Периферийное сканирование и качество устанавливаемых компонентов

Алексей Иванов, *alexey@jtag.com*

Сегодня практически любой отечественный производитель электроники подтвердит, что ему приходилось сталкиваться с контрафактной элементной базой. Подделывают как пассивные компоненты, так и активные вплоть до сложных интегральных схем. Другая насущная проблема — это то, что даже при трудоемком и не всегда эффективном входном контроле остается опасность повреждения или изменения параметров компонентов при пайке во время эксплуатации.

Мы решили взглянуть на данную проблему с точки зрения технологии периферийного сканирования JTAG. Сразу оговоримся, что в данной статье не будет предложено панацеи от контрафакта или тотальной проверки функциональности активных компонентов после пайки. Впрочем, ни один метод электроконтроля плат не создавался для выявления контрафакта и некачественной компонентной базы, в т.ч. метод периферийного сканирования по стандарту IEEE 1149.1, который был изначально разработан для производственного тестирования межсоединений на цифровых платах.

Тем не менее, в последнее время наблюдается тенденция использования тестового оборудования, предназначенного для контроля собранных печатных плат, с целью выявления признаков некачественной элементной базы. Мы постараемся выделить основные свойства и возможности JTAG-теста, которые могут помочь в борьбе с такими явлениями. В основном, речь пойдет о тестах, проводимых на платах с установленными компонентами, поэтому отсева некачественных компонентов до монтажа периферийное сканирование тоже не обеспечит, конечно, если не тестировать компоненты в составе специальной оснастки. Но проблема настолько актуальна на сегодняшний день, что любое подспорье будет полезно, тем более если было выбрано периферийное сканирование для теста, локализации дефектов монтажа и программирования устройств на выпускаемых изделиях.

Первый вид теста, который может оказаться полезным, — это тест инфраструктуры JTAG-цепочек изделия. На рисунке 1 показан результат с данными, полученными при проведении этой проверки. Во время теста инфраструктуры проверяется не только целостность цепей JTAG-сигналов (TDI, TDO, TMS, TCK и TRST), но и архитектура периферийного сканирования компонентов в JTAG-цепочках. В эту архитектуру, помимо всего прочего, входят регистр команд (Instruction Register) и, опционально, но в подавляющем большинстве случаев, регистр идентификационного номера (Identification Register). IDENT-тест как часть теста инфраструктуры, к примеру, считывает идентификационный код микросхемы с поддержкой периферийного сканирования. Этот 32-битный номер содержит в себе название производителя микросхемы, ее обозначение и версию. Конечно, содержимое данного регистра не является железной защитой от подделок, однако представим себе следующую ситуацию, когда под видом одной версии процессора выдается другая, более дешевая или забракованная, запрещенная к продаже. Для этого достаточно произвести перемаркировку на корпусе. Последствия использования такого компонента могут быть разными: от легких, в виде нарушения функциональности при определенных режимах, до серьезных, например, невозможности запрограммировать внутреннюю память EEPROM при производстве и настройке из-за ее неправильного размера. Практика показывает, что часто для такого вида поддельных компонентов ID-код остается прежним, что и понятно, ведь в процессе подделки максимальное, на что способен злоумышленник — это перемаркировка или корпусирование, а кристалл, как можно догадаться, остается неизменным. Для сложных цифровых ИС, например ПЛИС или процессоров, такой вид контрафакта характерен и представляет собой подавляющее число прецедентов.

Приведем случай с одним предприятием, выпускающим электрон-

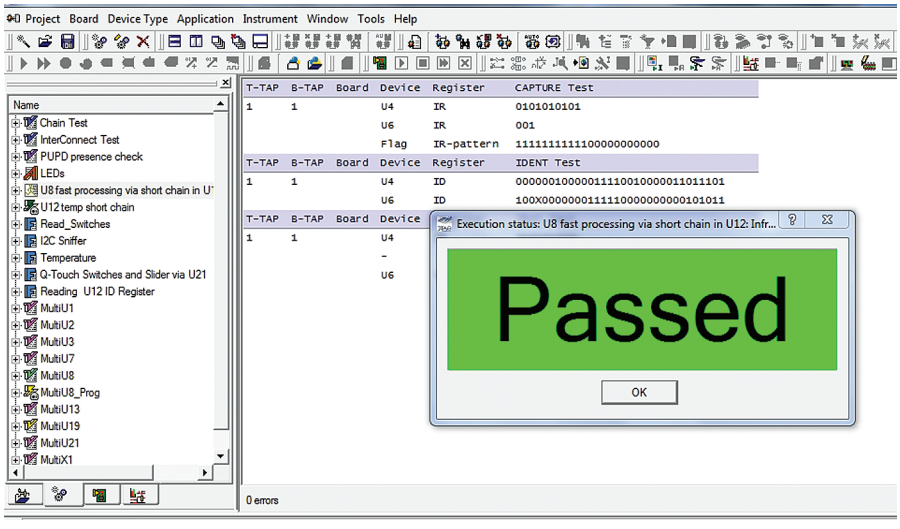

Рис. 1. **Результаты проведения теста инфраструктуры компонентов с поддержкой стандарта IEEE 1149.1** (периферийного сканирования)

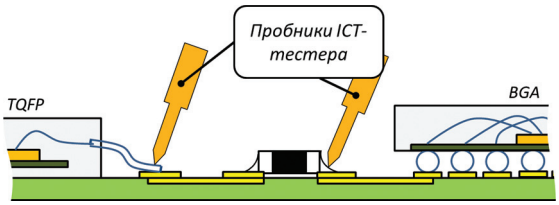

Рис. 2. **Пробники внутрисхемного тестера** (ICT) **проверяют только наличие соединения на ПП**

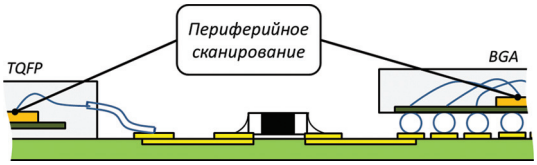

Рис. 3. **Ячейки периферийного сканирования располагаются на кристаллах микросхем, включая в тест соединения в корпусе ИС**

ные цифровые модули. Была закуплена партия процессоров известной марки (впоследствии оказавшихся поддельными). При этом кристалл, который скрывался под корпусом, не соответствовал заявленной версии и при тесте инфраструктуры считанный ID-код отличался одним битом от ожидавшегося. Дальнейшие проверки показали, что параметры закупленных компонентов соответствовали версии, отличной от заявленной на коробке, и партия была забракована.

В другом наглядном примере при тесте инфраструктуры JTAG-каналов вообще отсутствовал регистр идентификационного номера, хотя в спецификации на микросхему он значился. Дело в том, что ID-регистр не является обязательным по стандарту IEEE 1149.1 и, возможно, исследуемая партия компонентов представляла собой неофициальную «сырую» версию, а в окончательной, коммерчески-доступной версии все необходимые регистры должны быть реализованы.

Кроме того, при тестировании инфраструктуры также проверяется регистр периферийного сканирования и его длина. Это тоже может служить подспорьем в проверке, показывающей, какие на самом деле версии компонентов установлены на плате, т.к. длина данного регистра может отличаться в разных версиях.

Следует заметить, что тест инфраструктуры полезен не только для локализации поддельных компонентов, но и для изделий, в которых используются разные версии компонентов в одинаковых типах корпусов. Не такая уж и редкость, когда операторы-установщики их путают. То есть IDENT-тест в этом случае используется для определения ошибок монтажа, тем более что изначально тест инфраструктуры был введен для электроконтроля цепей JTAG-каналов и локализации в них дефектов.

Все дальнейшие проверки, следующие за тестом инфраструктуры, связаны с тестированием внешних цепей и компонентов по отношению к самим микросхемам, поддерживающим периферийное сканирование. Периферийное сканирование выделяется среди других методов электроконтроля тем, что тестирование связей проводится фактически от кристалла до кристалла ИС. При этом проверяется не только проводник на плате, но и разварка внутри корпуса. Внутрисхемное тестирование (In-Circuit Test, ICT), например, при всех его достоинствах фактически обеспечивает «прозвонку» связи между пробниками. В зависимости от подготовленности изделия и типа тестера (адаптерный или с летающими щупами) пробники могут контактировать с контактными точками на плате или выводами компонентов (см. рис. 2). Таким образом, если при статическом повреждении или в результате перегрева в печи внутренние проволочные соединения от кристалла ИС до ее выводов повреждаются, внутрисхемный тест такие дефекты вряд ли обнаружит — это не в его компетенции. Следует заметить, что в арсенале внутрисхемного теста есть косвенный метод, который может использоваться для сигнализации такого рода дефектов, — это измерение узловых импедансов между выводами микросхемы. Однако для этого требуется статистика, снятая с исправных плат, а, кроме того, необходим физический доступ к цепям для их контакта с пробниками тестового адаптера или установки Flying Probe. Периферийное сканирование использует внутреннюю архитектуру, реализованную на уровне кристалла. Соответственно, проверка производится от кристалла до точки (если используется комбинация ICT-теста и JTAG) или от кристалла до кристалла, включая разварку (см. рис. 3).

Благодаря тестированию межкомпонентных связей, связей JTAG-микросхем с «кластерами» (такими как ОЗУ, ПЗУ, логика) проверяются как работа драйверов и сенсоров, так и путь сигнала от кристалла до вывода ИС. Что касается «кластеров», узлов без поддержки периферийного сканирования, то при тестировании используется их функциональная логика, поэтому снова проверяются связи внутри корпусов таких элементов. Практика проведения JTAG-теста межкомпонентных связей на нескольких предприятиях выявила дефекты в разварке, которые появились уже после монтажа и привели к отказу изделий.

Порой бывает сложно определить, в какой именно момент появился дефект: изначальный брак компонента, статическое повреждение при перемещении его со склада на производственную линию, перегрев при оплавлении в печи и т.д. Тем не менее, организовать проверку сложного компонента до его установки на плату все-таки можно, но для этого необходима оснастка. Она требуется не только для подачи сигналов JTAG-интерфейса на микросхему (это пять сигналов — TDI, TDO, TMS, TCK и TRST), но и для подключения каналов IO-модуля. Ведь в составе платы «приемниками» или «источниками» сигналов являются окружающие микросхемы, также поддерживающие периферийное сканирование, или логические кластеры, а если тестировать ИС в составе оснастки, IO-модуль станет заменителем данной «периферии». Конечно, для каждого проверяемого типа компонента требуется своя оснастка (зависящая от типа корпуса, количества выводов, шага), поэтому целесообразно проводить такой входной контроль для особо «ценных» ИС или компонентов,

часто оказывающихся некачественными.

Следует еще раз подчеркнуть, что метод периферийного сканирования основан на использовании регистра сканирования, который, хоть и использует драйверы и сенсоры самой ИС, но работает отдельно от внутреннего функционального ядра, поэтому рассматривать такую технику как средство верификации именно ядра процессора или блоков ПЛИС не следует. Да и вообще, вопрос этот довольно-таки сложный, т.к. получить полную тестовую спецификацию на ИС практически невозможно, даже если купить многомиллионное тестовое оборудование для микросхем.

Очевидно, JTAG-тест, как и метод измерения узловых импедансов для ICT-теста, — это все-таки косвенные проверки. Тем не менее, среди регистров JTAG, необходимых по стандарту IEEE 1149.1 для тестирования внешних связей или проверки ID-кода, производители процессоров и ПЛИС внедряют дополнительные, необходимые, например, для отладки. Эти регистры не являются стандартными и отличаются в зависимости от архитектуры ИС. Таким образом, в зависимости от типа ядра, помимо стандартных процедур периферийного сканирования, таких как тест инфраструктуры или межкомпонентных связей, для разных архитектур можно выполнить различные дополнительные проверки, связанные именно с «внутренностями» ядра. Можно, например, записать и считать внутреннюю память или состояние определенных контрольных регистров. Для этого может использоваться, в частности, ПО JTAG ProVision в комбинации с JTAG Live CoreCommander.

Эксплуатационные дефекты могут проявляться у компонентов, скажем, только при определенных критических температурах. Задача локализации дефекта в таких случаях сложна, т.к. неисправность проявляется в отказе целого изделия. Сам факт отказа не дает ответа на вопрос о типе и местоположении дефекта, а внутрисхемный тест в условиях камеры тепла/холода неприменим. При этом если протестировать изделие при комнатной температуре, неисправность может пропасть.

Среди причин, которые могут вызвать отказ изделия на пониженной или повышенной температуре, могут быть не только дефекты пайки или последствия нанесения влагозащитного покрытия на изделия. Контрафактные компоненты могут не соответствовать заявленному в спецификации температурному диапазону. В этом случае мы снова имеем дело с использованием более дешевых версий кристаллов «под маркой» более дорогих.

Периферийное сканирование — это метод, требующий для тестирования только один или несколько кабелей для подключения JTAG-интерфейса, поэтому данную технику электроконтроля очень удобно применять для диагностики дефектов, проявляющихся на критических температурах, т.к. кабель легко провести в камеру. Среди компонентов, у которых заявленный температурный диапазон не соответствует действительности, могут быть, например, микросхемы ОЗУ или ПЗУ. Такие компоненты довольно просто тестируются при помощи периферийного сканирования, а создание тестов, проверяющих связь JTAG-компонентов с ними, происходит автоматически. При этом, в отличие от внутрисхемного теста, тестируются не только линии связи с памятью (или логикой), но и используется их функциональность, т.е. проверяется еще и собственно компонент. Про отдельно устанавливаемые на плату флэш-ПЗУ следует отметить, что в их стандартный тест при помощи периферийного сканирования входит проверка ID-кода микросхемы, который можно считать по последовательной или параллельной шине данных автоматически. Этот записанный производителем ID-код хранится в определенном адресном пространстве и различается в зависимости от изготовителя, типа и объема ПЗУ.