Multicore Processing in the Avionics Industry

Needs and Concerns

April 21, 2017

Greg Arundale – Rockwell Collins

Rockwell Collins

Outline

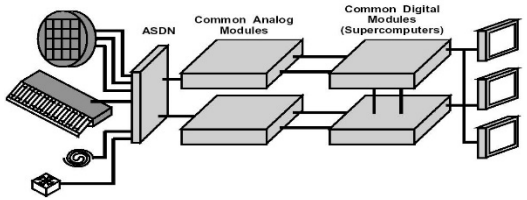
- Introduction
- Avionics Systems
  - Evolution, Overview and Challenges
- Multicore
  - Why Multicore
  - Roadblocks & Issues
  - State of the industry, CAST32A
  - Harmonization between Industry, FAA and EASA
- Safety and Security
- Current and Future State
  - What is the future beyond PPC
  - Leveraging other industries safety, e.g. Automotive
  - Potential research

Introduction

- Multicore processors are the path to higher performance
- Most industries have adopted multicore processors
  - Consumer
  - Computing
  - Automotive
  - Telecom
  - Networking
- These other industries investments drive technology into the Avionics Industry
- Questions
  - What problems do multicore processors have?
  - Are they usable in safety-critical products?
  - How do the certification authorities view them?

Avionics Systems Evolution

- Avionics systems have evolved from Independent systems, to Federated, to Integrated Avionics systems
- As systems evolve further to Advanced Avionics, higher processing power is needed
- Multi-Core processing is poised to fill this need



Advanced Avionics

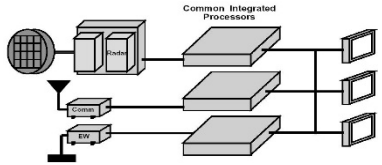
Network Centric Systems

Service Oriented Architectures

Network Centric ->

Information Centric ->

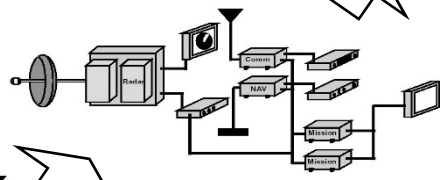
Knowledge Centric



Integrated Avionics

Open Systems

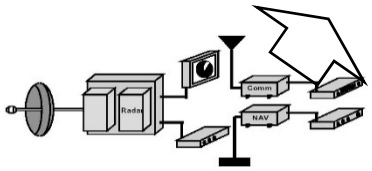
i.e. CoRE, 777 AIMS, etc.



Federated Avionics

Federated Subsystems

i.e. EFIS/EICAS, LFDS



Independent Avionics

Dedicated Subsystems

i.e. ANS-70 (Area Nav)

Increasing Capabilities

Graphics Source:
Joint Advanced Strike Program
Avionics Architecture Definition Appendices

Avionics Overview

- **Modern Avionics are Highly Integrated (e.g. Cabinet-Based)**
  - **“Federated” Units Less Common**
- **Computation Modules Use Host Processor With “Partitioned” Operating System**
  - **Allows Hosting of Apps with Differing Criticality Levels**
- **Ethernet (-like) Networks Connects Cabinets, Sensors, Displays**
  - **With Avionics-Grade Quality of Service**
  - **High-Speed, Good Connectivity**
  - **Support For Legacy Buses Using Concentrators**

Rockwell Collins

The Avionics Challenge

- The Avionics Industry presents several issues for modern microprocessors
  - Safety-Critical Equipment
  - Environment (Temperature, Power Consumption, SEU, others)
  - Product Longevity (Procurement, Wear-out)
  - Certification (Process Adherence, Artifact Availability)
  - Determinism (with shared Caches and Multiple Cores)
  - Increasing Performance Demands

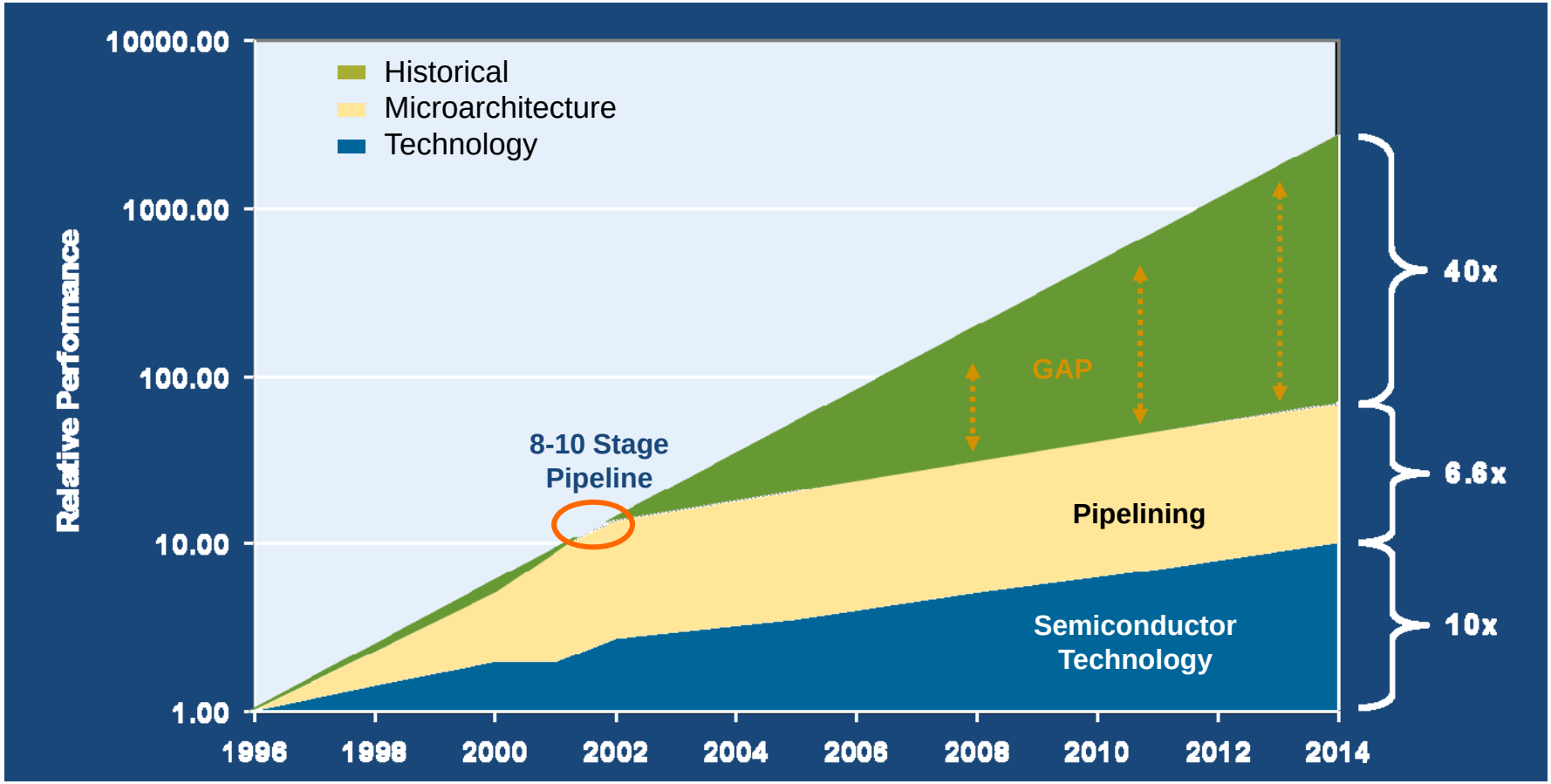
- Problems have been exacerbated by multicore SoCs
  - SoC integration reduces visibility and ability to monitor
  - Shared memory and peripherals resource management becoming critical, particularly for DAL A/B applications
  - Multicore complexity complicates design, analysis, certification
  - Control and peripheral logic now designed by SoC Supplier, not Applicant

- The challenge is for the Avionics Industry to take advantage of the investments from other industries

Rockwell Collins

Performance Scaling and Technology Challenges - why the move to Multicore

- Clock rate improvements slowing: 40%/year to 12%/year
- Pipelining has increased by factor of 4 in last decade, not possible in next decade



Source: UT Dept. Computer Science

Approved for Public Release

Roadblocks to use of Multicore Processors in Avionics

1. Emerging Certification Guidelines from Certification Authorities
   - Artifact list generated from industry collaboration being used for eval
   - MCFA Industry Group
   - CAST-32A provides guidance, but requirements are still based standards like
     - DO-254, ARP 4754A, ARP 4761, DO-178B/C, etc

2. Lack of Access to Certification Artifacts for Complex COTS Components
   - Being addressed with multiple SoC vendors
   - MultiCore For Avionics (MCFA) Industry Working Group

3. Trade-offs between determinism and performance with highly integrated devices
   - Concern with Core to Core interference and shared resources
     - Strong HW (Hypervisor) based partitioning maintains separation
   - Multi-Threaded architecture (typically not used for DAL-A)
     - Each thread uses common resources within a core

Multicore Issues

- Performance
  - Cores are often lower performance than legacy single-core devices
  - Resource conflicts also slow performance
  - Hypervisor adds overhead
  - *May need to split big applications across two or more cores*
- Debug
  - Synchronization and atomicity issues; halting multiple cores
  - *Need new training and tools to debug multicore designs*
- Determinism
  - Conflicts occur when accessing shared resources
  - *Need architectural framework to preserve determinism*
- Certification
  - The certification authorities view multicore with apprehension
  - *Need industry and certification authorities to work together to mitigate concerns*
    - *CAST-32A and EASA CRI provide guidance*

MCFA – Avionics Industry Working to Fill Gaps

- The MultiCore For Avionics Group was formed in late 2010
  - Formed to assist Avionics Suppliers to certify equipment which use SoCs
- MCFA is an Ad Hoc working group
  - Currently sponsored by component suppliers
  - Open to companies which certify products in civil airspace
  - Partnerships with multiple Multicore Suppliers
- Founding Members Include: BAE Systems, Barco, Boeing, EADS, Elbit, GE Aviation Systems, Honeywell, Rockwell Collins, Thales and others
- MCFA Goals:
  - Develop a partnership between SoC Suppliers and the Avionics Industry
  - Find industry consensus on SoC Supplier data to be requested
  - Transfer basic SoC design and verification information to group members
  - Allow review of other artifacts which are then summarized for the group
  - Minimize SoC Supplier effort by providing data to the whole group

Safety+Security: Techniques & Requirements

- **Safety**
  - **What system does**
- **Security**
  - **What system doesn't do**
- **General Increase in Security Concerns**
  - **Concern: Malicious Behavior in Safety Critical Domains**
- **Redundancy Management**
  - **Asynchrony a particular challenge**
- **Increasing Sophistication of Security Systems**
  - **Functional Behavior part of Security Story**

Identify and apply dual-use specification and analysis techniques for establishing safety and security properties of high-assurance systems

Rockwell Collins

Multicore Security Certification Issues

- **Confidentiality - limiting information access and disclosure**
  - Information Flow Control
  - I/O Port Control
  - Data Isolation
  - Sanitization
- **Availability - assurance that information resources are accessible when needed**
  - Cores must not unduly influence another core through denial of service
- **Integrity - trustworthiness of information**
  - Integrity checks applied to information flow
  - Encryption techniques can be used
- **Authenticity - assurance of data source**
  - Authentication
  - Protect against redirection, hijacking, or man-in-the-middle attacks

Security Summary

- Security & Safety have some common evaluation criteria, e.g.
  - Separation / data isolation / data integrity
  - Availability / Redundancy
  - Need to ensure cores do not adversely influence each other

- Processor evaluation may be able to leverage COTS information e.g.
  - Design Artifacts
  - Design Review Artifacts
  - Test / Validation Artifacts

- There are different / more stringent certifications levels depending on the system in which the COTS processor is planned to be used

- Desire to leverage dual-use information and evaluation for both safety and security where possible

Rockwell Collins

Current State and Future Considerations

- FAA and EASA have released guidelines addressing multicore certification

- Avionics Industry Certified Multicore Variants
  - Heterogeneous multicore
  - Homogeneous multicore with one core active
  - Multi-treading disabled
  - Working towards multiple civil and military multicore systems certifications

- Multicore Processors for Avionics Applications
  - Most common single and multicore processor in certified systems has been PowerPC
  - Recent consolidation of silicon vendors opens the question of PPC long term viability
    - What is the next multicore for avionics processor?
    - Highly speculative at this time

- Can other industries safety initiatives be leveraged

Other Industries Safety Standards

- Domains of primary interest (and their associated safety standards) include
  - Avionics (DO-178B/C, DO-254, ARP4754A)
  - Automotive (ISO 26262)
  - Military (MIL-STD-882E, MIL-HDBK-516C)
  - Additional domains of potential interest include
    - Construction equipment (ISO 15998)
    - Railway (EN5012X)
    - Space (ECSS-Q30, Q40, Q80)
    - Automation and industrial control (IEC 61508, IEC 61511, IEC 62061, ISO 13849)
    - Nuclear plants (IEC 60880, IEC 61226, IEC 61513).

Comparisons *

Standard	Safety	Hazard
ISO 26262	Absence of unreasonable risk.	Potential source of harm caused by malfunctioning behavior of the item. **Malfunctioning Behavior**: failure or unintended behavior of an item with respect to its design intent.
MIL-STD-882E	Freedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.	A real or potential condition that could lead to an unplanned event or series of events (i.e., mishap) resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.
DO-178C	No clear definition provided. Based on Failure Condition Category in the standard, the definition is similar to MIL-STD-882E.	No definition provided.

Measure	ISO 26262 Hardware and Software	MIL-STD-882E for Hardware	MIL-STD-882E for Software	DO-178C (Software only)
Severity	√	√	√	√
Probability of Operational Scenario (Exposure)	√			
Probability of Mishap Occurrence		√		
Controllability	√			
Software Control Category			√	

- There are many parallels, and differences between Avionics, Automotive and Military safety standards
- Gap analysis must be understood in order to leverage Automotive Safety components in Avionics systems

* Table Source: DoT "Assessment of Safety Standards for Automotive Electronic Control System" DOT HS 812 285

Comparisons *

Failure Rate Limits (probability/hour)	ISO/IEC 61508 (Industrial)	ISO 26262 (Automotive)	EN50126, EN50128, EN50129 (Rail)	DO-178B/C, DO-254 (Aviation)	ISO 13849 (Machinery)
$10^{-4} – 10^{-5}$					PL a
$10^{-5} – 10^{-6}$	SIL1	ASIL A	SIL1	DAL C	PL b
					PL c
$10^{-6} – 10^{-7}$	SIL2	ASIL B	SIL2		PL d
$10^{-7} – 10^{-8}$	SIL3	ASIL C	SIL3	DAL B	PL e
		ASIL D4			
$10^{-8} – 10^{-9}$	SIL4		SIL4		-
$< 10^{-9}$	-		-	DAL A	-

* Derived from: Olsson et al, “Standards-oriented, domain-specific aspects in reusing software in SafeCer domains”

Closing Remarks

- The Avionics Industry has come a long way towards use of Multicore processors in Safety Applications
- Certification Authorities have released guidelines on Multicore Processor use in Safety Applications
- Leveraging investments of other industries improves ability to meet the needs of increasing architectural complexities
- There is still a lot of room for Innovative Research in Methods to address Safety Architectures where Multicore Processors will be used
- Questions & Comments?