Challenges and Solutions for Aerospace Software Systems

Vann M. Knight
vann.m.knight@boeing.com
Agenda

- Introduction
- Aerospace domains
- Cross domain considerations
- Domain specific considerations
  - Commercial aircraft
  - Military flight management
  - Mission systems
  - Intelligence Surveillance Reconnaissance
  - Unmanned
  - Space
Boeing Aerospace

Programs (400+)
- 787-3
- 787-8
- 787-9
- 767-200ER
- 767-300ER,F
- 767-400ER
- Customer Support
- Material Management
- Maintenance Services
- Fleet Enhancements
- Flight Operations
- Delta II
- Delta IV
- 777-200ER,LR
- 777-300ER
- 777 Freighter
- KC-767
- C-17
- P-8A MMA
- 737-600
- 737-700
- 737-800
- 737-900,ER
- F/A-18 E/F
- F-15E
- T-45
- AV-8B
- Harpoon
- SLAM-ER
- JDAM
- SDB
- 747-400F,ER,ERF
- 747-8
- Advanced Logistics Services
- Integrated Logistics
- Maintenance Modification & Upgrades
- Training Systems & Services

Sites (30+)
- Decatur, Alabama
- Huntsville, Alabama
- Mesa, Arizona
- Anaheim, California
- Edwards AFB, California
- El Segundo, California
- Huntington Beach, California
- Long Beach, California
- Seal Beach, California
- Washington DC
- Cape Canaveral, Florida
- Ft. Walton Beach, Florida
- Kennedy Space Center, Florida
- Macon, Georgia
- Wichita, Kansas
- St. Louis, Missouri
- Heath, Ohio
- Portland, Oregon
- Philadelphia, Pennsylvania
- Oakridge, Tennessee
- Houston, Texas
- San Antonio, Texas
- Auburn, Washington
- Everett, Washington
- Frederickson, Washington
- Kent, Washington
- Renton, Washington
- Seattle, Washington
- Tukwila, Washington
- Brisbane, Sydney & Melbourne, Australia
- Winnipeg, Manitoba, Canada

Customers
- Commercial Airlines
- U.S. Air Force
- NASA
- U.S. Navy
- U.S. Marine Corps
- U.S. Army
- Foreign Governments

Oversight Bodies
- Federal Aviation Administration (FAA)
- Defense Contract Mgmt Agency (DCMA)
- Defense Contract Audit Agency (DCAA)
- Foreign Agencies (e.g., CAA)

Copyright © 2009 Boeing. All rights reserved.
Domains

- Commercial Aircraft
- Flight management
- Mission
- ISR
- Unmanned
- Space

Software Intensive Systems
Considerations

- **Key Cross Domain Considerations**
  - Maintain controlled flight
  - Safety
Quality Attributes

- Quality attributes drive architecture decisions
  - Scheduling, data flow, fault management

- Examples (run time and design time)
  - Performance
    - Hard real time
    - Soft real time
  - Safety
  - Security
  - Affordability
  - Availability
    - H/W redundancy
    - Fault tolerance
  - Interoperability
    - With external systems
  - Maintainability
    - Long term life cycle
  - Portability
    - Long term life cycle
  - Composability, reusability, scalability
    - Extremely large size of S/W systems
Middleware

- Active research field
- Moves domain independent complexities out of applications
- Facilitates development by large distributed teams
- Enables
  - Heterogeneous systems
  - Code portability
  - Location independence
  - OS independence
Commercial Aircraft Systems

- Large passenger airliners
  - 100+ passengers
- Two main players
  - Fierce competition for market share

- Each new aircraft design is a huge business and technical undertaking
Commercial Aircraft Systems

**Challenges**
- Safety, safety, safety
- Economy of operation and acquisition
- Verification increasingly difficult
  - Large volume of software
- ARINC-653 supports co-hosting but constrains allowable features

**Solutions**
- Rigorous design, build and test processes
- Federal verification
- Federated->integrated architecture
- Multi critical components co-hosted
- Integrated Modular Architecture
- Model Based Architecture
Integrated Modular Architecture

Benefits
- Replace federated architectures
- Fewer line replicable units
- Lower power consumptions
- Less wiring
- Weight reduction

Challenges
- Multi-critical components co-hosted
- ARINC-653 constrains allowable features
  - Cache memory not allowed
  - Multi core and multiprocessor configurations
    - Pipelined processors lead to non-deterministic execution (and are restricted)
Model Based Development

- Uses higher level domain specific building blocks
- Used to build and verify complex software systems
- Generate config file $\leftrightarrow$ Generate (almost) complete system
- Often used for specific domains where automation allows higher level abstractions
  - Control systems
  - Graphical User Interfaces
  - Design captured in “building blocks”

Concerns

- Code size increases
- Execution time increases

Effective usage requires multi-disciplined team

- Design constraints
- Efficiency
Military Flight Controls

- Fighters, Transports, Tankers, Unmanned, Rotorcraft

- Inherently periodic
  - Control laws
  - Determinism
  - Hard real time
  - Timer generated interrupts
    - Inputs → processing → outputs

- Evolution
  - Mechanical → hydro-mechanical → analog → digital
Military Flight Controls

- **Challenges**
  - Safety
  - Affordability
  - Availability
  - New aircraft are inherently unstable
    - Require higher rate control

- **Solutions**
  - Multi channel
  - Redundancy
  - Voting schemes
  - N-version programming
  - Standards, processes, reviews
Avionics Mission Computing

- Pilot vehicle interaction
  - Controls and displays
- Sensor control and processing
- Aircraft health and status
- Weapons control
- Payload control

- Characteristics
  - Hard and soft real time
  - Frequent updates
  - Highly modal
Avionics Mission Computing

**Challenges**
- Long service life
e.g. B-52, 1955 -> ??
- Mixture of hard real time and soft real time
- Size weight and power
- Affordability
- Availability

**Solutions**
- Software reconfiguration vs redundancy
- COTS hardware and software
- Product line software and component oriented architecture
- Flexible event based processing
Unmanned Air Systems

- Comprised of unmanned air vehicles and control stations
- Wide range of sizes
- Variety of functionality
  - Remotely piloted
  - Fully autonomous

- Usages
  - Intelligence Surveillance Reconnaissance
  - Cargo and transport
  - Weapon delivery
Unmanned Air Systems

- **Challenges**
  - Communications and navigation
    - Higher criticality vs. manned
  - Autonomy

- **Solutions**
  - Redundancy
  - Robust contingency automation
    - e.g. loss of comm protocol
    - Alternate routes/airfields
  - Varying levels of autonomy
    - Defined by functions vs. system
Intelligence, Surveillance, Reconnaissance

- Sophisticated Sensor Systems
- Systems to monitor
  - Airspace, seas, land masses
- Air traffic control
- Shipboard defense
- Fire detection systems
- Often responsible for
  - Common operating picture
  - Shared situational awareness
Intelligence, Surveillance, Reconnaissance

**Challenges**

- Information Assurance
- Information Integration

**Example**

- Classified sensor capability
- Multiple classifications of data on board
- Strict data separation
- Require various clearance levels
Intelligence, Surveillance, Reconnaissance

**Solutions**

- **Hardware solutions**
  - Physical separation
  - Partition data and services based on classification
  - Users have access based on clearance level

- **Software Solutions**
  - Software partitions
  - Operating system accommodates required separation
  - Overlapping with safety critical ARINC 653 solutions
    - Time and space partitioning
    - Movement of data low to high, relatively easy
    - Movement of data high to low
      - Requires sanitization
      - Cross domain guard
      - Configured with rules for allowable transfers
Satellites and Spacecraft

- **Satellites**
  - Communication links
  - Navigation signals
  - Weather tracking
  - Terrain mapping
  - Space imaging

- **Spacecraft**
  - Shuttle
  - Space station

- **Duration**
  - Few months to > 15 years

MARISAT-F2 decommissioned after 32 years service!
**Satellites and Spacecraft**

- **Evolution**
  - 60’s, 70’s and 80’s
    - Most flight logic on the ground
    - Technical challenges
      - Confined space, weight, power and extreme environments
    - Limited to command delivery and telemetry encoding
  - By 2000’s
    - Onboard flight control
    - Power and thermal subsystems
Satellites and Spacecraft

- **Challenges**
  - Extremely high availability and reliability
  - Remote access
  - Harsh environments
  - Autonomy
  - Hard real time
  - Deal with unforeseen hardware anomalies gracefully
Satellites and Spacecraft

- **Solutions**
  - Rigorous qualification
    - White box testing
    - Automated branch and logic testing
    - Black box testing
      - Independent verification and validation team
      - Final qualification test -> hardware in the loop
  - Anomalies
    - Safeguard until control is re-established and anomaly resolved
    - Normal operations discontinued
    - Conserve critical resources
Summary

- Wide range of challenges and solutions
- Conservative approaches

- Paper entitled:
  - “Challenges and Solutions for Embedded and Networked Aerospace Software Systems”

- Planned for inclusion in
  - IEEE Special Edition
  - Aerospace and Automotive Software
  - Scheduled early 2010