Airborne Electronic Hardware Lessons Learned Panel

2008 National Software and Airborne Electronic Hardware (SW & AEH) Conference
Panel members

Martha Blankenberger
  – Company DER
  – Rolls Royce

Tammy Reeve
  – FAA Consultant DER
  – Patmos Engineering Services, Inc.

Karen Brack
  – Staff Engineer - ASIC and FPGA Design
  – Honeywell Aerospace Electronic Systems

Randall Fulton
  – FAA Consultant DER
  – SoftwAir Assurance, Inc.
Planning

• Get hardware management plans and standards finalized early in the project

• Hold a meeting with the assigned FAA specialist to get agreement on approach for compliance

• Get approvals for PHAC and other plans/standards before the development starts
Planning

• Make sure plans state the “how” to meet objectives from DO-254 and don’t just repeat the objectives.
• Configuration management procedures need to address baselining and change control for development activities.
• Verification plan need to be clear on form of procedures or results.
• Verification plan should address board level testing.
Standards

• Defining and applying standards can help designers engineers, rather than impede.
  – A good set of design standards will facilitate avoiding pitfalls in designs.
  – A good set of planning standards will facilitate addressing all appropriate topics in the PHAC and planning documents.

• Putting standards in the transition criteria can put emphasis on compliance with the standards.
Requirements

• Definition of “derived” requirement
• Requirements need to contain:
  – Signals; specific registers
  – Timing information
  – Traceability to “system” (parent) requirement
• Requirements need to omit:
  – Traces to ICDs
  – Design details
• Scope is analogous to a timing diagram for the device
Requirements

• Have a clear definition for derived requirement vs. High level requirement
• Traceability and tagging standards need to be well defined
• Feed back of derived requirements to SSA should be defined and understood (also put in the plans )
• SRAM device selection considerations should be understood and architectural/ design mitigation taken where required
• COTS Cores identified
• Re-use should be identified and planned for
Requirements

• AEH requirements review process should include safety engineers.
  – AEH designers may not be fully aware of the impact to safety considerations by derived implementation requirements

• Requirements review should include a function-by-function consideration of whether abnormal and exception conditions are clearly specified.
Design/Code

• Design Architecture not defined.
• Device vendor specific elements are not managed in separate hierarchical blocks.
• Not planning for obsolescence and future growth
• Registered outputs are not used (where possible)
• HDL based entry, C/C++ and/or schematic entry standards are not defined or applied.
• Vendor supplied cores are not clearly identified and the vendor specific tailoring for the cores are not included in the design documentation.
• Design is not properly constrained for timing of clock domains, I/O, multicycle paths and false paths.
Implementation: Manufacture and HW Test

- Place and Route of device should be fixed in the tool options.
- Optimizations on an incoming netlist should be understood or controlled as part of the build procedure.
- If Device level partitioning is used, it needs to be defined and controlled for repeatability in the place/route for the physical device.
- Device programming procedures and build procedures need to be repeatable and the tools under configuration control (HCI/HECI)
Verification/Test

- Testbench need to be repeatable and traceable to the requirements
- Testbench needs to have comments for maintainability and understanding of testing approach.
- For level A and B devices, the “elemental analysis” coverage report analysis should include a justification for those areas that or not 100%
- Gate-level simulations with or without full timing are not performed and/or the results of this activity are not kept
- When using continuous monitors in simulation testbenches, the test procedure needs to show that appropriate inputs are applied to stimulate the conditions being monitored.
Off-shore development

• Oversight is needed
• Practices may not be compliant
• Developers may put too much faith in tools
• A supplier management plan detailing what objectives the off-shore company is satisfying should be defined.
Dissimilarity

• Shorts cuts sought
  – Real dissimilarity often avoided

• Designers confuse different functions with dissimilarity
  – Then use same devices and tools

• Entire tool chain should be included in considerations
Tools

• Synthesis tools
  – Default settings often use one hot state machine type designs
  – Many times designers are not cognizant of the issues
  – Optimization targets the use of the least number of gates
  – Many tools will change intended function
    • Glitches at power up
    • Device lock up
Tools

• Tool assessment should include:
  – consideration of automated checking in simulation testbenches
  – consideration of automated checking in laboratory testing and production testing for verification credit

• Tool assessment should be performed early to avoid the need for late tool qualifications because automated checking was used.