FAA Status on Multi-Core Processors

April 2014

John Strasburger

Outline

- FAA Certification Process
- How is the Civil Aviation Community Addressing MCPs?
- Challenges
- CAST 32
- Processor Evolution
- Summary
- Questions

FAA Certification Process

FAA Cert Process

- **FAA has airworthiness standards which are codified in Title 14 of the Code Of Federal Regulations**
  - Part 23 – normal, utility, acrobatic, commuter category airplanes
  - Part 25 – transport category airplanes
  - Part 27 – normal category rotorcraft
  - Part 29 – transport category rotorcraft
- **These rules establish the minimum requirements**

Note: there are also airworthiness standards for aircraft engines, baloons and propellers

FAA Cert Process (cont)

- **No specific Part 23, 25, 27, or 29 rules for software or multi-core processors**
- **FAA has rules of general applicability that may be applied**

Note: Part 33.28 (g) does have a standard for engine control software

FAA Cert Process (cont)

25.1301 Function and installation.

(a)Each item of installed equipment must--

(1) Be of a kind and design appropriate to its intended function;

(2) Be labeled as to its identification, function, or operating limitations, or any applicable combination of these factors;

(3) Be installed according to limitations specified for that equipment; and

(4) Function properly when installed.

FAA Cert Process (cont)

25.1309 Equipment, systems, and installations.

(a) The equipment, systems, and installations whose functioning is required by this subchapter, **must be designed to ensure that they perform their intended functions under any foreseeable operating condition**.

(b) The airplane systems and associated components, considered separately and in relation to other systems, must be designed so that--

(1) **The occurrence of any failure condition which would prevent the continued safe flight and landing of the airplane is extremely improbable**, and……

FAA Cert Process (cont)

- An applicant for a Type Certification or Supplemental Type Certification
  - Must **show** compliance to the applicable rules such as 1301 and 1309
  - Proposes a means of compliance
- Advisory Circulars (AC) can provide one acceptable means of compliance
  - AC 20-115C identifies DO-178C as an “acceptable means of compliance for the software aspects of airborne systems and equipment certification”
- FAA **finds** compliance to the rules

FAA Cert Process
Issue Papers

- Provide a vehicle to document the negotiation and resolution of certification issues that may require special emphasis for resolution
- Become project specific and proprietary
- When we invoke an identical issue paper for numerous projects, this indicates mature policy suitable for written guidance (e.g. Advisor Circular)
  - We are not yet there for MCPs

How is the Aviation Community Addressing MCPs?

How is the Aviation Community Addressing MCPs? MCP Issue Paper

- **Has been harmonized with the European Aviation Safety Agency (EASA) Certification Review Item (CRI)**
- **Harmonized technical content can be found in Certification Authority Software Team CAST 32 which has 24 objectives**
  - http://www.faa.gov/aircraft/air_cert/design_approvals/air_software/cast/cast_papers/media/cast-32.pdf
- **AeroSpace and Defence and EASA working group is revising the CRI objectives**
  - Expect < 24 objectives

How is the Aviation Community Addressing MCPs? MCFA

- **Multi-Core For Avionics (MCFA)**
  - Industry working groups established to address the challenges of multi-core certification
  - Provides a consistent set of data to support certification projects
  - Provided considerable feedback on the MCP CRI
- **Civil aviation industry has already expended considerable resources on MCPs**
    - Have proprietary solutions

How is the Aviation Community Addressing MCPs? 1st Workshop

- **January 2013 at EASA to discuss the CRI with MCFA**
  - Airbus Commercial, Airbus Military, BAE, BARCO, Boeing, Cassidian, CMC, Dassault Aviation, EADS, Elbit, Eurocopter, Freescale, GE, Rockwell-Collins, SAAB, Thales, UTC Aerospace
  - EASA presented the MCP features that caused concern – industry agreed with these concerns.
  - Industry feedback "*EASA/FAA has a good understanding of the subject material*."
  - Suggested we introduce objectives and reorganization of topics.
  - Issue paper and CRI were revised to incorporate industry suggestions

How is the Aviation Community Addressing MCPs? 2nd Workshop

- **Cologne 8-10 July 2014**
- **Goal of the workshop:**
  - Sharing of technical knowledge on MCP technology
  - Sharing of experience on usage of MCP
  - Discussion on concerns
  - Sharing of research studies
- **Industry attendees**
  - Airbus Aircraft, BAE System, Barco, Boeing, Airbus Defence and Space, CMC Electronics, Dassault Aviation, EADS, ELBIT, Airbus Helicopter, Freescale, GE Aviation, Rockwell Collins, SAAB, Sagem, Thales Avionics, UTC Aerospace Systems, Honeywell, Green Hills, Wind River, Sysgo, DDC-I, Verocel
- **Certification Authority attendees**
  - FAA, EASA

How is the Aviation Community Addressing MCPs? 2nd Workshop

- **Many educational presentations and excellent discussions**
  - Keep your configuration simple and work with the MCP manufacturers to minimize the likelihood of interference
  - Need to characterize the performance of your configuration in the lab
  - Memory/cache management is key
  - Applicants should clearly define the roles
    - Platform, OS, application providers and integrators
  - MCP maturity may be tied to the feature set in the applicants usage domain
    - If you are using a unique feature set, then your implementation may be less mature
  - Disabling cores may not be simple as we thought
  - Interference gets worse as the number of cores increase

How is the Aviation Community Addressing MCPs? FAA Conference

- **FAA National System, Software, and Airborne Electronic Hardware Conference – Sept 2014**
  - ½ Day of Airborne Electronic Hardware Track dedicated to the MCPs
  - Multi-core Processors: Why, What and How - John Strasburger, FAA
  - Multi-Core Processors – Preventing Certification from Knocking Down Your Door - Patrick Huyck, Green Hills Software
  - Time Partitioning Challenges in Multi-core Avionics Platforms - Larry Miller, Honeywell

How is the Aviation Community Addressing MCPs? Research

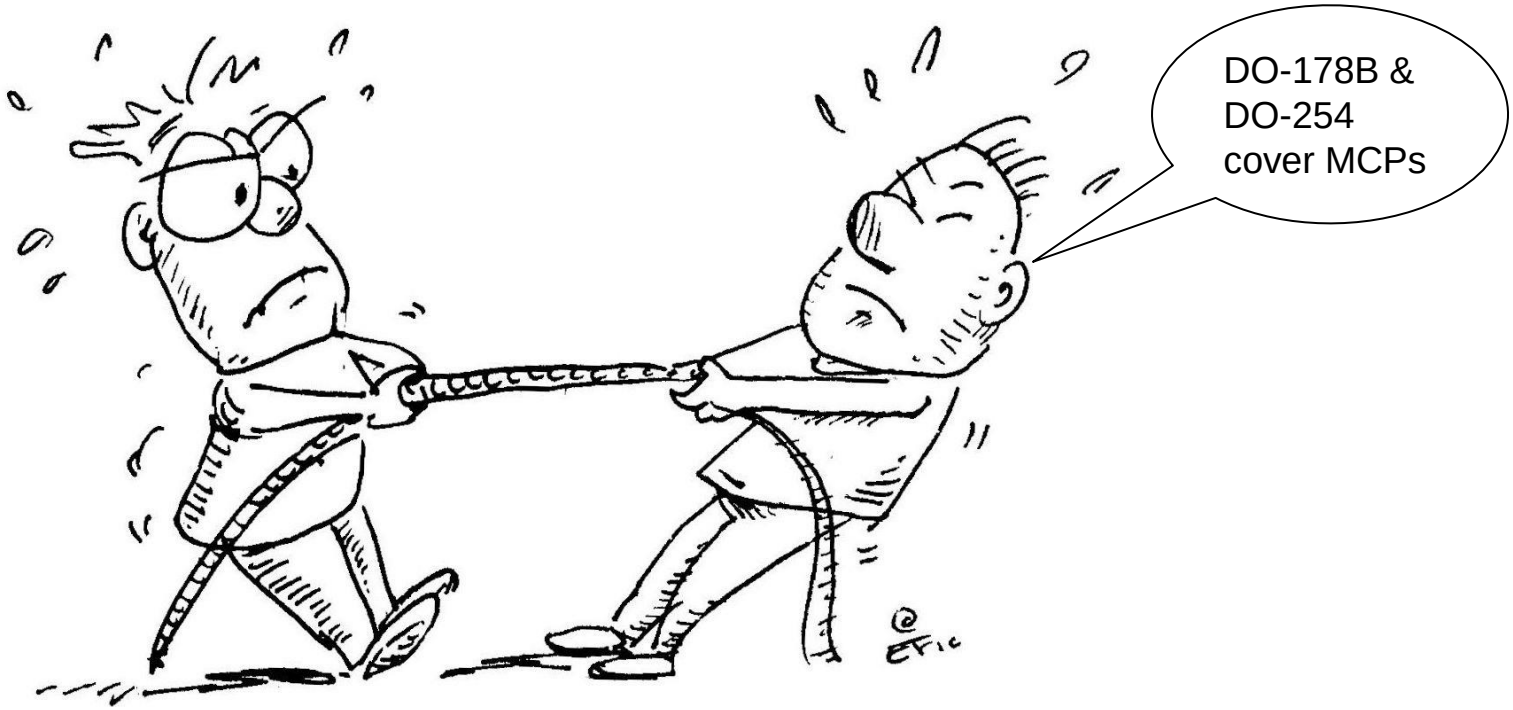
- **FAA**
  - "Handbook for the Selection and Evaluation of Microprocessors for Airborne Systems"
    - http://www.faa.gov/aircraft/air_cert/design_approvals/air_software/research/
  - AFE 75 – COTS Assurance
  - "Identification of Issues with Multi-Core Processors" just starting
- **EASA**
  - "MULCORS - Use of Multicore Processors in airborne systems"
    - http://www.easa.europa.eu/system/files/dfu/CCC_12_006898-REV07%20-%20MULCORS%20Final%20Report.pdf

Challenges

Challenges

Need MCP Guidance

Don't Need MCP Guidance



Challenges (cont)

- **CAST 32 has limited applicability**
  - Does not address IMAs
  - No more than two active cores
  - Most industry feels that the CAST 32 objectives adequately cover more than 2 active cores
- **Small company versus large company**
  - Small may need more help
- **Incremental verification**
- **Is DO-178B/C and DO-254 sufficient**
- **Evaluating a proposed approach of measuring WCET**

Certification Authority Software Team (CAST) 32

CAST 32 Content

- **Definitions**
- **Current scope**
  - Up to Two Active Cores
  - Single systems
- **When does it apply**
  - Levels A, B, and C applications
    - Smaller subset of objectives for DAL C applications.
  - If only one core active – just two objectives
  - Depending on the project – specific objectives may not apply
- **Exempted configurations**
  - When two identical cores run in lock step
  - Processors linked by conventional data buses, and not by shared memory, shared cache, a coherency fabric / module / interconnect

CAST 32 (cont)

Topics

- **Configuration Settings**
  - Analyze, determine and document the configuration for required, unused and dynamic features
- **Processor Errata**
  - Assess the errata
  - Process in place to continue to obtain errata
- **Software Hypervisors and MCP Hardware Hypervisor Features**
  - Comply with DO-178B/DO-178C
- **MCP Interference Channels**
  - Identify all interference channels and verify means of mitigation for each of those channels
- **Shared Memory and Cache**
  - Prevent disruptions to deterministic software execution
  - Analysis and tests to determine worse case effects of share memory and cache

CAST 32 (cont)

Topics

- **Planning and Verification of Resource Usage**
  - Allocate, manage and measure resource and interconnect usage
  - Verify resource and interconnect demands do not exceed the capacity.
- **Software Planning and Development Processes**
  - Identify the software architecture
  - Describe the development and verification planned to demonstrate it executes deterministically
- **Software Verification**
  - Target MCP environment or justify something else
  - Software complies with DO-178B or DO-178C
  - Verified that the data and control coupling between all software components hosted via shared memory

CAST 32 (cont)

Topics

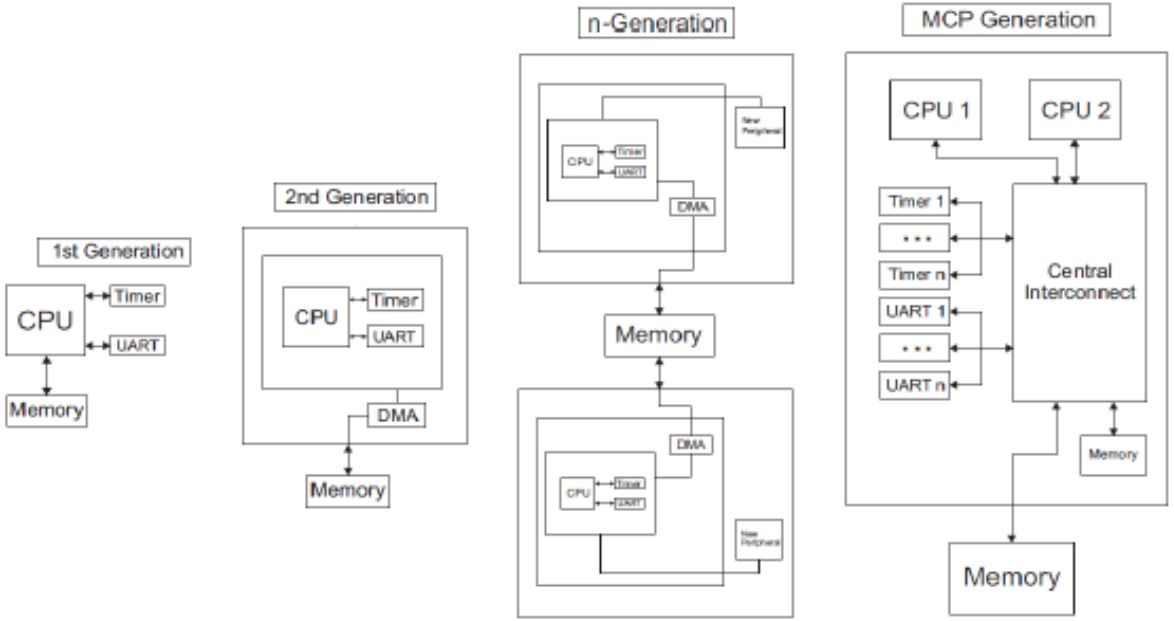
- **Discovery of Additional Features or Problems**
- **Error Detection and Handling and Safety Nets**

CAST 32 (cont)

- **Each topic/issue includes**
  - Rationale describing the issue
  - One or more objectives
  - Suggested activities in an appendix
- **Table that shows which of the 24 objectives apply by development assurance level**

Evolution of Processor/Peripheral Integration

- Evolution toward faster, smaller, and more complex is a recurring theme in avionics and electronics in general
- Through this evolution, fielded avionics have a proven track record via current design assurance



Evolution of Processor / Peripheral Integration

Slide Source GARMIN

Summary

- Civil aviation suppliers and certification authorities have expended considerable resources on MCPs
- We are all still learning
- Today's IEEE workshop is a great venue to share information
- FAA and EASA guidance is still evolving
- MCPs is the next step in processor evolution
- Special thanks to Lui and Heechul

Questions