


Frédéric Faubladier

Aix- October 2013

AEH certification evolution

thinking without limits

EUROCOPTER
AN EADS COMPANY

Agenda

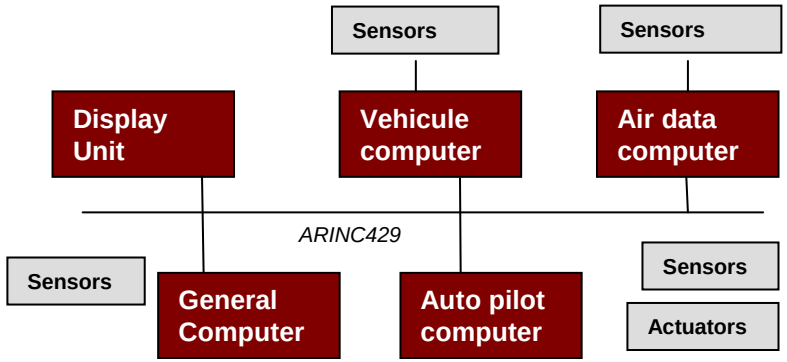
- Airborne Electronic certification evolution:

- Illustration of multi discipline involvement
  - complex COTS
  - Single event upset
  - Management of OPR
  - Management of LRU design assurance

- Major Pitfalls and conclusion

Avionic evolution

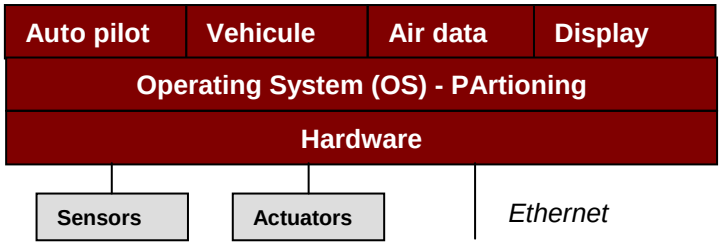
avionics – 90



- Each function is separate LRU
- Main constituents of the LRU:
  - Microprocessor
  - ASIC/PLD
  - Parallel BUS
  - Bus: ARINC 429,

- **Complexity**
  - SW
  - FPGA/ASIC

Avionic : 2010

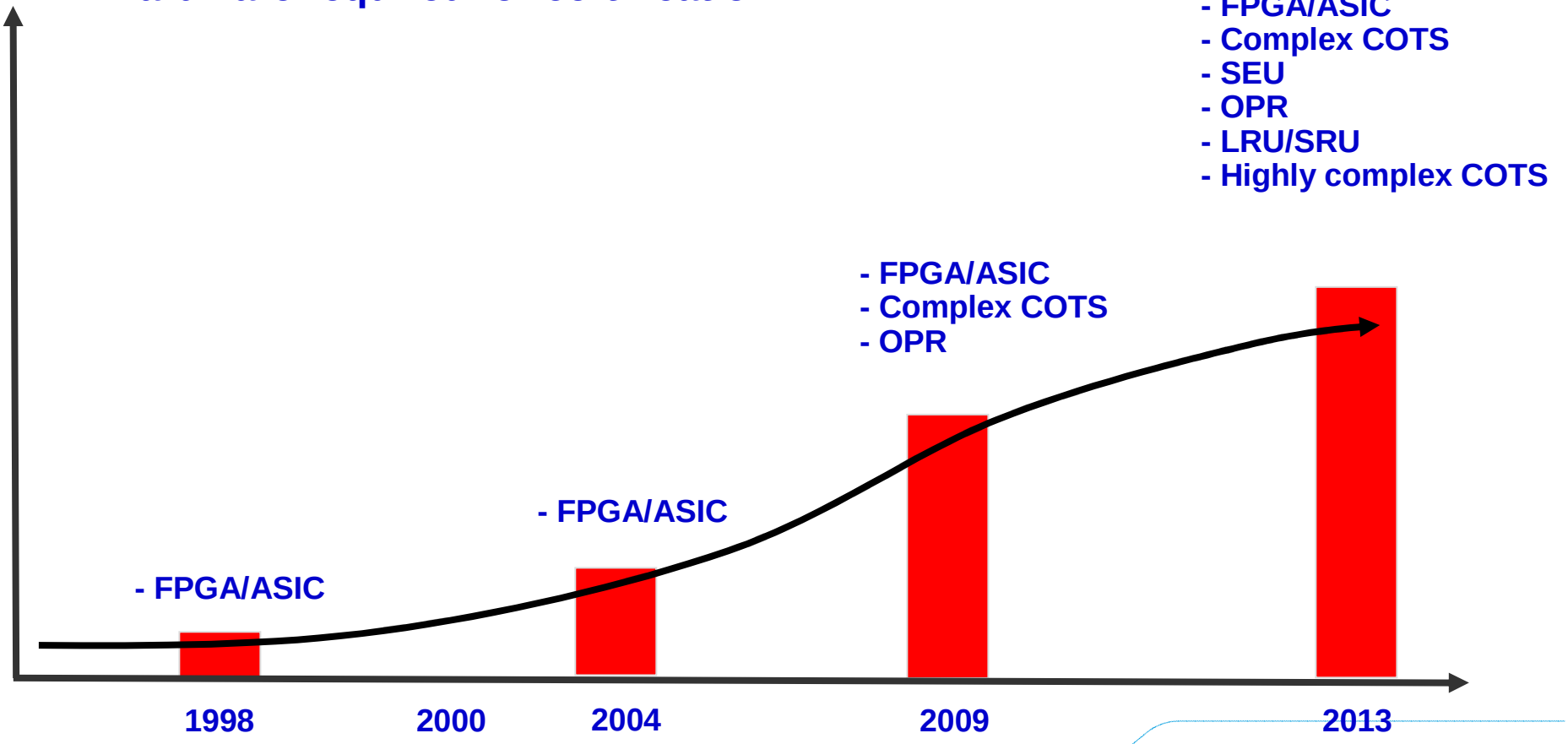


- Multiple function in single LRU
- Main constituents of the LRU
  - Microcontroller to System on chip
  - Million cell FPGA with IP
  - Multi -Bus: PCI, Ethernet, ARINC, RS, CAN
  - Radiation sensitivity

- **Complexity**
  - SW
  - FPGA/ASIC
  - Equipment design and architecture

AEH Certification topics evolution

Requirements for Airborne electronic Hardware required for certification



Airborne Electronic certification evolution

End 90': Complex Electronic certification

- **Scope:** Design assurance for FPGA and ASIC based on application of DO254
- **Impact:** ASIC/FPGA designer using modeling language

2013: Airborne Electronic Hardware

- **Scope:** Design assurance for FPGA/ASIC based on ED80/DO254

+ Design assurance for LRU/SRU
+ Management of Single events upset
+ Management of Highly complex COTS
+ Management of Graphical processor
+ management of OPR

Scope Certification Memo

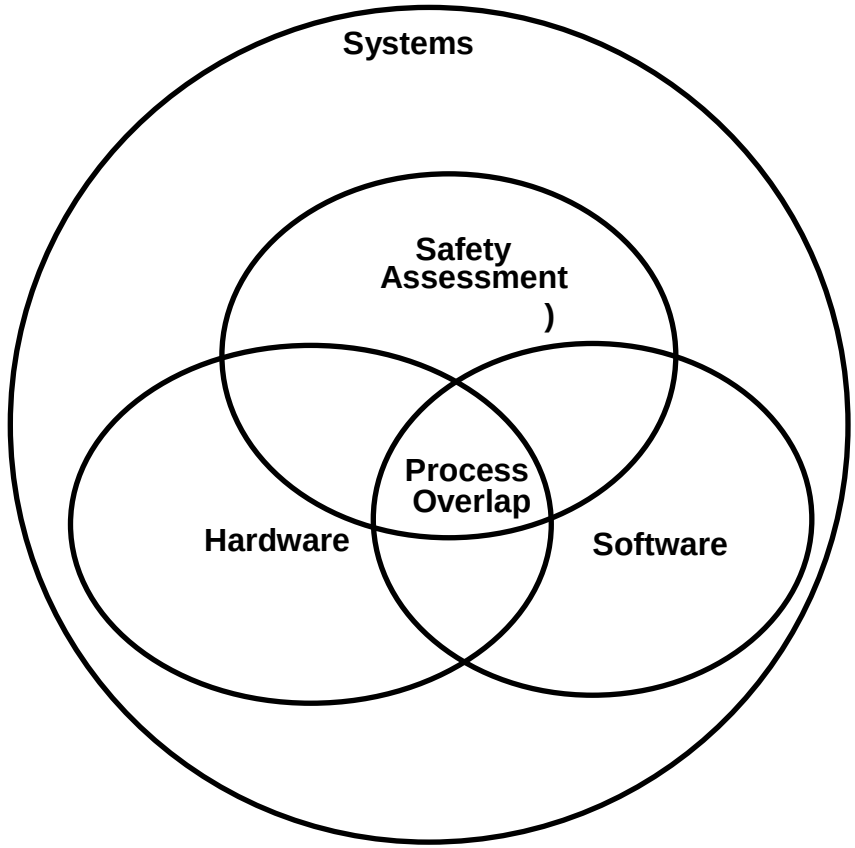
- **Impact:** FPGA designer, Equipment, Software, Hardware designer, Safety specialist

- ..\..\..\04- technique Support\05- Applicable documents\Regulations\EASA\Cert Memo\Release\EASA CM-SWCEH-001 Development Assurance of Airborne Electronic Hardware.pdf

Statement

- Airborne electronic design assurance aspects is no more limited to hardware level aspects, but need to include
  - System levels,
  - Software levels,
  - All hardware levels
  - Safety aspects

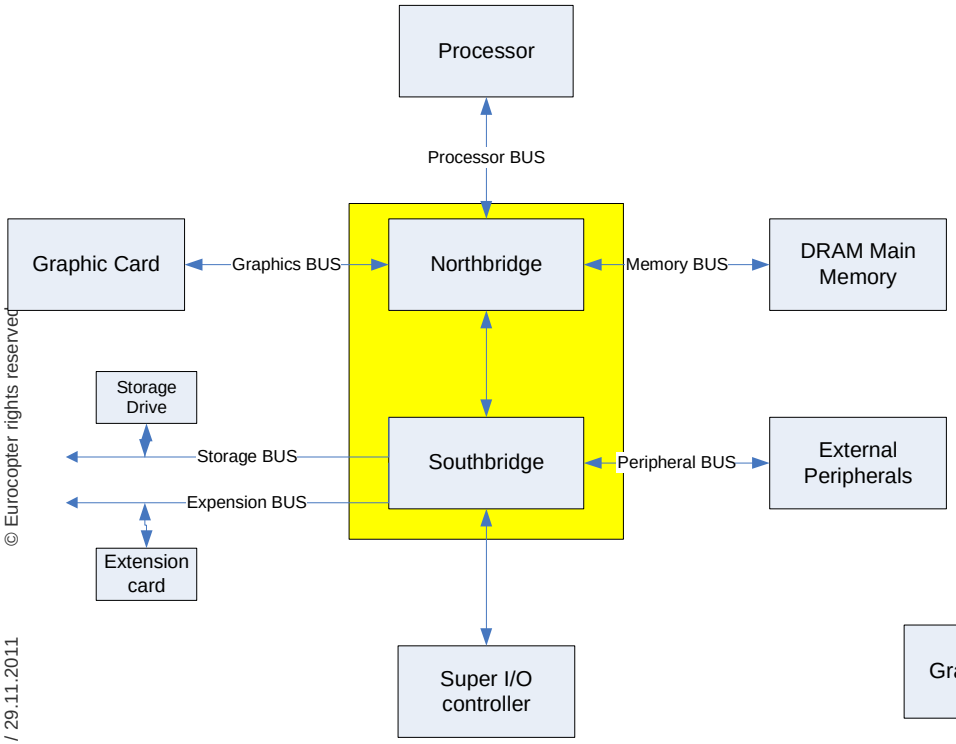
Process overlap has taken more and more importance



Agenda

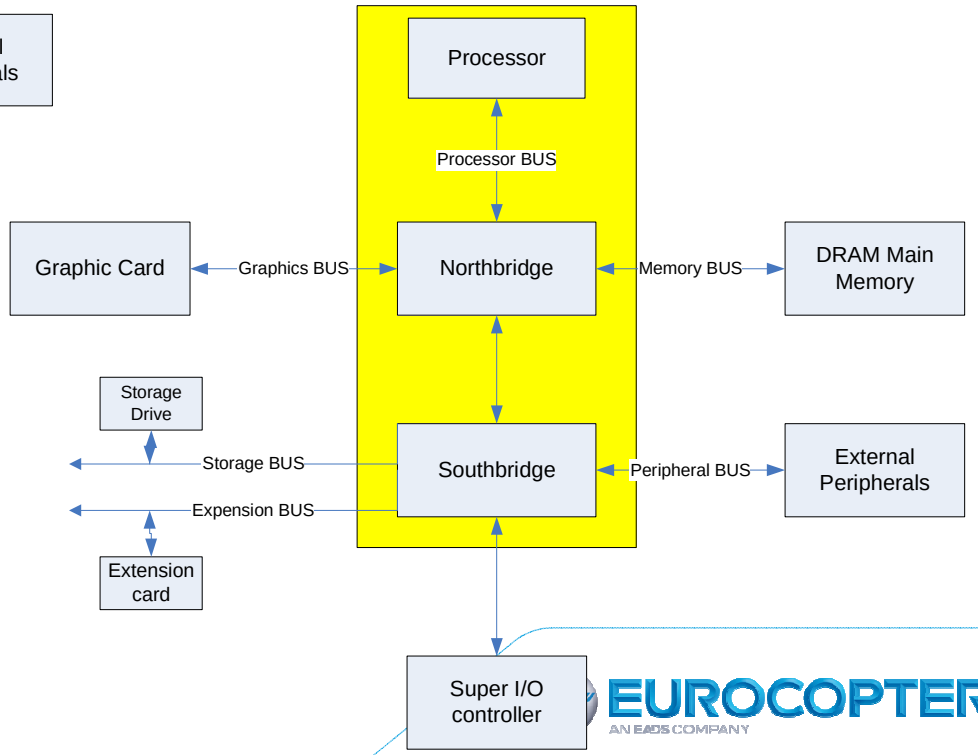
- Airborne Electronic certification evolution: From pure HW to mul-discipline involvement
- Illustration:
  - complex COTS
  - Single event upset
  - Management of OPR
  - Management of LRU design assurance
- Major current Pitfalls and conclusion

Complex COTS- Recall of the concern



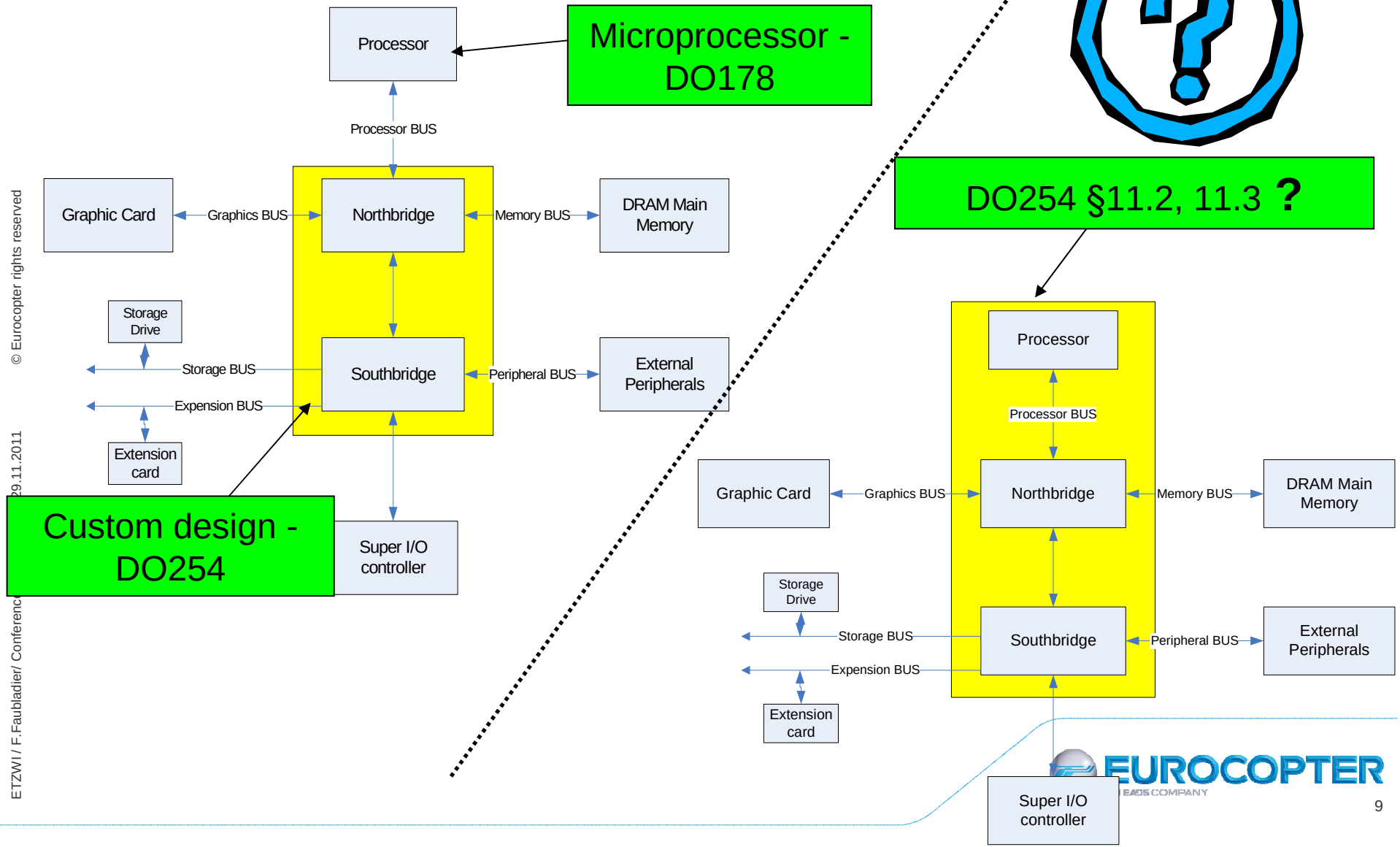
90' CPU Board Architecture-
Based on processor + customized design (ASIC)

CPU Board Architecture
Based SOC microcontroller or SoPC using IP blocks



EUROCOPTER
AN EADS COMPANY

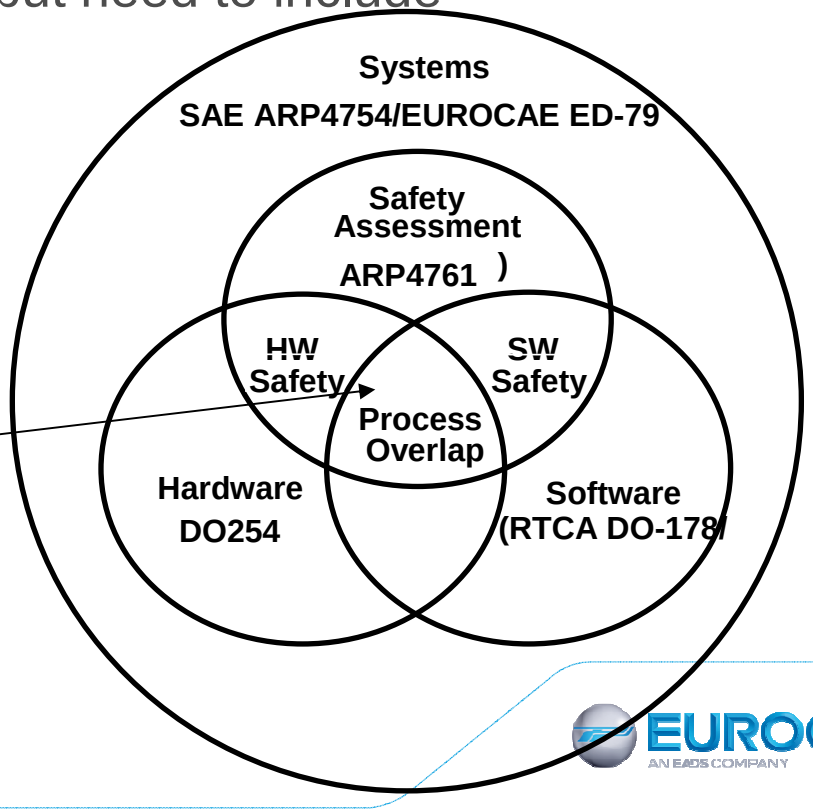
Complex COTS – Recall of the concern



Complex COTS – Guidelines (ref AEH certification meo)

- ED80/D0254 does not address properly this concern
- AEH certification memo gives guidelines how to manage complex COTS
- Main statement: Complex COTS certification aspects cannot be limited to component level aspects, but need to include
  - System levels,
  - Software levels,
  - hardware levels
  - Safety aspects.

Complex COTS assessment positioning



Complex COTS – Certification guidelines allocation

Allocation of Guidelines

Hardware:	**System:**	**Software:**	**Safety:**
- Component selection - Data analysis -Service experience analysis -Errata analysis	- Usage domain aspects - Architectural mitigation - HW/HW and HW/SW integration	-Implementation of requested configuration -Implementation of errata workaround	Safety analysis: Functional failure path

Complex COTS : Impact on development process

- Example of information flow between COTS activities and all development processes
  - Domain usage definition impacting the configuration of the COTS through register programming (SW) or pin implementation (HW)
  - Integration of the problem reports workaround that may have an impact on hardware or/and software requirements.
  - Implementation architecture, including fault containment and fault mitigation strategies,
  - Prohibited functionalities due to determinism issue

→ Derived requirements need to be fed back to the system, software, hardware and safety process

Complex COTS – Impact on safety analysis

- Example of addionnal safety analysis due to complex COTS usage:
- Extract of certification memo:
  - Architectural mitigation should be implemented in any case in which one or more instances of the COTS component could cause a Catastrophic failure effect without any other contributing faults occurring

    The results of Common Cause Analysis performed by the applicant should be taken into account. For example, the anomalous behaviour or failure of identical COTS components (common design), implemented in redundant system architecture, should not lead to a Catastrophic failure condition.

→ additional safety analysis from aircraft to complex COTS devices

SEU/MBU – Recall of the concern

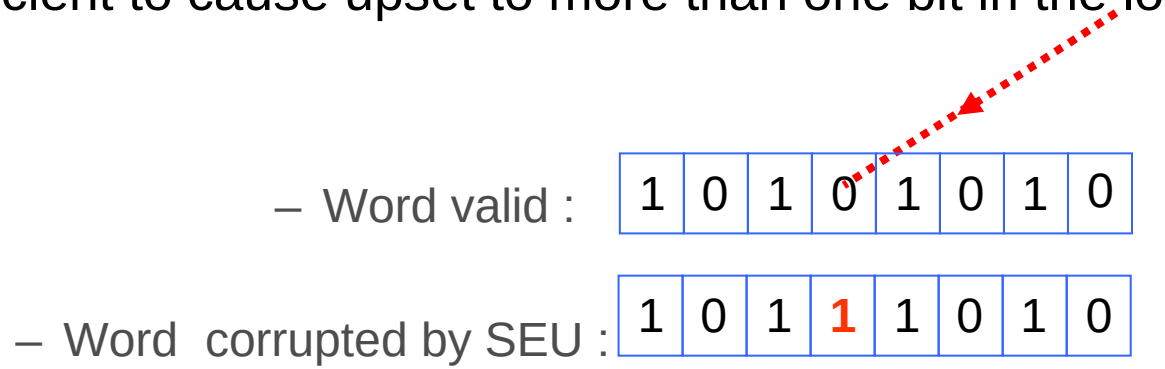
Atmospheric radiation environment (cosmic rays)

SEU : Single Event Upset

Occurs in a semiconductor device when the radiation effect is sufficient to change a cell's logical state level

MBU : Multiple Bit Upset

Occurs in a semiconductor device when the radiation effect is sufficient to cause upset to more than one bit in the localized area



SEU/MBU - Guidlines

safety requirements (occurrence rates of undesired events) shall be met taking into account the SEU/MBU risk.

- ED80/D0254 does not address properly this concern
- AEH certification memo gives guidelines how to manage SEU

Atmospheric radiation – R&R

- AEH guideline allocation

Hardware:	**System:**	**Software:**	**Safety/reliability**
-Identification of sensible component -Calculation of Single event rate (SER) -Implement of mitigation technique at Hardware level (parity, ECC)	- System Architectural mitigation (dual channel with cross talk) - HW/HW and HW/SW integration	-Implementation mitigation means (CRC applicatif) -Triplication of data and voting	-Determine Altitude and latitude -Integrate SER in safety analysis at aircraft level) -Asses the MTBUR and potential NFF

Atmospheric radiation – Impact on development process

- Exemple of overlap between Atmospheric radiation activities and all processes
  - Impact on component selection
    - RAM versus Flash
    - FPGA versus ASIC
  - Impact on development process
    - Hardware architecture and specification
      - CRC, parity, triplication
    - Software specification
      - Triplication, cross check
    - System architecture and specificationi:
      - redundancy, cross talk

Open problem management – R&R

OPR: AEH certification memo

Hardware:	**System:**	**Software:**	**Safety:**
- Problem reported - Root causes analysis - Problem corrected	-Problem reported during the integration	-Problem reported -Root causes analysis - Problem corrected	-Impact analysis -Classification according to effect at aircraft level

Only the equipment integrator can determine the classification of the OPR based on impact analysis

OPR – Impact on development process

Overlapping process

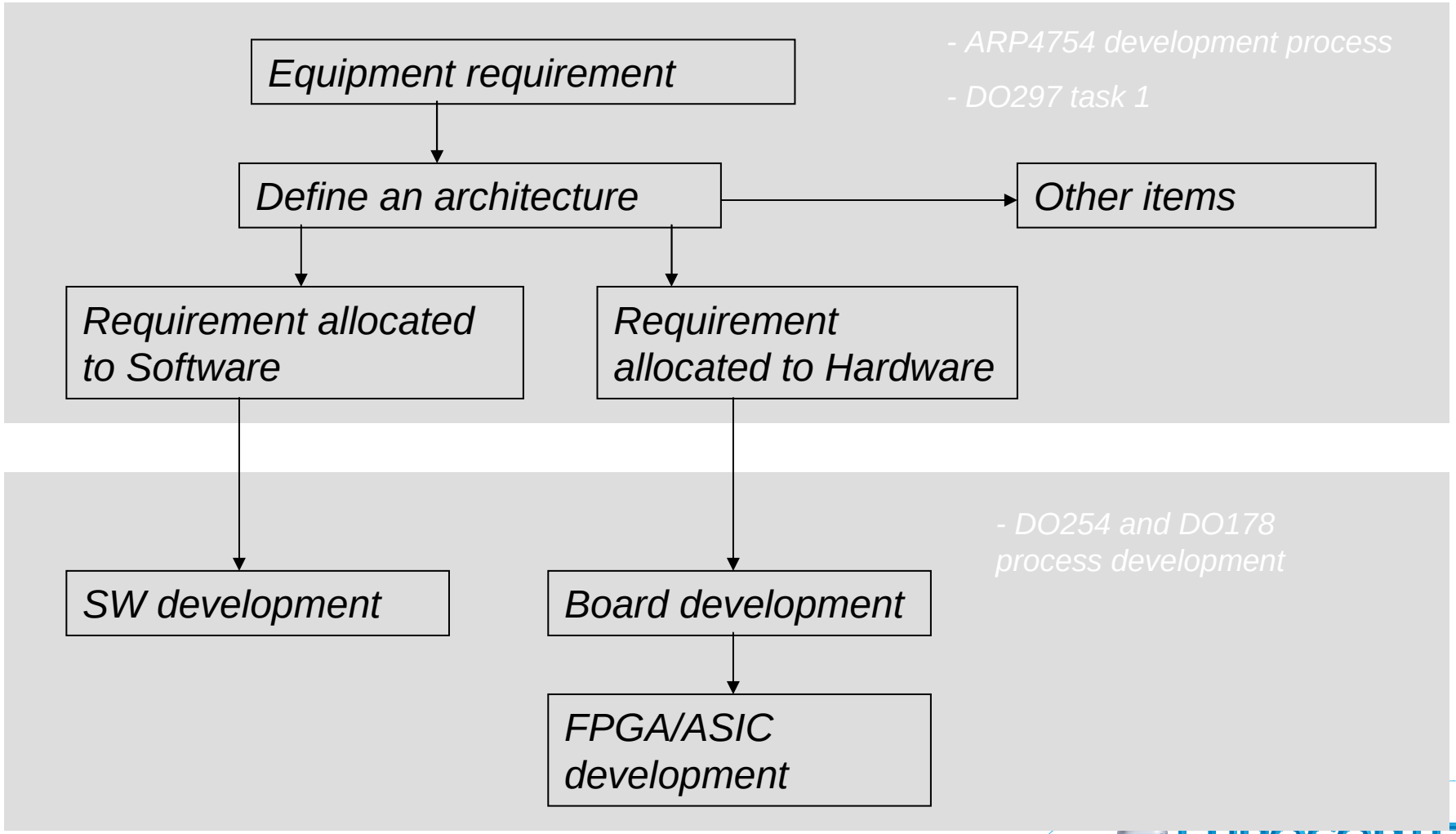
- HW: HW problems have to be reported in the HAS (Hardware Accomplishment summary)
- SW: SW problems have to be reported in the SAS (Software Accomplishemnt summary)
- Equipment supplier shall identify the limitation in the DDP at equipment level
- Equipment integrator in the aircraft shall perform an impact analysis at aircraft level: “System certification summary “ and give an appropriated classification

LRU design assurance

- According to certification memo, LRU and SRU may be submitted to application of DO254 .
  - Question: Can DO254 standalone be sufficient to cover the design assurance of LRU which mix HW and SW configuration item, HW configurations items ?
  - Answers: No
    - Need to consider architecture definition based on safety spefic analysis
    - Allocation requirement to HW and SW
    - Need to define a strategy of integration and verification at equipment level

LRU design assurance need to addressed properly at system and software level

LRU design assurance



LRU design assurance

- Exemple:
  - To develop & justify that the equipment architecture is consistent with its requirements defined in the specificationq
    - General architecture: Identification of configuration Item
    - Mode and state: Power up, Fail mode, maintenance, data loading
    - Interruption: PFI, Failure mode
    - Internal bus topology (Protocol, master/slave/ Burst)
    - CPU load, Memory frequency (RAM, Flash, NVM)
    - Partitioning control
    - Cooling concept
    - Internal power distribution,
    - …

Agenda

- Airborne Electronic certification evolution: From pure HW to mul-discipline involvement

- Illustration:
  - complex COTS
  - Single event upset
  - Management of OPR
  - Management of LRU design assurance

- Major current Pitfalls and conclusion

Main pitfalls

- Development assurance are still based on the concept of separation of responsibilities between various disciplines
  - Approaches are incongruent with the demands of integrated architectures
  - Management of interaction between system, SW, HW and safety are poorly addressed
- Top-down approach: From Aircraft function to HW is consolidated by a bottom up approach too late.
  - Identify HW issue and managed properly at system level
- System aspects of equipment is often not addressed
  - Validation purpose, architecture definition justification
  - Allocation justification to HW and SW
  - Organization for HW/HW and HW/SW Integration and verification
  - Management and demonstration that hardware issues are well managed at other levels

Conclusion

- The good design quality of FPGAs/ASIC and SW do not conduct to a good design quality of equipment/system
- Due to introduction of new technology, the airborne electronic aspects addresses topics beyond hardware aspects related to ED80/D0254
- A lot of activities regarding HW is now strongly linked with several filed of competence (HW, SW, system, aircraft)
- Facing this reality, EASA launched a call to “re-open DO254”
  - 2014: Find an agreement on the perimeter of DO254 change, define working group
  - 2018/2019: Release DO254A

End of presentation

Questions ?

EUROCOPTER
AN EADS COMPANY