

УДК 621.37.037

DOI: 10.32362/2500-316X-2019-7-1-57-79

КОНТРЕИНЖИНИРИНГ РАДИОЭЛЕКТРОННЫХ СРЕДСТВ

**М.С. Костин[@],
Д.С. Воруничев,
Д.А. Корж**

МИРЭА – Российский технологический университет, Москва 119454, Россия

[@]Автор для переписки, e-mail: kostin_m@mirea.ru

Изложены результаты научно-практических исследований в области спецпроектного реинжиниринга и контрреинжиниринга изделий радиоэлектронных средств. Представлены методы и средства спецпроектного реинжиниринга функциональных модулей многослойных печатных плат и корпусных микросхем. Приведены базисные конструкторско-технологические решения реинжиниринга многослойных печатных плат радиоэлектронных изделий, основанные на физических принципах разрушающего и неразрушающего декомпозиционного исследования: механообработка и химическое травление, стереолазерное структурирование, тепловизионная электротермия, рентгенографический анализ. Сформулированы положения и методология схмотехнического анализа принципиальной архитектуры электрических цепей и сигнальных процессов радиоэлектронных изделий по конфигурации печатного узла, его электронной компонентной базе и их связным топологиям. Рассмотрены методы и средства реинжиниринга радиотехнических цепей и сигналов, позволяющие воспроизвести перечень электронной компонентной базы и принципиальную схмотехнику, а также исследовать основные системотехнические характеристики радиоэлектронного устройства в четырех основных режимах: функциональном, внутрисхемном, периферийном и идентификационной визуализации. Обсуждаются методы и средства аутентичной воспроизводимости радиоэлектронных изделий по ряду конструктивных и радиотехнических идентификаторов. Предложены и сформулированы конструкторско-технологические решения по обеспечению противодействия реинжинирингу изделий радиоэлектронных средств.

Ключевые слова: спецпроектный реинжиниринг, контрреинжиниринг, техническое противодействие, радиоэлектронное изделие, прототипная декомпозиция, сигнальные процессы.

COUNTERREENGINEERING OF ELECTRONIC DEVICES

**M.S. Kostin@,
D.S. Vorunichev,
D.A. Korzh**

MIREA – Russian Technological University, Moscow 119454, Russia

@Corresponding author e-mail: kostin_m@mirea.ru

The paper presents the main results of scientific and practical research in the field of special design reengineering and counterreengineering of radioelectronic devices. Methods and means of special design reengineering of functional modules of multilayer printed circuit boards and case microcircuits are presented. The basic process design for the reengineering of multilayer printed circuits of radioelectronic products is presented. The design is based on the physical principles of destructive and non-destructive decomposing test: mechanical processing and chemical etching, stereolaser structuring, IR imaging electrothermics and X-ray analysis. The article formulates positions and methodology of the circuit analysis of the basic architecture of electrical circuits and signal processes of radio electronic products by the configuration of the printed circuit, its electronic component base and their connected topologies. The article considers methods and techniques for the reengineering of radiotechnical circuits and signals enabling to reproduce the list of the electronic component base and the essential circuit technique, as well as to study the basic circuit characteristics of the appliance in four main modes: functional, in-circuit, peripheral and identification visualization. The methods and means of authentic performance of radioelectronic devices for a number of constructive and radio-technical identifiers are considered. Technical methods and solutions for counterreengineering of radioelectronic devices have been developed.

Keywords: special project reengineering, counterreengineering, technical countermeasures, radio electronic device, prototype decomposition, signaling processes.

Введение

Обеспечение экономической и информационно-технической безопасности (ИТБ) в области радиоэлектронной промышленности и сектора ОПК сегодня является одной из приоритетных задач Государственной программы импортозамещения. При этом доминирующие позиции в сфере обозначенных направлений занимают спецпроектные исследования в области реинжиниринга и контрреинжиниринга радиоэлектронных средств (РЭС). Сегодня реинжиниринговые исследования, позволяющие путем обратного анализа разработать научно-практическую стратегию проектирования и производства изделий РЭС в технически защищенном от копирования исполнении, являются неотъемлемым инструментом конкурентоспособной навигации. Отсюда целью обозначенной стратегии является безошибочный выбор номенклатуры электронной компонентной базы (ЭКБ) и реализация аппаратных и программных средств защиты радиоэлектронного изделия от преднамеренного реинжиниринга.

Таким образом, актуальность и ключевые задачи реинжиниринга заключаются в:

1) техническом противодействии спецпроектным исследованиям поставляемых на экспорт оригинальных РЭС двойного назначения либо импортируемых РЭС, изготовленных иностранными партнерами в рамках программ внешнеэкономической кооперации;

2) исследовании современных методов и средств реинжиниринга РЭС, которые играют ключевую роль в обеспечении ИТБ изделий радиоспецтехники, реализуемых на базе импортной ЭКБ, с целью идентификации элементов и электрических цепей, реализующих программно-аппаратные решения средств РТР и внутрисистемного подавления РЭП;

3) активной модернизации изделий РЭС (принимая во внимание объем морально устаревшего радиоэлектронного оборудования и ЭКБ, находящихся в стадии долгосрочной эксплуатации средств вооружения военной техники, а также допускаемый Главным управлением вооружения ВС перечень импортной ЭКБ, возрастает необходимость активной модернизации для продления жизненного цикла радиоэлектронной аппаратуры; реинжиниринг в таких случаях применяется к оригиналу радиоэлектронного изделия, когда рабочая конструкторская документация на образец утрачена или недоступна);

4) защите изделий РЭС от контрафактного производства в целях поддержания конкурентоспособности и показателей экономического роста от экспортных поставок выпускаемых изделий (рис. 1).

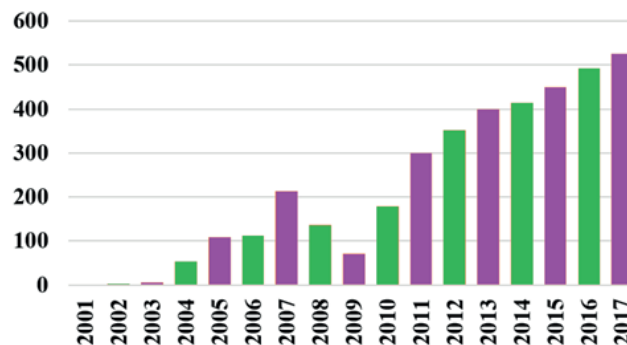


Рис. 1. Ежегодная динамика совокупных убытков мировых компаний радиоэлектронной индустрии от контрафактного производства РЭС средствами реинжиниринга (млрд. USD) [1].

Предметной областью спецпроектного реинжиниринга РЭС являются:

- реинжиниринг конфигурации печатной топологии МПП методами разрушающей (абразивное шлифование, химическое травление, лазерное структурирование, термовоздушное расщепление, фрезерование) и неразрушающей (рентгенографический анализ, ТВЭТ) послойной декомпозиции;
- схемотехнический реинжиниринг многослойных печатных узлов (МПУ): функциональный, внутрисхемный, периферийный (системотехнический);
- реинжиниринг сигнальных и радиофизических процессов МПУ;
- реинжиниринг интегральных устройств ЭКБ (ИМС-логика, ПЛИС, микропроцессоры, цифровые устройства памяти и т. д.).

1. Реинжиниринг многослойных печатных плат

Чтобы разработать комплекс мер противодействия спецпроектному реинжинирингу, необходимо провести исследования методов и средств, позволяющих идентифицировать конструктивные особенности РЭС по топологии печатной платы изделия. При этом особый интерес представляют платы с многослойным распределением печатной топологии – МПП. Как известно, современный реинжиниринг МПП цифровых устройств позволяет

не только восстановить аутентичность спеченой топологии, но и в высоковероятной степени воссоздать принципиальную схему радиоэлектронного изделия в целом [1]. Таким образом, это позволяет выявить номенклатуру интегрированных в МПП электронных радиоэлементов (ЭРЭ). Зная номенклатуру, возможно определить тип микросистемного устройства (как, например, приемопередатчик на ПЛИС) и узнать основные параметры его схемотехнической архитектуры.

Одной из радикальных классификаций методов реинжиниринга МПП является классификация по принципу физического декомпозиции РЭС: разрушающего и неразрушающего воздействия.

Определяющими факторами при выборе того или иного метода и средств реинжиниринга являются:

- 1) конструкция печатного узла;
- 2) материалы, из которых изготовлен печатный узел;
- 3) тип монтажа, примененный в печатном узле.

Стоит отметить, что данные факторы будут определяющими и для выбора технических мер по противодействию реинжинирингу. Так, при проведении послойного топологического анализа появляется возможность слой за слоем воссоздать исследуемый печатный узел и впоследствии создать его прототип с целью модификации в дальнейшем. Кроме того, возможна разработка комплекса мер по защите от спецпроектных исследований, что позволит обеспечить экономическую и интеллектуально-информационную защиту перспективных отечественных РЭС и разработок.

Среди разрушающих способов деструктуризации МПП различают следующие: послойного шлифования, лазерного и химического травления, фрезерования и термовоздушного расщепления [2]. Реинжиниринг разрушающего воздействия не гарантирует отсутствие повреждений топологии МПП повышенной плотности монтажа или трассировки, потому не является прогрессивным. Он применяется только тогда, когда исключается эффективность применения методов неразрушающего прототипирования, позволяющих восстанавливать топологию с применением косвенных методов экспертного анализа: стереолазерное и оптическое сканирование, тепловизионная электротермия, рентгенографический анализ и радиосенсорное исследование, применяемое для контактно-локационного анализа при восстановлении схемотехнической конфигурации печатного изделия [1].

1.1. Прототипирование методом разрушающей декомпозиции печатных узлов

Послойная декомпозиция образца печатного изделия относится к методам разрушающего спецпроектного исследования топологии МПП и является наиболее радикальным техническим решением в области реинжиниринга радиоэлектронных средств, позволяющим получить печатный рисунок, переходя от одного стека топологии к другому. Главной целью данного этапа прототипирования является получение топологии каждого слоя, поэтому после разрушения очередного слоя МПП ее необходимо зафиксировать. Это можно сделать с помощью стереооптического сканирования.

Стереооптическим данный процесс называется благодаря применению лазерно-оптических систем, позволяющих регистрировать как печатную топологию МПП, так и поперечный срез межслойных соединений при помощи специализированных сканеров

и адаптированного ПО, как, например, ScanCAD [3]. Важно отметить, что данный метод теряет свою актуальность, если необходимо исследовать печатные модули со встраиваемыми ЭРЭ, так как при послойной декомпозиции почти во всех случаях будет происходить повреждение встроенных в плату радиодеталей (рис. 2). Заметим, что повсеместное и активное внедрение изготовления печатных узлов со встраиваемой ЭКБ свидетельствует о несостоятельности данного метода при попытке воссоздания прототипа таких печатных узлов.

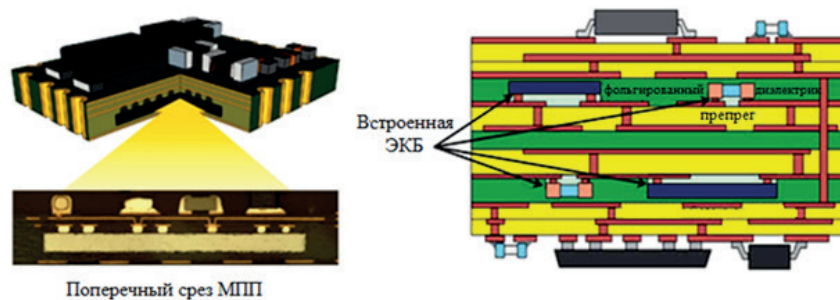


Рис. 2. Поперечный срез конструктивной реализации МПП со встраиваемой ЭКБ.

1.2. Прототипирование методом неразрушающей декомпозиции печатных узлов

Если применение разрушающих методов реинжиниринга невозможно из-за особенностей исследуемого образца, как описано выше, либо других технических ограничений, обычно прибегают к следующим неразрушающим методам:

- 1) рентгенографический анализ;
- 2) тепловизионная электротермия.

Рентгенографический анализ. Метод позволяет – в отличие от разрушающих методов – исследовать топологию и проводить внутрисхемный анализ печатного узла, не прибегая к физическому воздействию, и сохранять его структуру целостной. Однако в классическом варианте нормального (под углом 90°) рентгеновского сканирования рентгенографический анализ не позволяет различить межслойную топологию МПП. Чтобы решить данную проблему, прибегают к режиму углового облучения МПП. Таким способом достигается послойное сканирование топологии медных слоев, а специализированное ПО позволяет получить данные топологии по двум угловым проекциям (рис. 3а, б). Регистрация рентгенограммы изображений слоев топологии МПП происходит посредством компьютерной томографии, которая заключается в получении и наложении с помощью программно-числовой обработки изображений каждого слоя.

Среди специализированного оборудования рентгенографического анализа внутрисхемной топологии печатных плат хорошо зарекомендовала себя установка Nordson DAGE XD7600 NT Ruby X-ray Inspection System [4]. Так, на рис. 3в представлены результаты анализа 4-х-слойной МПП, полученные посредством наложения изображений слоев и их программно-числовой обработки.

Стоит подчеркнуть, что для получения качественной рентгенографической томограммы медной топологии печатной платы необходимо, чтобы исследуемый участок топологии выделялся на контрастном фоне диэлектрика. Отсюда следует, что одним из возможных вариантов противодействия данному методу реинжиниринга является закры-

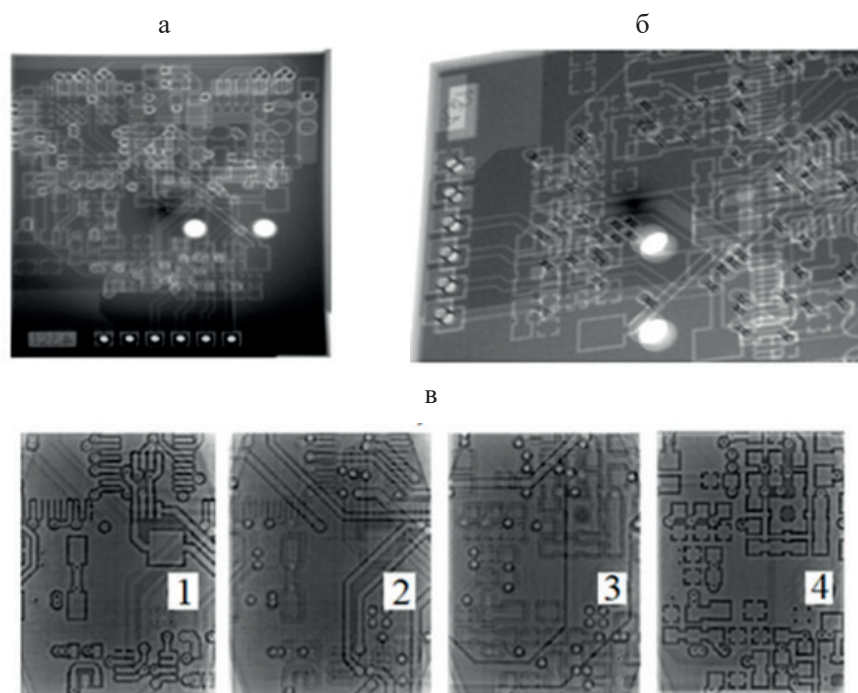


Рис. 3. Рентгенографический анализ многослойной топологии, полученный на установке DAGE XD7500 VR X-ray Inspection System: а) облучение МПП под прямым углом 90°; б) облучение МПП под углом 30°; в) послойная томограмма образца платы.

тие слоя медной топологии от рентгеновских лучей. Действительно, уровень контрастирования находится в прямой зависимости от связанного с ним материала мишени (ЭРЭ, материала проводящего слоя), его физической плотности, физико-химических свойств и атомного числа. В таком случае обеспечивается рентгенографическая блокировка защищаемого участка цепи, позволяющая существенно понизить четкость или вовсе исключить возможность анализа внутрислойной топологии. То есть для создания активных зон рентгенографической блокировки нужно конструктивно использовать в структуре МПП композитные материалы, которые обладают большим атомным числом. Такой блокинг-материал (с атомным числом из диапазона 70–82: вольфрам, тантал, золото, свинец и т. д.) может применяться для нанесения между препергами конструкции МПП в виде фольги или путем напыления на проводники. Его получают путем добавления блокинг-частиц в смолистую основу либо в структуру препергов, путем добавления в припой и др.

Эффективность использования блокинг-материалов показана на рис. 4. Так, на рис.4а изображена рентгенографическая томограмма исследуемой 6-ти-слойной МПП. В отличие от предыдущей (рис. 3), на одном из периферийных слоев данной платы нанесен блокинг-материал (атомное число 73), основанный на припое с примесью тантала, который поглощает рентгеновские лучи.

Важно отметить, что размещение блокинг-материалов на всей площади МПП не является, в принципе, целесообразным. Оно оправдано только в местах коммутации печатных проводников (рис. 4б–д). Правильно подобранное расположение блокинг-материалов и использование встроенной ЭКБ во внутренней структуре МПП делает ее фактически полностью неуязвимой для рентгенографического анализа и разрушающих методов реинжиниринга.

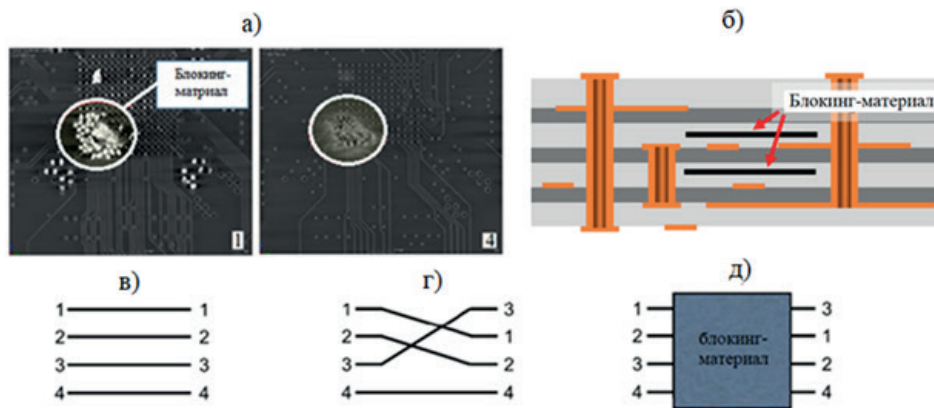


Рис. 4. Использование блокинг-материала в структуре МПП:

- а) образование гамма-шумов в области нанесения блокинг-материала при сканировании МПП методом рентгенографического анализа;
- б) поперечный срез МПП со встроенным блокинг-материалом;
- в) фрагмент узловой топологии оригинала печатного изделия;
- г) неоднозначно структурированная топология;
- д) структурированная топология под слоем блокинг-материала.

Тепловизионная электротермия. Концептуальное решение технологии тепловизионной электротермии (ТВЭТ) заключается в создании индукционного нагрева медных проводников МПП с целью термографического проявления рисунка печатной топологии, скрытой в слоях диэлектрического основания платы, в инфракрасном диапазоне при помощи тепловизора высокого чувствительного и матрично-пиксельного разрешения [5].

Индукционный и диэлектрический электронагревы основаны на выделении тепловой энергии непосредственно в нагреваемом образце МПП при возникновении в нем наведенных вихревых токов Фуко и выделении тепла по закону Джоуля-Ленца в проводниках и токов смещения – в диэлектриках с выделением тепловой энергии вследствие влияния диэлектрических потерь. Основным требованием, предъявляемым к ВЧ-индукторам в ТВЭТ-технологии, является применение конструкций открытого типа с целью нагрева МПП с одной стороны платы и тепловизионной термографии – с противоположной стороны диэлектрического основания. В частности, для реализации тепловизионной электротермии можно использовать два основных конструктива индукторов открытого типа: плоские спиральные и магнитопроводные катушечные.

Поскольку побочный диэлектрический нагрев, создающий тепловой шум, проявляется на частотах свыше 30 МГц, ТВЭТ проводящей топологии МПП осуществляется путем воздействия ближнего поля маломощного плоского ВЧ-индуктора (до 0.5 Вт) и ограничивается частотой 30 МГц. Регистрация ИК-излучения образца МПП осуществляется в среднем диапазоне 8–9.5 мкм с чувствительностью 0.03 °С, что соответствует температурному интервалу +30...+80 °С при среднем нагреве образца около +55 °С, фоновом диэлектрическом нагреве до +26 °С и температуре окружающего пространства +22 °С [5].

Подчеркнем, что ТВЭТ-технология не предусматривает разрушающего воздействия, в чем и состоит ее преимущество. В качестве тепловизора в ТВЭТ-технологии, как правило, применяются инфракрасные камеры среднего спектрального диапазона 7.5–14 мкм, например, RAZ-IR PRO-2 с тепловой чувствительностью менее 0.03 °С [5].

Принцип реализации ТВЭТ-технологии следующий. В результате воздействия магнитных полей, наводимых ВЧ-токами (рис. 5а), происходит индукционный нагрев проводящих слоев на поверхности и внутри диэлектрического основания испытуемого образца МПП. Тепловизионные исследования могут проводиться в двух режимах термографической регистрации: в фоновом и инверсном (рис. 5б–в). Использование инверсного режима является наиболее предпочтительным, поскольку катушка индуктора образует тепловое излучение, которое мешает контрастному восприятию и распознаванию термографического изображения.

Локализуя ВЧ-индуктор в заданной области образца МПП, а также управляя частотой и мощностью ВЧ-генерации, удастся осуществить оптимальную настройку четких очертаний топологии токопроводящего печатного рисунка на тепловизионной камере в заданном слое. Для детального рассмотрения фрагментарных элементов топологии может быть использован способ нагревания печатных проводников контактным методом ВЧ-токами малой мощности.

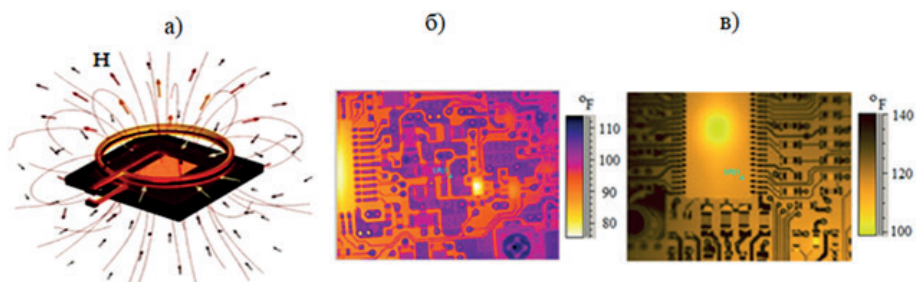


Рис. 5. Образец платы в поле ВЧ-индуктора (а); фоновый (б) и инверсный (в) тепловизионные снимки топологии МПП.

Исследование современных методов и средств реинжиниринга изделий МПП, а также анализ технологии производства и номенклатуры ЭКБ позволяют разработать комплекс технических мер и проектно-конструкторских рекомендаций противодействия спецпроектным исследованиям изделий РЭС, как, например, внедрение в структуру диэлектрической подложки МПП встраиваемых чипов электрорадиоэлементов, исключающих возможность эффективного применения реинжиниринговых средств разрушающей декомпозиции ввиду опасности повреждения ЭКБ. В то же время с целью обеспечения противодействия средствам рентгенографической деструктуризации предлагается применение внутрислойных блокинг-материалов из элементов с высоким атомным числом, препятствующих проникновению рентгеновских лучей в сегментированную область неоднозначно структурированной топологии.

Одним из предложенных в работе способов защиты изделия от исследования методом ТВЭТ является локальное внедрение в структуру диэлектрического основания микрополосковых встречно-бифилярных катушек, закрывающих участки перераспределения коннекции с двух сторон по аналогии с блокинг-материалом и тем самым компенсирующих наводимое поле плоского ВЧ-индуктора. Устойчивость конструкции МПП одновременно к обоим рассматриваемым методам можно достичь комбинированием представленных решений.

Среди прочих находят применение также иные конструкторско-технологические рекомендации контрреинжиниринга РЭС, основанные на принципах визуального измыш-

ления: добавление в печатный узел избыточной активной и пассивной ЭКБ; включение слоев с «холодной» топологией, усложняющих анализ цепей. В качестве компонентов могут быть неработоспособные (непроводящие или всегда открытые) транзисторы, мнимые (непроводящие) вертикальные межсоединения, избыточные проводящие дорожки и т. д.

Противодействием схемотехническому прототипированию может послужить исключение расположения тестовых площадок и/или элементов трассировки на боковых поверхностях МПП. Кроме всего прочего, применение технологий тестирования JTAG, или периферийного схемотехнического анализа, в значительной степени компенсирует недостаток физического доступа, создавая бесконтактную альтернативу тестированию цепей, недоступных для ИСТ-адаптеров.

Анализ и обработка отсканированной топологии МПП требует послойной геометрической векторизации. Используя векторизацию, можно воспроизвести трассировку и изготовить прототип целевой МПП, что затем позволит модифицировать ее топологию и исследовать конфигурацию электрических цепей по ряду идентификаторов. Посредством такой идентификации просто выявить функциональную принадлежность и тип РЭУ. Определяющими идентификаторами способны выступать конкретные выводы шин заземления, а также цепи обвязки ПЛИС, цифровых интерфейсов, микропроцессоров, схем памяти и др.

Среди средств программно-числовой обработки сканированной топологии оригиналов МПП в задачах спецпроектного реинжиниринга находит применение модульный функционал таких специализированных пакетов, как Drupht, Aplite и Phiplastic.

2. Реинжиниринг сигнальных процессов в печатных модулях

Реинжиниринг схемотехнической конфигурации радиоэлектронных цепей печатного узла заключается в воспроизведении перечня ЭКБ, реконструкции электрической принципиальной схемы, а также в параметрическом исследовании сигнальных процессов и основных характеристик и принципов работы радиоэлектронного устройства [2].

Задача реинжиниринга сигнальных процессов решается схемотехническим анализом МПП. Различают следующие виды схемотехнического анализа:

- функциональный;
- внутрисхемный;
- периферийный;
- метод идентификационной визуализации, используемый в качестве вспомогательного при реализации вышеприведенных методов [3].

Целью функционального анализа является исследование и регистрация основных характеристик печатного узла. Функциональный анализ разделен на три этапа:

- 1) на первом этапе МПП рассматривается как многоплюсник;
- 2) на втором этапе исследуются отдельные функциональные узлы и цепи, на которые разбивается МПП;
- 3) на третьем этапе рассматривается ЭКБ, входящая в состав функциональных узлов и цепей МПП.

Для аппаратной реализации функционального анализа МПП необходимо специальное стендовое обеспечение для сигнального моделирования РЭС, в составе которого на-

ходится исследуемый печатный узел. Однако на практике ни один вид анализа не применяется по отдельности. Как правило, это комбинированное исследование: например, комбинация функционального и внутрисхемного анализа или функционального анализа с периферийным.

Внутрисхемный анализ заключается в радиотехнической идентификации цепей или компонентов схемы радиоэлектронного изделия. В качестве аппаратных средств реализации методом внутрисхемного анализа на практике применяют специальное ИСТ-оборудование в составе с внутрисхемным анализатором цепей, оснащенный тестовой контактно-иглочной адаптерной матрицей или подвижным турбопозиционным манипулятором (рис. 6) [6]. Внутрисхемный анализ может применяться не только для анализа печатного узла, но и для анализа отдельных участков и локально расположенных ЭРЭ.

Внутрисхемный анализ, как и функциональный, не предполагает разрушающих воздействий на МПП. При этом для выполнения внутрисхемного анализа, например, по отношению к пассивным цепям исследуемого образца печатного узла исключается необходимость в дополнительном питании компонентной базы, что позволяет произвести локальную идентификацию радиоэлементов, исключая опасность их повреждения [3]. Но есть ограничения. В частности, анализ и исследование активных элементов возможно только при включенном питании. Чтобы компенсировать недостатки матричного доступа ИСТ-адаптера, который для внутрисхемного анализа требует гальванического контакта тестирующих электродов с проводниками печатного узла МПП, можно воспользоваться технологией JTAG-тестирования. Таким образом, применение методов периферийного анализа в схемотехническом реинжиниринге программируемых цифровых устройств является исключительным. Отсюда периферийный анализ печатных узлов, построенных на ядре процессорной или ПЛИС-конфигурации, не нуждается в контакте пробников с внутрисхемной сигнальной топологией печатного узла.

Известно, что программируемые цифровые устройства РЭС отличаются специальными способами криптографической защиты кодировок от внутрисистемного реинжиниринга, как, например, создание динамических псевдослучайных переменных, исключающих открытое чтение машинного кода [7].

Целевой задачей сигнального и схема-архитектурного анализа программируемых цифровых устройств на ПЛИС является также recompilation кода прошивки в схему, через которую возможно восстановить цифровую архитектуру при помощи программно-отладочных сред ISE Web PACK Design Software и Quartus II.

Автоматизация режимов и методов схема-архитектурного анализа сегодня предлагает эффективные технические решения на базе специализированного оборудования: диагностическая система Pin Point или Fault Finder, внутрисхемный матричный адаптер Flex Fixer, автоматизированный пробник Auto Point DT с «летающим щупом» и др. [3].

Матрица тестовых контактных точек МПП служит своеобразным реперным индикатором для удобного и быстрого схемотехнического реинжиниринга и радиотехнического анализа печатного узла. Таким образом, в качестве технических мер обеспечения контрреинжиниринга периферийным исследованиям предлагается исключение с боковой поверхности диэлектрического основания МПП тестовых точек и ключевых сигнальных шин данных. Исключение возможности доступа к JTAG-порту является одним из дей-

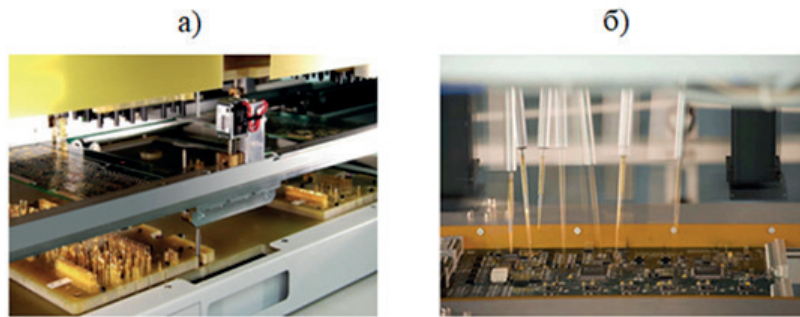


Рис. 6. Внутрисхемный ИСТ-адаптер: а) тестовые щупы матричного типа; б) тестовые щупы «летающего» типа.

ственных способов снижения эффективности периферийного анализа. Это достигается на этапе отладки и прошивки ПЛИС путем его конструктивного устранения.

Реинжиниринг ПЛИС осложняется повышенной степенью технической и криптографической защищенности таких систем. Так, одним из примеров защит является формирование в *Assembler* или скрипте *VHDL* фиктивных и случайных переменных. В то же время одним из наиболее действенных способов контрреинжиниринга программируемых цифровых устройств являются аппаратно-конструктивные решения, поддерживающие, к примеру, технологию токового выжигания сигнальных конвекторов *JTAG*-интерфейсов.

3. Прототипная декомпозиция интегральных микросхем

Если при реинжиниринге МПП возможно использование и разрушающих, и неразрушающих методов, то при спецпроектном исследовании топологии интегральных микросхем (ИМС) применяют только разрушающие методы. К ним относятся:

- 1) механическое фрезерование ИМС;
- 2) послойное химическое травление ИМС;
- 3) комбинированный метод (последовательное сочетание 1-го и 2-го методов);
- 4) лазерная декапсуляция ИМС.

Выбор того или иного метода и средства декапсуляции во многом будет зависеть от конструкции, материалов кристалла, корпуса и типа реализации технологии интегральной сборки: полупроводниковая, пленочная, гибридная или смешанного типа [8].

3.1. Прототипная декапсуляция корпусных микросхем

Химическая декапсуляция. Главной целью исследования в процессе реинжиниринга является кристалл ИМС, препятствием к которому является корпус чипа. Следовательно, чтобы получить доступ к кристаллу, необходимо произвести химическое травление корпуса, которое осуществляется с помощью концентрированной азотной или серной кислоты.

Рынок профессионального оборудования для декапсуляции чипа достаточно широк, однако среди прочих зарекомендовал себя программируемый установочный комплекс декапсуляции *PS103S (PS105)*. Данный комплекс обеспечивает выбор из 25 режимов травления пластика и применяется для декапсуляции чипа в процессе анализа отказов ИМС (рис. 7).

Основной проблемой данного метода является слабо контролируемая длительность воздействия кислот, так как длительное воздействие разрушает не только корпус ИМС,

но и может повредить сам кристалл и его соединительные проводники. Проблема решается применением плазмохимического и сухого химического травления.

На практике находят применение установки плазмохимической декапсуляции типа Е373 и Е401.

Механическая декапсуляция. Помимо метода химической декапсуляции, широко применяется механический метод. Он используется в качестве подготовительного этапа перед химическим травлением, а также самостоятельно при декапсуляции корпуса ИМС. Стоит отметить, что данный метод подходит не только для ИМС с полимерным корпусом, но и для ИМС с керамическим и металлокерамическим корпусами.

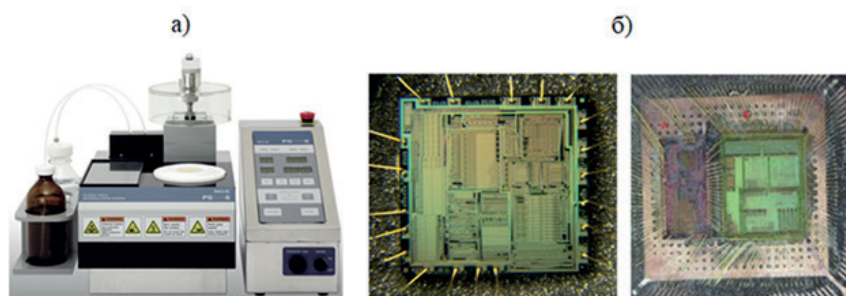


Рис. 7. Установки декапсуляции для сухого травления ИМС с ЧПУ PS 103S (PS105) (а) и снимки кристаллов ИМС после химической декапсуляции полимерного корпуса (б).

Сущность механического метода заключается в физическом воздействии на корпус ИМС с помощью фрез. Производители предлагают широкий спектр современного оборудования, которое с помощью микрофрез осуществляет прецизионное и быстрое удаление материала корпусов ИМС. Характерно, что декапсуляция корпуса ИМС может осуществляться как на самой печатной плате, так и в процессе предварительного демонтажа ИМС с ее поверхности при помощи паяльной станции. Такую комбинацию операций можно провести, например, с помощью фрезерно-шлифовального станка с ЧПУ LY-1001 и паяльной установки RW-SV520 (рис. 8).

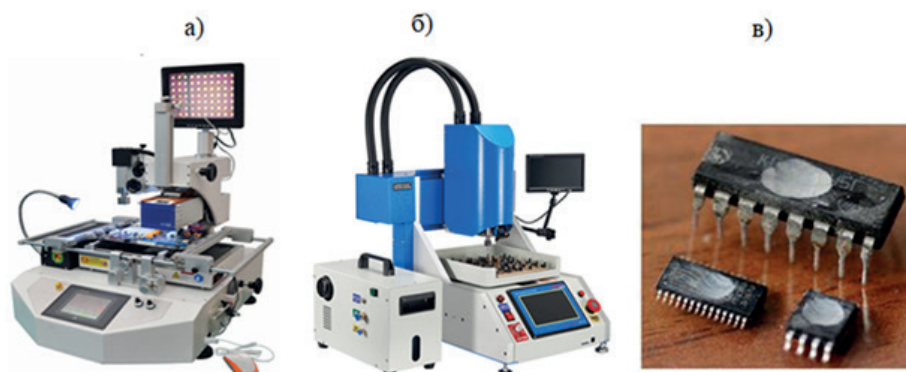


Рис. 8. Установки демонтажа и механической декапсуляции ИМС: паяльная микровизионная станция RW-SV520 (а); прецизионный микровизионный фрезерно-шлифовальный станок LY-1001 (б); образцы ИМС, прошедшие фрезерную обработку (в).

Термическая (лазерная) декапсуляция. Технология лазерной декапсуляции заключается в удалении слоя полимерного, или керамического, или металлокерамического материалов корпуса ИМС. Метод эффективен при вскрытии корпусов с медными и серебряными проводниками, его можно использовать также и для полимеров, практически не растворимых в кислотах (рис. 9).

Лазерный метод, как и метод механообработки, в технологическом цикле декапсуляции ИМС часто предшествует химическому или плазмохимическую травлению в качестве подготовительной операции, оставляя надкристалльный слой материала корпуса около 100 мкм [9]. Метод применяется также самостоятельно. Подобно методу механической декапсуляции, он подходит для полимерных, керамических и металлических корпусов ИМС типа BGA. Для решения задач реинжинирига ИМС методом лазерной декапсуляции наиболее эффективной оказалась установка Falit и ее модификация PL101i (PL121i).

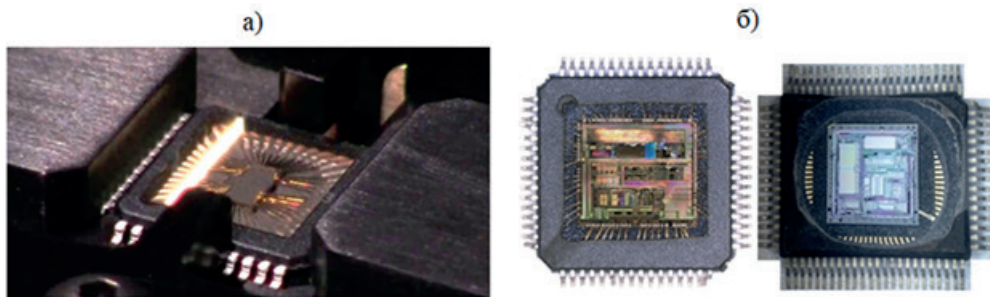


Рис. 9. Фрагмент процесса лазерной декапсуляции чипа (а); декапсулированные образцы микросхем (б).

3.2. Анализ кристалльной топологии микросхем

Неотъемлемым инструментом для изучения и анализа топологии ИМС в реинжиниринге является микровизор. Микровизоры – это новое поколение микроскопов, имеющих аппаратно-программный комплекс для регистрирования и обработки изображений, для решения задач микровизионного атомно-силового анализа. Существует несколько видов микровизоров, отличающихся по функционалу и своим возможностям. Допустим, для простого оптического исследования топологии ИМС с постобработкой изображений можно эффективно использовать цифровые микровизоры серии μ Vizo (рис. 10а). Однако, если появляется потребность в разрешении 0.5 мкм, целесообразно использовать электронный микроскоп. Например, электронный микроскоп серии JEOL JIB-4601F в отличие от конкурентов обладает ионной пушкой, что позволяет применять его как универсальный инструмент для реинжиниринга ИМС разрушающим методом (рис. 10б). Учитывая уже приведенные недостатки разрушающих методов, нельзя исключить и применение атомно-силовой микроскопии (АСМ), основанной на взаимодействиях Ван-дер-Ваальса.

Используют сканирующие зондовые и оптические микроскопы, например, серию Certus Optic, главным достоинством которой является разрешающая сила, позволяющая получать изображения с разрешением от 0.1 до 10 нм (рис. 10в).

На основании изложенных методов и средств предлагаются следующие методы противодействия спецпроектным реинжиниринговым исследованиям ИМС на различных уровнях:

- на уровне чипа:

- 1) использование фиктивной ЭКБ. В качестве компонентов могут быть неработоспособные (непроводящие или всегда открытые) транзисторы, мнимые (непроводящие) вертикальные межсоединения, избыточные проводящие дорожки, то есть элементы, которые никак не влияют на характеристики изделия в целом;

- 2) использование избыточных слоев топологии в ИМС;



Рис. 10. Установки микровизионной, растрово-электронной и атомно-силовой микроскопии: микровизоры μ Vizo-101 (а); электронные микроскопы типа JEOL JIB-4601F (б); зондооптический микроскоп Certus Optic U (в).

3) использование в структуре ИМС «скрытых» (не видимых микровизионными способами) функциональных компонентов;

- на уровне защитных покрытий и физико-химической структуры корпуса:

1) изготовление корпуса ИМС из материалов, устойчивых к методам механического, химического и термического разрушающих воздействий;

2) использование встраиваемых электронных систем защищенного доступа самоуничтожения. Так, например, в структуру корпуса ИМС вводят пьезокристалл, который под воздействием механической деформации индуцирует высоковольтный разряд, разрушительно действующий на элементы КМОП-логики;

3) использование химических примесей в структуре корпуса ИМС (как правило, полимерного). Так, при попытке химического травления корпуса данная примесь вступает в реакцию с кислотой, что приводит к экзотермической реакции, и кристалл уничтожается.

- на уровне аппаратной блокировки:

1) блокировка доступа к интерфейсу ввода/вывода данных ПЗУ [10, 11]. Реализовать механизм можно следующим способом: выполнить выжигание одного или нескольких выводов микросхемы, предназначенных для чтения/записи данных в ПЗУ, подав на порт ИМС предельно допустимый ток;

- на системно-технологическом уровне:

1) использование специализированной ячейки памяти – бита защиты, отвечающего за отключение доступа к данным. В простейшем варианте этот бит контролирует функцию чтения программного интерфейса;

2) криптографические средства защиты;

3) размещение специальной сетки в корпусе чипа, на которой непрерывно контролируется изменение емкости [2, 12], что позволяет идентифицировать и блокировать сигнальное тестовое или деструктурирующее воздействие путем затирания ключевых кодовых данных;

4) применение технологии стохастической аутентификации на базе технологии физически неклонируемых функций [13]. Так, на производстве изделие ИМС получается уникальным за счет неконтролируемых факторов (погрешностей и случайностей). Эти особенности можно регистрировать и использовать как уникальный идентификатор.

4. Методы и средства высокоточного стереолазерного сканирования элементов с многопрофильной геометрией

Для получения трехмерных моделей объектов в реинжиниринге используется метод обратного моделирования по физическим объектам. Первым этапом обратного моделирования обычно является процесс 3D-сканирования, т. е. процесс определения координат точек, принадлежащих поверхностям проектируемых изделий. Полученные модели могут быть экспортированы в CAD-системы и в дальнейшем модифицироваться. В промышленном производстве с помощью 3D-сканирования может осуществляться:

- контроль точности изготовления – устанавливается степень отличия от проектной документации;
- раскрытие дизайна, функционирования и способа производства продукции конкурентов;
- цифровое архивирование для воспроизводства устаревших компонентов, изделий с утерянной конструкторской документацией, а также геометрических моделей из устаревших систем проектирования без необходимости повторного проектирования;
- разработка компонентов для существующих товаров и изделий, разработка упаковки по форме физического объекта (переоборудование и вторичный рынок);
- репродукция в масштабе существующих объектов (модели и макеты);
- производство оснастки для ремонта, обновления и замены изношенных деталей [14].

4.1. Методы получения трехмерных моделей

В настоящее время существуют различные бесконтактные оптические методы получения геометрических моделей (рис. 11).

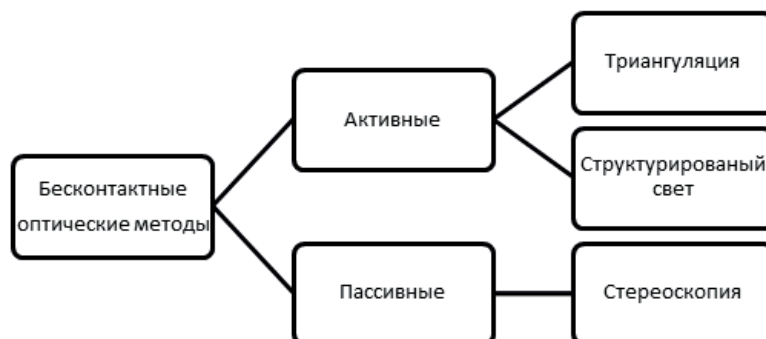


Рис. 11. Бесконтактные оптические методы для получения трехмерных моделей.

Бесконтактные оптические методы получения трехмерных моделей делятся на две группы: активные и пассивные. Активные 3D-сканеры излучают на объект сканирования свет, луч лазера, ультразвук или рентгеновские лучи и считывают отражение. Действие пассивных 3D-сканеров (не содержащих источники излучения) основано на принципе обнаружения отраженного окружающего излучения.

Бесконтактные 3D-сканеры также можно разделить по принципу работы на три основные технологии сканирования:

- триангуляции;
- структурированного освещения;
- стереоскопии.

Триангуляция основана на проецировании лазерного луча на объект сканирования. Все искажения воспринимаются измерительной камерой, которая отслеживает положе-

ние лазерного луча; полученные данные передаются на компьютер.

Сканирование на основе структурированного света заключается в проецировании на объект линий, образующих уникальный узор, каждое изменение которого сканируется приемной камерой.

Стереоскопия представляет собой фотографирование исходного объекта с различных ракурсов и воссоздание на основе полученных изображений трехмерной модели, координаты точек получают в результате компьютерной обработки.

4.2. Сканирование изделий РЭС методом триангуляции

Системы триангуляционного сканирования используются для воссоздания трехмерной структуры объектов с использованием структурированной подсветки. В основе принципа работы лазерных триангуляционных измерителей лежит метод определения расстояния между лакируемым объектом контроля и приемником излучения канала регистрации.

Эта технология названа триангуляцией, потому что лазерная точка, камера и сам лазерный излучатель образуют своеобразный треугольник. Известна длина одной стороны АВ этого треугольника – расстояние между камерой и лазерным излучателем (рис. 12а). Известен также угол лазерного излучателя α . А вот угол камеры β можно определить по расположению лазерной точки в поле обзора камеры [15]. Эти три показателя полностью определяют форму и размер треугольника (рис. 12б) и указывают на расположение угла лазерной точки.

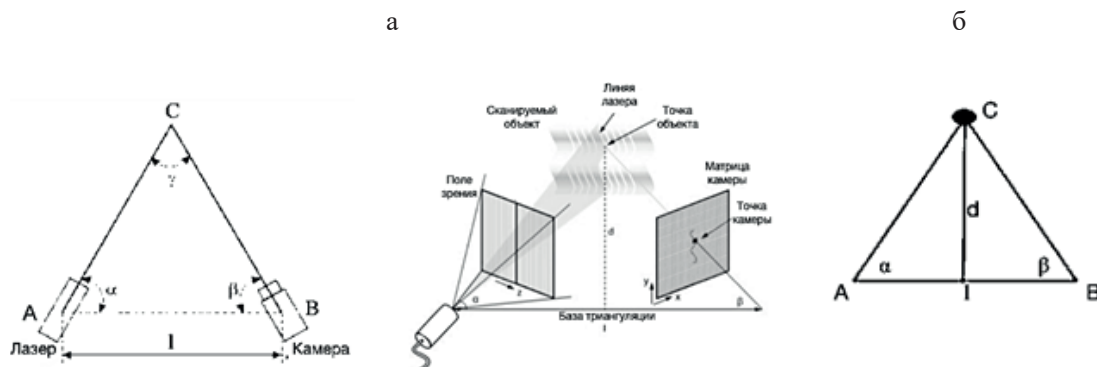


Рис. 12. Геометрия построения триангуляционных систем.

В большинстве случаев, чтобы ускорить процесс получения данных, вместо лазерной точки пользуются лазерной полосой.

Для определения координат точки на плоскости необходимо найти высоту d (расстояние от точки С до базы триангуляции) в треугольнике ABC (рис.12б), для чего воспользуемся формулой определения катетов в полученных прямоугольных треугольниках:

$$d = \frac{l \cdot \sin(\alpha) \cdot \sin(\beta)}{\sin(\alpha + \beta)} \quad (1)$$

Чтобы построить 3D-модель объекта, необходимо знать пространственные координаты. Получить их можно, рассмотрев модель на рис. 13.

Зная координаты на плоскости, можно найти координаты для построения 3D-модели по следующим формулам:

$$X = \frac{\tan(\alpha) \cdot l \cdot x}{f + x \cdot \tan(\alpha)} \quad (2)$$

$$Y = \frac{\tan(\alpha) \cdot l \cdot y}{f + x \cdot \tan(\alpha)}, \quad (3)$$

$$Z = \frac{\tan(\alpha) \cdot l \cdot f}{f + x \cdot \tan(\alpha)}, \quad (4)$$

Дальность действия сканеров такого типа составляет от 10 см до 25 м, ошибки в измеряемых углах, вызванные влиянием атмосферы (рефракцией и затуханием электромагнитных колебаний), практически не оказывают влияния на результаты измерений. Точность получения пространственных координат точек объекта триангуляционными сканерами составляет от 50 мкм до 0.3 мм и в основном зависит от величины измеряемого расстояния, инструментальных ошибок прибора, методических ошибок, связанных с точностью математических решений, положенных в основу управляющего программного продукта сканера, а также от материала, текстуры и формы сканируемого объекта.

Идеальными для сканирования триангуляционным сканером являются однородные отражающие поверхности, так как это позволяет избежать ошибок при определении углов.

Если объект или сканер переместится в пространстве, то результаты сканирования будут ложными. Поэтому так важно устанавливать и объект, и сканер на фиксированной платформе и свести возможность вибрации к минимуму. Следовательно, сканирование объектов в движении практически невыполнимо.

4.3. Сканирование структурированным светом

3D-сканеры, работающие по технологии структурированного света, как правило, состоят из источника структурированного света – проектора и нескольких видеокамер. Проектор проецирует на сканируемый объект световую сетку, форма и искажения которой фиксируются видеокамерами. Алгоритмы обработки изображений и триангуляции преобразуют эти искажения в облако 3D-точек. Облако точек можно использовать непосредственно для анализа объекта или легко экспортировать в различные форматы моделирования САПР.

Для каждой камеры необходимо определить, будет ли данный пиксель непосредственно подсвечиваться проектором в каждом отображаемом изображении (рис. 14).

Преимуществами 3D-сканера, использующего структурированный свет, является скорость и точность работы.

Вместо сканирования одной точки в один момент времени структурированные сканеры сканируют одновременно несколько точек или все поле зрения сразу. Сканирование всего поля зрения занимает долю секунды, а сгенерированные профили являются более точными, чем лазерные триангуляции. Это полностью решает проблему искажения данных, вызванную движением. Кроме того, некоторые существующие системы способны сканировать даже движущиеся объекты в режиме реального времени.

4.4. Сканирование методом стереоскопии

Рассмотрим пассивный бесконтактный метод сканирования – стереоскопию. Сканеры, работающие по данному методу, не имеют источника света, используется отраженный свет из окружающей среды. Стереоскопические системы предусматривают использова-

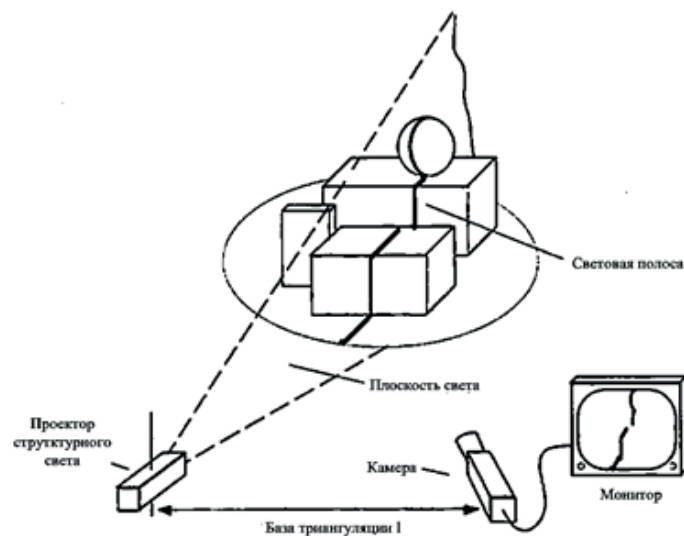


Рис. 14. Построение системы сканирования структурированным светом.

ние нескольких видеокамер. Камеры должны быть сонаправлены, но могут находиться в разных местах. Получая снимки с каждой из камер, определяют расстояние z (рис. 15а) до каждой точки изображения и затем вычисляют их координаты [16].

Для определения z (расстояния до точки P сканируемого объекта) нужно воспользоваться соотношениями подобия треугольников PNC_r , PMC_r , $p_l LC_l$ и $p_r RC_r$ (рис. 15б). Проекция точки P (сканируемого объекта) лежит в левой и правой плоскостях изображения в точках p_l и p_r . Установим за начало координат левый центр линзы:

$$z = \frac{b \cdot f}{(x'_l - x'_r)} \quad (5)$$

Таким образом может быть установлена глубина в различных точках сканируемого объекта. Из-за дискретности цифровых изображений значения неравенства являются це-

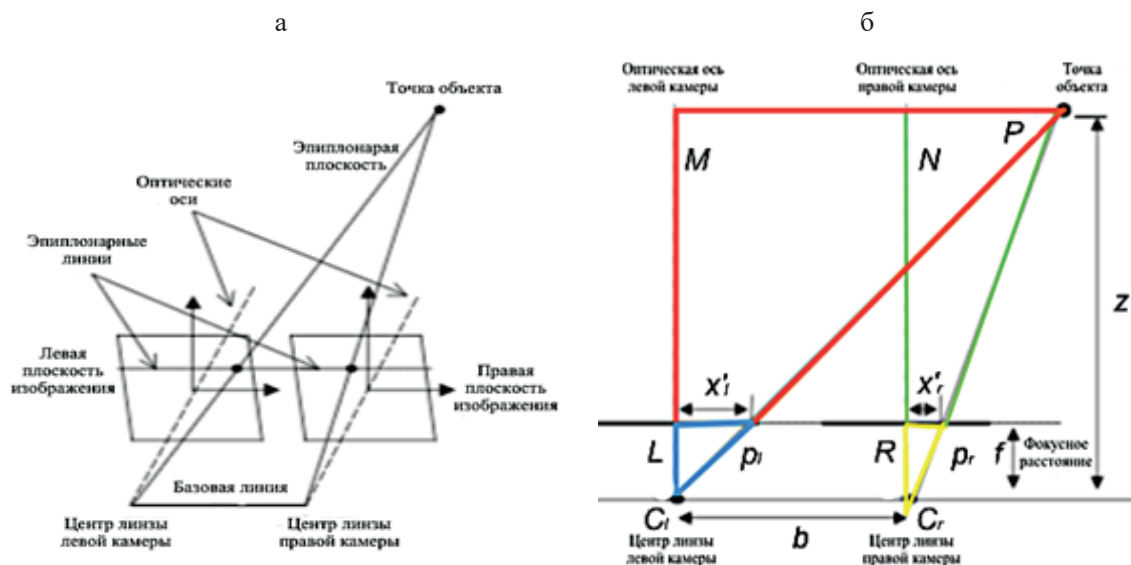


Рис. 15. Геометрия построения стереоскопических систем.

лыми числами. Точность вычисления глубины для заданной точки повышается за счет увеличения базового расстояния b . Однако такие широкоугольные методы стереоскопии создают другие проблемы. Например, когда базовое расстояние увеличивается, уменьшается доля всех точек облака, которые наблюдаются на обеих камерах. Более того, даже те области, которые видны обеими камерами, скорее всего, будут выглядеть по-разному на одном изображении по сравнению с соответствующими областями другого изображения из-за искажений, создаваемых перспективной проекцией, что затрудняет идентификацию сопряженных пар.

4.5. Прототипирование радиоэлектронных изделий

Рассмотрим процесс прототипирования (рис. 16). В общем случае процесс включает следующие этапы: визуальный анализ конструкции изделия; сканирование; создание и редактирование триангуляционной модели (при использовании бесконтактных методов сканирования, основанных на технологиях структурированного белого света и лазерного луча); построение базовых поверхностей; контроль базовых поверхностей; создание прототипа посредством 3D-печати; построение 3D-модели; контроль 3D-модели и ее доработка (при необходимости).

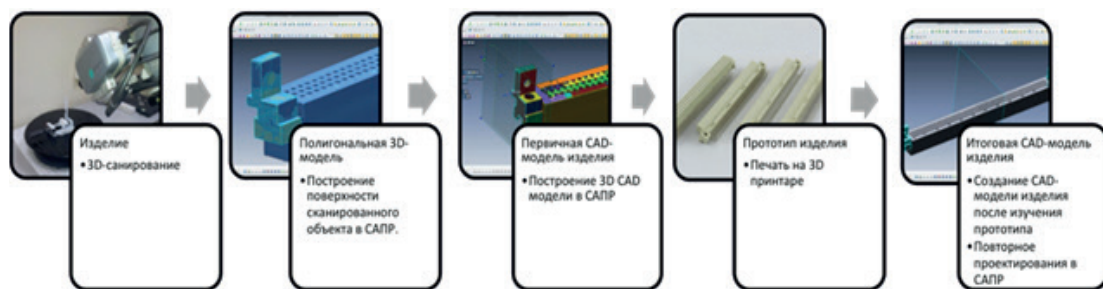


Рис. 16. Процесс прототипирования радиоэлектронных изделий.

Сначала происходит процесс сканирования объекта и создания облака точек, которые с помощью САПР моделируются в поверхности объекта через неоднородный рациональный В-сплайн, NURBS (математическая форма, применяемая в компьютерной графике для генерации и представления кривых и поверхностей) или же редактируемые CAD-модели (также известные, как объемные (монокитные) модели) (рис. 17).



Рис. 17. Этапы получения CAD-модели.

Существует несколько подходов, позволяющих получить параметрическую САПР-модель. Одни предполагают только экспорт NURBS-поверхности, оставляя САПР инженеру, чтобы завершить моделирование. Другие – используют данные сканирования для создания редактируемой функциональной модели.

Таким образом, комплекс технических мер противодействия стереолазерному и инфракрасному прототипированию может быть представлен следующими предложенными

техническими рекомендациями: создание шероховатой поверхности, использование отражающих материалов и использование полупрозрачных покрытий.

Действительно, одной из причин расходимости пучка лазера является шероховатость (неоднородность) поверхности. Когда лазерный луч попадает на край объекта, луч разделяется на две части. Одна часть луча отражается от края поверхности, а другая часть движется дальше, чтобы попасть на следующую поверхность (рис. 18а). В результате информация от одного лазерного импульса, который отправляется обратно в приемник (камеру), поступает из двух разных мест в пространстве. Координаты для такой точки относительно положения сканера будут вычисляться на основе среднего числа возвращенных сигналов, и поэтому координаты точки не будут соответствовать действительности.

При использовании сканирования высокого разрешения увеличивается вероятность попадания луча на край, и полученные данные будут показывать шум сразу за краями объекта. Сканеры с меньшей шириной луча помогают решить эту проблему, но остается ограничение по дальности действия, так как при ее увеличении увеличивается ширина луча.

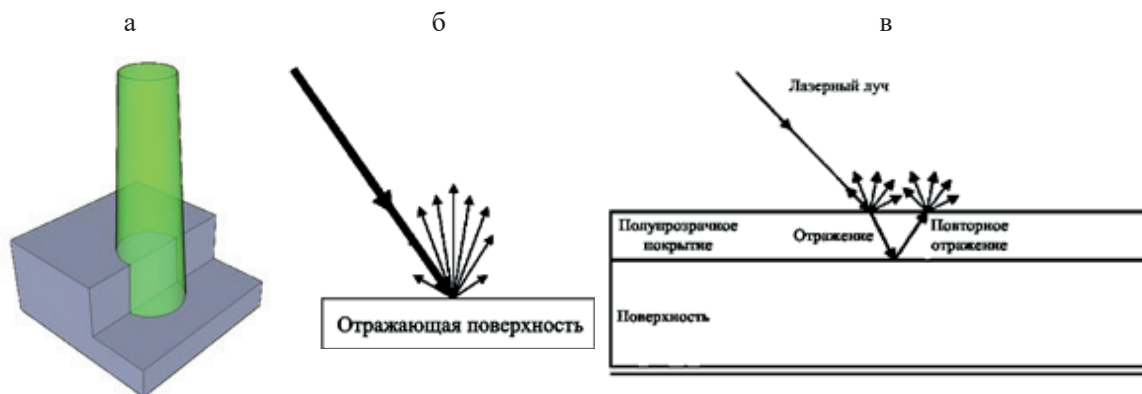


Рис. 18. Попадание луча лазера на поверхность объекта.

Поскольку сканеры регистрируют отражение лазерного луча от поверхности, необходимо учитывать физические законы отражения и оптические свойства материалов. Лучи монохроматического света обычно отражаются во многих направлениях (рис. 18б).

На лазерный луч влияет поглощение сигнала, проходящего через воздух, отражение материала сканируемого объекта и угол между лазерным лучом и нормалью к поверхности. Это означает, что для очень темных (черных) поверхностей, поглощающих большую часть видимого спектра, отраженный сигнал будет очень слабым, поэтому точность координат точки исказится. Поверхности с высокой отражательной способностью (т. е. яркие поверхности) дают более надежные и точные измерения диапазона. Однако, если отражательная способность объекта слишком высока (металлическая поверхность, светоотражающая лента и др.), лазерный луч полностью отклоняется в направлении зеркального отражения и попадает на другую поверхность. Отклонение приводит к тому, что получаемые координаты не являются координатами точки, на которую указывает лазер, или точка вообще не принадлежит сканируемой поверхности.

Помимо эффектов отражения, ряд материалов имеет полупрозрачное покрытие, которое позволяет лазерному лучу преломлять и отражать в самом материале. Эти эффекты приводят к сложению констант при измерении расстояния, что необходимо учитывать при вычислении (рис. 18в).

Заключение

Конструкторско-технологические решения производства печатных модулей и интегральных микросборок усложняются, приобретая комплексную направленность реализации оригинальных технических предложений с внедрением перспективных материалов и разработок, что усиливает спрос на специфическую деятельность, связанную с развитием процесса разработки новых методов спецпроектного реинжиниринга – параметрического прототипирования изделий РЭС. Одной из стратегий спецпроектных реинжиниринговых исследований является создание нового прототипного изделия и параметрическое исследование и диагностика с целью повышения его качества и надежности и т. д. Однако без знаний способов реинжиниринга невозможна организация противодействия ему, поэтому проводимые исследования в этой области имеют ключевую роль в обеспечении информационно-технической безопасности радиоэлектронной аппаратуры.

Рассмотренные в работе методы и средства спецпроектного прототипирования конструкций радиоэлектронных изделий и особенности технологий производства позволяют выработать комплекс технических мер противодействия спецпроектным исследованиям.

Литература:

1. Костин М.С., Воруничев Д.С. Реинжиниринг радиоэлектронных средств: монография. М.: Московский технологический университет (МИРЭА), 2018. 132 с.
2. Костин М.С., Воруничев Д.С., Марков Д.В. Реинжиниринговые исследования печатных плат с многослойной топологией в аспектах обеспечения технического противодействия // Оборонный комплекс – научно-техническому прогрессу России. 2018. № 1. С. 47–56.
3. Keng Tiong Ng. The art of PCB reverse engineering (standard edition): Unravelling the beauty of the original design. USA: Create Space Independent Publishing Platform, 2015. 372 p.
4. Asadizanjani N., Shahbazmohamadi S., Tehranipoor M., Forte D. Non-destructive PCB reverse engineering using X-ray micro computed tomography // Proceed. of the 41st International Symposium for Testing and Failure Analysis, ASM. Oregon, USA: ASM Int., 2015. P. 1–5.
5. Костин М.С., Воруничев Д.С. Тепловизионная электротермия топологии печатных плат в магнитном поле плоского ВЧ-индуктора // Журнал радиоэлектроники [электронный журнал]. 2017. № 9. URL: <http://jre.cplire.ru/jre/sep17/7/text.pdf> (дата обращения 09.11.2018).
6. Bukroyd A. In-Circuit Testing. USA: Butterworth-Heinemann, 2015. 168 p.
7. Костин М.С., Воруничев Д.С., Марков Д.В., Латышев К.В. Реинжиниринг радиоэлектронных цепей и сигналов печатных узлов с многослойной топологией в аспектах обеспечения технического противодействия // Оборонный комплекс – научно-техническому прогрессу России. 2018. № 3. С. 49–56.
8. Castillo-León J., Svendsen W. Lab-on-a-Chip devices and micro-total analysis systems: a practical guide. USA: Springer, 2015. 243 p.
9. Flich J., Bertozzi D. Designing Network On-Chip Architectures in the Nanoscale Era. USA: Chapman and Hall/CRC, 2010. 528 p.
10. Li W., Wasson Z., Seshia S. Reverse engineering circuits using behavioral pattern mining

// In: Hardware-Oriented Security and Trust (HOST), International Symposium on IEEE. USA: IEEE, 2012. P. 83–88.

11. Guin U., DiMase D., Tehranipoor M. Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead // J. Electronic Testing. 2014. V. 30. № 1. P. 9–23.

12. Curtis S.K., Harston S.P., Mattson C.A. The fundamentals of barriers to reverse engineering and their implementation into mechanical components // Res. Eng. Design. 2011. V. 22. № 4. P. 245–261.

13. Böhm Ch., Hofer M. Physical Unclonable Functions in Theory and Practice. USA: Springer Science & Business Media, 2012. 270 p.

14. Середович В.А., Комиссаров А.В., Комиссаров Д.В., Широкова Т.А. Наземное лазерное сканирование: монография. Новосибирск: СГГА, 2009. 261 с.

15. Akyol O., Duran Z. Low-cost laser scanning system design // J. Russ. Laser Res. 2014. V. 35. № 3. P. 244–251.

16. Torrance R., James D. The State-of-the-Art in IC Reverse Engineering // In: Cryptographic Hardware and Embedded Systems (CHES) // Lecture Notes in Computer Science. Berlin: Springer, 2009. V. 5747. P. 363–381.

References:

1. Kostin M.S., Voronichev D.S. Reengineering of radio electronic equipment: monograph. Moscow: Moscow Technological University (MIREA), 2018. 132 p. (in Russ.)

2. Kostin M.S., Voronichev D.S. Reengineering study of PCB with multi-layer topology in aspects ensuring technical counteraction. *Oboronnyy kompleks – nauchno-tekhnicheskomu progressu Rossii* (Defense complex – for scientific and technical progress of Russia). 2017; 1: 47-56. (in Russ.)

3. Keng Tiong Ng. The art of PCB reverse engineering (standard edition): Unravelling the beauty of the original design. USA: Create Space Independent Publishing Platform, 2015. 372 p.

4. Asadizanjani N., Shahbazmohamadi S., Tehranipoor M., Forte D. Non-destructive PCB reverse engineering using X-ray micro computed tomography. *Proceed. of the 41st International Symposium for Testing and Failure Analysis, ASM*. Oregon, USA: ASM Int., 2015. P. 1-5.

5. Kostin M.S., Voronichev D.S. Thermal vision electrothermia of the topology of PCB in the magnetic field of the flat HF-inductor. *Zhurnal radioelektroniki* (Electronic network journal) [electronic network journal]. 2017; 9. URL: <http://jre.cplire.ru/jre/sep17/7/text.pdf>. (in Russ.)

6. Bukroyd A. In-Circuit Testing. USA: Butterworth-Heinemann, 2015. 168 p.

7. Kostin M.S., Voronichev D.S., Markov D.V., Latyshev K.V. Reengineering of electronic circuits and signals of node PCB with multi-layer topology in aspects ensuring technical counteraction. *Oboronnyy kompleks – nauchno-tekhnicheskomu progressu Rossii* (Defense complex – for scientific and technical progress of Russia). 2018; 3: 49-56. (in Russ.)

8. Castillo-León J., Svendsen W. Lab-on-a-Chip devices and micro-total analysis systems: a practical guide. USA: Springer, 2015. 243 p.

9. Flich J., Bertozzi D. Designing Network On-Chip Architectures in the Nanoscale Era. USA: Chapman and Hall/CRC, 2010. 528 p.

10. Li W., Wasson Z., Seshia S. Reverse engineering circuits using behavioral pattern mining. In: Hardware-Oriented Security and Trust (HOST), International Symposium on IEEE.

USA: IEEE, 2012. P. 83-88.

11. Guin U., DiMase D., Tehranipoor M. Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead. *J. Electronic Testing*. 2014; 30(1): 9-23.

12. Curtis S.K., Harston S.P., Mattson C.A. The fundamentals of barriers to reverse engineering and their implementation into mechanical components. *Res. Eng. Design*. 2011; 22(4): 245-261.

13. Böhm Ch., Hofer M. Physical Unclonable Functions in Theory and Practice. USA: Springer Science & Business Media, 2012. 270 p.

14. Seredovich V.A., Komissarov A.V., Komissarov D.V., Shirokova T.A. Terrestrial laser scanning: monograph. Novosibirsk: SGGa (Siberian State Academy of Geodesy) Publ., 2009. 261 p. (in Russ.)

15. Akyol O., Duran Z. A low-cost laser scanning system design. *J. Russ. Laser Res.* 2014; 35(3): 244-251.

16. Torrance R., James D. The State-of-the-Art in IC Reverse Engineering. Crypto-graphic Hardware and Embedded Systems (CHES). *Lecture Notes in Computer Science*. Berlin: Springer, 2009; 5747: 363-381.

Об авторах:

Костин Михаил Сергеевич, кандидат технических наук, доцент кафедры конструирования и производства радиоэлектронных средств Института радиотехнических и телекоммуникационных систем ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

Воруничев Дмитрий Сергеевич, заместитель директора Института радиотехнических и телекоммуникационных систем ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

Корж Дмитрий Алексеевич, инженер кафедры конструирования и производства радиоэлектронных средств Института радиотехнических и телекоммуникационных систем ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

About the authors:

Mikhail S. Kostin, Ph.D. (Engineering), Associate Professor of the Chair of Design and Production of Radio Electronic Equipment, Institute of Radio Engineering and Telecommunication Systems, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow 119454, Russia).

Dmitriy S. Vorunichev, Deputy Director of the Institute of Radio Engineering and Telecommunication Systems, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow 119454, Russia).

Dmitriy A. Korzh, Engineer of the Chair of Design and Production of Radio Electronic Equipment, Institute of Radio Engineering and Telecommunications Systems, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow 119454, Russia).

Для цитирования: Костин М.С., Воруничев Д.С., Корж Д.А. Контрреинжиниринг радиоэлектронных средств // Российский технологический журнал. 2019. Т. 7. № 1. С. 57–79. DOI: 10.32362/2500-316X-2019-7-1-57-79

For citation: Kostin M.S., Vorunichev D.S., Korzh D.A. Counterreengineering of electronic devices. *Rossiyskiy tekhnologicheskij zhurnal* (Russian Technological Journal). 2019; 7(1): 57-79. (in Russ.). DOI: 10.32362/2500-316X-2019-7-1-57-79