CREATIVE ELECTRONIC SYSTEMS

CES - Creative Electronic Systems S.A.

ETT 2014: Certification for Avionic Mission Computers

January 2014

Version 0.7

Abstract

Certification for Avionic Mission Computers

Given the growing capabilities of airborne platforms, mission systems are becoming ever more critical. This presentation is proposing new ways to consolidate the seemingly contradicting requirements for safety and performance. Safety-critical computers can not use the latest technology due to the prohibitive cost of certification. In order to keep certification costs acceptable, they must stay simple and robust. On the other hand, cutting-edge mission systems handle vast amounts of data, perform complex processing functions and accept last-minute updates, and for today's highly capable military platforms, the consequences of a mission failure can be huge. Therefore, "mission-critical" is rapidly becoming synonymous with "safety-critical". We need to find ways to combine the high performance and flexibility of new technology with the reliability of safety-critical systems.

Introduction

Name Wayne McGee

Working in the field of embedded real time software and computing since 1977

Company CES-CAL: Morgan Hills, California, USA

US subsidiary of CES S.A., Geneva

~100 employees of 17 nationalities

founded in 1981

Supplier of computer modules (single board computers, peripherals) and systems for aerospace, defense, physics, telecom markets

Certification vs. Certifiability

- **Certification**
  - Of an aircraft is the responsibility of the airframe manufacturer, who has to prove to the certification authority that the aircraft operation is safe, according to a multitude of standards.
  - The process of certification of the complete aircraft relies on the *certifiablity* of each component.
- **Certifiability**
  - Of a component or subsystem has to be proven by the subsystem supplier, who has to provide the required *certification evidences*.
  - Building on these *certification evidences*, the airframe manufacturer demonstrates that the component or subsystems, as used in the aircraft, complies with the applicable safety regulations.

Design Assurance Level (DAL) requirements

- First assumption of authority: “every failure is catastrophic” -> DAL A
- Lower criticality has to be proven (ex. isolation from flight control) via safety assessment
- Depending on use case of the computer

- Not only airborne material affected (ex. ground control stations)

safety assessment vs. design assurance level (DAL)

Safety assessment

- NOE: no effect on functional capabilities or crew workload
- MIN: inconvenience to occupants, slight crew workload increase
- MAJ: discomfort, possibly injuries to occupants, significant workload incr.
- HAZ: serious injury, single fatalities, high flight crew workload,…
- CAT: multiple casualties

DAL (DO-178B/C) objectives

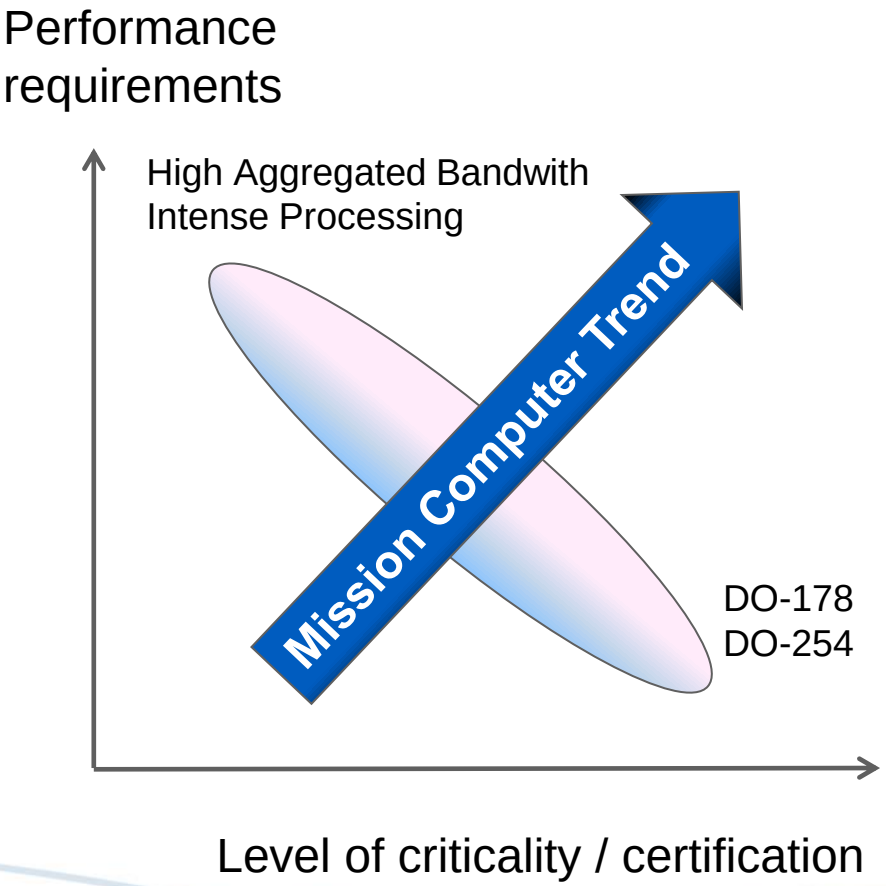
- DAL E: none
- DAL D: software is a black box, no insight required
- DAL C: software is a white (i.e. transparent) box, same objectives as A/B, less rigid verification
- DAL B: like C, rigorous verification
- DAL A: like B plus Modified Condition / Decision Coverage

Certification Dilemma

- High DAL requires very traditional technology of modest complexity (traceability)
- Modern performance oriented technologies are not usable (prohibitive certification costs, if certification is possible at all)
- Certification evidences for highly integrated modern components (microprocessors, video processors, …) may not be available because vendors are not prepared to make the corresponding effort for a niche market.
- Growing capabilities and complexity of airborne platforms demand performance
  - Handling of vast amounts of data
  - Increasing number and variety of interfaces
  - Support for different sensors
  - Data storage and throughput
  - Complex processing functions

Safety vs. performance

- Mission computer trend
  - Points to ever increasing demands in aggregate bandwidth and processing performance
  - While, at the same time, mission computers become more and more safety critical
- Classical certification standards (DO-178, DO-254)
  - Tend to prefer simple systems, built from components of low complexity or long service history (i.e. “old” technology)



Civil vs. Military Aviation

- Civil Aviation
  - Large quantities make high NREs affordable.
  - Larger available volume makes it easier to spatially partition systems of different criticality
  - A full custom design is the best choice to ensure a minimal certification effort for the required function.

- Military Aviation
  - Low quantities (i.e. small number of aircrafts in a family) limit the affordable NRE.
  - Small volumes (e.g. UAVs) make it attractive to combine functions of different criticality in the same box (or on the same chip).
  - Need to be on the edge of technology.
  - Strong drive to use COTS or MCOTS.

Functions of Airborne Mission Computers

- Flight management
- Mission management
- Payload management
- Sensor support
- Data storage

Technical Approach

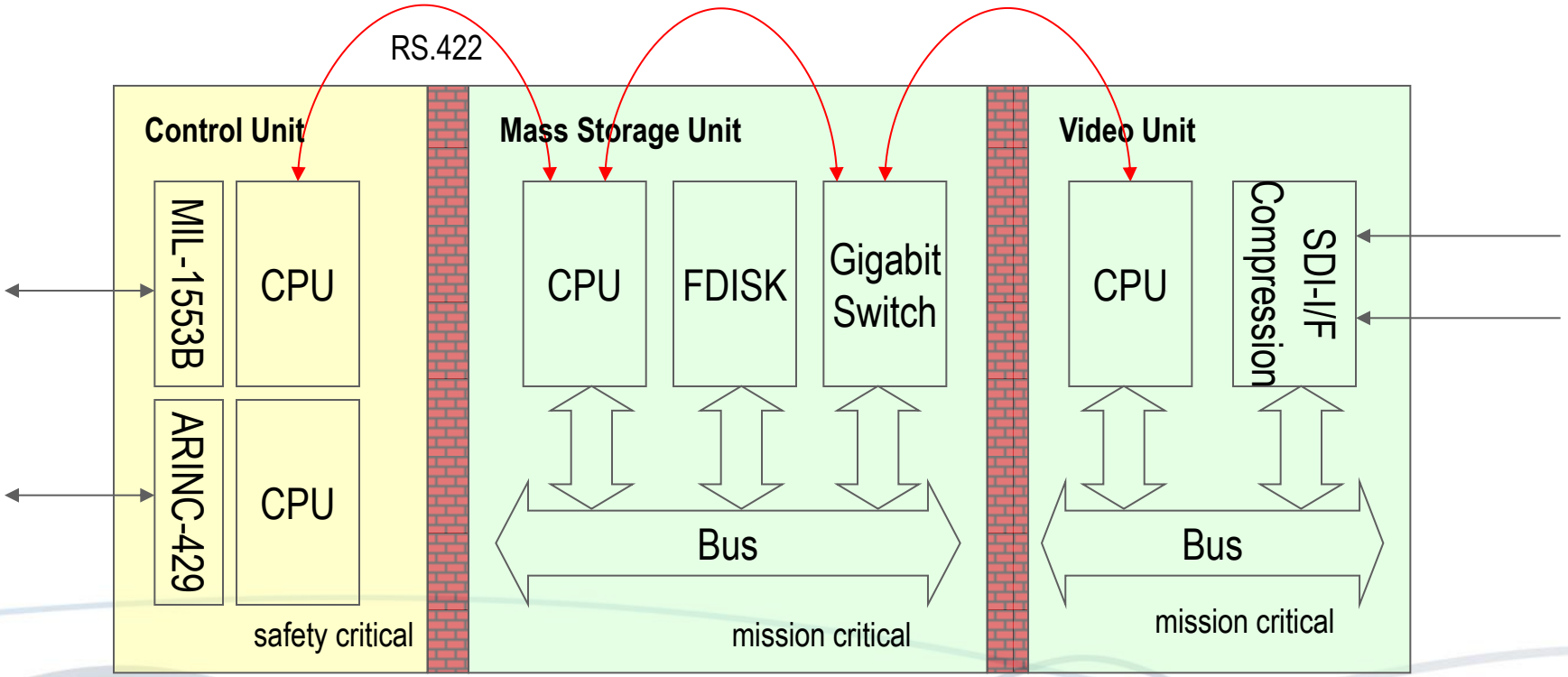
- Conceptual design with certification and costs in mind
- Design partitioning / Segregation
- Based on avionic standards ((sealed) ATR, ARINC-600)
- Powerful and rugged multiprocessing architecture (OpenVPX, VITA-74, VME, PMC, XMC)
- Use of components with certification support
- Composed of COTS components
- Custom processing and I/O functionalities in the FPGA
- Certifiable BSPs (VxWorks 653, Integrity…)
- Use of integrated components (virtualization, hypervisor)

Best practices and quality standards

- Best practices and widely used quality standards for development (EN9100, AS9100C, ..) are the baseline on which specific Design Assurance Levels (DAL) can be added if required.
- Provision for a DAL-C and higher must be done early in the design process to ensure future certification.
- By respecting these precautions, functional prototyping can start much earlier than the actual certification process.
- Design for certifiability then implies the elaboration of a large number of documents (see DO-178/DO-254 Document Requirement Lists (DRLs)) for planning, specification, design, configuration control and verification, such as
  - DO-178B/C: PSAC (Plan for Software Aspects of Certification), … (8 planning, 3 design, 3 conformity)
  - DO-254: PHAC (Plan for Hardware Aspects of Certification), …(6 planning, 4 design, 3 conformity)

Segregation – Traditional Implementation

- Multiprocessing architecture with different levels of safety
- Well defined, narrow interface to safety critical component (s. red lines below)



Conclusion

- Designing systems to both high safety and high performance standards remains a complex task.
- It requires a strong development process, and experience built up from lessons learned, in order to make the right design choices.
- BUT this is what we'll need more and more (e.g. driven by the need certify UAVs for the use in civil airspace).
- Civil and Military Aviation follow different business models, in terms of quantities, affordable NRE, performance and safety requirements. Safety regulations are conservative by nature, technology is innovative and pushing the limits to achieve certification.

CREATIVE ELECTRONIC SYSTEMS

With you all the way…