Introduction to JTAG

A consortium of companies called the Joint Test Access Group came together to define a standard for boundary-scan testing of ICs and boards.

One disadvantage of shrinking technology is that the testing of small devices gets exponentially more complex. When circuit boards were large, we tested them with techniques such as bed-of-nails, which employed small spring-loaded test probes to make connections with solder pads on the bottom of the board. Such test fixtures were custom made, expensive, and inefficient, and much of the testing could not be performed until the design was complete.

As board dimensions got smaller and surface-mount packaging technology improved, if devices were mounted on both sides of a circuit board, no attachment points were left for the test equipment.

Boundary scan

To find a solution to these problems, a group of European electronics companies formed a consortium in 1985 called the Joint Test Action Group (JTAG). The consortium devised a specification for performing boundary-scan hardware testing at the IC level. In 1990, that specification resulted in IEEE 1149.1, a standard that established the details of access to any chip with a so-called **JTAG port**.

The specification JTAG devised uses **boundary-scan technology.**

Advantages of boundary-scan technology:

1. Enables engineers to perform extensive debugging and diagnostics on a system through a small number of dedicated test pins.
2. Signals are scanned into and out of the I/O cells of a device serially to control its inputs and test the outputs under various conditions.
3. The primary advantage of boundary-scan technology is the ability to observe data at the device inputs and control the data at the outputs independent of the application logic.
4. Another benefit is the ability to reduce the number of overall test points required for device access. With boundary scan there are no physical test points. This can help lower board fabrication costs and increase package density.
5. Boundary scan provides a better set of diagnostics than other test techniques. The boundary-scan cells observe device responses by monitoring the input pins of the device. This enables easy isolation of various classes of test failures, such as a pin not making contact with the circuit board.
6. Boundary scan can be used for functional testing and debugging at various levels, from internal IC tests to board-level tests. The technology is even useful for hardware/software integration testing.

Today, boundary-scan technology is probably the most popular and widely used design-for-test technique in the industry.

Test pins

Devices communicate to the world via a set of I/O pins. Devices that support boundary scan contain a shift-register cell for each signal pin of the device. These registers are connected in a dedicated path around the device's boundary. The path creates a virtual access capability that circumvents the normal inputs and provides direct control of the device and detailed visibility at its outputs.

During testing, I/O signals enter and leave the chip through the boundary-scan cells. The boundary-scan cells can be configured to support external testing for

interconnection between chips or internal testing for logic within the chip.

To provide the boundary scan capability, IC vendors add additional logic to each of their devices, including scan registers for each of the signal pins, a dedicated scan path connecting these registers, four or five additional pins, and control circuitry. The overhead for this additional logic is minimal and generally well worth the price to have efficient testing at the board level.

With the proper wiring, you can test multiple ICs or boards simultaneously. An external file, known as a Boundary-Scan Description Language (BSDL) file, defines the capabilities of any single device's boundary-scan logic.

Boundary-scan technology is also used for **emulation**. The emulator front-end acts as the scan manager by controlling the delivery of scan information to and from the target and the debugger window. (Of course, when a host controls the JTAG scan information, it needs to know if other devices are connected in the scan chain.)

JTAG also allows the internal components of the device (the CPU, for example) to be scanned. This means you can use JTAG to debug embedded devices by allowing access to any part of the device that is accessible via the CPU, and still test at full speed. This has since become a standard emulation debug method used by silicon vendors. JTAG can also provide system level debug capability. Having extra pins on a device provides additional system integration capabilities for benchmarking, profiling, and system level breakpoints.