Выявление поддельных ИС

Поддельные микросхемы стали огромной проблемой для производственных компаний, которые пытаются найти альтернативные источники поставок ИС. Но есть один инструмент, который в значительной степени упрощает процесс выявления подделок.

Алан Лаун (Alan Lowne)
Перевод Сергей Шихов

sergey@acont.ru

В статье речь пойдет о том:

- почему поддельные интегральные схемы представляют опасность;
- какие типы подделок существуют, и какие способы их выявления применяются;
- как защитить себя от поддельных деталей.

При сложившемся на рынке глобальном дефиците микросхем компании-изготовители отчаянно пытаются сохранить свои производственные линии, обеспечивающие потребителей электронными товарами и автомобилями. Одним из решений, которое выбирают многие компании, становится теневой рынок — несертифицированные поставщики устаревших компонентов, а также компонентов, долгое время пробывших на складе. Подобное решение позволяет обеспечить производство нужными микросхемами, но при этом возникает проблема, которую сложно обнаружить и устранить, — поддельные ИС.

Например, предприниматель из Массачусетса несколько лет назад был приговорен к 37 месяцам тюремного заключения за импорт тысяч поддельных интегральных схем из Китая и Гонконга, перепроданных подрядчикам ВМС США и установленных на атомных подводных лодках. Ему также удалось продать компоненты сотням другим независимым дистрибьюторам и брокерам в США и странах Европы, и таким образом поддельные ИС оказались в заказах правительственных подрядчиков и производителей коммерческих изделий.

Согласно маркировке, изготовителями поддельных микросхем являлись более 30 различных поставщиков. Этот пример и неизвестное количество аналогичных случаев явно подтверждают, что наличие контрафактных изделий в цепочке поставок становится серьезной проблемой.

ИС несложно подделать, в отличие от банкнот. Изготовление двойников, похожих на настоящие, не требует большого мастерства. Нужно просто найти более дешевые аналоги в таком же корпусе и нанести другую маркировку. Источником сложившейся ситуации стала высокая стоимость некоторых электронных изделий, и это делает уязвимой всю производственную цепочку от сборочного цеха до конечного пользователя. Невозможно подсчитать количество компаний, в распоряжении которых оказались партии поддельных устройств.

Подделка полупроводников принимает угрожающие масштабы и оказывает влияние на огромное количество электронных систем, используемых потребителями, предприятиями, а также объектами военно-промышленного комплекса. Обнаружение подделок приобретает все большую важность во всем мире как среди производителей электронных устройств, так и среди поставщиков различных компонентов.

По оценке Ассоциации полупроводниковой промышленности, использование поддельных электронных компонентов обошлось производителям более чем в $7,5 млрд. Мало того что компании несут убытки, испытывают неудобства и сдвигают сроки поставок, присутствие на рынке поддельных ИС наносит огромный ущерб репутации производителей оригинальной продукции.

Что же собой представляют поддельные компоненты?

Есть несколько способов изготовления поддельных изделий:

- на пустые корпуса наносится маркировка, аналогичная маркировке оригинальных ИС;
- на более дешевые ИС наносится маркировка, соответствующая маркировке более дорогих микросхем;
- на ИС с похожими, но более низкими техническими характеристиками, наносится маркировка с более высокими техническими характеристиками, соответствующими более дорогим ИС;
- предлагаются ИС, извлекаемые из печатных плат.

Самый распространенный метод подделки — продажа товаров с новой маркировкой. Совсем несложно удалить имеющуюся маркировку с дешевой микросхемы и нанести новый логотип и новое обозначение детали или другое название производителя, или другое значение скорости, а затем продать полупроводник ничего не подозревающему покупателю, у которого нет возможности убедиться в оригинальности изделия. Иногда микросхема — это просто пустой корпус без кристалла внутри (рис. 1).

Вполне вероятно, что собранная система даст сбой еще до выхода с завода-изготовителя. В таком случае потребуется дорогостоящее исследование и доработка, при этом в наличии не будет детали, которой можно было бы заменить дефектный компонент, что приведет к остановке производственной линии! Но отказ поддельных ИС может произойти уже при эксплуатации системы, и тогда стоимость ремонта будет в десятки раз выше, чем до выхода изделия с завода-изготовителя.

В качестве подделок также могут использоваться ИС, извлекаемые из забракованных печатных плат. На них наносится логотип другого производителя,

Рис. 1. На первый взгляд маркировка на корпусе микросхемы очень похожа на оригинальную. Можете определить, какая из этих микросхем оригинальная?

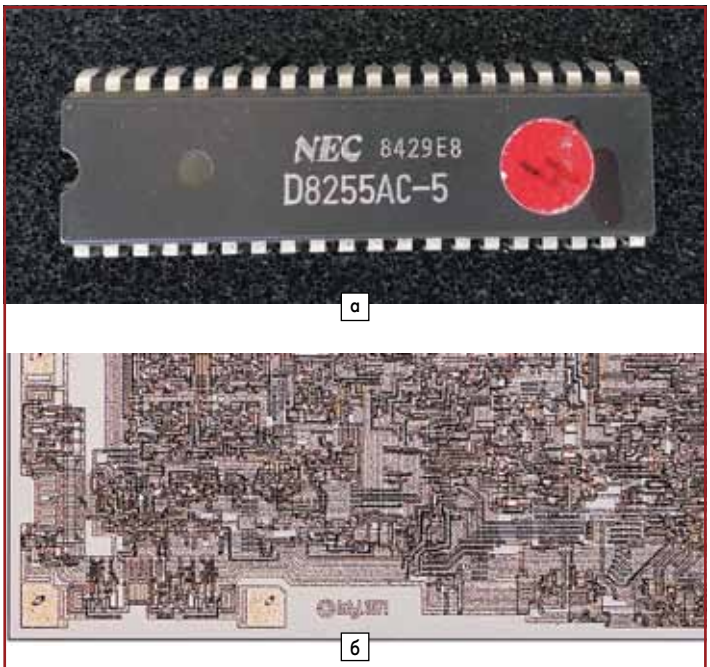

Рис. 2. В данном случае после удаления верхней крышки (б) можно увидеть, что маркировка (а) на внешнем корпусе не соответствует характеристикам кристалла

они попадают в цепочку поставок, и их приобретают ни в чем не повинные покупатели, даже не подозревающие о том, что данные изделия могут оказаться неоригинальными.

Как правило, абсолютно невозможно определить поддельные компоненты до момента их установки на печатную плату и проведения первых испытаний конечного изделия. При обнаружении отказа необходимо запустить дорогостоящую процедуру выявления дефектных компонентов с последующим их извлечением из всех печатных плат на производственной линии. Может потребоваться отзыв всех партий конечных изделий, что напрямую скажется на чистой прибыли компании.

Одно из возможных технических решений данной проблемы — визуальный контроль изделий на наличие ошибок в маркировке, но для проведения такого контроля нужны должным образом подготовленные сотрудники с большим опытом, способные различить нюансы маркировки. Также одним из решений может служить электронное тестирование или рентген-контроль всех входящих партий.

Существует и разрушающий метод контроля — полное извлечение кристалла для проведения визуальной оценки под микроскопом, что влечет потерю прибыли, так как происходит разрушение компонента (рис. 2). Это длительный процесс, который сопровождается значительными финансовыми затратами, а кроме того, необходимо содержать штат квалифицированных контролеров, проводить их обучение и использовать дорогостоящее оборудование.

Скрининг

Некоторые дистрибьюторы рекламируют свои услуги по проверке компонентов со сроком выполнения «всего два дня». В большинстве случаев это неприемлемо. Подобные компании предлагают такие методы исследования, как рентген-контроль, рентгенофлуоресцентный анализ (XRF), демонтаж корпуса, испытание с подогревом растворителя, визуальный контроль и проверка качества пайки, сопровождающиеся составлением подробных отчетов, причем нам всего-навсего нужно знать, является ли деталь годной. В действительности такой подход применим только для изделий военного назначения или для крупносерийного производства.

Один из способов — проведение функционального испытания на образце ИС, например, логический ввод/вывод, соответствующий таблице истинности. Данный метод позволяет определить явные проблемы: неправильная логическая схема или отказ микросхемы. Однако он упускает из виду тонкие «недопустимые» проблемы — контрольные признаки того, что компонент является подделкой. Для семейств ИС предыдущих поколений часто доступны разные варианты скорости. Обычное испытательное оборудование с таким уровнем возможностей тестирования скорости стоит очень дорого.

Решение проблемы

Но есть инструмент, который можно использовать для быстрой и дешевой проверки подлинности поступающих ИС с применением статистически надежной процедуры, подходящий для любых устройств в любом исполнении, простой в обращении и обеспечивающий быстрое заключение «годный/под сомнением/дефектный». Один из таких универсальных инструментов — детектор поддельных ИС ABI Sentry, представляющий собой устройство на базе ПК, способное за считаные секунды определить подлинность деталей.

Удобство и простота обращения обеспечивают возможность использования оборудования на любом этапе входного контроля. Анализ выполняется в фоновом режиме, а оператору остается лишь прочитать одно из следующих возможных заключений: «Годное устройство», «Пустое устройство» или «Дефектное устройство» и принять решение о необходимости отправки поставщику подробного отчета.

ABI Sentry — это настольное устройство, в котором используется расширенная форма тестирования зависимости напряжения и силы тока на любом кристалле ИС для определения его электрических характеристик или «сигнатуры» (рис. 3). Тестирование зависимости напряжения

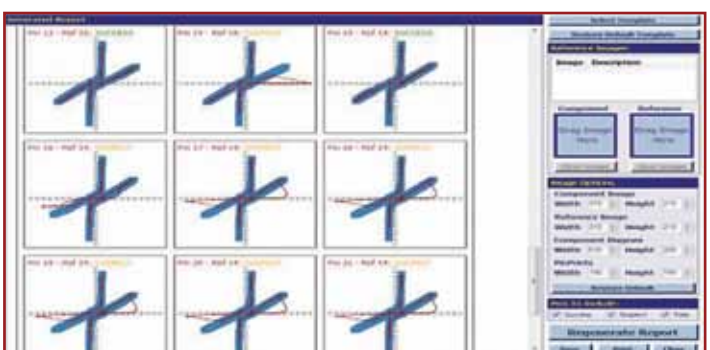

Рис. 3. Тестирование зависимости напряжения и силы тока основано на определении формы волны напряжения между двумя выводами ИС и измерении того, как меняется потребляемый ток при изменении прилагаемого напряжения

и силы тока основано на определении формы волны напряжения между двумя выводами ИС и измерении того, как меняется потребляемый ток при изменении прилагаемого напряжения. Указанное изменение напрямую связано с характеристиками устройства, его внутренней структурой и параметрами процесса изготовления.

Устройство тестирует все возможные комбинации выводов на исследуемой ИС и обеспечивает более глубокое понимание ИС по сравнению с простыми системами, которые ограничиваются контролем зависимости между выводами и землей. Матричное тестирование зависимости напряжения и силы тока, реализованное в детекторе Sentry, позволяет выявить отличия между устройствами с разными функциональными характеристиками, но изготовленными по одной технологии. Данное испытание позволяет обнаружить перемаркированные поддельные ИС с похожей схемой расположения выводов ИС.

Установление сигнатуры

Параметры зависимости напряжения и силы тока, собираемые детектором Sentry, называются PinPrints и представляют собой уникальную сигнатуру устройства. Вначале Sentry используется для тестирования годного изделия для получения сигнатуры «золотого стандарта». Затем сигнатуры тестируемых неизвестных микросхем сравниваются с сигнатурой годного изделия, и устанавливается возможное несоответствие.

Незначительные расхождения свидетельствуют о том, что микросхемы изготовлены разными производителями или относятся к разным партиям одного и того же производителя. Однако при выявлении существенных отличий можно предположить, что микросхемы имеют дефекты или являются подделкой. Детектор Sentry можно настроить для каждого типа ИС, установив допуски, определяющие точку, достижение которой подтверждает дефектность тестируемого устройства.

При отсутствии эталонных изделий возможны два альтернативных варианта. Эталонные данные можно экспортировать с других детекторов, имеющихся в распоряжении пользователя, или из библиотек и импортировать в базу данных Sentry. Второй вариант (который нельзя назвать оптимальным) — выполнить тестирование всех изделий из партии. При выявлении расхождений годность всей партии ставится под сомнение, и вся партия признается бракованной. Очень легко определить ИС без кристалла — на всех контактах будет прямая линия «нулевого ответа» при разомкнутом контуре.

В составе детектора Sentry предусмотрен набор разъемов ZIF для подключения адаптеров DIP, SOIC, BGA, SSOP, а также дискретных компонентов. Система работает по принципу сравнительного анализа для быстрого изучения параметров новых компонентов с последующим тестированием незнакомых изделий. Хорошо изученный компонент блокируется в разъеме ZIF, после чего подключаются все выводы тестируемого образца. Производится автоматическое измерение отклика компонента на тестируемый образец с последующим сохранением информации в качестве эталона.

Выполняется проверка сочетания электронных настроек Sentry (напряжения, частоты, сопротивления источника и формы волны), формирующих сигнатуру каждого из выводов ИС. Затем детектор сравнивает уникальные электрические характеристики известных компонентов с характеристиками тестируемых устройств. Проверяются все возможные сочетания выводов, максимально повышая вероятность сбора информации об условиях внутреннего отказа. Детектор Sentry способен быстро определить, все ли кристаллы установлены и соответствуют ли параметры кристаллов заявленным значениям, а также наличие всех соединительных проводов, точность разводки и возможные варианты значений полного сопротивления вывода. Результатом тестирования становится заключение о годности изделия, обеспечивающее высокий уровень уверенности в подлинности компонентов.

Поскольку изделия становятся все более и более сложными, тестирование 100% деталей представляется обременительным, а испытание одного или двух компонентов, например, из 200 является вполне реальной задачей. Опыт показал, что отклонения в подозрительной партии обнаруживаются задолго до завершения такого испытания. Тем не менее 100% изделий проходят неразрушающий контроль с использованием детектора поддельных ИС Sentry.

При помощи детектора Sentry можно выявить изделия с отличающейся внутренней структурой или детали без структуры, а также компоненты, изготовленные другим производителем. Библиотека сохраненных устройств Sentry, управление которой реализовано посредством специального программного обеспечения, устанавливаемого на ПК, к USB-порту которого подключается детектор, формируется путем добавления информации о хорошо изученных устройствах.

Для каждого изделия можно создать электронный пакет документов, состоящий из фотографий маркировки, технического описания и других данных, облегчающих последующее подтверждение целостности изделия. Предусмотрена возможность формирования и хранения подробных отчетов для обеспечения прослеживаемости и контроля качества. Sentry защищает предприятия от поддельных устройств, так как позволяет обнаружить дефектные детали прежде, чем они станут источником проблем.

Аппаратное обеспечение Sentry

В состав детектора Sentry входят все элементы аппаратного обеспечения, необходимые для определения электрических характеристик ИС с количеством выводов до 256 (рис. 4). Кроме того, для тестирования устройств с количеством выводов более 256 (BGA, QFP) есть возможность поворота для испытания и сравнительного анализа всех выводов.

Конструкция детектора Sentry предусматривает наличие четырех 48-контактных разъемов с нулевым усилием сочленения (ZIF) и двухрядным расположением выводов. Эти разъемы могут напрямую использоваться для DIP-компонентов предыдущего поколения, а также для установки различных дополнительных переходников, предназначенных для разных типов ИС. Если необходимо, на переходной панели может быть несколько разъемов для ИС, чтобы одновременно выполнять тестирование нескольких ИС или для сравнения характеристик двух ИС. Если использовать расширитель, то можно подключить специальные переходники с количеством выводов свыше 256.

Детектор ABI Sentry имеет прочный металлический корпус 26,9×25,4×9,1 см, его вес составляет 3,6 кг. Для подключения разных

Анна ШАЛАЕВА, руководитель отдела внешней кооперации А-КОНТРАКТ:

Поставка контрафактных электронных компонентов является одним из ключевых рисков закупочной деятельности. Компания, приобретающая комплектацию, должна решать данную проблему, применяя весь спектр доступных методов, как технических, так и технологических.

Одним из неочевидных инструментов нивелирования рисков, связанных с поставкой некачественной продукции, может стать система оценки и выбора поставщиков. Взвешенный подход к разработке такой системы позволяет в большинстве случаев избежать риска либо принять его обдуманно, а значит, контролировать ситуацию на всех этапах. Важно понимать, что расширение пула поставщиков, как и работа с непроверенными каналами поставок, далеко не всегда может оказаться выигрышной стратегией, особенно в период кризиса. Даже в нынешней сложной рыночной ситуации необходимо оценивать все риски и неукоснительно следовать по пути, который позволяет в долгосрочной перспективе отследить всю цепочку поставок.

Так, в А-КОНТРАКТ применяется система оценки поставщиков, которая учитывает опыт работы лидеров рынка — наших партнеров в области качества, и опыт нашего сотрудничества в целом. Вместе с ключевыми поставщиками мы ежегодно определяем направления развития закупочной деятельности, расставляем приоритеты, отдаем предпочтение проверенным и надежным каналам поставок, исключаем каналы, которые, по нашей оценке, ненадежны.

Весь наш богатый опыт работы в этом направлении говорит о том, что цепочки поставок в компании должны быть выстроены таким образом, чтобы качество продукции контролировалось и регулировалось отделом закупок, в том числе и на стороне поставщика. Безусловно, одной системой оценки поставщиков не обойтись, но работа с официальными, проверенными каналами позволяет диверсифицировать риски и минимизировать потери.

микросхем можно устанавливать отдельные сменные переходники. Предусмотрен широкий ряд дополнительных переходников, позволяющих выполнять тестирование всех самых распространенных типов корпусов ИС, в том числе DIP, SOIC, PLCC, QFP и даже BGA. Для упрощения работы конструкция Sentry не предполагает наличия дисплея или клавиатуры, так как детектор подсоединяется к USB-разъему ПК, на который устанавливается специальное бесплатное программное обеспечение ABI.

Заключение

Детектор ABI Sentry — это пример практического решения проблемы выявления поддельных ИС, принцип работы которого основан на быстром анализе специальной библиотеки характеристик компонента для перекрестной проверки каждой детали. Проблемы со сроками поставки ИС напрямую влияют на напряженный производственный график, поэтому выявление любых деталей, которые не являются «настоящими», до того, как они поступят в производство, потенциально может сэкономить каждому производителю много времени и денег. А также поможет поддерживать на высоте такую нематериальную, но при этом очень важную составляющую бизнеса, как репутация бренда.

Рис. 4. В состав детектора Sentry входят все элементы аппаратного обеспечения, необходимые для определения электрических характеристик ИС с количеством выводов до 256