



## ETSO Workshop 2007 Electronic Hardware Qualification Complex Hardware

*Friedhelm Runge*  
Parts & Appliances – Avionics PCM

04./05.12.2007

1



European Aviation Safety Agency

## Overview

- What is “complex hardware”
- When is complex hardware qualification required?
- Design process follows ED-80/DO 254 principles
- Certification Liaison = interaction with authority
- Form of Approval

04./05.12.2007

P&A Section

2

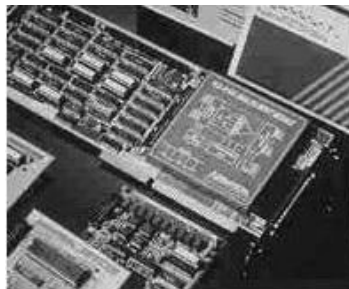


European Aviation Safety Agency

## Complex Hardware Definition

- ED-80 §1.6: A hardware item is identified as simple only if a comprehensive combination of deterministic tests and analyses appropriate to the design assurance level can ensure correct functional performance under all foreseeable operating conditions with no anomalous behaviour.

When an item cannot be classified as simple, it should be classified as complex. An item constructed entirely from simple items may itself be complex. Items that contain a device, such as an ASIC or a PLD, can be considered simple if they meet the criteria of simple as described in this section.



04./05.12.2007

P&A Section

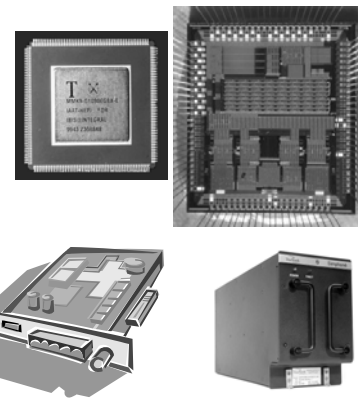
3



European Aviation Safety Agency

## Example of Complex Hardware

- The guidance in this document is applicable, but not limited to, the following hardware items:
- 1. Line Replaceable Units (LRUs).
- 2. Circuit Board Assemblies.
- 3. Custom micro-coded components, such as Application Specific Integrated Circuits (ASICs) and Programmable Logic Devices (PLDs), including any associated macro functions.
- 4. Integrated technology components, such as hybrids and multi-chip modules.



04./05.12.2007

P&A Section

4



## Certification Requirements

- **Aircraft Level: CS 25.1309 + CRI** requires Electronic Hardware Qualification for complex hardware used in critical systems
- **FAA TSO: recent published TSOs like C3e dated 15.10.2007: Electronic Hardware Qualification.** If the article includes a complex custom micro-coded component, develop the component to the guidance in FAA advisory circular (AC) 20-152, *RTCA, Inc. Document RTCA/DO-254, Design Assurance Guidance for Airborne Electronic Hardware*. The hardware design assurance level should be consistent with the failure condition classification defined in paragraph 3.b of this TSO
- **ETSO: Will be required in new ETSOs. See NPA 2007-14**
- **Optional assessment: Electronic Hardware Qualification is optional but can be handled within the ETSO/TSO process**



## Certification Principles

- As the ability to test the system performance under all conditions may not exist, a controlled design process approach is used.
- Similar approach as used for software. The same principles apply.
- Apply controlled design process with a phased approach. The transition from one development phase into the next one is done in a controlled environment. Including a design life cycle process.
- Process requirements as defined in ED-80/DO-254 "Design Assurance Guidance For Airborne Electronic Hardware"



## Process Phases

- **Planning process**
- **Design process**
  - ✦ Requirements capture process
  - ✦ Conceptual design process
  - ✦ Detailed design process
  - ✦ Implementation process
  - ✦ Production transition process
  - ✦ Acceptance test
  - ✦ Series production
- **Validation and verification process**
- **Configuration management process**
- **Process assurance**



## Development Assurance Levels

- There are five system development assurance levels, Level A through Level E, corresponding to the five classes of failure conditions: catastrophic, hazardous/severe major, major, minor and no effect.
- Initially, the hardware design assurance level for each hardware function is determined by the System Safety Assessment process using an Function Hazard Analysis to identify potential hazards and then the Preliminary System Safety Assessment process allocates the safety requirements and associated failure conditions to the function implemented in the hardware.
- The same Level definition is used for hardware and software.



## Difference in Approach in accordance to elected Level

### → Level defines

- ✦ detail of documentation e.g. the availability of certain documents describing and documenting the process including transitions
- ✦ independence requirements for checking function



## Certification Liaison

### Minimum required documentation to be delivered to Certification Authority

- **PHAC** Plan for Hardware Aspects of Certification describes system, planned approach, life cycle definition, tools to be used, schedule ... The PHAC should be submitted to the certification authority for review at a point in time when the effects of design changes on the program are minimal.
- **HAS** **HARDWARE ACCOMPLISHMENT SUMMARY** describes the main achievements and results.
- **Top-Level Drawing** (Hardware Configuration Index **HCI**): The top-level drawing uniquely identifies the hardware item and identifies all assemblies, subassemblies, components and relevant documentation that define the hardware item.
- Assessment done by document review and process audit.
- Early involvement in the design process is necessary.



## Recording of Compliance

- To be mentioned in the DDP equivalent to the statement regarding the achieved software level.
- Remark on the Certificate: ED-80/DO-254 Electronic Hardware Design Assurance has been demonstrated.



## Summary

- Complex hardware ≠ simple hardware
- Critical systems require complex hardware qualification
- Design Process principles following ED-80/DO 254 requirements
- Similar to software qualification
- Early liaison with authority
- Remark on ETSO Approval, DDP statement



European Aviation Safety Agency

## Further Questions

---



---

04./05.12.2007

P&A Section

13