

Scopes Deliver Advanced JTAG Debug Capabilities

Joel Woodward, Agilent Technologies, Inc.

JTAG, also known as IEEE 1149.1, is one of the most successful electronic standards of all time. Invented over 20 years ago to uncover printed circuit board manufacturing, JTAG is now used in nearly 100% of printed circuit boards and has become a critical part of many integrated circuits. Processors, FPGAs, and other sophisticated chips often include a JTAG TAP (test access port) controller for accessing sub-blocks for configuration, communication, and debug.

In short, JTAG scan chains are a critical piece of nearly every electronic design. JTAG has become a critical technology for not only manufacturing testing, but also for development teams. What happens when the JTAG scan chain isn't functioning properly? New tools enable advanced JTAG scan chain debug at both the physical and protocol layers.

The Need for JTAG Protocol Decode

Design teams working on system-level products assume the JTAG chain is functional. If the scan chain doesn't work properly, a common debug methodology is to reach for an oscilloscope to assess physical layer characteristics. What does TCK look like? Are there loading problems? Does the scan chain have a timing problem? While this approach helps determine if there are physical layer problems, there isn't an equivalent method of viewing JTAG at the protocol level.

A number of teams need access to rapid JTAG decode. For example, a design team may be reading and writing to ASIC register via JTAG, not because JTAG is a good vehicle for this, but because JTAG is the only available connection to a specific connection. A company developing Ethernet or USB to JTAG programming cables may need to verify that the translation was done correctly. A medical device or military application may require the team to access subsystems via JTAG and decode the information on the JTAG bus. An IC vendor may need to resolve an issue with a third-party tool vendor that interacts with the silicon via JTAG. These are a few examples of teams who need JTAG protocol decode, in real time, using non-intrusive tools. They are trying to solve issues that may have roots at the protocol layer or the physical layer on JTAG scan chains that have a wide variety of potential variations.

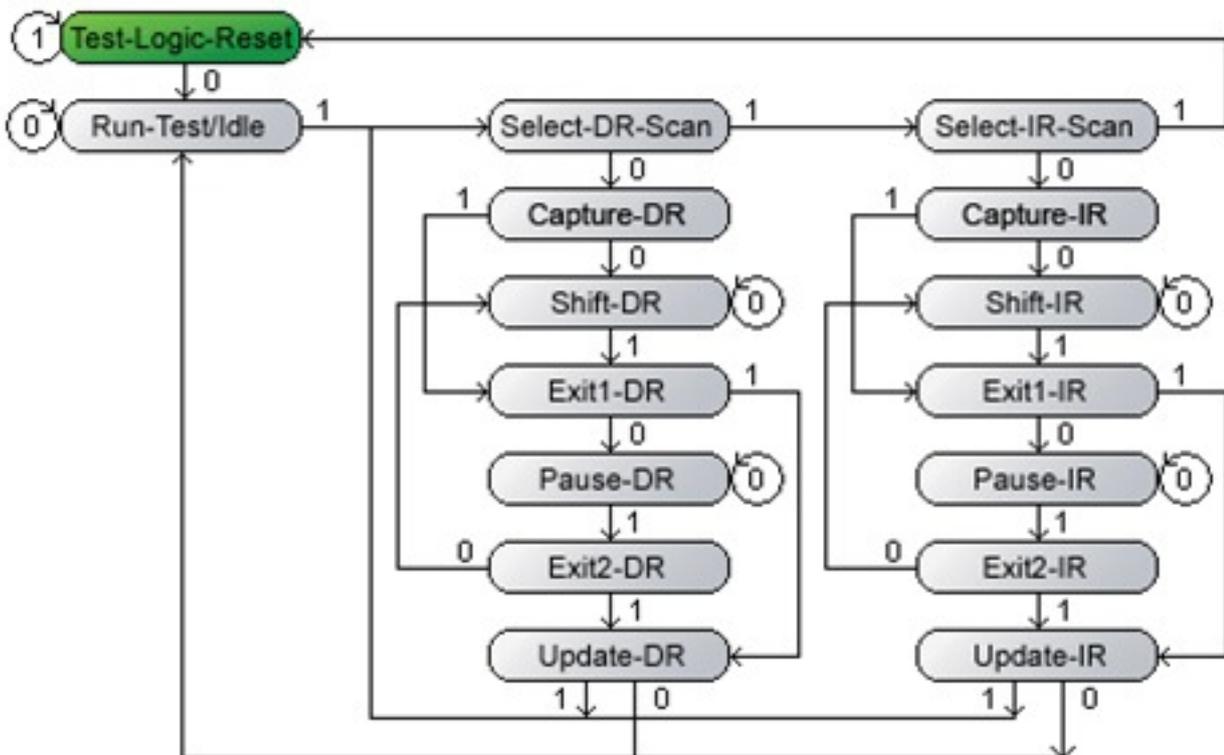
While most development teams don't need to frequently decode JTAG scan chains, when the need arises, the task is extremely complex, error prone, and requires significant time. Experienced engineers know the challenges and difficulty of decoding JTAG traffic, which can take weeks of full time attention given the complexity associated with decoding JTAG protocol. The process typically starts with acquiring waveforms from all four JTAG signals on a logic analyzer or scope and then trying to manually decipher this cryptic information. Decoding JTAG has several challenges. To gain a better understanding of the complexity, here is a brief description of a JTAG scan chain.

Scopes Deliver Advanced JTAG Debug Capabilities

Published on Electronic Component News (<http://www.ecnmag.com>)

For several years oscilloscopes have provided serial protocol decode for standard buses. These applications are typically sold and licenses on a protocol basis. For example, a development team could choose to add licenses for I2C and PCIe protocol decode application to their oscilloscope, to extend the instrument's measurement capabilities. For oscilloscope vendors, the task of developing applications to decode protocol on buses like I2C, SPI, and RS-232 while not trivial, is much easier than decoding JTAG. Most serial buses enable acquisitions that can be decoded forward-backward, backward-forward, or allow any portion of the acquisition to be decoded independent from the rest of the acquisition. JTAG is more complex.

While considered a serial bus due to its boundary scan nature, JTAG includes four primary signals: TCK, TMS, TDO, TDI, and an optional fifth signal, TRST. The JTAG TAP (test access port) contains sixteen different states, each determined by the previous state and the current TMS signal transition. Hand-decoding JTAG signals captured on a traditional logic analyzer or oscilloscope requires the user to start decoding when the TAP controller is in reset or idle, and then start working through each successive state. Signals on JTAG scan chains cannot be acquired and decoded from arbitrary starting points. The decode only makes sense when done by following the TMS signal as it determines the state of the JTAG TAP controller.



The TAP controller complexity is just one issue that makes JTAG protocol difficult. The second issue that makes JTAG decode difficult is that the JTAG scan chain can include an arbitrary number of devices. The devices can be in any arbitrary order, and each device can have its own unique opcodes. Without additional knowledge of the specific devices on the chain, the order of the devices, and the opcodes for each device, JTAG decode is impossible. For example, the scan chain contents may tell

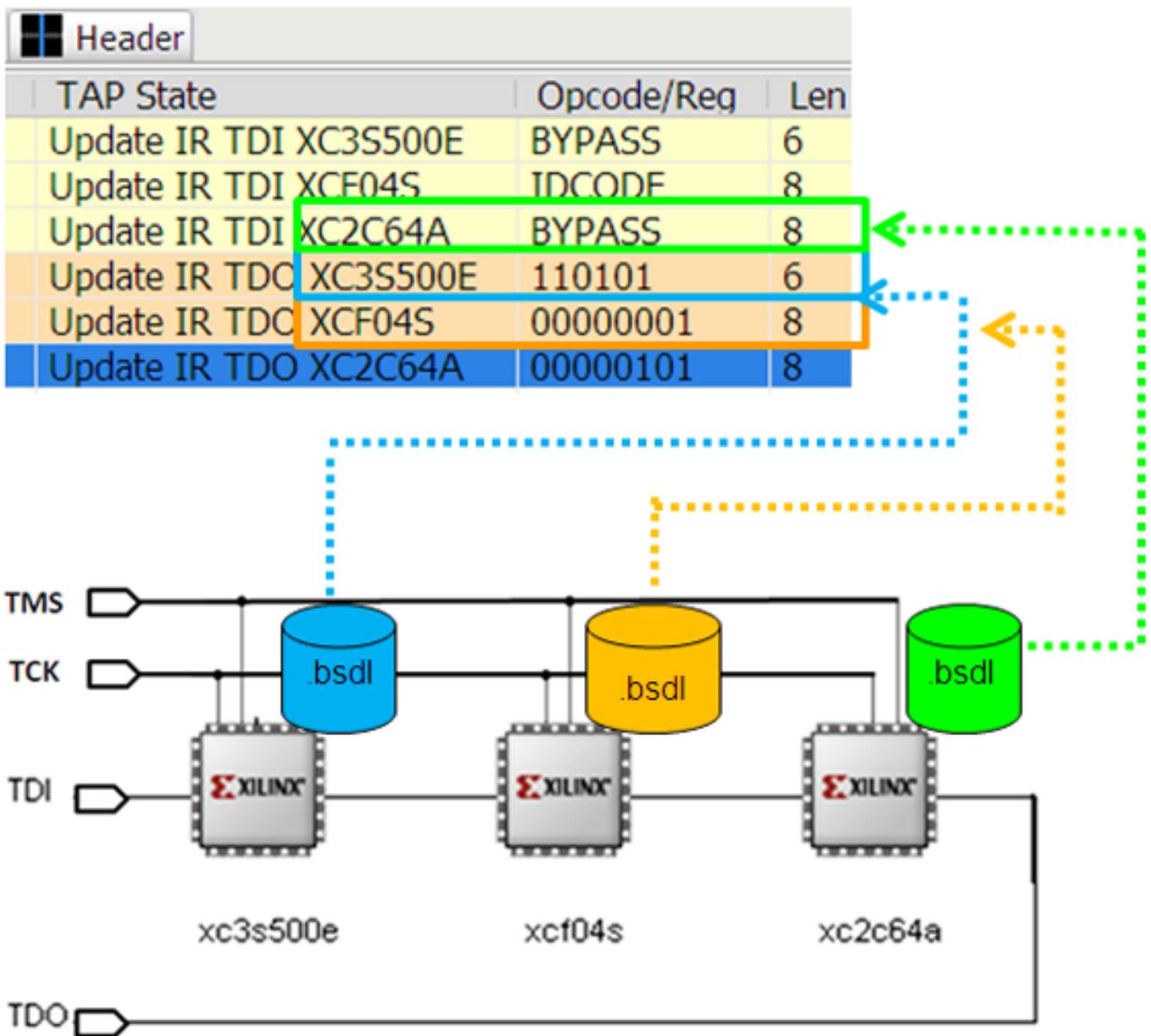
the 3rd device, in a chain of 12 devices, to execute a test and return the results of the test via the scan chain. The scan chain includes instruction register and data register values that are specific for a unique device. Each device has its own set of instruction opcodes each with a length that is specific to the device. For users to attempt to manually decode JTAG they must keep track of the TAP controller, and apply a myriad of information about device-specific information and order of devices on the scan chain. The task is overwhelming, can be very frustrating, and impossible to do in real time. Sometimes teams resort to building temporary JTAG tools that automate the decode for a specific scan chain. This requires unplanned time, and forces the team to become experts in an area in which they don't need to become experts.

Scope-based JTAG Decode

As previously discussed, the nature of JTAG requires oscilloscope vendors to be more innovative than with any other protocol decode. Part of this innovation is the ability to read in a BSDL file. BSDL files were incorporated into the IEEE standard and are a VHDL subset. BSDL files are available from silicon vendors and each BSDL file describes one version of an IC. Included in each BSDL file are the registers and public opcodes used in a JTAG-compliant IC. Private instructions may exist confidentially within an IC vendor, but are not described in the BSDL file. Included in the BSDL file is one instruction register, a minimum of a 1-bit bypass register, one boundary scan register and optionally a 32 bit device ID register. The registers other than the instruction register are called data registers.

Scopes Deliver Advanced JTAG Debug Capabilities

Published on Electronic Component News (<http://www.ecnmag.com>)

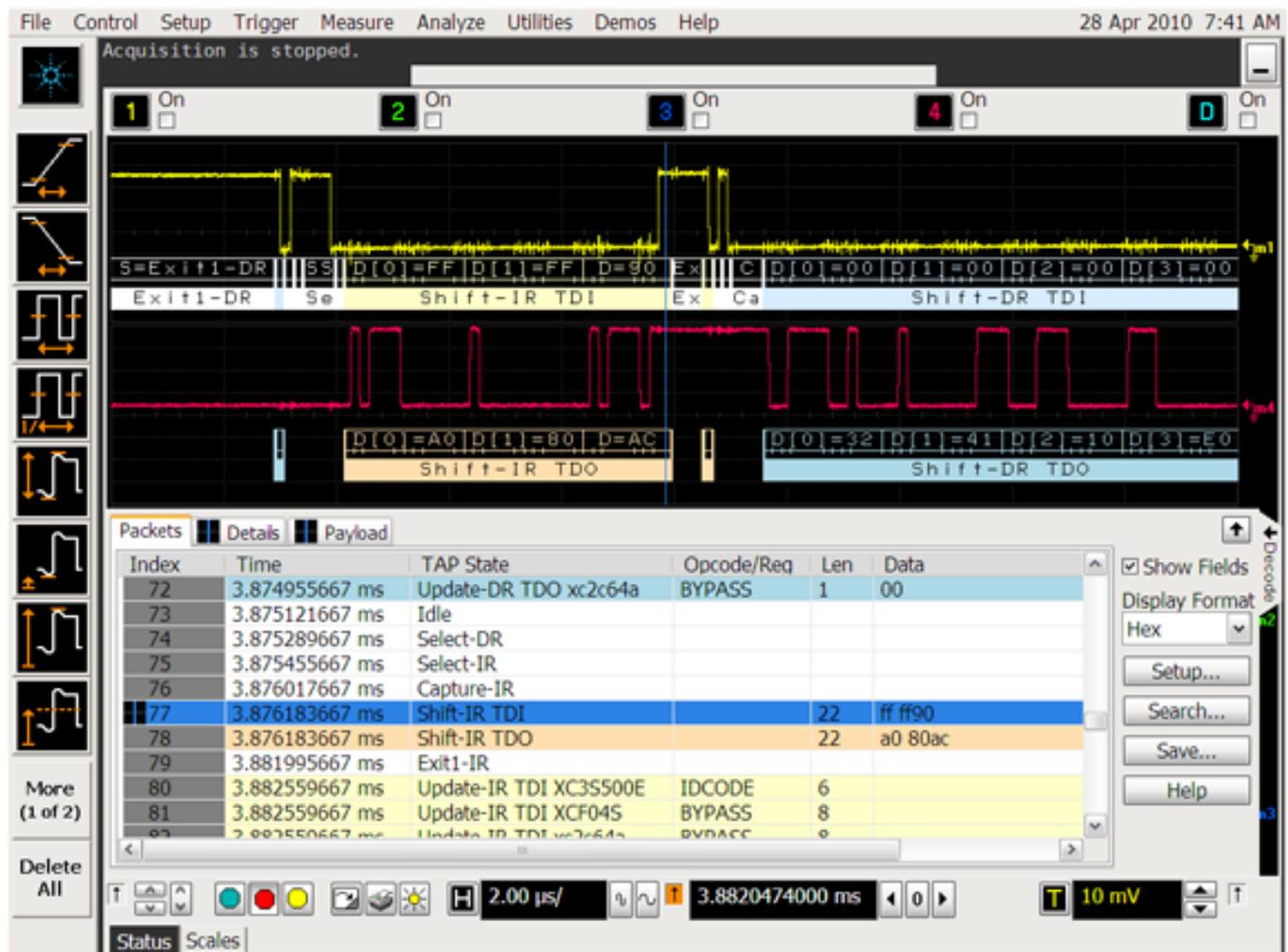


In order for an oscilloscope to provide meaningful JTAG decode, it must be able to import BSDL files for each device on the scan chain. If a BSDL isn't available for a specific device, the device must be set to BYPASS mode and the instruction length specified.

The BSDL file includes public instructions mnemonics associated with specific binary values. Instructions that are not included in the BSDL file are called private instructions. If private instructions are known by user, these can be added to the BSDL file using a text editor giving the oscilloscope JTAG decode the ability to display both private and public instructions. Importing and using BSDL file information enables the scope-based protocol to more effectively provide useful decode information to the user. For example, the protocol decode will include device names, which is extremely valuable in understanding JTAG on chains that have multiple devices.

Scopes Deliver Advanced JTAG Debug Capabilities

Published on Electronic Component News (<http://www.ecnmag.com>)



Oscilloscopes can also provide additional error detection based on information in the BSDL file and knowledge of the scan chain. For example, the oscilloscope can display a packet error, A bad Shift-DR TDO length if the number of bits shifted does not correspond to the expected register length for the IR Opcodes given, or display a "bad shift-DR TDO length" error if the actual IDCODE shifted in does not match the IDCODE in the BSDL file.

While many designers are looking for easier ways to decode JTAG protocol, the oscilloscope-based solution provides an excellent start and utilizes a tool that most engineers need for other purposes. JTAG protocol decode application software enables the oscilloscope to be used across a wide variety of scan chains, in real time, across both physical to protocol layers, and enables JTAG activity to be shown time correlated with other system events.

Source URL (retrieved on 12/18/2014 - 3:04am):

<http://www.ecnmag.com/articles/2010/07/scopes-deliver-advanced-jtag-debug-capabilities>