

How Do You Review Someone Else's VHDL Design?

Dr. Rod Barto

3312 Moonlight

El Paso, Texas 79904

915-755-4744

rbarto@klabs.org

rod.barto@att.net

Two Parts to the Answer

- How does one perform a design review, in general?
 - Most design review tasks are independent of how the design is presented
- What does VHDL add to the task?

Basic Design Rule

- The designer should know and be able to prove:
 - The design meets the spec
 - The design passes a worst case analysis
- The designer presents this proof to the reviewer
- The reviewer verifies the proof

Ideal Design/Review Flow

- Designer designs and analyzes
- Reviewer concurrently reviews
- Things that cause disasters:
 - Waiting until the end of the design to do the analysis
 - Waiting until the end of the design to do the review

What is Design Review?

- Scope of review ranges from the most superficial to the most detailed
 - Most superficial: Attend PDR, CDR, FDR, rely on contractor's review presentation
 - More detailed: Also attend peer reviews
 - Most detailed: Additionally, obtain all schematics, VHDL files, etc., perform some analyses and review all others, maintain contact with engineers.

Most Superficial Review

- PDR, CDR, FDR are basically for management
- Too late to discuss real problems in the design: they should already have been dealt with
- From a technical standpoint, are mostly useless.

Attending Peer Reviews

- Peer reviews should be where engineers discuss the technical aspects of the design
- Therefore, the reviewer must be cognizant of the design and requirements, otherwise the meeting will be spent bringing the reviewer up to speed
- This requires the reviewer to spend time with the design outside of the reviews

Most Detailed Review

- In the most effective reviews, the reviewer
 - Has access to all design documentation
 - Understands the specification
 - Performs analyses of selected circuits
 - Understands the design in relation to the whole system
 - Maintains contact with the designers

In Any Event:

- Design review should add to the quality of the design
- The reviewer should not be a burden to the design process
- In some sense, the reviewer becomes part of the design team.
 - But, reviewer must maintain independence, especially if reviewer represents customer

Who is the Reviewer?

- In a customer/contractor relationship, the reviewer is part of the customer organization
- Within a company, reviewers could be part of the reliability organization
- Projects can also be partitioned into designers and reviewers
- Outside reviewers can also be brought in

Problems In Design Review

- Biggest problem: inadequate design documentation, giving rise to questions such as
 - What does this thing do?
 - How does this implement the spec?
 - How does this work?
- Documentation is the designer's responsibility

Designer's Responsibilities

- Make the design reviewable
 - Documentation
 - Theory of operation
 - Proof that spec and WCA are met
 - Organization
 - Partitioning into logical components
 - Presentation
 - Readability of schematics, etc.
- How would you, the designer, explain your design to someone else?

Two Reasons for Reviewability

- The design will be reviewed
 - In peer review
 - By reviewer
- The design will also be transferable
 - Lead designers quit
 - Transferability should be a management requirement

Reviewer Response to Poor Documentation

- Ask a lot of questions
 - Of the designer
 - Of the system engineer
 - Of the scientists
- Reverse engineering
- The reviewer should not automatically assume that the designer understands the design.

Special VHDL Problem

- Poorly written code
 - Endless structural VHDL
 - Endless spaghetti VHDL
- Writing good code is difficult
- Understanding design by reading code extremely difficult
- Documentation and comments crucial

Problem: Management Interference

- “We don’t have time to do worst case analysis, we have hardware to build” (actual quote from a manager)
- Management is often more concerned with budget and schedule than design quality
- Design reviewers are often seen to be a hindrance rather than an asset

Problem: Over-Reliance on Reviewer

- Design organizations may attempt to push off analysis tasks to reviewer
 - Only reasonable if the reviewer is brought in explicitly to do the analysis
 - Designers should be responsible for analyzing their own designs
 - Reviewer should have wider view
 - Customer representatives work for customer
- Design organizations should nourish in-house analysis capabilities

Problem: Lack of Contractual Awareness

- Very common that neither reviewer nor design organization understands what is contractually required and permitted
 - Deliverables
 - Analysis requirements
 - Access to work in progress
- Paper: “Contractual Issues in Technical Monitoring”, R. Barto, MAPLD 2001
(www.klabs.org)

Problem: Lack of Analysis Standards

- Worst case analysis is not a highly developed concept in most design orgs
- Formal analysis requirements rarely exist
- For reviews to be effective, analysis standards must be agreed upon

When Does Review Start?

- Ideally, when the design starts
 - Set analysis standards
 - Set documentation standards
 - Reviewer maintains contact with designers and adds to the design process
 - PDR, CDR, FDR are formalities: the real work has already been done.
- Rarely happens

Most Common Design Path

- Design started at contractor under IRAD
 - Not treated as flight project
 - No analysis performed
 - Limited documentation
- Design touted in proposal as completed system
- Original designers leave company
- Contractor builds flight boards
- Problem found in test
- Analysis and review task started

General Rules of Design Review

- The amount of work the reviewer has to do is inversely proportional to the amount of work the designer does in making the design reviewable.
- The later in the process the review starts,
 - The harder the reviewer has to work to make a complete review
 - The more likely that errors will be designed into the system

The Best Case

- Review starts with design
 - Detailed documentation maintained
 - Analysis performed along with design
 - Reviewer in contact with designers
- Reviewer's task:
 - Monitor design in progress
 - Perform selected analyses, review others
- High probability of mission success

The Worst Case

- Review started late in design cycle
 - Limited documentation
 - Little or no analysis
 - Limited contact with designers
- Reviewer's task:
 - Lots of reverse engineering
 - Problems found in analysis require redesign
 - Management reluctant to redesign or continue review
- High probability of mission failure

Quick Design Assessment: The Finger Test

- Scan through drawings, find some circuit that looks hard to analyze, point to it, and ask, “Show me in the analysis where you analyzed this circuit”
- Do this 10 or so times
- Give the analysis a grade:
Number of times the circuit was analyzed
Number of circuits you ask about

Tools for Analysis: Simulation

(My own opinions, based on experience)

- Not as useful as one might think
 - Might be difficult to figure out simulation vectors
 - Asking designer for vectors is essentially relying on the designer to verify design
 - Output can be difficult to interpret
- Most useful for well partitioned design
 - Investigating behavior of portion of design
 - Verifying design modules

Tools: computer programs

- Extremely useful
 - Modeling complex systems
 - Performing analyses over wide ranges of parameters
 - Automating analysis tasks
- Even a simple program can provide insight

Most Important Tool:

- Your thought and logical reasoning
- There is no algorithm for design review
- Based on the type of work you have to do (simple review or reverse engineering),
 - Partition the design into simple blocks
 - Start with what you understand and move out
 - Ask all the questions you need to
 - Model and simulate as necessary

What VHDL Adds to the Review Process

- Probably, an awful lot more work!!
- VHDL has serious problems:
 - It hides design details
 - It is not WYSIWYG: What you see (as your design concept in VHDL) may not be what you get (as an output of the synthesizer)
 - Coupled with FPGAs, it encourages bad design practices

VHDL Hides Design Details

- Connectivity hard to follow in VHDL files
 - Especially true for translations from schematics
- Signal flows through sequential circuits can be hard to follow through processes
- Interactions between logical blocks can be difficult to understand
- Spelling errors undetected circuit errors

VHDL is not WYSIWYG

- Signals intended to be combinational can end up being sequential, and vice versa
- Sequential circuits can have unexpected, undesirable SEU behavior
 - Paper: “Logic Design Pathology and Space Flight Electronics”, R. Katz, R. Barto, K. Erickson, MAPLD 2000
- The designer gives up some control over the design to unvalidated software

VHDL and Bad Design Practices

- VHDL and FPGAs combine to allow designers to treat design as software
 - Especially for Xilinx FPGAs, for which there is no reprogramming penalty
- Rather than designing by analysis, designers simply “try” design concepts

Combined Effects of VHDL

Hidden design details

+ Non-WYSIWYG nature

+ Bad design practices

⇒ Designer can lose control of design

i.e., the designer loses understanding of what is in the design, then adds erroneous circuitry until simulation looks right

Worst Case Result

- A design that works in simulation for expected conditions, but with flaws that show up in unusual conditions
 - Passed on with little documentation by engineers who become unavailable
- ⇒ **A total programmatic disaster!!**
An extremely common occurrence!

Solution to VHDL Problem

- Detailed design review
- Make sure designs are transferable
- Don't use VHDL
 - Still have synthesizer problems
 - Can lose control of design with schematics (but it's harder)

Elements of Analysis

1. Part Parameters and Deratings

- Data book part parameters may not match the part's operating environment.
- Derate for
 - Temperature
 - Age
 - Voltage
 - Radiation
 - Excess load capacitance

2. Timing analysis

- Analyze, for each clocked device:
 - t_{SU} and t_H for all clocked inputs
 - t_{PW} of clocks, asynchronous set, clear, and load inputs
 - Set and clear recovery time
 - Show all clock inputs and asynchronous inputs are free from both static (010 or 101) and dynamic (001011 or 110100) hazards.

Other Timing Analysis Items

- Parallel clocking
- Clock skew
- Timing of analog circuitry
- Minimum propagation delays
- Calculation of pulse shortening
- Transition times in delay calculations

3. Gate Output Loading

- Show that no gate output drive capacities have been exceeded
- High output drive currents may:
 - Affect output voltage levels and propagation delays
 - Cause thermal problems resulting in part damage

4. Interface Margins

- All gates must have their input logic level thresholds met.
 - Different part families
 - Digital and analog part interfaces
- Decreased interface margins
 - Increase noise susceptibility
 - Can affect the operation of some parts
 - Increase I_{CC} of CMOS parts

Other Input Considerations

- Many parts have maximum input transition times
- Analyze input requirements of analog circuits
- Driving mixtures of TTL and CMOS

5. State Machines

- Analyze state machines for
 - Unused states and lock-up
 - Simultaneous assertion of flip-flop sets and clears
 - Reset conditions and homing sequences
- Be careful with asynchronous state machines

6. Asynchronous Interfaces

- I.e., where the set-up and hold times of incoming signals at receiving flip-flops cannot be guaranteed.
- Synchronize asynchronous inputs
- Don't use synchronizers to solve timing problems

7. Resets

- POR assertion and release voltages
- Reset t_{PW} must consider
 - Longest reset t_{PW} specified for parts
 - Power supply ramp rate
 - Oscillator start-up time
- Reset should be synchronized
- No unintended execution of external Commands on power-up

8. Part Safety Conditions

- Protection of ESD sensitive parts
- Input voltage levels
- Tri-state output overlap
- Floating inputs
- Use of internal IC protection diodes
- Absolute maximum ratings!

9. Cross-Strap Signals

- Must provide fault isolation
 - No powering of modules via cross-strap circuitry
 - Failure of one box does not cause failure of another
 - Sharing of cross-strap gates

10. Circuit Interconnections

- Signal integrity
 - Termination of high edge-rate signals
 - Drivers and receivers for off-board signals
- Noise considerations
 - Off-board connections of edge-sensitive inputs
 - Edge rates of harness signals
 - Harness noise threat model
 - Noise susceptibility analysis of input circuitry

11. Bypass Capacitance Analysis

- On-board bulk and bypass capacitance
 - Power supply line inductance
 - Circuit operating frequency
 - Component current requirements
 - Vendor recommendations
- Capacitor frequency response
- Capacitor placement

12. Special Pins

- Know what each pin on every device does and make sure it is properly used
 - Mode pin on FPGAs
 - JTAG pins
 - No-connect pins