

2003 FAA National Software Conference

Complex Hardware (ASIC/PLD) Experiences

2003 National Software Conference

Complex Hardware (ASIC/PLD) Experiences

September 16 - 19, 2003

Jeff Knickerbocker
jeff@sunrise-cert.com
(651)674-7593

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

1

Overview

-
- Examination of five different applicants
 - Varying organizational size
 - » Small < 10 team members
 - » Medium ≤ 50 team members
 - » Large > 50 team members
 - Varying system complexity
 - » Small < 5 PLDs in system
 - » Medium ≤ 20 PLDs in system
 - » Large > 20 PLDs in system
 - Varying applicant expertise in terms of civil approvals
 - » Neophytes < 3 years of civil approval background
 - » Novice ≤ 10 years of active civil approval background
 - » Seasoned > 10 years of active civil approval background
 - Varying certification authorities
 - Various certification methods (TSO/TC)

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

2

2003 FAA National Software Conference

Complex Hardware (ASIC/PLD) Experiences

Early Adapter – Feel Our Pain

- Attributes:
 - Medium organization
 - Small systems
 - Seasoned applicant
 - Level B with designs on Level A
 - No SC-180 representation
 - Weak internal processes (initially)
 - Passive/aggressive approach to regulatory approvals
- Two ASICs in what is typically a TSO'd device
- The customer wants a TSO on the circuit card vs. a TSO on a typical “black box”
 - That has never been done - somebody is going to pay for this and it is not us!
 - **We paid for it...**
- DO-XXX is coming! We are going to die!
 - Start with DO-178B
 - You can't apply DO-178B to ASICs...
 - Somebody is going to pay for this and it is not us!
 - **We paid for it...**

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

3

Feel Our Pain!

- DO-178B to SC-180 draft 15, to draft 16, to DO-254
 - Get ready with DO-178B
 - Get ready with SC-180 draft 15
 - Get ready with SC-180 draft 16
- The government regulator changed!
 - Now we have to do DO-254 and we are two years into the project!
 - DO-254 is here! We are dead!
 - Somebody is going to pay for this and it is not us!
 - **We paid for it...**

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

4

2003 FAA National Software Conference

Complex Hardware (ASIC/PLD) Experiences

Feel more of our pain!

- **YOU WILL PROVIDE A SAFE PRODUCT!**
 - How????!!!!
- **YOU HAVE TO DEMONSTRATE SOME KIND OF FUNCTIONAL COVERAGE METRIC FOR YOUR CHOSEN APPROACH TO DEMONSTRATE CORRECT BEHAVIOR**
 - But we want to use a 4GL approach – how am I going to do this?
 - But we want to use VHDL with block diagrams- why should I do this?
 - We always use schematic capture with architectural block diagrams and never did this before
 - Even if we use vendor supplied mega-functions?
 - Somebody is going to pay for this and it is not us!
 - **We paid for it...**
- Traceability!
 - That's for software sissies!
 - There is no way we are doing traceability!
 - **We did full traceability...**
- **YOU MUST DEMONSTRATE SOME KIND OF COVERAGE METRIC FOR YOUR CHOSEN VERIFICATION APPROACH TO DEMONSTRATE NO ANOMALOUS BEHAVIOR**
 - We want toggle coverage
 - We want structural coverage
 - We want to do an FMEA
 - Somebody is going to pay for this and it is not us!
 - **We paid for it...**

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

5

Please feel our pain...

- What do you mean we need better CM and defined life cycle data?
 - What do you mean we need controlled life cycle in addition to traceability?
 - We never did that before!
 - We are going to release our outline drawing when we are done...
 - We are not going to release our requirements, design, and implementation data!
 - **We released our life cycle data...**
 - And we even found out life was better when we actually made our CM systems work!
- We can only justify Level B for our system but we want Level A approvals on PLDS!
 - **IF YOU CANNOT JUSTIFY LEVEL A IN THE SYSTEM, WE WILL NOT GIVE YOU LEVEL A. YOU WILL HAVE TO COME SEE US AGAIN WITH A LEVEL A PRODUCT. WE WILL TALK AT THAT TIME...**
 - Somebody is going to pay for this and it is not us!
 - **We paid for it...**

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

6

2003 FAA National Software Conference

Complex Hardware (ASIC/PLD) Experiences

Have you not felt our pain yet?

- Different chips but similar problems...
 - We have a very complex COTS chip we want to migrate to commercial avionics
 - » Functional failure paths for an ASIC?!?!?
 - » How do I do that for a highly integrated stochastic process?
 - We want to consolidate discrete components into a single chip
 - » Functional failure paths for an ASIC?!?!?
 - » How do I do that for glue logic?
 - Somebody is going to pay for this and it is not us!
 - **We paid for it...**
- Our tool vendor screwed up and we have to re-spin the ASIC adding a year to the program!
 - Somebody is going to pay for this and it is not us!
 - **We paid for it...**
- When we were finally done,
 - We did an FFPA, FMEA, structural coverage analysis, toggle coverage, test vectors, simulations at various levels, functional testing, qualification testing, integration testing, system testing, and on, and on...
 - In reality all was planned for with one exception – the FFPA
 - **And we paid for it...**

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

7

At least learn from our pain...

- Creating PLDs for commercial avionics takes a lot of money
 - You can make a small fortune developing ASICs and FPGAs...
 - To do so you need to start with a large fortune
 - You can make an even smaller fortune if you are not careful...
- Create a coherent, technically appropriate development and verification plan early!
 - Consider current state-of-the-practice processes - DO-254 was not initially available but...
 - » Mentor, Sun Microsystems, Xilinx, et al all had, and have, very good guidance available for PLD development – it is not necessarily for safety critical systems, but it is for very-large volume/low margin systems
 - » There is a fair amount of overlap between safety critical approaches and approaches used to reduce development risk (recalls and loss of market share cannot be tolerated – get it right before you ship it mentality)
- Involve the regulatory officials early - in the case of personnel transitions go the extra mile to ensure a smooth hand-off
 - Emphatically telling the regulatory officials what you will and will not do does not seem to impress or influence them in a positive fashion
- Choose your technology partners carefully
 - Selecting the cheapest foundry that really doesn't want your low-volume avionics business may not be cost wise - guaranteed you will get what you pay for
- End of story – after 4 years the circuit card now has a TSO and is being sold into domestic and international markets (circa 2003)

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

8

2003 FAA National Software Conference

Complex Hardware (ASIC/PLD) Experiences

Kicking and Screaming Our Way to Approval (maybe)...

- Attributes:
 - Large organization
 - Large systems
 - Seasoned applicant
 - All Levels
 - Good SC-180 representation
 - Defined internal processes deliberately vague
 - Uncooperative and arrogant approach to regulatory approvals
- Primarily TSO'd devices
- Most frequently heard phrases and behaviors...
 - No one has ever done this before so nobody knows how to do it...
 - We never had to do this before...
 - Customer Z never made us do this and they "got certified"...
 - We cannot afford to do this...
 - We will have to run that by management before we can even think about doing that...
 - That is not expressly called out in our defined processes...
 - Well it may be required, but we know Congress-person/Senator So-and-so will work the political chain and get alleviation...
 - Prove that it is not safe...

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

9

Still kicking and screaming...

- Individual designers did well with smaller parts
 - Both schematic capture and VHDL approaches (designer specific)
 - Lots of informal simulation work (there always is some)
 - Extensive Build-Test-Fix cycles (hack?)
 - Very limited defined requirements (all levels)
 - "Gross" architecture may be documented
 - Lower level architecture non-existent
 - Very limited traceability (little granularity)
 - Development in-the-small did not scale to more complex PLDs
 - » More complex devices were very error prone after customer delivery – still a perception that this supplier's hardware is "junk" even after things got somewhat better
 - No real consideration given to verification activities other than test
 - No real means to address coverage of elements or anomalous behavior
- Organizational Challenges
 - Poor CM practices on both development and manufacturing sides of the house
 - Weak to non-existent QA function
 - QA had strict adherence to process compliance – ensure checklists are signed
 - No desire evident to achieve DO-254 compliance (words and no actions)
 - No commitment to advancing organizational verification skills that would be technology appropriate

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

10

2003 FAA National Software Conference

Complex Hardware (ASIC/PLD) Experiences

Kicking and screaming works but at what cost?

- Very tough sell to regulatory authorities and customers
 - Compliance is very hard to find...
- Still not DO-254 compliant
 - Limited success with regulatory and customer approvals at this point
 - Will be difficult to achieve regulatory approval on future systems which call out the new AC
 - Organizational processes do not support DO-254 compliance and it seems work has not yet started in this area – it takes a long time to turn processes around in a large organization

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

11

Lessons taken from kicking and screaming

- Choose suppliers carefully
 - Pass on those suppliers that have a demonstrated record of poor performance
 - It is not worth the time, effort, or aggravation (not to mention potential litigation)
 - If you know you are getting a “kicker and screamer”...
 - Evaluate processes early against current state-of-the-practice and document deficiencies
 - Work mitigation plans with the regulatory authorities where there are deficiencies
 - Work with the integrating organization (customer) to ensure they understand supplier deficiencies and what is going to be involved with sub-standard suppliers
 - Involve the regulatory authorities directly in the review process
 - Be vigilant as a DER
 - It is not worth your reputation and career to placate “kickers and screamers”
 - Do not sign off on an 8110-3 if the approach or data is questionable
 - Just because Company X DERs approved, it doesn't mean they know what they are doing
 - Report pressure to “sign-off” to the regulatory authority (8110.37C)
 - When the political games and threats start...
 - » We will go to your management...
 - » We will go to your ACO...
 - » We will go to the directorate...
 - » We will go to headquarters...
 - » We will go to Congress...
- Get out of the way! When such machinations work, and they sometimes do, don't sacrifice your own integrity!**

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

12

2003 FAA National Software Conference

Complex Hardware (ASIC/PLD) Experiences

Legacy - Boeing Already Made Us Do It!

- Attributes:
 - Large organization
 - Large systems
 - Seasoned applicant
 - Levels A & B
 - Little SC-180 representation
 - Well defined internal processes
 - Very cooperative

- Approvals primarily through TC process

- Most frequently heard phrases and behaviors...
 - Not anxious to invest in old parts...

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

13

Legacy – don't make us spend any more \$

- Technology and Process Attributes
 - Well defined but old processes (circa 1994)
 - Good CM
 - Weak QA (check for signatures on checklist variety)
 - Primarily schematic capture with limited VHDL
 - Data packaging in terms of DO-254 sub-optimal (but it was a long time before DO-254)
 - Limited but adequate traceability (not fully proven yet)
 - » Requirements -> architectural blocks -> implementation -> black box V&V

- Roll forward approach (no design or technology changes)
 - Create a PHAC
 - » Identify what is and is not available
 - » Identify processes
 - » Closely link PLD functionality to aircraft level FHA
 - » Identify previous applications and airframes
 - » Identify previous proof of TC traceability (baseline traceability)
 - » Provide an analyses of operation environment and enveloped for previously approved against the currently planned environment and envelopes
 - » Map legacy life cycle data and processes into suggested DO-254 approach and annotate differences with rationale

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

14

2003 FAA National Software Conference

Complex Hardware (ASIC/PLD) Experiences

Legacy – we still want to meet your needs

- Roll forward approach (continued)
 - Customer DER sample legacy data against claims made in the PSAC
 - Perform extensive system validation and verification tests including:
 - » Qualification testing
 - » HIRF/Lightning testing
 - » In-target software testing
 - » Developmental flight testing
 - » Formal flight testing
 - Create a HAS
 - » Document any differences from the PHAC
 - » Document any new concerns not identified in the PHAC and the means of mitigation

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

15

Legacy – Lessons

- Lessons learned
 - Cooperation is a really good thing and will buy a lot of goodwill
 - Involve the regulatory authorities early and often – needless risk has been introduced due to late involvement
 - Be honest and complete, but open-minded when trying to shoehorn into DO-254
 - Ensure data is available to support service history claims
- Status
 - System is not approved
 - » Software work continues
 - » PLD data is still being examined
 - » Equipment has done very well in developmental flight tests

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

16

2003 FAA National Software Conference

Complex Hardware (ASIC/PLD) Experiences

Simple – Really!

- Attributes:
 - Medium organization
 - Small systems
 - Novice applicant
 - Level C
 - No SC-180 representation
 - Well defined internal processes
 - Very cooperative
- Approvals primarily through TC process
- Most frequently heard phrases and behaviors...
 - We really want this to be simple – can we really do that?

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

17

It is simple – trust me

- Organizational attributes:
 - Good CM
 - Strong QA
 - Talented designers that understand the technology
- Data and design attributes
 - No CM or QA plans outside of organizational standards
 - No verification plans
 - No process definition outside of PHAC
 - Requirements and architecture document
 - VHDL implementation in Build-Test-Fix approach
 - HAS will be created
- V&V Attributes
 - Exhaustive bench tests
 - Multiple system integration tests (multiple vendors)
 - Qualification tests
 - HIRF and Lightning tests
 - Developmental flight test
 - Formal flight test
- DER provided 100% review of all data and waveforms – witness > 50% of tests

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

18

2003 FAA National Software Conference

Complex Hardware (ASIC/PLD) Experiences

Simple Lessons

- Lessons learned
 - Cooperation is good
 - Sometimes devices really can be simple
 - Healthy paranoia on the part of an applicant is not always a bad thing
 - “Product” is just as important as “process”
- Status
 - System has not yet been approved
 - Bench verification and validation work is complete
 - Developmental flight testing is going well
 - No real hurdles are expected to come along

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

19

Simple? Yes, no, maybe, what is simple?

- Attributes:
 - Small organization
 - Small systems
 - Neophyte applicant
 - Level A
 - No SC-180 representation
 - What are internal processes?
 - Very cooperative and lots of “heart”
- Approvals primarily through TC process
- Most frequently heard phrases and behaviors...
 - Can you send us a copy of DO-254?

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

20

2003 FAA National Software Conference

Complex Hardware (ASIC/PLD) Experiences

It is complex; Wait – no it isn't

- Interesting attributes
 - Initially assumed complex
 - Took a run at creating “process documents” that would satisfy “complex” guidance
 - Initial process definition attempt quite rough – but still trying
 - Outsourced some of the implementation and verification work
 - No software in the system
 - VHDL implementation
 - Design was closely coupled to aircraft FHA
 - Traceability in place but not hi-fidelity (inexperienced)
 - Plans and documents submitted after the device was built
 - Weak QA
 - Weak CM
 - Several architectural blocks but each block truly was simple

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

21

Can we make it simple for sure?

- DER evaluation of data revealed the following:
 - Plans were likely overkill for “simple” but inadequate for “complex”
 - Architectural blocks truly were “simple” and could be exhaustively tested (but had not been exhaustively tested yet)
 - Block or partition interfaces could be fully exercised with equivalence class testing
 - CM and QA issues could be resolved by pulling all of the data into the airframer's systems
- Supplier was given a choice
 - Keep running at planning documents and follow up with “complex” assurance activities
 - Or go to “simple” and:
 - » Augment with exhaustive tests on partitions
 - » Demonstrate interface tests were truly equivalence class tests
 - » Visit ACO with the airframer to coordinate the shift in direction
 - » Update PHAC to reflect the approach
- ACO bought into the approach
- The supplier chose the latter and didn't look back

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

22

2003 FAA National Software Conference

Complex Hardware (ASIC/PLD) Experiences

Lessons on getting to “simple”

- Choose cooperative suppliers – even small ones
- Question the supplier if you suspect they may have a case for “simple”
- Evaluate the data to make a final determination before calling in the ACO
- Coordinate with the ACO if it is worthwhile to change directions
- Take over some parts of the integral processes if need be

Not the converse is probably more likely with knowledgeable suppliers and is harder to deal with – be suspicious when there is a very cavalier or aggressive approach sales pitch for “simple”

DO-254 Complex – Just Do It!

- Attributes:
 - Medium organization
 - Medium systems
 - Novice applicant
 - Levels A/B/C
 - No SC-180 representation
 - Started with DO-178B and SC-180 Draft 16
 - Excellent CM and QA groups
 - Very cooperative and determined to succeed
- Approvals primarily through TC process
- Most frequently heard phrases and behaviors...
 - When are you going to come see us again?
 - Come critique our approach
 - Are we on the right track?
 - When are you going to start flying our devices and provide feedback?

2003 FAA National Software Conference

Complex Hardware (ASIC/PLD) Experiences

We may not be big but we are excellent...

- PLD Team Attributes
 - Small, tight knit, mature group of developers
 - Committed to action - we decided to get into the commercial side of things and we will make it work
 - Developers spent as much time defining and documenting technical appropriate processes as they did designing
 - Did not hesitate to iterate design or process if it was not "right"
 - Consulted with DER, customer, and other consultants as needed to "get it right"
 - We can certainly do this better than the SW guys
- Verification Team Attributes
 - Responsible for Systems, SW, and HW
 - Independent of Systems, SW, and HW
 - Know the systems as good or better than developers
 - Mature team members
 - Friendly competition with the development organization
 - Respected by the development organization

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

25

DO-254 – Just another challenge to beat

- DO-254 is just another spec...
 - Use the TOC to develop a set of life cycle data
 - Allocate documentation we would normally do into DO-254 data item "buckets"
 - Of course we use the aircraft level FHA – who wouldn't?
 - Traceability? You betcha – how else would we know when we are done?
- Testing
 - Behavioral testing? Who wouldn't do it at multiple levels of simulation starting with initial VHDL compilation through back-annotation of the final model?
 - Coverage? Of course we do that with our VHDL tools
 - Naturally we do system, qualification, and HIRF/Lightning testing
 - Hurry up and do your developmental flight testing and give us feedback
 - When is formal flight testing scheduled?

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

26

2003 FAA National Software Conference

Complex Hardware (ASIC/PLD) Experiences

Lessons with a winning team

- Suppliers with integrity are worth their extra initial cost (cheaper in the long run)
- Can do attitudes, pride, and competence are a refreshing approach
- Self-policed teams don't need policemen
- Well thought out and documented processes and designs are expensive but it beats the alternative
- Keep communication channels open, don't assume you have all the answers as a DER, and get ready for an exciting ride

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

27

Closing Comments

- Attitude matters – yours and theirs
- Your own integrity is more important than any short term comfort realized by placating a corrupt organization
- Be open-minded and explore multiple solutions for any given problem
- Don't be afraid to spend money to save money in the long term
- Start writing down the approach early and allow yourself to iterate if it doesn't work the first time
- You don't know everything – get help when you can get it or need it

QUESTIONS OR COMMENTS?

Copyright © 2003 by Sunrise Certification & Consulting, Inc. All Rights Reserved

28