УДК 004.056.5; 001.891.55
doi: 10.26583/bit.2024.1.01

Юлия М. Московская[1], Андрей Н. Денисов[2], Александр Ю. Никифоров[3]
[1]Акционерное общество «Экспериментальное научно-производственное объединение СПЕЦИАЛИЗИРОВАННЫЕ ЭЛЕКТРОННЫЕ СИСТЕМЫ», Каширское ш., 31, Москва, 115409, Россия
[2]НПК «Технологический центр», пл. Шокина, 1 стр. 7, Москва, Зеленоград, 124498, Россия
[3]Национальный исследовательский ядерный университет «МИФИ», Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: ymmos@spels.ru, https://orcid.org/0009-0008-7409-5619
[2]e-mail: A.Denisov@tcen.ru, https://orcid.org/0009-0009-6382-1141
[3]e-mail: aynik@spels.ru, https://orcid.org/0000-0002-2427-663X

СИСТЕМА ОБЕСПЕЧЕНИЯ КАЧЕСТВА ДОВЕРЕННОГО МИКРОЭЛЕКТРОННОГО ПРОИЗВОДСТВА

Аннотация. Доверенность как свойство изделий микроэлектроники в основном «закладывается» на стадии его разработки и обеспечивается гарантиями качества и надёжности, квалификацией и опытом разработчика, рациональным выбором ключевых технических решений, реализующих заданные функциональные и эксплуатационные характеристики, а также парированием основных угроз его безопасности. Аналогично формирование доверенности изделий при их опытном и серийном производстве обеспечивается результатами эффективного взаимодействия и рационального сочетания двух систем: обеспечения качества и безопасности предприятия-изготовителя изделий (т.е. использования доверенных процессов) и контроля производственных партий и образцов готовых изделий. Это взаимодействие реализует взаимный «трансфер доверенности» между производственным процессами и готовой продукцией – возможность взаимно распространить доверенности (как свойства) процессов и готовой продукции. На стадии серийного производства необходимо прежде всего обеспечить стабильность функциональных и эксплуатационных характеристик, а также приемлемые технико-экономические показатели изделия при сохранении заложенных при его разработке уровней качества и безопасности. В статье представлены результаты анализа критичных стадий производства изделий микроэлектроники, типовых угроз, возникающих на этих стадиях, и методов их парирования. Представленный подход позволяет реализовать доверенное производство изделий микроэлектроники.

Ключевые слова: доверенность, качество, производственный процесс, риски, угроза, уязвимость, стадии производственного процесса.
Для цитирования: МОСКОВСКАЯ, Юлия М.; ДЕНИСОВ, Андрей Н.; НИКИФОРОВ, Александр Ю. СИСТЕМА ОБЕСПЕЧЕНИЯ КАЧЕСТВА ДОВЕРЕННОГО МИКРОЭЛЕКТРОННОГО ПРОИЗВОДСТВА Безопасность информационных технологий, [S.l.], т. 31, № 1, с. 42–53, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1600. DOI: http://dx.doi.org/10.26583/bit.2024.1.01.

Iuliia M. Moskovskaia[1], Andrey N. Denisov[2], Alexander Yu. Nikiforov[3]
[1]Joint Stock Company "Experimental Research and Production Association SPECIAL ELECTRONIC SYSTEMS", Kashirskoe sh., 31, Moscow, 11540, Russia
[2]Scientific-Manufacturing Complex "Technological Centre», Shokina Square, 1, bld. 7, Zelenograd, Moscow, 124498, Russia
[3]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Kashirskoe sh., 31, Moscow, 115409, Russia
[1]e-mail: ymmos@spels.ru, https://orcid.org/0009-0008-7409-5619
[2]e-mail: A.Denisov@tcen.ru, https://orcid.org/0009-0009-6382-1141

[3]*e-mail: aynik@spels.ru, https://orcid.org/0000-0002-2427-663X*

The quality assurance system of the trusted Microelectronic production

Abstract. Trust (in reliable and safe operation) in a microelectronics product is mainly «laid down» at the stage of its development and is managed by guarantees of quality and reliability, the developer's qualifications and experience, a rational choice of key technical solutions that implement specified functional and operational characteristics, as well as parrying the main threats to its safety. Similarly, trust in products during their pilot and mass production is managed by the results of effective interaction and a rational combination of two systems: (1) managing the quality and protection of the manufacturer of products (i.e., using trusted processes) and (2) controlling production batches and samples of finished products (i.e., checking the reliability of a complex of technical means). This interaction implements a mutual «transfer of trust» to production processes and finished products – the possibility of spreading trust in production processes to trust in finished products and vice versa. At the stage of mass production, it is necessary first of all to ensure the stability of functional and operational characteristics, as well as acceptable technical and economic indicators of the product while maintaining the quality and protection levels inherent in its development. The article presents the results of an analysis of the critical stages of the microelectronics products production, typical threats arising at these stages, and methods of their parrying. There results allow us to build trust in such products (trust in their reliability and quality).
Keywords: power of attorney, quality, production process, risks, threat, vulnerability, stages of the production process.
For citation: MOSKOVSKAIA, Iuliia M.; DENISOV, Andrey N.; NIKIFOROV, Alexander Yu. The quality assurance system of the trusted Microelectronic production. IT Security (Russia), [S.l.], v. 31, no. 1, p. 42–53, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1600. DOI: http://dx.doi.org/10.26583/bit.2024.1.01.

Введение

В течение двадцати лет XXI века аппаратура отечественной гражданской инфраструктуры практически полностью комплектовалась электронной компонентной базой (ЭКБ) иностранного производства (ИП) – зачастую из «недружественных» стран. Изделия для критической гражданской инфраструктуры закупались через официальных дистрибьютеров, имели соответствующие гарантии и техническую поддержку. Входной контроль у потребителя в большинстве случаев ограничивался контролем документации, маркировки и целостности упаковки. Доверие к ЭКБ, таким образом, опиралось на репутацию, техническую и информационную поддержку и гарантии «раскрученных» товарных знаков – брендов. Объемы поставок варьировались от миллионов штук в год (например, в связи, коммунальном хозяйстве, автоэлектронике) до единичных (уникальных) электронных систем (например, для топливно-энергетического комплекса и промышленных объектов), скомплектованных «на заказ». Информация о конкретных разработчиках и изготовителях брендовой ЭКБ, по сути, не имела значения для потребителей.

С 2022 г. практически вся брендовая электроника стала для России труднодоступной. Остро встала задача обеспечения технологической независимости и суверенитета, под которыми по умолчанию понималось импортозамещение ЭКБ ИП (на ЭКБ отечественного производства (ОП) [1–2]). В силу уровня своего развития при этом практически сразу проявились «особенности» ОП:

– технический уровень и имеющиеся мощности отечественных предприятий позволяют производить тысячи образцов активной ЭКБ (АЭКБ – интегральных схем и электронных модулей, а также других электронных изделий, реализованных по технологиям микроэлектроники или с использованием микроэлектронных компонентов), а не миллионы в соответствии с реальными потребностями;

– отсутствует возможность просто купить готовые изделия со склада: изготовление начинается лишь после заказа и оплаты (авансового платежа), срок изготовления и поставки продукции ОП после заказа может составлять более полугода (и достигает одного года!);

– стоимость отечественных изделий АЭКБ значительно выше стоимости аналогичных брендовых аналогов ИП;

– слабо развита или отсутствует техническая и информационная поддержка потребителя ЭКБ (руководства по применению, полная, информативная и достоверная техническая документация, типовые технические решения, консультации по включению и проектированию, отладочные комплекты и проч.) [3].

Также очевидны многочисленные проблемы с качеством, в том числе функциональностью, надежностью, стойкостью к условиям эксплуатации, а также безопасностью поставляемой продукции как ОП, так и новых поставщиков ИП из дружественных стран [4]. Всё это подтверждает необходимость предъявления требований и установления критериев и методов оценки соответствия заявленным требованиям для качественных и безопасных, т.е. доверенных изделий.

Далее следует ввести некоторые термины и определения, которые не претендуют на отточенность и «финишность» формулировок, но вполне отражают суть объективных свойств изделия.

В данной работе под «**доверенностью**» понимается подтвержденное свойство продукции (ЭКБ, изделия, компонента) соответствовать заявленным требованиям **качества** (свойства удовлетворять потребности в соответствии с назначением, в том числе – по функциональным и эксплуатационным характеристикам, надежности и стойкости к внешним воздействующим факторам) и **безопасности** (свойства защищенности от внешних и внутренних угроз и их последствий), в том числе, информационной, технологической и функциональной.

Под «**доверенным**» понимается изделие, обладающее свойством доверенности. Доверенные стадия, процесс или субъект жизненного цикла изделия – обладают свойствами (объективно способны) обеспечивать реализацию доверенных изделий.

И, наконец, под «**доверием**» потребителя понимается его состояние его убежденности в том, что изделие и, соответствующие процесс, стадия или субъект жизненного цикла обладает свойством (соответствует критериям) доверенности применительно к конкретным потребностям назначения и применения.

Доверенность изделия микроэлектроники в основном «закладывается» на стадии его разработки и обеспечивается квалификацией и опытом разработчика, рациональным выбором ключевых технических решений, реализующих заданные функциональные и эксплуатационные характеристики, а также парированием основных угроз его безопасности. Доверенность подтверждается действующей системой менеджмента качества и безопасности разработчика с одной стороны и положительными результатами тестирования и испытаний образцов изделий: предварительных, приемочных и квалификационных (терминология по ГОСТ 16504) – с другой.

Обеспечение доверенности изделий микроэлектроники при их серийном производстве достигается в результате эффективного взаимодействия и рационального сочетания двух систем: (1) менеджмента качества и безопасности (СМКиБ) предприятия-изготовителя изделий (т.е. использования доверенных процессов) и (2) контроля производственных партий и образцов готовых изделий (т.е. проверки доверенности продукта). Это взаимодействие, по сути, реализует взаимный «трансфер доверенности» производственных процессов и готовой продукции – возможность распространения

доверенности процессов производства на доверенность готовой продукции и наоборот. На практике требования полноты, информативности и достоверности контроля работоспособности изделий микроэлектроники «недоверенного происхождения», особенно, сложно-функциональных, сверхбыстродействующих и прецизионных, определяют чрезмерный уровень затрат на испытания и тестирование готовых изделий, которые во многих случаях вообще не могут быть реализованы в рамках имеющихся временных, организационно-технических и финансовых ресурсов. Поэтому именно использование доверенных процессов, подтвержденных действующей СМКиБ, перенос центра тяжести с контроля готовой продукции на обеспечение и контроль стабильности процессов ее создания обоснованно позволяет смягчить требования по итоговому объему испытаний готовой продукции и, в конечном счете, обеспечить ее конкурентоспособность по соотношению «качество и безопасность / цена». При этом очевидно, что это соотношение сильно зависит от конкретного назначения и области применения изделия.

В данной статье представлены предложения по облику системы обеспечения доверенности изделий микроэлектроники на стадии «производство», для которой необходимо, прежде всего, обеспечить стабильность функциональных и эксплуатационных характеристик, а также приемлемые технико-экономические показатели изделия при сохранении заложенных при его разработке уровней качества и безопасности.

1. Организация взаимоотношений потребитель-поставщик-изготовитель, разработчик в системе доверенного производства

Обеспечение доверия к изделиям (ЭКБ) заключается в формировании убежденности потребителя в соответствии изделий его ожиданиям (потребностям назначения, документации). Доверие потребителя основано на репутации разработчика, изготовителя и поставщика, на информации об изделии и процессах его разработки, производства и поставки, а также на результатах испытаний по подтверждению соответствия изделия требованиям назначения с учетом данных по разбросам и запасам значений параметров-критериев годности относительно заданных норм. На стадии серийного производства доступной для экспертизы документацией является, как минимум:

- техническая и эксплуатационная документация на изделие (технические условия);
- протоколы испытаний и контроля изделий и производственных партий;
- документация системы менеджмента качества (СМК)[1] производства.

Уровень доверия к поставщику определяется полнотой и достоверностью информации об изделии и о предприятиях-субъектах его жизненного цикла – разработчике и изготовителе, а также предприятий их кооперации [5–7]. Всю полноту ответственности за качество и безопасность изделия микроэлектроники несет предприятие-правообладатель комплекта конструкторской документации (КД), в т.ч. технических условий (ТУ) на изделие, который маркирует образцы своим товарным знаком. На практике правообладателем (так называемым, калькодержателем) изделия может являться предприятие полного цикла, или его разработчик (при контрактном производстве), изготовитель (при контрактной разработке), поставщик, потребитель (создатель аппаратуры) или коммерческий инвестор.

Наиболее высокий уровень доверенности ЭКБ потенциально обеспечивается при его производстве на предприятии полного цикла, где стадии разработки, изготовления и

[1]ГОСТ ISO 9001-2011 Системы менеджмента качества. Требования

поставки осуществляются в рамках единого юридического лица. Наличие и соблюдение аттестованной системы СМКиБ и программы обеспечения качества (ПОК) всех процессов, оперативное взаимодействие разработчиков и технологов в ходе освоения производства, «доведения» (устранения ошибок и неоптимальностей) и модернизации изделия), анализа его отказов, проведения дополнительных испытаний в интересах потребителя позволяют наилучшим образом обеспечить трансфер доверенности процессов разработки, производства и поставки на само изделие.

В случае, если поставщиком изделия является фабрика при контрактной разработке сторонним дизайн-центром, может быть обеспечена полнота информации о наличии и соблюдении аттестованной системы СМК и ПОК и возможность проведения дополнительных испытаний в интересах потребителя. Вместе с тем процесс освоение производства, оперативная коррекция изделия (при необходимости) или анализ его отказов (в т.ч. брака) без оперативного взаимодействия с разработчиком и, соответственно, знаний особенностей реализации изделий, могут быть затруднены даже при наличии на фабрике полного комплекта КД.

Если правообладателем изделия является разработчик (дизайн-центр) с контрактным изготовлением образцов на сторонней фабрике, то информация о техпроцессе может сводиться к наличию на фабрике СМК и ПОК и, возможно, результатов статистического контроля технологических процессов по параметрам-мониторам, полученным от изготовителя. Более полную информацию о производственных процессах можно получить из результатов исследований тестовых структур контроля технологии, изготовленных совместно с поставочной микросхемой. При этом необходимо отметить, что разработка достаточно информативного тестового кристалла является весьма непростой задачей.

Во всех остальных вариантах правообладателя доверенность изделия зависит от наличия оперативного взаимодействия поставщика изделий с его разработчиками и изготовителями, предоставления ими полной и достоверной информации о своих СМКиБ, процессах, заложенных в изделии ключевых технических решениях и результатах испытаний.

Таким образом, при любой форме кооперации доверенное изделие должно быть изготовлено в производственном процессе, который обеспечивает трансфер доверия от процессов производства на изделие за счет наличия аттестованной СМКиБ и ПОК, конкретные данные которых является «открытым» для поставщика и потребителя [6, 7].

2. Нормативное регулирование процесса производства

Современное производство регулируется комплексом нормативных документов ОСТ 11 20.9926[2], ОСТ 11 1000[3], ОСТ 11 14.1012[4], ОСТ 11 14.1011[5], разработанным для оборонной продукции в развитие ОСТ В 11 0998[6], но распространенными и на продукцию народно-хозяйственного назначения. Данные стандарты достаточно подробно

[2]ОСТ 11 20.9926 «Микросхемы интегральные. Требования к элементам производства. Сертификация системы качества и производств».
[3]ОСТ 11 1000 «Микросхемы интегральные. Типовая форма построения и изложения программы обеспечения качества.
[4]ОСТ 11 14.1012 «Микросхемы интегральные. Технические требования к технологическому процессу. Система и методы операционного контроля».
[5]ОСТ 11 14.1011 «Микросхемы интегральные. Система и методы статистического контроля и регулирования технологического процесса».
[6]ОСТ В 11.0998 «Микросхемы интегральные. Общие технические условия».

регламентируют правила, процессы и элементы производства, порядок обеспечения и контроля работоспособности и стабильности готовой продукции[2-6].

Анализ указанных стандартов показывает, что в целом они обеспечивают нормативную основу для доверенных производств, но были разработаны более четверти века назад, ориентированы преимущественно на предприятия полного цикла, производящие оборонную продукцию.

В целом, приведенные стандарты требуют актуализации с учетом развития и особенностей современных контрактных микроэлектронных производств и потребностей электронных систем и комплексов для критической гражданской инфраструктуры в условиях реального спектра имеющихся рисков и угроз и, следовательно, необходимости задания и обеспечения требований безопасности (функциональной, технологической, информационной), которые в действующих стандартах отсутствуют.

Дополнительная проблема состоит в реальном (а не только бумажном!) исполнении положений этих стандартов на предприятиях. Поэтому в качестве потенциально доверенных следует рассматривать лишь производства, на которых эффективно действует документированная, доступная для экспертизы и развивающаяся система управления и контроля процессов производства и готовой продукции.

3. Стадии производства и их уязвимости

Технологический процесс является основным источником рисков потребителя, которые могут реализоваться в (1) срыве сроков поставки и (2) поставке некачественной и/или небезопасной продукции.

С целью выявления уязвимостей стадий производства, определенных в соответствии с ОСТ 11 20.9926, объединим их в следующие группы:

1 Организация производства.
   - Организация и управление производством.
   - Управление качеством.
   - Организация маркетинговой деятельности.

2 Технология.
   - Управление технологическим процессом.
   - Обеспечение качества.
   - Обеспечение идентификации и прослеживаемости продукции.
   - Организация контроля качества и испытания.

3 Инфраструктура.
   - Обеспечение и управление технической документацией.
   - Обеспечение и обслуживание средств технического оснащения.
   - Обеспечение условий производства.
   - Организация обращения с готовой продукцией и браком.

4 Материалы.
   - Обеспечение сырьем, материалами.
   - Обеспечение полуфабрикатами и комплектующими изделиями.

5 Оборудование.
   - Обеспечение контрольно-измерительным оборудованием.
   - Обеспечение испытательным оборудованием.
   - Метрологическое обеспечение.

6 Персонал.

7 Разработка.

Определение на каждой стадии производства возможных угроз, степени их влияния (степень уязвимости) и разработка мер их парирования позволит управлять рисками [7, 8].

4. Качественная оценка риска на каждой группе

Выявление и оценка опасности угроз реализации рисков Поставщика осуществляется путем определения уязвимостей на каждой стадии производства. В данной статье для выявления уязвимостей стадий производства использовался метод диаграммы Исикавы (диаграмма «рыбьей кости», англ. Fishbone Diagram) [9]. Соответствующая диаграмма применительно стадиям производства изделий микроэлектроники представлена на рис. 1.

Рис. 1. Диаграмма Исикавы. Определение уязвимостей каждой стадии производства

Парирование угроз состоит в проведении комплекса мероприятий (рис. 2), позволяющих защитить уязвимые точки каждой стадии производства.

Информация для оценки рисков, которую поставщик должен предоставить потребителю:

- положения ПОК и СМК и данные об их аттестации;
- документация на изделие: ТУ (спецификации), руководство по эксплуатации
- результаты статистического контроля технологического процесса, подтверждающие его стабильность (результаты измерений тестовых структур);
- результаты контрольных испытаний изделия в производственном процессе (приемо-сдаточных, типовых, квалификационных, сертификационных…), в том числе и результаты входного контроля материалов;
- результаты работы по анализу брака и рекламаций;
- информация об оборудовании в ПОК;
- данные о метрологическом контроле оборудования;
- информация об инфраструктуре в СМК и ПОК.

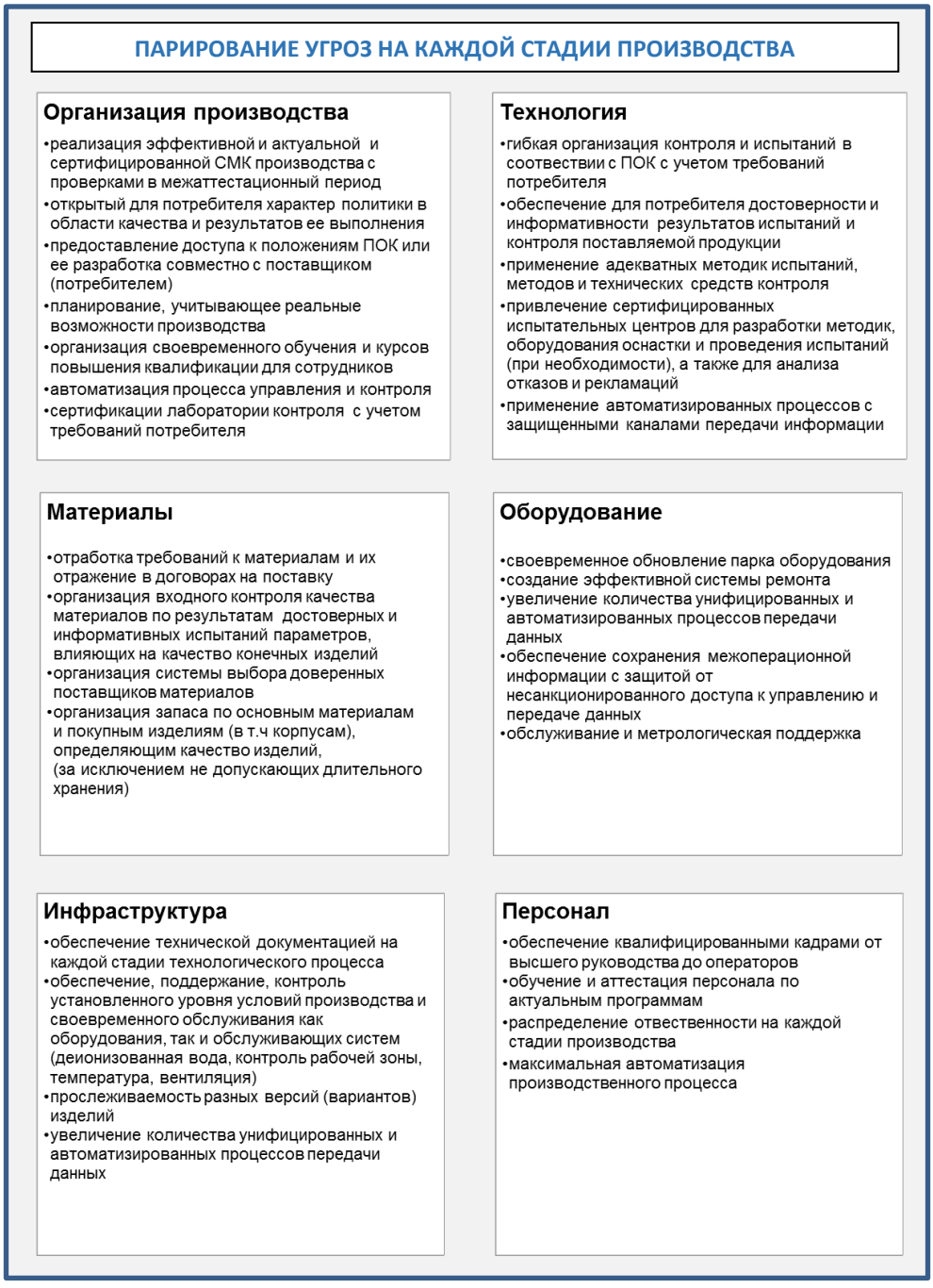

Рис. 2. Мероприятия, позволяющие парировать угрозы на каждой стадии производства

Оценка риска включает в себя анализ репутации производителя и разработчика, в том числе и степени готовности к работе с потребителем: оперативность обработки запросов в отдел маркетинга и в службу поддержки в целом, оперативность при работе с несоответствующей продукцией и т.д.

Таким образом, система обеспечения качества доверенного производства позволяет разработать модель угроз на каждой стадии производства доверенного изделия и разработать меры парирования. Это позволит оценить требуемую для потребителя степень доверенности к изделию на основе полноты и достоверности информации, полученной

поставщиком о производителе и разработчике изделия, их репутации на рынке и оценки соблюдения требований нормативной документации. Эти принципы работают и для изготовления изделий на иностранных кремниевых фабриках дружественных государств в случае, когда изготовитель предоставляет необходимую документацию.

5. Методы оперативного контроля стабильности технологического процесса

Аттестованная СМК доверенного предприятия априори предполагает наличие статистического контроля производственного процесса и готовой продукции (приемо-сдаточные испытания, контроль партий пластин, периодические испытания). При наличии соответствующих требований проводят испытания на стойкость к внешним воздействующим факторам, в том числе и к радиационным воздействиям.

В случае изготовления изделия на контрактном производстве (отечественном или иностранном) полнота информации о технологической линейке (изделии) может быть недостаточной. В этом случае требуется проверка достоверности полученной информации и установления статистической устойчивости ТП [10–11]. В этом случае предпочтительным вариантом является изготовление совместно с поставочной микросхемой тестового технологического кристалла, который позволит провести анализ качества выполнения операций технологического маршрута, определить параметры устойчивости и повторяемости технологического процесса [12].

Анализ электрических характеристик позволяет выявить статистические разбросы, но не всегда позволяет определить их причину. Дополнительное применение радиационных методов контроля позволит провести углубленный анализ причин и источников нестабильности технологического процесса с учетом реакции не только функциональных, но и паразитных структур.

В частности:

Применение рентгеновских методов позволяет выявить [13–15]:

− изменение чувствительности характеристик изделия к изменению поставщика материалов;

− качество выполнения технологических операций и диэлектрических слоев (радиационная отбраковка), влияние температуры и легирования;

Применение лазерных методов позволяет выявить [16–18]:

− дефекты, которые могут влиять на надежность изделия в процессе эксплуатации (скрытые дефекты металлизации, пробои и утечки оксидных слоев, повреждение *p-n* переходов и подложки, посторонние включения);

− чувствительность изделия к инжекции ошибок и возникновению тиристорного эффекта;

− недекларированные схемно-топологические коррекции;

− недекларированные возможности, внесенные на фабрике (закладки) – сравнением карт откликов при лазерном сканировании.

В случае использования для изготовления изделий недоверенных контрактных производств в дополнение к испытаниям тестовых структур необходимо проведение испытаний образцов продукции каждой производственной партии. При получении стабильных результатов контроля изделий на нескольких первых поставках в дальнейшем возможно проведение данных испытаний на периодической основе. Также, крайне желательно параллельное освоение производства изделия на взаимно дублирующих контрактных производствах (в разном процентном соотношении) с целью резервирования каналов их поставки, повышения уровня технологической безопасности и снижения рисков потребителя.

Заключение

Доверенность изделия обеспечивается необходимым и достаточным комплексом мероприятий по снижению до приемлемых рисков реализации уязвимости каждой из угроз на каждой стадии производства. Доверенное производство – основа обеспечения доверенности изделия.

Количественная оценка риска возможна при наличии полной и достоверной информации о степени уязвимости поставки от реализации угроз на каждой стадии производства и от выполнения мероприятий, направленных на их парирование с учетом требований потребителя.

Дополнительное применение радиационных методов контроля позволит провести углубленный анализ причин и источников нестабильности технологического процесса с учетом реакции не только функциональных, но и паразитных структур.

СПИСОК ЛИТЕРАТУРЫ:

1. Покатаева Е., Петровская Е., Импортозамещение и обеспечение качества. Электроника. Наука. Технология. Бизнес. 2018, № 3(174), с 40–48. DOI: 10.22184/1992-4178.2018.174.3.40.48. – EDN: YWJSDW.
2. Эннс В. Меры по развитию отечественной микроэлектроники в современных условиях. Электроника: Наука, Технология, Бизнес. 2022, № 6, с. 86–92. DOI: 10.22184/1992-4178.2022.217.6.86.92.
3. Бобрышев А.Д., Гудкова О.Е. Исследование причин медленного внедрения современных концепций организации производства в оборонно-промышленном комплексе. Инновации. 2020, с. 20–29. URL: https://maginnov.ru/ru/zhurnal/arhiv/2020/innovacii-n-4-2020/issledovanie-prichin-medlennogo-vnedreniya-sovremennyh-koncepcij-organizacii-proizvodstva-v-oboronno-promyshlennom-komplekse?ysclid=lqdv0ibtke308578787 (дата обращения: 20.12.2023).
4. Федорец В.Н., Белов Е.Н., Балыбин С.В. Технологии защиты микросхем от обратного проектирования в контексте информационной безопасности: научно-популярное издание. Техносфера. Мир электроники, 2019. – 216 с. URL: https://www.elibrary.ru/item.asp?id=44143092 (дата обращения: 20.12.2023). – EDN: LJHRGC.
5. Гонтаренко Т.И., Ващенко Н.В. Оценка систем менеджмента как критерий выбора поставщиков. Известия ТулГУ. Технические науки. 2020, № 10. URL: https://cyberleninka.ru/article/n/otsenka-sistem-menedzhmenta-kak-kriteriy-vybora-postavschikov (дата обращения: 23.11.2023).
6. Мишура Л.Г., Васильева Ю.В. Оценка поставщика с учетом требований ГОСТ Р ИСО 9001. Экономика. Право. Инновации. 2020, № 2, с. 4–9. – EDN: ASYOOD.
7. Гавдан Григорий П. и др. Устойчивость технологических процессов в аспекте безопасности критической информационной инфраструктуры. Безопасность информационных технологий, [S.l.], т. 30, № 2, с. 38–52, 2023. DOI: http://dx.doi.org/10.26583/bit.2023.2.02. – EDN: UZXZIW.
8. Мосолов Александр С.; Краснов Андрей Е.; Урбан Николай А. О применении метода анализа уязвимостей технологического процесса производственного объекта для обеспечения информационной безопасности АСУ ТП с учётом взаимосвязи компонентов. Безопасность информационных технологий, [S.l.], т. 29, № 3, с. 38–52, 2022. DOI: http://dx.doi.org/10.26583/bit.2022.3.03. – EDN: VDEBLC.
9. Исикава К. Японские методы управления качеством. Сокр. пер. с англ. Под ред. А.В. Гличева. М.: Экономика, 1988. – 215 с. URL: https://pqm-online.com/assets/files/lib/books/ishikawa2.pdf (дата обращения: 23.11.2023).
10. Смирнов Дмитрий О. Функциональная безопасность и недоверенная электронная компонентная база. Безопасность информационных технологий, [S.l.], т. 29, № 2, с. 128–143, 2022. DOI: http://dx.doi.org/10.26583/bit.2022.2.10. – EDN: ITCJXN.
11. Смирнов Д.О., Безродный Б.Ф., Беспалов А.В. Интегральные микросхемы. Проблема доверенности. Наноиндустрия. 2021, т. 14, № S7 (107), с. 340–342. DOI: 10.22184/1993-8578.2021.14.7s.340.342. – EDN: XRMFCW.
12. Сивченко А.С. Оценка надежности суб-100-нм КМОП ИС с использованием ускоренных испытаний тестовых структур. Наноиндустрия. 2021, т. 14, № S7 (107), с. 192–195. DOI: 1993-8578.2021.14.7s.192.194. – EDN: ATEEEW.
13. Катеринич И.И., Курин Ф.М., Попов В.Д. Метод радиационно-термической отбраковки и повышения надёжности МОП интегральных схем. Вопросы атомной науки и техники. Серия: Физика

радиационного воздействия на радиоэлектронную аппаратуру. 1996, № 3–4, с. 127. URL: http://vant.niipriborov.ru/vant.php (дата обращения: 23.11.2023).
14. Давыдов Г.Г., Яшанин И.Б., Скобелев А.В., Маслов В.В. Влияние режима имплантации бора на дозовую деградацию тока потребления КМОП КНС БИС. Вопросы атомной науки и техники. Серия: Физика радиационного воздействия на радиоэлектронную аппаратуру. 2009, № 4, с. 33–35. URL: https://www.elibrary.ru/download/elibrary_12855522_17742288.pdf (дата обращения: 23.11.2023).
15. Московская Ю.М. Прогнозный контроль радиационной стойкости БИС с учетом стабильности производства. Тезисы докладов 20-й Всероссийской научно-технической конференции «Радиационная стойкость электронных систем» «Стойкость – 2017», 2017. – 287 с. URL: https://rusneb.ru/catalog/000200_000018_RU_NLR_BIBL_A_011660120/?ysclid=lqdvxl6wmj555498278 (дата обращения: 23.11.2023).
16. Можаев Роман К. и др. Обзор лазерных сканирующих методов исследований микроэлектронных полупроводниковых структур. Безопасность информационных технологий, [S.l.], т. 29, № 4, с. 105–125, 2022. DOI: http://dx.doi.org/10.26583/bit.2022.4.09. – EDN: VOONPG.
17. Skorobogatov S. Side-channel attacks: new directions and horizons Design and Security of Cryptographic Algorithms and Devices (ECRYPT II) Albena, Bulgaria, 29 May – 3 June 2011. URL: https://www.cl.cam.ac.uk/~sps32/ECRYPT2011_2.pdf (дата обращения: 11. 23.2023).
18. Xanthopoulos C. et al. IC laser trimming speed-up through wafer-level spatial correlation modeling. 2014 International Test Conference, Seattle, WA, USA. 2014, p. 1–7. DOI: 10.1109/TEST.2014.7035329.

REFERENCES:

[1] Pokatayeva E., Petrovskaya E. Import substitution and quality assurance. Electronics: Science, Technology, Business. 2018, no. 3(174), p. 40–48. DOI: 10.22184/1992-4178.2018.174.3.40.48 (in Russian). – EDN: YWJSDW.
[2] Enns V. Measures for the development of domestic microelectronics in the present context. Electronics: Science, Technology, Business. 2022, no. 6, p. 86–92. DOI: 10.22184/1992-4178.2022.217.6.86.92 (in Russian).
[3] Bobryshev A.D., About Gudkova.E. Investigation of the reasons for the slow introduction of modern production organization concepts in the military-industrial complex. Innovation. 2020, p. 20–29. URL: https://maginnov.ru/ru/zhurnal/arhiv/2020/innovacii-n-4-2020/issledovanie-prichin-medlennogo-vnedreniya-sovremennyh-koncepcij-organizacii-proizvodstva-v-oboronno-promyshlennom-komplekse?ysclid=lqdv0ibtke308578787 (accessed: 12.20.2023) (in Russian).
[4] Fedorets V.N., Belov E.N., Balybin S.V. Technologies of protection of microcircuits from reverse engineering in the context of information security: a popular scientific publication. Technosphere. The World of Electronics, 2019. – 216 p. URL: https://www.elibrary.ru/item.asp?id=44143092 (accessed: 12.20.2023) (in Russian). – EDN: LJHRGC.
[5] Gontarenko T.I., Vashchenko N.V. Assessment of management systems as a criterion for choosing suppliers. Izvestiya TulSU. Technical sciences. 2020, no. 10. URL: https://cyberleninka.ru/article/n/otsenka-sistem-menedzhmenta-kak-kriteriy-vybora-postavschikov (accessed: 11.23.2023) (in Russian).
[6] Mishura L.G., Vasilyeva Yu.V. Supplier evaluation taking into account the requirements of GOST R ISO 9001. Economy. Right. Innovation. 2020, no. 2, p. 4–9 (in Russian). – EDN: ASYOOD.
[7] Gavdan Grigory P. et al. Sustainability of technological processes in the aspect of security of critical information infrastructure. IT Security (Russia), v. 30, no. 2, p. 38–52, 2023. DOI: http://dx.doi.org/10.26583/bit.2023.2.02 (in Russian). – EDN: UZXZIW.
[8] Mosolov Alexander S.; Krasnov Andrey E.; Urban Nikolai A. On the application of the vulnerability analysis method of the technological process of a production facility to ensure the information security of an automated process control system, taking into account the interconnection of components. IT Security (Russia), v. 29, no. 3, p. 38–52, 2022. DOI: http://dx.doi.org/10.26583/bit.2022.3.03. – EDN: VDEBLC.
[9] Ishikawa K. Japanese methods of quality management. Translated from English. Edited by A.V. Glichev. M.: Encyclopedia, 1988. – 215 p. URL: https://pqm-online.com/assets/files/lib/books/ishikawa2.pdf (accessed: 11.23.2023) (in Russian).
[10] Smirnov Dmitry O. Functional security and an untrusted electronic component base. IT Security (Russia), v. 29, no. 2, p. 128–143, 2022. DOI: 10.26583/bit.2022.2.10 (in Russian). – EDN: ITCJXN.
[11] Smirnov D.O. Bezrodny B.F., Bespalov A.V. Integrated circuits. The problem of power of attorney. Nanoindustry. 2021, v. 14, no. S7 (107), p. 340–342. DOI: 10.22184/1993-8578.2021.14.7s.340.342 (in Russian). – EDN: XRMFCW.

[12] Sivchenko A.S. Evaluation of the effectiveness of sub-100 nm CMOS IC using accelerated research methods within the framework of the Nanoindustry project. 2021, v. 14, no. S7 (107), p.192–195. DOI: http://dx.doi.org/10.22184/1993-8578.2021.14.7s.192.194 (in Russian). – EDN: ATEEEW.

[13] Katerinich I.I., Kurin F.M., Popov V.D. Method of radiation-thermal rejection and reliability improvement of MOS integrated circuits. Issues of atomic science and technology. Syria: Physics of radiation effects on radiolectronic equipment. 1996, no. 3–4, p. 127. URL: http://vant.niipriborov.ru/vant.php (accessed: 11.23.2023) (in Russian).

[14] Davydov G.G., Yashanin I.B., Skobelev A.V., Maslov V.V. Influence of the boron implantation regime on the dose degradation of the consumption current of CMOS KNS BIS. Issues of atomic science and technology. Series: Physics of radiation effects on radioelectronic equipment. 2009, no. 4, p. 33–35. URL: https://www.elibrary.ru/download/elibrary_12855522_17742288.pdf (accessed: 23. 11.2023) (in Russian).

[15] Moskovskaya Yu.M. Predictive control of radiation resistance of BIS taking into account the stability of production. Abstracts of the 20th All-Russian Scientific and Technical Conference "Radiation resistance of electronic systems" "Resistance – 2017", 2017. – 287 p. URL: https://rusneb.ru/catalog/000200_000018_RU_NLR_BIBL_A_011660120/?ysclid=lqdvxl6wmj555498278 (accessed: 11.23.2023) (in Russian).

[16] Mozhaev Roman K. et al. A review of laser scanning methods for the study of microelectronic semiconductor structures. IT Security (Russia), v. 29, no. 4, p. 105–125, 2022. DOI: http://dx.doi.org/10.26583/bit.2022.4.09 (in Russian). – EDN: VOONPG.

[17] Skorobogatov S. Side-channel attacks: new directions and horizons Design and Security of Cryptographic Algorithms and Devices (ECRYPT II) Albena, Bulgaria, 29 May – 3 June 2011. URL: https://www.cl.cam.ac.uk/~sps32/ECRYPT2011_2.pdf (accessed: 23. 11.2023).

[18] Xanthopoulos C. et al. IC laser trimming speed-up through wafer-level spatial correlation modeling. 2014 International Test Conference, Seattle, WA, USA. 2014, p. 1–7. DOI: 10.1109/TEST.2014.7035329.

Поступила в редакцию – 20 декабря 2023 г. Окончательный вариант – 5 февраля 2024 г.
Received – December 20, 2023. The final version – February 05, 2024.