works

Systems Engineering Lead
William W. Schoening
Technical Fellow
Boeing Phantom Works

Requirements Analysis Lead
Don O’Connell
Technical Fellow
Boeing Phantom Works

Core Study Team Member
Patrick H. Goertzen
Boeing Phantom Works

Core Study Team Member
Kenn Luecke
Boeing Phantom Works

Boeing MCAR Advisory Team Management
IDS Programs (Current, Emerging, Future)
Phantom Works Research Personnel
Boeing Technical Fellow Community
Includes Representative from The Insitu Group

Notes:
PI = Principal Investigator
IDS = Integrated Defense Systems
The Insitu Group is the manufacturer of the Boeing ScanEagle UAV

Green Hills Software
Makers of INTEGRITY and INTEGRITY-178B RTOS

LynuxWorks
Makers of LynxOS and LynxOS-178 RTOS

Wind River Systems
Makers of VxWorks, VxWorks for ARINC 653, & VxWorks for DO-178B RTOS

Objective Interface Systems
Makers of PCSeXpress and ORBExpress Middleware
Joseph M. Jacobs

Real-Time Innovations
Makers of DDS Middleware

Copyright © 2009 Boeing. All rights reserved.
Review of Boeing Approach

Boeing Research & Technology

Boeing MCAR Program Team

Air Force

Boeing Current, Emerging, and Future Programs

Boeing MCAR Advisory Team

Boeing R&D Teams

High Fidelity Boeing Needs

Industry-Leading Embedded Software RTOS and Middleware Teammates

Embedded RTOS Industry

Embedded Middleware Industry

Boeing Needs / Expectations

Customer Needs / Expectations

Platform Needs

NSF and the Academic Research Community

Boeing MCAR System, HCRTOS and Middleware Requirements Baseline
- Supports Air Force Goals
- Supports Boeing
- Supports Our Industry
- Have Confidence the Requirements are Achievable Due to Software Industry Teammate Involvement
- Ready for MCAD (Design)

Difficult Issues / "Open" Challenge Problems

Research Results

Architecture Insights

Research Results

Boeing Requirements Capture

Boeing Requirements Analysis

Boeing MCAR Requirements Definition Spiral
(System, HCRTOS, Middleware)

Working Group Meetings (4)

Inputs from Other Airframers

After 4th Working Group

Copyright © 2009 Boeing. All rights reserved.
Jim Barhorst – PI

**Green Hills Software**
- INTEGRITY and INTEGRITY-178B RTOS
- C-17, X-45 variant, Long-Term Mine Reconnaissance System (LMRS), F-22, F-35, Boeing 777-ER & 787, B-1B, Sikorsky S-92
- INTEGRITY-178B compliant with ARINC 653-2

**LynuxWorks**
- LynxOS and LynxOS-178 RTOS
- Boeing 777, KC-135, F-35, MH-60, MH-47, CH-47F

**Wind River Systems**
- VxWorks, VxWorks for ARINC 653, & VxWorks for DO-178B RTOS
- P-8A MMA, KC-767 Tanker, C-130 AMP, Boeing 787
Doug Stuart – PI

• Objective Interface Systems (OIS)
  • Makers of PCSexpress and ORBexpress Middleware
  • AWACS, AEW-737 Wedgetail, MH-60 Multi-Mission Helicopter, AH-64 Apache Longbow, CV-22,

• Real-Time Innovations (RTI)
  • Makers of DDS Middleware
  • Insitu Group UAVs, AWACS, B-1B, F-35
Top-Level MCAR Considerations

• Boeing Requirements Hierarchy / Categories
  • System
  • Application
  • Middleware
  • RTOS
  • Hardware
  • Composition Process
  • Tool Support

• Goal – MCAR Requirements that are
  • Achievable Technically
  • Affordable
  • Acceptable Risk
  • Adequately Meet Stakeholder Needs
Origin of Requirements

- Boeing Program Inputs
  - Programs across the lifecycle
  - Programs across platform space
- Customer Groups
  - AFRL, NASA, Army and Navy stakeholders
- RTOS and Middleware Industry
  - Team members via PIA
- Others in the MCAR community
  - Working Group collaborations
  - University Collaborators brokered by NSF
- The Boeing MCAR Advisory Team
- Boeing Core Team engineering judgment
- Architectural analysis and requirements validation
  - Formal Quality Attribute Workshop (QAW)
  - Formal Architecture Tradeoff Analysis Method (ATAM)
Additional MCAR Activities

• Participation at MCAR Working Groups
  • Perspectives shared among contractors
  • Perspectives from outside the group
• Interaction with NSF researchers
  • Helping guide the future
• The “group” white paper with Lockheed Martin and Northrop Grumman
  • Formal statement from the industry
• SBIR topic recommendations
  • Leveraging the investment
A Modular, Layered Reference Architecture

- Notional module layer view shows how major software components are grouped, & how a **Separation Kernel** is used to enforce partitioning.

- Each partition hosts a separate **Guest HC-RTOS** that does not interact with other Guest RTOS’.

- Each layer above the Separation Kernel or Hypervisor represents – applications, middleware, and Guest RTOS’.

- The **MCAR Middleware** layer also contains scheduling, resource management, power management, and fault tolerance/redundancy management components that are service based.
Formal Architecture Requirements Analysis Techniques Leveraged on Boeing Effort

• **QAW℠ (Quality Attribute Workshop)**
  • Boeing refinement of formal Software Engineering Institute (SEI)-defined process
  • Gathered key stakeholders to help describe, qualify and quantify desired architectural attributes (“Quality Attributes”) for an MCAR-based system

• **ATAM℠ (Architecture Tradeoff Analysis Method)**
  • Boeing refinement of formal SEI-defined process
  • Assessed the impact of architectural decisions on quality attribute requirements and business goals
  • Qualitative analysis assessed many quality attribute categories
    – E.g., modifiability, security, performance, extensibility, usability
Chronology of Formal Analysis Events

- QAW held prior to Working Group #2
  - Boeing stakeholders representing embedded flight system developers and R&D community
    - Proprietary articulation of future needs
  - Cognizance of manned and unmanned fixed-wing and rotary-wing DoD flight platforms, as well as commercial platforms
  - Explored dozens of run-time and design-time scenarios
    - Exploring requirements for system / application, middleware, and Real-Time Operating System (RTOS) capabilities
    - Exploring requirements for design analysis and V&V environments
    - Supporting Mixed-Criticality, Composability, Reconfiguration, Availability, Isolation, Separation, Security, Scheduling
• QAW used to define and understand architectural requirements
• Architectural requirements are those that describe qualities such as performance, availability, interoperability, data integrity and certification
• QAW populated with a wide variety of SMEs
• Workshop contents
  • Overview of the business drivers and architecture
  • Generate MCAR QAW type scenarios
  • Analyze scenarios to understand
    – Why a scenario is important
    – What is hard about it
    – What is an issue about it
    – Why the architecture must be concerned about the scenario
Quality Attributes Identified

• From the QAW:
  • Safety
  • Composability / Configurability / Modifiability / Portability / Integrability
  • Performance
  • Affordability
  • Confidence / Assurance / Reliability
  • Security
  • Availability
QAW Output

- Support multiple configurations of interest (identified in QAW)
  - Size, Weight, and Power – Small UAS to Large
  - Mission Duration – hours to years
  - Profile of vehicle capabilities and mission types – Multi-mission, simpler mission profiles
  - Leveraging a spectrum of embedded compute platforms – e.g., Multi-Core
  - Mixing criticality levels
    - Removing the pilot adds to the mix
    - Reducing weight of on-board avionics
  - Allocation to Application / Middleware / HC-RTOS

- Balancing Safety and Security
  - Safety is overriding concern
    - Mixing criticality levels
    - Blurring the line between flight and mission critical in unmanned systems
  - Security impacts safety
    - System of systems networks require security
  - Missions mandate security
ATAM held prior to Working Group #3
- Similar group of Boeing stakeholders representing embedded flight system developers and R&D community
  - Proprietary articulation of future needs
- Many QAW alumni with some additions
- Derive additional architectural requirements
- Evaluate the available architecture description for risks
- Identify and/or add potential architectural approaches to the architecture definition
ATAM Results / Issue Exploration

- Business case issues for MCAR
  - How to leverage the MCAR work onto projects
  - Assess roles of Government, USAF, OEMs, COTS vendors
  - Identified options for further analysis

- Evaluated system management requirements
  - Fault detection, isolation, recovery
  - Startup, shutdown as part of framework
  - Safe mode, and its implications

- Scope considerations
  - Small to large UAVs have differing requirements impacts
  - MLS, MILS and single level also quite different.
    - Potentially adds complexity
ATAM Results / Issue Exploration

- Architecture definitions
  - Multiple views
  - Capabilities and limitations of the RTOS and MW
    - Composability characteristics
    - Granularity of safety cert for them currently
    - Hierarchical scheduling
    - Resource management services
      - Reconfiguration for fault recovery
  - Compositional certification

- Separation Kernel / Partitioning Architecture Issues

- Metadata Issues
  - Metadata use and tool support
  - Partitioning and composability characteristics of components
  - COTS and application component metadata.

- Modeling and simulation as analysis aid

- Role of dependency analysis tools
Some Key Concepts

- **Modularity**
  - **Hardware**
    - Reconfigurability and Upgradeability issues
    - Multi-Core and Multiprocessing
  - **Software**
    - Configurable RTOS
    - Configurable Middleware
    - Configurable Application Software
  - **Certification/Verification**
    - Constructs justifying modular re-certification
    - Certification/Verification of configurations vs. systems
Some Key Concepts

• **Balancing Safety and Security**
  - Per MCAR Program Statement of Objectives (SOO) from AFRL, dated March 2007
    - “Define system functional requirements; considerations should include … Safety and security requirements”

• **Safety is overriding concern**
  - Mixing criticality levels
  - Blurring the line between flight and mission critical in unmanned systems

• **Security impacts safety**
  - System of systems networks require security

• **Some missions may mandate security**
Some Key Concepts

• Per MCAR Program SOO from AFRL, dated March 2007
  – “Define … Design Analysis and V&V environment requirements”

• Exploring next-generation design analysis and V&V environments
  • Tools needed to effectively exploit MCAR capabilities
  • Composition and Verification Tools needed
  • Need to bring composability and advanced analysis capabilities to the software engineering community
    – Including distributed development teams
    – Integrators and multiple suppliers (middleware, RTOS, application components and libraries)
Interesting Research Areas

• Unified partitioning approaches (safety and security) – a new approach to time space partitioning leveraging advances and mechanisms used in ARINC 653, Hypervisors/virtualization, and MILS separation kernels

• Middleware / RTOS collaborative scheduling – ensuring that middleware- and RTOS-level scheduling are consistent, compatible, and coherent
Interesting Research Areas

• Flight software composition including:
  • Composition tools – tools to actually build a system from components, configuration information, and a system design/model. Includes selecting, configuring, generating glue code, validating that the composition is "legal", generating certification data for the system instance, etc.
  • Middleware composition – how to compose middleware, in particular, addressing composition of middleware suites consisting of potentially multiple independent implementations of multiple services
  • RTOS composition – how to compose RTOS instances, in particular, different composition/configuration issues that might arise for host and guest RTOS's (and RTOS aspects and RTOS provided aspects of the partitioning mechanism)
Composable Certification

- Composable Certification
  - Certify components and their interfaces
    - Functional and Quality “interfaces”
  - Certify assemblies of components
    - In Application, Middleware, and RTOS layers
    - Example – light-weight RTOS for small platforms

- Traditionally
  - Certify a system as a whole from scratch

- Emerging
  - Reusable Software Components
    - FAA Advisory Circular AC20-148
  - Certify a component as part of a system
  - Use in subsequent systems without having to repeat “unit level” certification
Composable Certification

Metadata is crucial in the composition process
- Needed to defined in detail
- Used throughout composition

Supports composition of different sources of application software
- Matlab, MATRIXx, hand code, etc.
- C, Ada, Java, scripting languages etc.

Supports instrumentation for debugging
- Potentially dynamically configured based on certification
Summary

• MCAR architecture and technologies can revolutionize the affordable composition of feature-rich, certifiable embedded flight software
  • Addressing major platform cost and schedule risk

• Middleware and RTOS industry perspectives have been valuable

• Working Group cooperation with our competitors has been very effective

• “Programmatic Experiment” with NSF can be a model for on-going and future leverage of the academic research community