Relative Merits and Demerits of High Speed Digital Test Approaches
Every year

Digital designs run faster, and the number of protocols and technologies increase

These factors increase the difficulty of testing designs
There are many tools available for testing high speed digital systems

- Oscilloscopes
- Logic Analyzers
- BERT Testers
- Protocol Analyzers
- Dedicated Protocol Testers
- Switch and Router Testers
- Error Injectors
Each Test Technology has Strengths and Weaknesses
Oscilloscopes: Strengths and Weaknesses

**Strengths:**
- Eye Diagrams
- Jitter Analysis
- TDR
- High resolution (100GS/sec)

**Weaknesses:**
- Low Channel Count
- Poor Protocol Awareness (and therefore poor triggering)
- Can cost $100k (and up to $1M)
- Considerable Effort to Integrate
Logic Analyzers: Strengths and Weaknesses

**Strengths:**
- High Channel Count
- Good visibility at IO and peripheral circuitry
- High Resolution Timing Analysis (50GS/sec)

**Weaknesses:**
- State Mode is very slow (2.8GHz Clock)
- Poor Protocol Awareness
- Usually no Traffic Generation or a separate traffic generator
- Traffic Generator is loosely correlated and not protocol aware
- Weak for Fiber Optic Signals
- Weak for High Channel Count IO
BERT Testers: Strengths and Weaknesses

Two Types: BERT, or BERT with Jitter & Eye

Strengths:

- Generally Easy to use
- May be able to do Jitter and Eye Diagrams

Weaknesses:

- Doesn’t Do anything else
- May be very expensive ($250k for Jitter & Eye)
- Requires a separate instrument
- Considerable Integration Effort
Protocol Analyzers: 
*Strengths and Weaknesses*

**Strengths:**
- Can be inexpensive (WireShark is free)
- Can support many protocols (Wireshark >900)

**Weaknesses: Usually optimized for IT users**
- Only as good as the acquisition hardware
- May not run wire speed
- May only act as end device without TAPs
- A Mirror Port often drops and filters traffic
- Typically only a few ports
- May only support one technology (Ethernet)
- May not have pre-capture filtering
- Usually can’t send traffic
Dedicated Protocol Testers: *Strengths and Weaknesses*

**Strengths:**
- Usually optimized for one protocol

**Weaknesses:**
- Can be very expensive
- If you need another protocol – buy another analyzer
Switch and Router Testers

**Strengths:**

- Optimized for System test of Switches and Routers
- High Channel Count (and high traffic volume)
- Pre-Developed Applications for testing switches and routers
- Optimized for testing layers 2 through 3 with moderate layer 7 capability
Switch and Router Testers

Weaknesses:

- Not optimized for testing hardware
- Doesn’t interface for testing chip to chip links
- Doesn’t test backplanes
- Limited to switch, and router protocols (and perhaps telephony)
- Poor diagnostic capability
- Poor pre-capture filtering
- Poor triggering
- Limited capture buffers and analysis capability
Dynamic Protocol / Task Reconfiguration
A new type of Testing Technology

- Based on blank FPGA cards
- Choose the Function and Protocol
- Each Port-Pair can have a Different image
- Can be quickly changed from one technology to another
Dynamic Protocol Reconfiguration

• Allows you to reuse the test hardware for new projects
• Theoretically supports any 8B/10B encoded protocol
• Theoretically supports any 64B/66B encoded protocol
• Allows you to test mixed protocol systems
• Allows you to test and correlate, chip-to-chip links, backplane traffic, and IO
• Goes beyond router testing to other devices such as avionics, cyber security and video
Dynamic Protocol Reconfiguration
Currently Supports:

<table>
<thead>
<tr>
<th>Fibre Channel</th>
<th>Ethernet</th>
<th>AFDX</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCoE</td>
<td>iSCSI</td>
<td>SAS</td>
</tr>
<tr>
<td>SATA</td>
<td>Serial FPDP</td>
<td>SerialRapid IO</td>
</tr>
<tr>
<td>CPRI</td>
<td>OBSAI</td>
<td>PCIe</td>
</tr>
<tr>
<td>InfiniBand</td>
<td>Multi-Protocol</td>
<td>Custom Protocol</td>
</tr>
</tbody>
</table>
Protocol Database Editor

“See your data, your way”
Load Custom Protocols with Configuration

Protocols Available to all Tools

- Database
- Analyzer
- Traffic Generator
- Protocol Creator & Editor
- Frame Builder
- Impairment Tester
- Error Injector
- Trace Viewer

All Tools Time Correlated
Advanced Triggering

- Multi Port
- Multi Protocol
- Cross Trigger Scope
- Cross Trigger LA
- Makes them Smarter
A Methodology for “Bringing up a High Speed Digital Board”

- Data Integrity Testing
- Layer 2 Testing
- Conformance Testing
- Stress Testing
- QoS Testing
- Flow Control / Buffer Testing
- Interoperability Testing
- Negative Testing
In order to assure interoperability we write standards and specifications

- But, how do we know that our devices comply with these standards?
- How do we know that the standard is comprehensive and foresees all of the problems that can occur?
- Even if we comply with the standards will our product work and will it interoperate with designs from other companies?
Data Integrity Testing

- Test data paths within the device under test
- Loopback at various points in the design
- Ensures data paths can meet BER requirements of the protocol
Layer 2 Testing

- Send Framed Commands to Device
- Check data framing, CRC, link initialization
- Check code processes data correctly $f(x)$
- Check code responds correctly
Conformance Testing

- Send Valid Commands to Device and Check Responses
- Send Invalid Commands to Device and Check Responses
- Validate Time Critical Parameters
- Check Protocol Stacks and Response Times
- Check Auto-negotiation of link parameters
Stress Testing

- Send max frames per second and check operation
- Send max throughput and check operation
- Check device capacities (e.g. number of concurrent operations)
- Check operation with error conditions
- Check effect of latency on operation
QOS Testing

- Send frames to ports 1, 2 and 3 all directed to port 4
- Adjust traffic to overload port 4 transmitter
- Vary priority on frames sent to ports 1, 2 and 3
- Check all priority frames are retransmitted on port 4 using protocol analyzer
Flow Control/Buffer Testing

- Send Line Rate Traffic to Ports 1 and 2 directed to port 3
- Check port 3 runs at line rate.
- Check ports 1 and 2 are throttled back through flow control
- Check total frames on ports 1 and 2 equal port 3 (no dropped frames)
Interoperability Testing

- Check operation with real devices
- Check latency on overall system behavior
- Check system recovery in presence of errors
- Measure system performance
Are we done?
A Case for Negative Testing

In the real world a million things can go wrong

- It's a good idea to try many of these adverse scenarios
- It's better that you find the problem before the plane crashes
- The earlier you find the problem the less costly the solution
- Scopes, Logic Analyzers, and Protocol Analyzers typically don't have errored traffic capability
- Router Testers may have some capability
Types of Negative Traffic Testing

- **Common:**
  - Oversize frames, Undersize frames, and Bad CRC's

- **Better:**
  - Drop specific Frames (ARP Replies, SYN)
  - Corrupt specific bits (IP checksum)
  - Generate $10^n$ bit errors
  - Send Invalid Commands
  - Send Undefined Commands
  - Insert Delay
  - DO THE UNTHINKABLE
Glen Broderick
Director for US Mil-Aero Sales
Glen.Broderick@AbsoluteAnalysis.com
805-208-1381
You are invited to link to me on LinkedIn