SpaceWire Test, Validation and Certification: Experiences, Thoughts and Ideas

Barry M Cook, C Paul H Walker
4Links Limited

SpaceWire WG10
20-21 February 2008

Introduction and Content

Link design AND ~~System design~~

1. Why do we need validation / examples
2. How were errors found
3. Responsibilities
4. Economics – Characteristics
5. Economics – Models
6. Guidelines

Why

SpaceWire links *appear* to be easy to design

BUT

- There are subtleties that challenge even the experienced
  - Design tools offer limited help
- Design errors are going undetected
- Some errors have been caught early, some shortly before sign-off and some made it to silicon and products

Examples

Incorrect implementation of time codes	**Early detection**

Examples

Incorrect implementation of time codes	**Early detection**
Loss of data	**Last-minute detection**

Examples

Incorrect implementation of time codes	Early detection
Loss of data	Last-minute detection
Loss of flow-control	Silicon – SMCS332SpW Delayed router Product – SpW IP Tunnel

Examples

4Links®

Incorrect implementation of time codes	Early detection
Loss of data	Last-minute detection
Loss of flow-control	Silicon – SMCS332SpW Delayed router Product – SpW IP Tunnel
Incorrect timeout detection	Silicon – SMCS332SpW Product – SpW IP Tunnel

Examples

Incorrect implementation of time codes	Early detection
Loss of data	Last-minute detection
Loss of flow-control	Silicon – SMCS332SpW Delayed router Product – SpW IP Tunnel
Incorrect timeout detection	Silicon – SMCS332SpW Product – SpW IP Tunnel
Packets with error delivered as correct	Silicon – SMCS332SpW Product – SpW IP Tunnel

How were these found

Use Intelligence and Experience

- What to try, what to look for, what to try next

Use tools able to precisely control/measure test conditions

- Precise error injection
  - all possible SpW errors (functional and timing)
- Precise measurement of behaviour
  - full visibility of reactions (functional and timing)
- Ability to test over a range of conditions
  - within and beyond UUT specifications
  - to provoke asynchronous errors and determine margins

Responsibilities

- **Who, if anyone, is responsible for ensuring designs meet specifications?**
  - Suppliers
    - Self-certification / 3rd party service
  - Contractors
    - Use certification service
  - Agencies
    - List approved designs … Who checks conformance?
- **What should a contract specify?**
  - Behaviour
    - Must meet the specification
  - Implementation
    - Use design X – even if it contains errors and does not meet the specification

Economics - Characteristics

- Some errors are easily found
- Some errors are found only with carefully designed and executed test strategies
- Testing can never be guaranteed to find all errors
- Design reviews complement testing

Economics - Characteristics

- Some errors are easily found
- Some errors are found only with carefully designed and executed test strategies
- Testing can never be guaranteed to find all errors
- Design reviews complement testing

The better the design, the longer it takes to find errors – a perfect design will take forever!

Economics - Models

- Keep testing until the time/money runs out
  - Practical, but offers little comfort
  - Testing is at the end when time/money is in short supply
  - Do you spend money at the start to get the design right or at the end to find errors?

- Shared risk
  - e.g. Base price + Bounty paid for each bug found
    - The tester may choose to extend testing in the hope of finding more problems

Guidelines

- Test by someone other than the designer
  - introduce different assumptions
- Use the best tools available
- Develop a basic set of tests
  - may be automated
- Use intelligence to analyze results to see indication of further errors (not simple go/no-go decisions)
  - difficult to automate
- Characterize
  - Margins (can be a powerful indicator of reliability)
  - performance figures that are not part of the specification

Conclusions

4Links®

- **We have found errors in a number of designs**
  - **all were believed, by their designers, to be correct**
  - **all could have (more or less) serious consequences if deployed**
- **Verified/validated/certified components reduce risk for projects – both risk of failure and financial risk – *so long as that certification can be trusted***
- **A verification/validation/certification service should use the most experienced personnel with the best equipment available**
- **4Links is able to provide these and is offering such a service**