МИКРОЭЛЕКТРОННАЯ ЭЛЕМЕНТНАЯ БАЗА КОСМИЧЕСКИХ АППАРАТОВ: СОСТОЯНИЕ, ПРОБЛЕМЫ И ТЕНДЕНЦИИ РАЗВИТИЯ

MICROELECTRONIC COMPONENT BASE OF SPACECRAFT: STATUS, PROBLEMS AND TENDENCIES OF DEVELOPMENT

УДК 621.3.049.77:629.78(045)

БЕЛОУС АНАТОЛИЙ ИВАНОВИЧ
Д. т. н., заместитель генерального директора

СОЛОДУХА ВИТАЛИЙ АЛЕКСАНДРОВИЧ
К. т. н., генеральный директор

ОАО «ИНТЕГРАЛ» — управляющая компания холдинга «ИНТЕГРАЛ»
220108, г. Минск, Республика Беларусь,
ул. Казинца И. П., 121А, к. 327
+375 17 212-24-61

BELOUS ANATOLY I.
Sc.D, Deputy General Director

SALADUKHA VITALI A.
Ph.D, General Director

INTEGRAL JSC — INTEGRAL Holding Managing Company
Room 327, Build. 121A, Kazintsa I. P. St.,
Minsk, Republic of Belarus, 220108
+375 17 212-24-61

Решение задачи повышения надежности бортовой электронной аппаратуры космических аппаратов на уровне микроэлектронных компонентов. Затрагиваются вопросы обеспечения требуемых уровней надежности разрабатываемой отечественной ЭКБ, а также выявления контрафакта и аппаратных закладок при использовании импортных комплектующих и аутсорсинга при разработке и изготовлении ЭКБ.

Ключевые слова: ракетно-космическая техника; электронная компонентная база; тяжелые заряженные частицы; дестабилизирующие факторы космического пространства; аппаратная закладка; бортовая электронная аппаратура космических аппаратов.

The article deals with solving the task of enhancing reliability of the onboard electronic equipment of spacecraft at the level of microelectronic components. It highlights the aspects of ensuring the required levels of reliability of the developed national electronic component base, as well as revealing the counterfeit and backdoors when using the imported components and outsourcing during development and fabrication of the electronic component base.

Keywords: rocket-space equipment; electronic component base; heavy charged particles; destabilizing factors of outer space; backdoor; onboard electronic equipment of spacecraft.

ВВЕДЕНИЕ

Развитие современной ракетно-космической техники (РКТ) ставит перед разработчиками бортовой электронной аппаратуры жесткие требования — постоянное повышение надежности, улучшение габаритно-массовых характеристик, увеличение функциональных возможностей, снижение величины потребляемой мощности и повышение сроков ее активного существования. В последнее время к этим требованиям в связи с возникновением новых задач добавились требования обеспечения аппаратной безопасности — защиты от внедряемых злоумышленниками аппаратных троянов (аппаратных закладок).

Решение всех этих задач требует активного использования новых технологий и новых технических решений как на уровне электронных блоков, так и на уровне микроэлектронных компонентов: микросхем, «систем-на-кристалле» (СНК) и «систем-в-корпусе» (СВК).

Радиоэлектронная аппаратура (РЭА) является значимой составной частью как космической техники, так и современных высокоточных систем вооружения и военной техники, определяя эффективность их функционирования и живучесть в различных экстремальных условиях применения.

Можно выделить следующие основные факторы открытого космоса, негативно влияющие на системы и устройства космических аппарата (КА), включая бортовую радиоэлектронную аппаратуру [1]:

- воздействие космической радиации на КА;
- микрометеоритное воздействие на КА;
- наведенные электромагнитные импульсы.

Исходя из анализа известных статистических данных по отказам [1], надежность бортовой радиоэлектронной аппаратуры определяется в значительной степени используемой электронной компонентной базой (ЭКБ), а именно: ее устойчивостью к статическому электричеству, ионизирующему и электромагнитному излучениям. Поэтому к ЭКБ, применяемой в ракетно-космической технике, предъявляются крайне жесткие требования. В частности, к основным особенностям ЭКБ, применяемой в РКТ, относятся:

- широкая функциональная номенклатура (не менее 1500 типономиналов);
- крайне малая серийность (от 10–15 шт.(!) до 100 тыс. шт. на протяжении всего жизненного цикла изделия;
- высокие требования к надежности (безотказность, ресурс, сохраняемость), наработка на отказ не менее 150 000 часов;

- стойкость к воздействию ионизирующих излучений космического пространства (накопленная доза — от 50 до 150 крад), других специфических дестабилизирующих факторов космического пространства (ДФ КП), воздействие тяжелых заряженных частиц (ТЗЧ) (пороговое значение линейных потерь энергии (ЛПЭ) не менее 60 МэВ·см^2/мг);
- расширенный температурный диапазон (от −60 до +125 °С);
- необходимость обеспечения длительных сроков безотказной работы (15 лет и более).

Уже это краткое перечисление особенностей ЭКБ для РКТ говорит о том, что развитие космической микроэлектроники идет своим путем, несколько отличным от магистрального пути развития электроники общепромышленной. Прежде всего, это касается крайне низких потребных объемов выпуска, одним из следствий чего является высокая цена таких микросхем.

ИСТОЧНИКИ ПОСТАВОК ЭКБ ДЛЯ БОРТОВОЙ АППАРАТУРЫ КА

На рис. 1 представлены основные источники поставок различных категорий ЭКБ для бортовой аппаратуры КА.

Так, в настоящее время отечественные разработчики и изготовители бортовой аппаратуры для космических аппаратов используют следующие основные источники поставок ЭКБ:

- импортные изделия категорий military и SPACE;
- импортные изделия категории INDUSTRIAL;
- отечественные изделия специального и двойного применения.

Хотя каждый из этих источников имеет свои достоинства и недостатки, сразу же следует отметить, что использование импортной ЭКБ категорий military и SPACE в конструкции КА является крайне нежелательным в силу следующих основных причин:

1. Согласно правилам ITAR экспорт ЭКБ категорий military (для использования в военных системах) и space (радиационностойкие комплектующие) для космических применений возможен только с разрешения Госдепартамента США.

2. Возможна поставка изделия с внедренными злоумышленниками вредоносными программными и аппаратными закладками (аппаратные трояны).

3. Необходимость предоставления служебной информации о цели использования в конечном изделии (сертификат конечного потребителя) — обязательное условие подачи заявки на разрешение, предусматривающее обязательство обеспечения проверки соответствия сферы использования по первому требованию поставщика.

4. В отношении Российской Федерации, Республики Беларусь, Китайской Народной Республики во многих случаях по умолчанию применяется презумпция отказа (без объяснения причин, особенно в поставках ЭКБ категорий military и space (радиационно-стойкие комплектующие)).

Использование посредников и неофициальных источников также ненадежно и к проблеме внесения программных и аппаратных закладок добавляет еще проблему поставки контрафактных микросхем.

В последнее время в силу целого ряда объективных причин отечественные разработчики КА все чаще стали использовать более дешевую импортную ЭКБ категории качества INDUSTRIAL. Действительно, качественно проведенная дорогостоящая процедура скрининга (отбраковочных испытаний) теоретически позволяет отсеять большую часть потенциально ненадежных изделий. Тем не менее, конструкция изделий категории качества INDUSTRIAL в принципе не предусматривает (не гарантирует) обеспечения радиационной стойкости, поэтому

Рис. 1. Основные источники поставки ЭКБ для бортовой аппаратуры КА

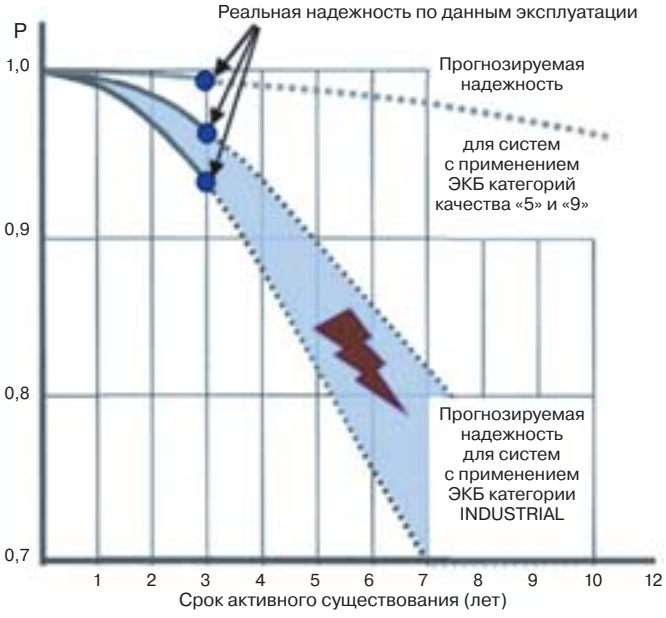


Рис. 2. Изменение надежности бортовой аппаратуры КА, использующей различные категории ЭКБ [2]

вероятность отказа на орбите таких изделий гораздо выше, чем у изделий категорий military и space.

На рис. 2 [2] представлена динамика изменения надежности бортовой электронной аппаратуры КА в течение всего срока активного существования аппарата для всех трех вариантов использования ЭКБ: категорий INDUSTRIAL, military и space.

Использование серийных отечественных изделий двойного и специального применения из «Перечня электронной компонентной базы, разрешенной для применения в разработке, модернизации, производстве и эксплуатации вооружения, военной и специальной техники» тоже не является панацеей, т. к., несмотря на все многолетние разговоры чиновников Минпромторга РФ и «Роскосмоса» об унификации, использовании «близких» изделий-заменителей, это всегда некоторый компромисс между заказчиком и разработчиком (уступка, например, по параметрам, производительности, габаритам). И зачастую цена этого компромисса в итоге оказывается неприемлемо высока. Тогда приходится создавать требуемую ЭКБ в рамках целевых проектов, как правило, с бюджетным финансированием в рамках федеральных целевых программ, что занимает как минимум 2–3 года с момента утверждения.

МЕТОДЫ ПОВЫШЕНИЯ РАДИАЦИОННОЙ СТОЙКОСТИ МИКРОСХЕМ

Обеспечение требуемых уровней стойкости/надежности разрабатываемой ЭКБ достигается применением целого комплекса различных методов, технических решений и системных подходов, большинство из которых наиболее детально рассмотрено в вышедших в 2017 году в издательстве ARTECH HOUSE (США, Англия) книгах Space Microelectronics Volume 1: Modern Spacecraft Classification, Failure, and Electrical Component Requirements и Space Microelectronics Volume 2: Integrated Circuit Design for Space Applications [2, 3].

В частности, на рис. 3 представлен один из вариантов упрощенного маршрута проектирования радиационно-стойких микросхем, включающий в себя проведение целого ряда дополнительных технологических операций, для реализации которых необходимо разрабатывать и изготавливать специальное технологическое и контрольно-измерительное оборудование.

Поэтому введение в производственный процесс дополнительных процедур и операций (1–5, 7–9) обуславливает и более высокую стоимость соответствующих НИОКР, большую продолжительность сроков реализации проекта, более высокую цену конечных изделий.

Что касается дополнительных испытаний, то их стоимость обычно определяется комплексами стандартов и дополнительными требованиями заказчиков, но в любом случае это увеличение конечной цены изделия. В существующих отечественных стандартах большинство методик испытаний ЭКБ на радиационную стойкость соответствуют имитации воздействий, присущих факторам ядерного взрыва (ЯВ). Но космическое пространство обладает совершенно иной спецификой. Это относительно низкие по сравнению с ЯВ по интенсивности электронное и протонное излучения от естественных радиационных поясов Земли, воздействующие на орбитальный космический аппарат в течение всего длительного времени активной работы, а также ТЗЧ и высокоэнергетические протоны.

Современные подходы к созданию специализированной ЭКБ, стойкой к дестабилизирующим факторам космического пространства, можно разделить на следующие большие группы [3]: технологические, конструктивные и схемотехнические. Кроме того, широко применяется обеспечение имитации (моделирование) влияния основных дестабилизирующих факторов (ДФ) космического пространства на этапе проектирования ЭКБ, а также моделирование условий космического пространства при лабораторных испытаниях экспериментальных образцов и готовой продукции на стойкость к новым, ранее не принимавшимся во внимание, деструктивным факторам космического пространства. К последним следует отнести пока широко не обсуждаемые в открытой печати проблемы воздействия так называемой космической пыли (SPACE DUST) на механизмы, электронную бортовую аппаратуру и человека [4].

К известным технологическим методам повышения радиационной стойкости следует отнести использование «специализированных» техпроцессов изготовления СБИС и материалов. Так, в частности, это давно известные разновидности технологии «кремний-на-сапфире» (КНС), «кремний-на-изоляторе» (КНИ), специализированные операции легирования и т. д. Все эти способы чрезвычайно дорогостоящи, и потому в настоящее время они реализованы только на небольшом числе мировых фабрик. В частности, ведущими производителями подобных изделий являются компании Honeywell (США), Peregrine Semiconductors (США) и ряд других.

К схемотехническим методам повышения радиационной стойкости, в т. ч. к ТЗЧ, относятся применение специальных библиотек элементов с мажоритированием на уровне вентилей, кодеров, декодеров Хэмминга, т. н. «усиленных» библиотек элементов, отбор специальных библиотечных компонентов и ряд других приемов, не все из которых обычно публикуются в открытой печати. Основным достоинством такого подхода является возможность его реализации на существующих фабриках, обладающих стандартной (предназначенной для массовой продукции) технологией. Такой подход сегодня получил специальное название Rad Hard Design. Так, французская компания MHS обеспечивает «космическим микросхемам» гарантированную стойкость порядка 100 крад (по объемному кремнию). Аналогичным путем уже много лет действует компания Aeroflex, которая использует

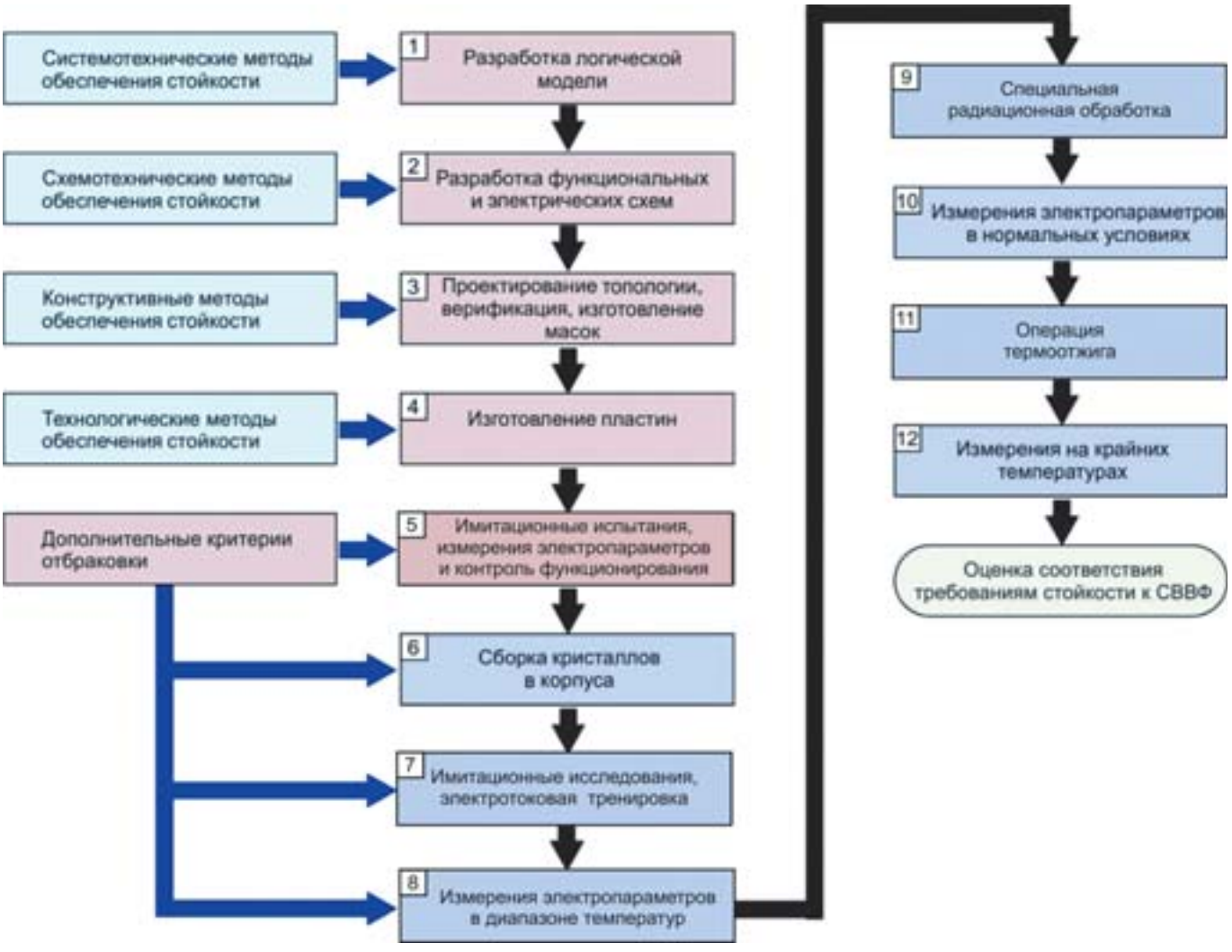


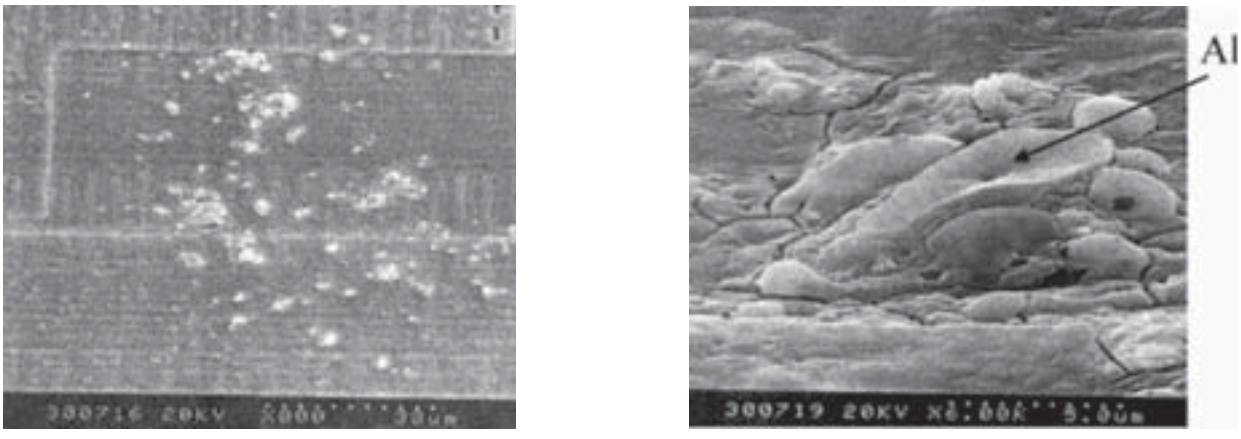
Рис. 3. Упрощенный маршрут проектирования ЭКБ двойного и специального назначения

обычные технологические линейки как собственные, так и ведущих производителей. При этом заказчик может использовать как уже существующие мощности ведущих зарубежных фабрик, так и производственные мощности отечественных предприятий: ОАО «НИИМЭ и Микрон», ОАО «Ангстрем», а также белорусского «Интеграла». Очевидно, что использование такого подхода обеспечивает повышение стойкости, сопоставимое с применением специальной технологии, но при существенно (в 5–7 раз) меньшей стоимости конечного изделия. Более подробно основные схемотехнические методы рассмотрены в работе [3].

К имитационным исследованиям, в частности, моделированию условий воздействия внешних факторов космического пространства на этапе испытания экспериментальных и опытных образцов ЭКБ, следует отнести использование специальных методик с применением специального оборудования и ускорителей частиц, позволяющих проводить испытания на устойчивость к воздействию потока частиц, сопровождающегося импульсным электромагнитным и ионизирующим излучением в лабораторных условиях, имитирующих космические. Здесь используются следующие методы испытаний и методики исследования, позволяющие определить устойчивость используемых материалов и базовых элементов микроэлектроники к воздействию основных деструктивных физико-химических факторов космического пространства: ударных волн, электромагнитного и ионизирующего излучений, эффектов сверхглубокого проникания частиц, с целью установить физические механизмы воздействия каждого из этих факторов, а затем целенаправленно разработать технологические и конструкторские решения для обеспечения защиты от их воздействия.

Отдельно следует отметить проблему разработки методов и оборудования для испытания материалов и базовых элементов бортовых электронных систем, в основу которых положен способ динамического нагружения испытуемого материала (изделия) высокоскоростным потоком частиц, имитирующий условия воздействия частиц «космической пыли», позволяющий регистрировать и измерять электрофизические параметры процессов взаимодействия потока таких частиц с испытуемыми объектами: импульс электромагнитного и ионизирующего излучения, ударно-волнового действия и проникания частиц; моделировать условия взаимодействия потоков частиц «космической пыли» с космическими аппаратами в лабораторных условиях и проводить на Земле испытания материалов и ЭКБ, применяемых в КА.

К сожалению, особенности этой темы пока не были опубликованы в отечественной и зарубежной научно-технической печати, поскольку в США и Англии эта тема официально закрыта для публикаций, а в России опубликованы только работы, относящиеся к частным моментам подобных исследований. Разве что иногда из телевизионных программ можно узнать отдельные эпизоды



а *б*

Рис. 4. Структурные дефекты в микросхемах после соударения с высокоскоростным потоком микрочастиц: а) включения в структуре микросхемы; б) оплавление и рост кристаллов

отечественных проектов в этой области, например, замена механических элементов (поручней) на орбитальном аппарате, поскольку космонавт Леонов повредил свои перчатки из-за эрозии этих поручней во время выхода в открытый космос.

На рис. 4 представлен внешний вид микросхем после воздействия на них таких высокоскоростных микрочастиц [4]. Здесь явно видны структурные нарушения (инородные включения, оплавление поверхности, рост объема отдельных фрагментов кристалла). В ряде случаев наблюдаются нарушения межсоединений в местах разварки проволоки к контактным площадкам и др.

Более подробно методы, материалы и специальное оборудование (ускорители частиц) рассмотрены в нашей работе [4], которая пока является первой публикацией на англоязычном книжном рынке, посвященной методическим, техническим и физическим аспектам этой проблемы.

К конструктивным способам повышения стойкости следует также отнести разработку специальных защитных материалов, использование специальных корпусов, методов локальной защиты и т. д. Получить высокую функциональность за приемлемую цену и с необходимыми массогабаритными характеристиками на сегодняшний день можно только с применением технологии интеграции кристаллов, изготовленных по различным технологиям в одном корпусе, т. е. с применением подхода (СВК).

ОСОБЕННОСТИ КОРПУСИРОВАНИЯ МИКРОЭЛЕКТРОННЫХ УСТРОЙСТВ КОСМИЧЕСКОГО НАЗНАЧЕНИЯ

В последнее время весьма актуальна проблема корпусирования микроэлектронных устройств для космических применений.

На рис. 5 в обобщенном виде представлена динамика развития корпусов микросхем, начиная с 1985 по 2015 гг. с привязкой к каждому новому поколению микроэлектронных технологий (от 0,25 мкм в 2000 г. до 40–28 нм в 2015 г.).

Как видно из этого рисунка, ежегодно на мировом рынке появляются несколько новых корпусных решений. К сожалению, не все типы этих корпусов пригодны для космических применений, поскольку большинство из них не решают одну из главных задач — ослабление эффектов влияния на кристалл радиационных воздействий и электромагнитных импульсов.

На рис. 6 представлены два варианта металлокерамических корпусов (отличаются только способом монтажа «крышки»), разработанных отечественным предприятием «Тестприбор». Использование таких корпусов существенно повышает их устойчивость к воздействию радиации, даже позволяет в отдельных случаях использовать кристаллы промышленной категории INDUSTRIAL для комплектации бортовой аппаратуры.

На рис. 7 представлена в обобщенном виде эволюция так называемой «объемной» (2D; 2,5D; 3D) сборки микроэлектронных устройств для космических применений, построенная в двух координатах: «уровень интеграции» и «функциональные возможности» с разбивкой этих показателей в свою очередь на три группы (низкий, средний, высокий) [5].

Наиболее существенные результаты в настоящее время были получены в области развития 3D-изделий на основе TSV-технологии (through silicon vias), когда за счет формирования сквозных кремниевых межсоединений (переходных отверстий) в кремниевых пластинах исключается операция разварки кристаллов в корпуса. Это позволяет обеспечить максимально возможный на момент выхода в печать этой книги уровень интеграции ИС. TSV-технология включает процессы формирования соединений, осаждения, заполнения, удаление металла с поверхности, утонения пластин, соединения/стекирования, инспектирования и тестирования.

Технология TSV позволяет также существенно увеличить объем информации, который можно записывать в микросхеме памяти бортового компьютера космической аппаратуры. Так как каждый кристалл в модуле памяти имеет одинаковую топологию, то возможно собирать 3D-модули, состоящие из абсолютно идентичных кристаллов, что позволяет многократно увеличивать объемы памяти для микросхемы по сравнению с однокристальными микросборками.

Следует привести характерный пример для понимания ситуации. Так, если бортовой компьютер известного американского космического аппарата Apollo-II, спроектированный специалистами Raytheon, с использованием более 4 тысяч микросхем и дискретных полупроводниковых приборов весил 32 кг, и при этом имел всего 36 Кбайт программной памяти, работал на тактовой частоте всего 2 МГц, то любой один современный процессор в подобном конструктивном исполнении, не выходя за габаритный размер 25 мм, может обеспечить на порядок более высокую производительность, чем весь бортовой управляющий комплекс Apollo-II.

Кроме техпроцесса выполнения сквозных переходных отверстий в кремниевых пластинах, используются дополнительные

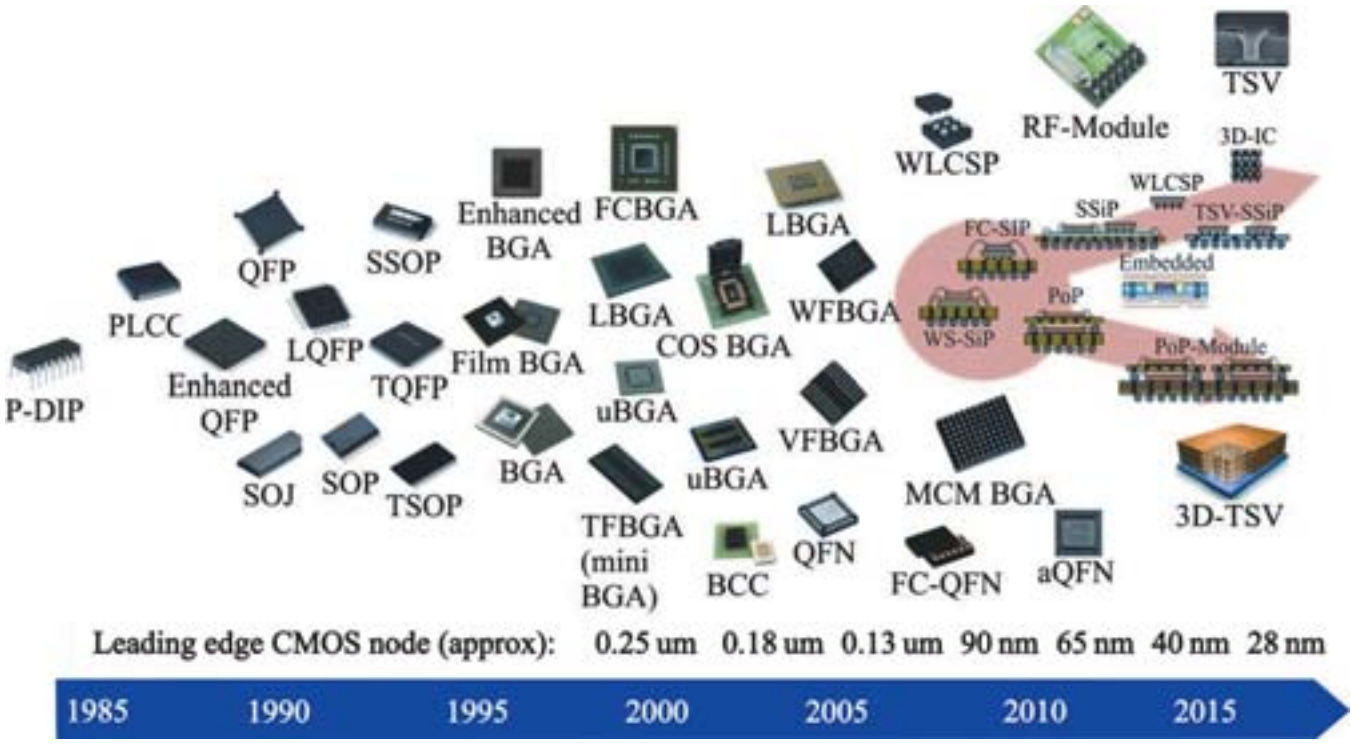


Рис. 5. Динамика развития конструктивных решений корпусов микросхем

операции утонения пластин, операции глубокого плазменного травления и операции заполнения переходных отверстий.

В зависимости от используемых проводящих материалов последовательности технологических операций различают два основных подхода при производстве 3D микросхем космического и военного назначения:

- Via First (выполнение переходных отверстий до формирования структур);
- Via Last (выполнение переходных отверстий после формирования структур).

При заполнении переходных отверстий соответствующим проводящим материалом (например, медью) до формирования структур (Via First) процесс заполнения отверстий не ограничен максимально допустимым пределом рабочей температуры для КМОП (450 °С). Данный подход не влияет на результирующий коэффициент выхода годных, но качественное заполнение отверстий является исключительно сложной в технологическом плане задачей. В случае заполнения переходных отверстий (Via Last) после формирования КМОП-структур результирующий коэффициент выхода годных понижается.

Следует отметить, что исторически начало технологии производства 3D микросхем было заложено в изделиях типа PoP (Package-on-Package — «корпус-на-корпусе»). Здесь уменьшение габаритов микроэлектронных изделий достигалось за счет монтажа корпусов в трехразмерные (3D) сборки с использованием межсоединений и коммутационных слоев, размещенных на самих корпусах. Такой прием давал разработчикам бортовых систем космических аппаратов возможность существенно сократить время передачи сигнала с одной микросхемы на другую, а также позволял использовать существующую технологию

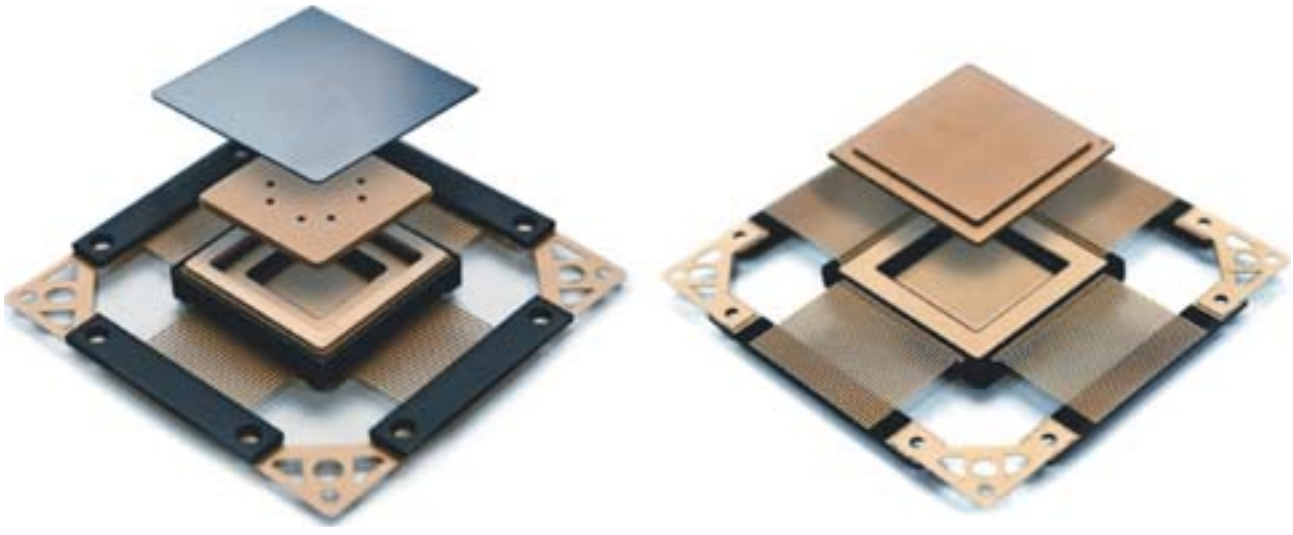


Рис. 6. Варианты конструкции корпусов для микросхем с элементами радиационной защиты кристалла

Рис. 7. Упрощенная диаграмма динамики развития технологий сборки микроэлектронных устройств для космических применений

поверхностного монтажа и уже имеющееся оборудование для обеспечения значительно большей степени интеграции модулей.

На рис. 7 показана графическая интерпретация эволюции различных типов конструктивного оформления микроэлектронных модулей типа 3D, которая показывает все многообразие используемых разработчиками технологий и конструктивных решений.

Применение технологии TSV при сборке гибридных модулей обеспечило дополнительный импульс развитию устройств типа SiP (System-in-Package — «система-в-корпусе», СВК), логическим продолжением которого стал так называемый «интерпоузер» — единый элемент, собранный на кристальном уровне без применения промежуточных операций разварки проволочных выводов для коммутации элементов микросборки.

Следует остановиться на рассмотрении ряда проблем, связанных с развитием этих новых направлений корпусирования.

1. Одной из основных проблем, с которыми сталкиваются разработчики подобных пространственно-ограниченных систем, является необходимость обеспечения достаточного количества требуемых им портов ввода-вывода, необходимых для организации быстрой связи с многочисленными важными устройствами современного космического аппарата, и при этом размещения их в таком небольшом корпусе. Эта проблема системно решается путем предоставления полной гибкости (универсальности) в использовании таких портов. Здесь ни один вывод не должен быть «лишним». Например, если проектируемая система не требует часто использовать последовательный интерфейс типа SPI, для него не нужно проектировать и специальные выводы, а освобожденные выводы должны быть переадресованы другой, более нужной цифровой периферии.

Что очень важно, такое переназначение в универсальной бортовой системе можно осуществить программным путем (динамическое программирование).

2. Обычно все заказчики (NASA, «Роскосмос», военные) хотят получить от разработчиков определенные гарантии работы в экстремальных условиях. На языке военных это называется «гарантия функционирования в четырех зонах». Эта концепция означает обеспечение не только функционирования, но и обеспечение всех уровней динамических, статических и электрических параметров электронной системы (СВК) во всем оговоренном диапазоне рабочих температур, напряжений питания и уровней входных сигналов.

3. Одной из основных конструкторских проблем становится проблема теплоотвода, которая в общем случае решается путем соответствующего размещения специальных теплопроводящих слоев, никак не связанных с проводящими межсоединениями, по которым передаются информационные и управляющие сигналы и обеспечивается питание базовых элементов. Здесь большинство ноу-хау заключается в особенностях использования разнообразных способов соединений между слоями интерпоузера, которые в любом случае сводятся к вертикальной сборке кристаллов в так называемый «стек» (chip stacking), где имеется множество различных вариантов соединений между горизонтальными слоями. Простейшее решение — кристалл памяти размещают непосредственно над кристаллами центрального процессора, длины межсоединений сокращаются почти в 10 раз и при этом снижается энергопотребление.

Надо сказать, что создание 3D сборок — это в основном теперь не научная, а чисто инженерная задача, но здесь есть серьезные проблемы и для ученых.

4. Научные проблемы в области 3D сборки сегодня сфокусированы в области разработки альтернативных подходов к передаче данных между горизонтальными слоями. В частности, в настоящее время разработан ряд так называемых «бесконтактных» методов обмена информацией между слоями 3D конструкции. Один из вариантов — включение миниатюрных индуктивностей в конструкции КМОП-кристаллов, что исключает механические связи, но повышает требования к точности согласования этих микроиндуктивностей между различными горизонтальными слоями. К сожалению, пока таким образом можно передавать только данные, а для разводки питания по слоям необходимо использовать омические соединения. Эта технология, как разновидности TSV,

получила собственное название — TCI (Through Chip Interface) — «интерфейс через кристалл».

Однако все эти проблемы в конечном итоге будут успешно разрешены, и ракетно-космическая промышленность в самое ближайшее время поставит разработчикам новые, не менее интересные проблемы: ведь интеграционные процессы — это и есть суть современной микроэлектроники.

НОВЫЕ УГРОЗЫ В КОСМИЧЕСКОЙ ЭЛЕКТРОНИКЕ: АППАРАТНЫЕ ТРОЯНЫ В МИКРОСХЕМАХ

Аппаратная закладка (*hardwareTrojan*, *hardware backdoor*) — вредоносная модификация исходной схемы. Результатом работы подобной аппаратной закладки может быть как полное выведение бортовой электронной системы из строя, так и нарушение ее нормального функционирования, например, несанкционированный доступ к информации, ее изменение по командам злоумышленника или блокирование всех или отдельных функций.

Относительная простота внедрения таких аппаратных закладок в современную микросхему не может не вызывать беспокойства. Модификации могут быть внесены в любую аппаратную часть микросхемы как на этапе разработки, так и в процессе производства.

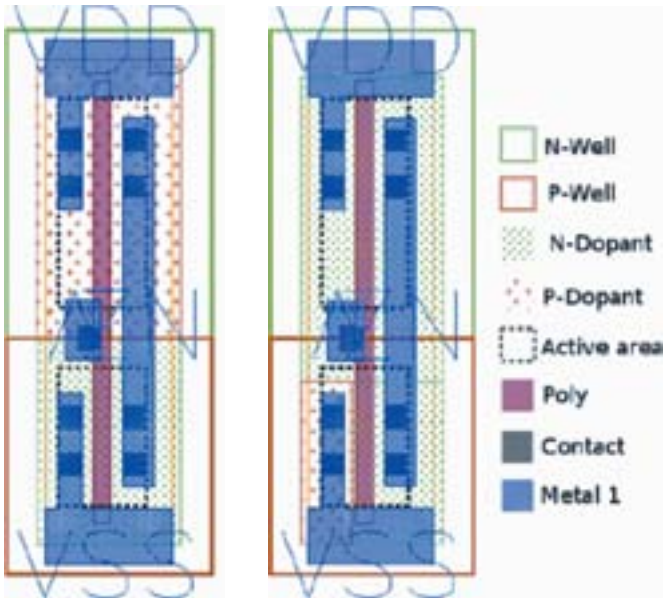
Благоприятным условием для их внедрения является использование сторонних (импортных) комплектующих и аутсорсинг при разработке и изготовлении: аппаратные закладки могут быть внедрены злоумышленником в состав IP-блоков библиотек и САПР, используемых любым отечественным разработчиком при проектировании ЭКБ. Аппаратные закладки могут быть внесены также и поставщиком фаундри-услуг на этапе изготовления в соответствии с поставленной злоумышленником задачей.

Таким образом, в группе риска находятся не только импортная ЭКБ (на Западе самым серьезным образом на уровне правительства занимаются этой проблемой), но и отечественная, спроектированная с использованием зарубежных библиотек и ПО, либо изготовленная по фаундри.

Выявление аппаратных закладок является весьма непростой процедурой и требует знания специальных методик, специального оборудования и высокой квалификации. Сегодня пока широко применяются два следующих подхода:

Анализ логической структуры чипа и нахождение подозрительных блоков. В случае с готовым кристаллом — полный реинжиниринг — обратное проектирование, т. е. восстановление подробной электрической схемы путем последовательного удаления и фотографирования каждого из активных и пассивных слоев чипа (в современных чипах может быть более десяти таких слоев) и дальнейшего сравнения с исходной схемой. Упрощенный вариант — это метод сканирования чипа рентгеновскими лучами, который позволяет анализировать структуру металлической разводки.

Применение специальных методик тестирования — например, «фаззинг» (fuzz testing). Путем посылки нестандартных запросов можно вычислить некоторые созданные или измененные со злым умыслом блоки тестируемой микросхемы. Подобная методика помогла Сергею Скоробогатову, бывшему студенту МИФИ, ныне сотруднику отдела безопасности в компьютерной лаборатории Кембриджского университета, совместно с коллегами из другой компании вычислить подобный «бэкдор» в китайском чипе PROAsic 3 компании Microsemi, что является пока одним из первых задокументированных фактов.



а *б*

Рис. 8. Сравнение фрагментов топологии микросхемы с «закладкой»: а) исходная топология; б) топология с внедренным аппаратным трояном (постоянно включенный транзистор)

Однако ни одна технология поиска и выявления закладок на сегодня не дает 100 % гарантии!

Например, группа ученых из США, Швейцарии и Германии разработала особый вид аппаратных троянов, которые практически невозможно засечь ни визуально, ни с помощью тестов. Ученые Becker, Regazzoni, Paar и Burleson совместно исследовали возможность и последствия умышленного нарушения процесса легирования (doping), а именно: изменения концентрации легирующей примеси в отдельных участках топологии кристалла, уже прошедшего все технологические операции изготовления микросхемы (до этапа сборки кристалла в корпус). По сути, меняется только маска легирования, даже количество легирующих примесей может остаться примерно таким же. Специалисты считают, что подобное вмешательство незаметно даже при сканировании электронным микроскопом и сравнении с «золотым» эталоном (не говоря о том, что такой эталон тоже может быть «атакован» злоумышленником).

В итоге (рис. 8) получается дефектный транзистор, который может всегда иметь только одно фиксированное напряжение на выходе или создавать ток утечки. В качестве примера, как подобная диверсия может повлиять на безопасность, ученые привели широко разрекламированный как абсолютно безопасный генератор случайных чисел в Intel-овском Ivy Bridge, в частности потому, что и его дизайн, и способ тестирования есть в открытом доступе.

Опасность отказов бортовой электронной аппаратуры космических аппаратов и различных современных систем вооружений вполне реальна и осознана. В США, например, в рамках Министерства обороны (DoD — Department of Defense) создан и давно функционирует так называемый совместный федеративный центр сертификации Joint Federated Assurance Center (JFAC), объединяющий ведущие профильные лаборатории и инженерные подразделения кибербезопасности целого ряда ведомств (Army, Navy, AF, NSA, DMEA DISA, NRO и MDA) с целью оперативного выявления программных и аппаратных закладок, а также

контрафактных изделий. Разработана долговременная стратегия по созданию доверенных и сертифицированных каналов разработки и производства и поставки изделий микроэлектроники.

ХОЛДИНГ «ИНТЕГРАЛ» И КОСМОС

Разработка и производство ЭКБ для систем вооружения и ракетно-космической техники является традиционным направлением деятельности ОАО «ИНТЕГРАЛ».

Именно за участие в космических программах СССР предприятие было награждено двумя орденами.

За более чем 40 лет работы в данной сфере предприятием накоплен значительный опыт проектирования и организации производства ЭКБ, а именно: высоконадежных интегральных микросхем и дискретных полупроводниковых приборов с повышенной устойчивостью к дестабилизирующим факторам.

Сегодня номенклатура выпускаемой продукции холдинга «ИНТЕГРАЛ» составляет более 2,2 тыс. типов интегральных микросхем, около 500 типов полупроводниковых приборов, 200 типов жидкокристаллических индикаторов и модулей, 150 видов изделий электронной техники. Причем микроэлектронная элементно-компонентная база (ЭКБ) специального и двойного назначения (категории качества «ВП» и «ОСМ») занимает значительную часть в номенклатуре.

Холдинг «ИНТЕГРАЛ» продолжает активно сотрудничать с российскими предприятиями ракетно-космической промышленности.

Из общего объема в 59,577 млн долл. США изделий категорий качества «ВП» и «ОСМ», поставленных в Российскую Федерацию, на сумму примерно 20 млн долл. США отгрузок пришлось на долю предприятий ФКА «Роскосмос».

НОВИЗНА ПОЛУЧЕННЫХ РЕЗУЛЬТАТОВ

Авторы считают, что в данной работе новыми являются следующие основные положения и результаты:

- источники поставок ЭКБ для космических и специальных применений должны быть пересмотрены — основным источником поставки должна стать продукция российской и белорусской микроэлектронной промышленности, осуществляемая под контролем соответствующих Представительств Заказчика;
- разработчикам бортовой аппаратуры космических аппаратов необходимо более активно использовать отечественные корпуса с элементами защиты от радиационных и электромагнитных воздействий;
- в области корпусирования микроэлектронных устройств космического и специального назначения наиболее актуальными на текущий момент являются проблемы обеспечения так называемых бесконтактных методов передачи информации между слоями 3D структур на основе индукционных и оптических методов, а также проблемы теплоотвода;
- в связи с появлением новых угроз кибербезопасности — встроенных в микросхемы аппаратных троянов (закладок) необходимо на правительственном уровне в срочном порядке разработать и реализовать комплекс технических и организационных мероприятий по противодействию этим угрозам, включая мероприятия по перепроверке уже полученных от зарубежных фаундри микросхем на предмет выявления подобных дефектов.

ЛИТЕРАТУРА:

1. Белоус А. И., Солодуха В. А., Шведов С. В. Космическая электроника. В 2-х томах. М.: Техносфера, 2015. — 1184 с.
2. Belous Anatoly, Saladukha Vitali, Shvedau Siarhei. Space Microelectronics Volume 1: Modern Spacecraft Classification, Failure, and Electrical Component Requirements // London, Artech House, 2017, p. 440, ISBN: 9781630812577.
3. Belous Anatoly, Saladukha Vitali, Shvedau Siarhei. Space Microelectronics Volume 2: Integrated Circuit Design for Space Applications // London, Artech House, 2017, p. 720, ISBN: 9781630812591.
4. Belous Anatoly, Saladukha Vitali, Shvedau Siarhei. Space Microelectronics Volume 3: High Velocity Microparticles // London, Artech House, 2017.
5. Васильев А. Современные технологии 3D-интеграции / Компоненты и технологии, 2010. — № 1. — С. 156–158.