Оригинальная статья
DOI: 10.21683/1729-2646-2017-17-3-10-16

Особенности современной микроэлектроники и вопросы построения систем управления высокой надежности и безопасности

Алексей П. Кирпичников, *Институт проблем управления им. В.А.Трапезникова РАН, Москва, Россия*
Станислав Н. Васильев, *Институт проблем управления им. В.А.Трапезникова РАН, Москва, Россия*

Резюме. Цель. *Обратить внимание читателей на тенденции роста количества техногенных катастроф, увеличение ущерба от них, возрастание количества человеческих жертв и связь этого феномена с микропроцессорными системами автоматики. Приводятся доводы о необходимости построения техники с повышенным функционалом безопасности в условиях воздействия многократно возросших аномальных природных и техногенных факторов. Описываются и анализируются специфика систем управления объектами критического приложения и последствия пренебрежения дополнительным контролем схемотехники и программного обеспечения. Особо отмечается возрастание риска от введения беспилотных технологий и массового их использования на железнодорожном и автомобильном транспорте. В статье рассматриваются проблемы устойчивости систем управления к сбоям и внешним воздействиям в зависимости от примененной элементной базы. Приводится статистика техногенных катастроф, рассматривается их связь с показателями неустойчивости систем управления. Отдельное внимание уделено особенностям современной микроэлектронной элементной базы и влиянию прогресса в этой области на помехоустойчивость систем и их сбойность. При этом отмечается увеличение количества опасных отказов систем, построенных на микроконтроллерах, выполненных по технологическим нормам 0,13 мкм и ниже. Значительное место отводится исследованию особенностей современных кристаллов, их топологии, в частности, главного элемента системы управления – микроконтроллера и цифрового сигнального процессора, анализируется влияние на кристалл внешних воздействий. Рассмотрены проблемы КМОП топологии в микропроцессорных узлах, показана зависимость увеличения влияния помех с переходом на новые модификации КМОП технологий. Обращается внимание на необходимость подготовки соответствующего класса специалистов для работы с этими системами, владеющих не только программированием, но обладающих глубокими знаниями в области физики, основ построения систем управления и их устойчивости.* **Результаты.** *Проведена сравнительная оценка устойчивости КМОП технологий с проектными нормами 0,5 мкм и 130 нм и получена разница значений пороговой мощности воздействия более 4000 раз. Отмечается, что большинство разработчиков, программирующих подобные системы, вводятся в заблуждение отсутствием у фирм-производителей электронных компонентов какой-либо открытой информации о сбойности процессорных элементов. Принимая за основной параметр цифры надежности изделия, они неверно оценивают уровень полноты безопасности, ошибочно используя вместо параметров сбойности цифры надежности микросхем, предоставляемые изготовителем. При этом стандартные методы повышения уровня безопасности, применяемые разработчиками (в частности, резервирование), часто оказываются неэффективными.* **Выводы.** *Для построения систем управления высокой надежности и безопасности необходимо учитывать особенность современной элементной базы, принимая во внимание факт, что новые поколения современных микросхем, ввиду своей сбойности, часто непригодны для построения высоконадежных систем. Представляется актуальным дорабатывать существующие стандарты и создавать новые механизмы повышения устойчивости и безопасности систем. Также отмечается необходимость обязательной поддержки соответствующего уровня образования и информированности широкого круга разработчиков, работающих с системами управления в областях транспорта, энергетики, систем промышленной автоматики, вооружений, и др. в части важности обеспечения необходимого уровня функциональной безопасности.*

Ключевые слова: *микропроцессорные системы управления, микроэлектронная элементная база, техногенные катастрофы, сбойные ошибки, УПБ, блок безопасности.*

Формат цитирования*: Кирпичников А.П., Васильев С.Н. Особенности современной микроэлектроники и вопросы построения систем управления высокой надежности и безопасности // Надежность. 2017. Т. 17, № 3. С. 10-16. DOI: 10.21683/1729-2646-2017-17-3-10-16*

Введение

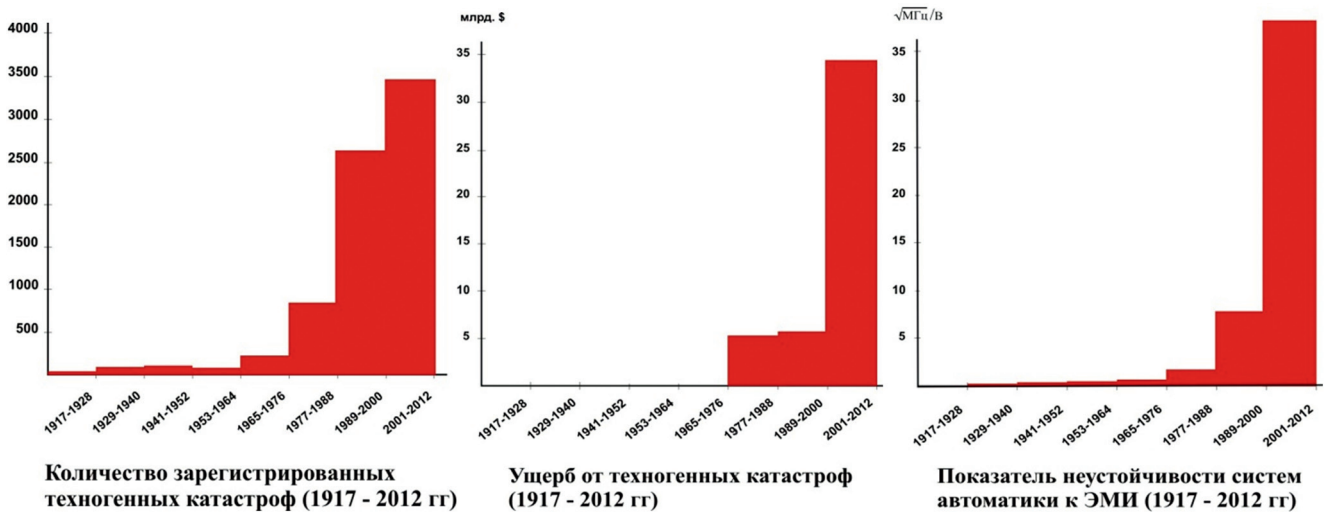
В последние десятилетия проявляется угрожающая тенденция непрерывного роста количества техногенных катастроф, сопровождающихся все большим ущербом и возрастанием количества жертв. Одной из основных причин следует полагать повсеместное внедрение микропроцессорных систем управления на замену старым релейным системам без учета особенностей современной элементной базы. Специфика систем управления объектами критического приложения предполагает очень высокий уровень безопасности, который практически недостижим на новых элементах без использования далеко не тривиальных методов. Как результат, объекты с наиболее напряженным графиком эксплуатации при модернизации систем управления неминуемо попадают в группу риска. Специалистам в области обработки сигналов и построений систем безопасности нужно обратить на это особое внимание и быть готовым к очень ответственной напряженной работе, что не всегда характерно для нового времени и даже непривычно для молодого поколения. Однако результат – сохраненные жизни – того стоит. Так что противопоказано пускать такие работы на самотек, пренебрегать дополнительным контролем схемотехники и программного обеспечения (ПО), входным контролем элементной базы и, тем более, отдавать решения по альтернативным компонентам на откуп снабжению. Последствия могут быть непредсказуемы и даже трагичны. Авторы уже касались этих аспектов безопасности применительно к железнодорожной тематике и метрополитену [1]. Более того, причиной для разработки блока безопасности «БАРС» систем управления электропоездов московского метро 81-760 для коллективов ИПУ РАН и ООО «АВТЭКС» явилось именно стремление противодействовать вышеперечисленным тенденциям.

Чрезвычайно важным представляется соответствующий уровень образования и общей информированности широкого круга разработчиков в части функциональной безопасности. Необходимость получения экстремально низких вероятностей опасного отказа (например, 10^{-9} час$^{-1}$ для SIL 4) делает практическое подтверждение уровня безопасности натурными испытаниями аппаратуры невыполнимой задачей, что часто переносит предмет в область теоретических построений и дает почву для различных легенд и несоответствий. Так, целым рядом производителей микроконтроллеров и процессоров цифровой обработки сигналов (DSP) объявлены новые микросхемы уровня SIL 3 со специальными средствами коррекции ошибок, выполненные по технологии 90 нм и даже 65 нм. Не всем инженерам известно, что микропроцессоры, выполненные по старым, но до сих пор использующимся технологиям КМОП 0,5 мкм и 0,35 мкм, при отсутствии схемотехнических и топологических ошибок де факто обеспечивали сбойность на уровне SIL 4 даже при воздействии слабых электромагнитных помех. Дополнительными мерами контроля эти цифры можно было улучшить еще на два порядка, что на практике редко требовалось, а стоял лишь вопрос отказов устройств по надежности. Тогда как современные микроконтроллеры и DSP, выполненные с технологическими нормами 0,13 мкм и ниже, даже с примененными средствами встроенной коррекции и в идеальных лабораторных условиях, не всегда могут продемонстрировать хотя бы уровень SIL 3 (10^{-7} час$^{-1}$) и никак не могут являться базой для построения устройств ответственного применения. Настоящая работа призвана хотя бы в некоторой степени закрыть этот информационный пробел.

Рост числа техногенных катастроф как тенденция последних десятилетий

Начнем рассмотрение с техногенных катастроф. Их количество (рисунок 1) увеличивается, и это очевидно, поскольку оно пропорционально, с одной стороны, общему количеству единиц используемой техники, а с другой – увеличению степени ее влияния на критические события. Последнее проявляется как в части разнообразия внедрений (применений на объектах), так и в вариациях масштабной шкалы последствий: как результат – получаем нелинейную (степенную) зависимость. Несмотря на ограниченность масштаба событий, влияние их велико и специфика очевидна: техника, особенно энергонасыщенная, при нарушении контроля (отсутствии надежно функционирующих систем безопасности) – это стихия. Последствия от техногенных катастроф всегда локально более разрушительны, хотя бы по той причине, что расположена техника (в отличие от вулканов) почти всегда вблизи и среди людей. Особое место при этом занимает транспорт и, в частности, системы автоматики железнодорожного транспорта и метро. Помимо обычных рисков, неумолимый прогресс (а на самом деле, непонимание истинной ситуации и подверженность популизму) диктует повсеместное внедрение автоматов, беспилотных технологий и пр., что существенно повышает требования к системам управления и узлам цифровой обработки сигналов (ЦОС). Отдельного рассмотрения заслуживают планы по массовому использованию беспилотного автомобильного и авиатранспорта (хочется надеяться, что при этом не будут забыты стандарты ГОСТ Р МЭК 61508 и ISO 26262), что существенно отразится на безопасности жизни.

Пока же статистика и без этих новых и многообещающих трендов выглядит ужасно. Обратимся к цифрам – речь идет о статистике техногенных и природных катастроф и их последствий за последние 100 лет (основываясь на материалах исследовательского центра CRED − Centre for Research on the Epidemiology of Disasters) [2]. Так, за 30 лет с 1910 г. по 1940 г. (при населении Земли ок. 2 млрд чел.) количество зарегистрированных техногенных катастроф составило лишь



Количество зарегистрированных техногенных катастроф (1917 - 2012 гг)

Ущерб от техногенных катастроф (1917 - 2012 гг)

Показатель неустойчивости систем автоматики к ЭМИ (1917 - 2012 гг)

Рисунок 1 − Статистика техногенных катастроф и изменение устойчивости автоматики

162 при пострадавших и жертвах ~50 тыс. чел. с общим ущербом ~$102,5 млн. Но за такой же период с 1982 г. по 2012 г. (при населении Земли ок. 7 млрд чел.) эти цифры составили для техногенных катастроф ~6,7 тыс. с пострадавшими и жертвами 4 млн. чел. и ущербом ~$45,5 млрд. То есть рост по числу катастроф составил **35 раз,** а по нанесенному ими ущербу − **450 раз**! Приведенные на рисунке 1 графики говорят сами за себя (для удобства при обработке данных использованы интервалы по 12 лет, что близко, с одной стороны, к циклам солнечной активности, а с другой – к типовому времени между модернизациями капиталоемкого оборудования).

Человеческому мышлению в популяции свойственна инерционность реакции (задержка в одно поколение и более). С другой стороны, всегда присутствует «высокочастотная фильтрация», когда мелкие тактические события затеняют глобальные тенденции, особенно те из них, где постоянная времени − более нескольких десятилетий, и поколение привыкает. Это предполагает адекватную реакцию в реальном времени на происходящее, в лучшем случае, лишь со стороны нескольких профессиональных сообществ, при игнорировании обществом в целом.

Как и чем будет пытаться реагировать современное человечество на угрозу своей безопасности и увеличение количества катастрофических событий? Наиболее вероятно – все теми же микропроцессорными защитами, системами сбора, обработки и управления. Нас в такой ситуации должны волновать, по крайней мере, чисто профессиональные вопросы обеспечения функционала безопасности, т.е. создания техники, работоспособной в жестких условиях, когда вероятность аномальных по величине воздействующих факторов возрастает многократно. Так какова же типичная стойкость автоматики к различным воздействиям (влажность, удары, электромагнитные поля и пр.), и как она менялась на протяжении столетия? Если в части механической прочности и тщательности изготовления ответ очевиден, то в отношении электромагнитной стойкости необходимо сделать некоторые оценки. В качестве критерия возьмем условный параметр порогового воздействия, вызывающего сбой такой системы [3, 4] и, по аналогии со спектральной плотностью шума, будем измерять его в единицах $В/\sqrt{МГц}$. Промежуточные выкладки опускаем, а результаты в виде обратных величин показаны на правом графике рисунка 1. Особое внимание следует обратить на близость характера последних двух гистограмм: ущерба и неустойчивости систем управления.

Глядя на приведенные графики, становится ясно, что необходимо переделывать стандарты и обсуждать дополнительные, нерыночные механизмы повышения устойчивости систем управления ответственных применений. В условиях нарастающего потока сбоев, приводящих к катастрофическим событиям, «прецедентное» мышление с запоздалой реакцией может не сработать. Приняв это к сведению, перейдем к рассмотрению специфики современных микроэлектронных технологий.

Общие проблемы современной микроэлектронной элементной базы

Перечень элементной базы, применяемой в системах управления и обеспечения безопасности, весьма широк и включает множество активных и пассивных компонентов: от резисторов, конденсаторов и транзисторов до больших интегральных схем и радиочастотных модулей. По каждому из разделов этого списка следовало бы рассмотреть влияние модернизированных технологий (и, прежде всего, применения нанотехнологий) на надежность элементов, их стойкость к внешним воздействиям и изменение вероятности ошибки при выполнении функций в схеме. Результатом такого рассмотрения, в частности, стало выявление нового типа дефектов компонентов поверхностного монтажа − связанных с механическими воздействиями, присутствующими в процессе производства, эксплуатации изделий и незащищенностью поверхностей модулей, на которых расположены компоненты. Для большинства электронных

модулей мы имеем ситуацию, когда правила монтажа мало изменились за десятилетия, но повысилась плотность размещения, и с компонентов исчезли корпуса (а если остались, то лишь в виде тонких слоев покрытий, не защищающих от механических воздействий), т.е. по старым стандартам большинство современных модулей рассматривались бы как микросборки и требовали соответствующей дополнительной защиты, которой теперь пренебрегают. Другим обнаруженным фактором стало изменение характера пробоя активных элементов, что связано, прежде всего, с использованием низковольтных технологий и существенно более тонких слоев в структуре полупроводника, чем в предыдущих поколениях аналогичных изделий. Отдельного упоминания заслуживает повсеместное применение силовых изделий на МОП транзисторах, что, с одной стороны, уменьшило потери мощности при коммутации, но с другой – существенно увеличило вероятность пробоя таких ключей на замыкание (в связи с упомянутыми проблемами внедрения нанотехнологий). Этот список можно было бы продолжать, обсуждая влияние каждого из факторов на безопасность и отказоустойчивость систем управления, но мы вынужденно ограничимся вышесказанным.

Рассмотрим, хотя бы кратко, главный элемент системы управления, которым, безусловно, является процессорный узел – микроконтроллер, DSP и др. – тот элемент, от которого зависит правильность выполнения алгоритма и безопасность реакций системы.

Пример такого высокотехнологичного компонента, хорошо знакомого, но едва ли узнаваемого в этом виде для IT специалиста, показан на рисунке 2.

Отметим здесь, что большинство разработчиков, связанных с программированием систем, мало понимают, что, собственно, представляет собой та микросхема (кристалл), для которой они программируют − как объект физики и радиотехники. В качестве примера рассмотрим популярный процессор на базе ядра Cortex M3, пришедший на смену хорошо зарекомендовавшему себя ARM7. На рисунке 2 показано, что представляет собой такой процессор без корпуса и привычной матрицы выводов: прежде всего, мы видим не один, а два отдельных кристалла, смонтированных один поверх другого. Верхний представляет собой FLASH-память и соединен с нижним (вычислительное ядро) длинными петлями перемычек разварки. Анализ этих связей сразу же позволяет сделать вывод о различии помехоустойчивости режимов работы с ОЗУ и FLASH уже за счет этих контуров. А другими факторами влияния на стойкость будут разница технологии самих кристаллов, нюансы монтажа, печатных плат (PCB) и прочее. Однако в наши задачи не входит рассмотрение специфики отдельного компонента. Поэтому коснемся, хотя бы кратко, общих проблем КМОП (CMOS) технологии, по одной из модификаций которой выполнено большинство современных микропроцессорных узлов.

Проблемы КМОП технологии в современных микропроцессорных узлах

Прежде всего, обратим внимание на такой малопопулярный факт: логический вентиль КМОП, как и любой каскад, построенный на активных компонентах, в момент переключения является усилителем. Например, в случае инвертора (см. схему в левой части рисунка 3) один транзистор является нагрузкой для другого, и типовой

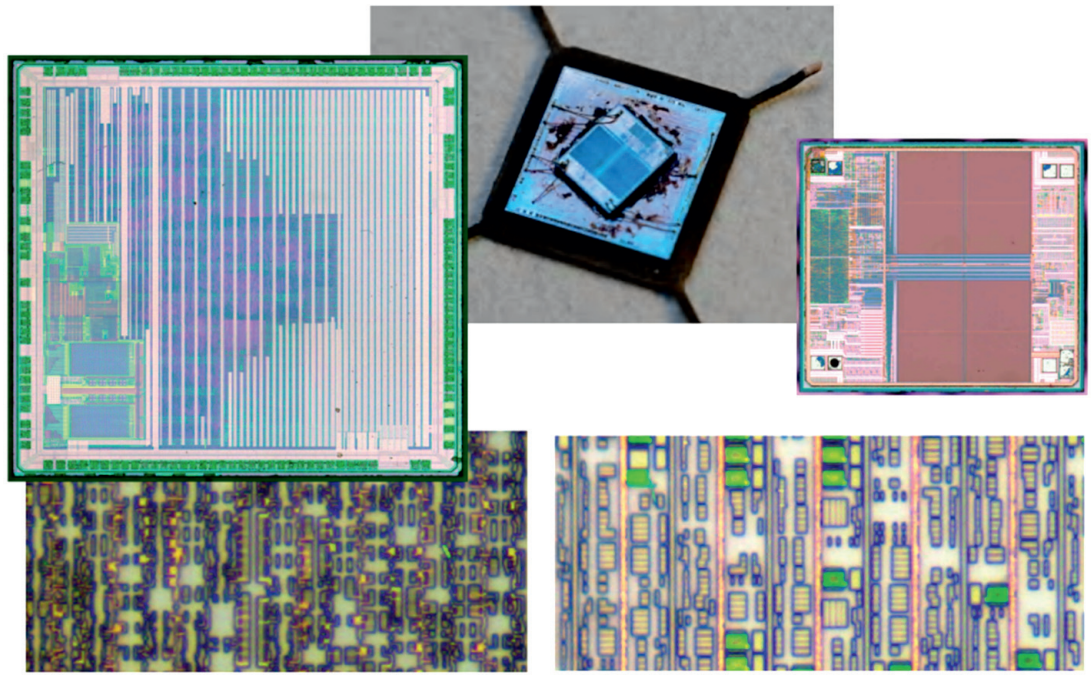
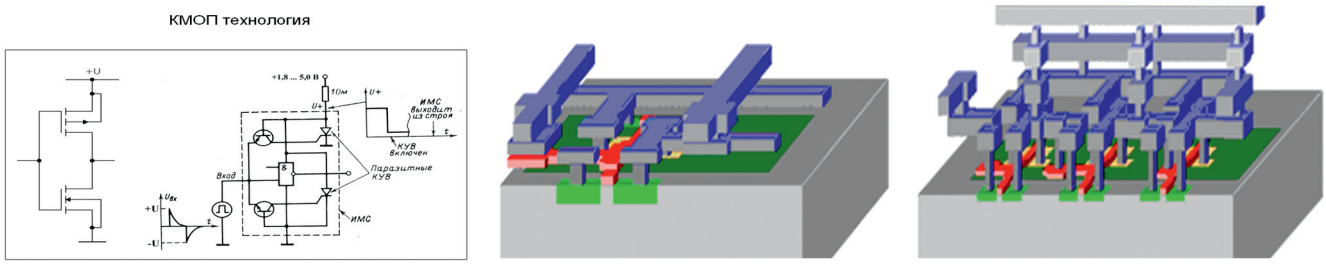


Рисунок 2 − Микроконтроллер Cortex M3 без крышки корпуса и матрицы выводов.
Слева в масштабе показан кристалл процессора, справа – FLASH-память, ниже, более крупно – элементы топологии



Логический элемент КМОП (CMOS)

0,5 мкм, 2 слоя металла до 200К транзисторов, 90 МГц

0,13 мкм , 7 слоев металла до 500 млн транзисторов, 1,5 ГГц

Рисунок 3 – КМОП технологии: разная плотность расположения слоев металлизации и полоса частот вентилей для 0,5 мкм и 0,13 мкм

коэффициент усиления такой пары обычно получается около 80 – 100 в широкой полосе частот. В правой части рисунка показано, что эта полоса частот изменилась с 90 МГц до 1,5 ГГц с переходом от 0,5 мкм к 0,13 мкм. При этом нужно учесть, что пороговое напряжение и питание транзисторов для новой технологии снизилось как минимум в 4 раза. Это означает, что энергию помехи схема, выполненная по технологии, показанной на рисунке 3 справа, может потребить из полосы в 16 раз более широкой, при том, что ее стойкость к амплитуде помехи как минимум в 4 раза ниже.

Опуская промежуточные выкладки, отметим, что помехоустойчивость используемых в настоящий момент модификаций КМОП технологий с различными проектными нормами к внешнему энергетическому воздействию отличается на порядки. Делая сравнительную оценку для представленных на рисунке вариантов **0,5 мкм** и **0,13 мкм**, получим значение по мощности влияющей помехи, отличающееся более чем в **4000** раз **(!)**. Сравнение стойкости для **0,5 мкм** и **90 нм** демонстрирует нелинейность этой зависимости, и расчет дает уже более **15 000** раз – и все это не в пользу новых кристаллов, таких удобных для пользователей и программистов. Это заставляет задуматься о правомерности применения технологий с нормами менее 0,25 мкм для устройств критических приложений. Следует учитывать, что уровень электромагнитного шума в современной цивилизации очень высок в местах большого скопления людей и энергонасыщенных объектов инфраструктуры. Таким образом, эксплуатация каждого устройства безопасности, не обладающего достаточной стойкостью, превращается в игру в рулетку.

Рассмотрев коротко влияние внешних факторов, обратимся к факторам внутренним (т.е. скрытым в самих микроэлектронных изделиях). Если для предыдущих поколений микропроцессорных устройств обсуждался как значительный – фактор влияния на кристалл радиации, в частности, керамических элементов корпуса, вызывавший с конечной вероятностью сбойное переключение вентилей схемы, то теперь, безусловно, доминирующим эффектом является плохая магнитная совместимость плотно расположенных элементов и блоков самого кристалла, как видно на рисунках 2 (внизу) и 3. Фактором увеличения сбойности является близкое расположение активных элементов и плотная многослойная разводка связей с эффектами перекрестных наводок. При этом нужно отметить, что для большинства современных процессоров максимальная длина одной связи на кристалле может достигать 1 см и более, что также в разы превышает типичный параметр длины связи для предыдущих поколений схем.

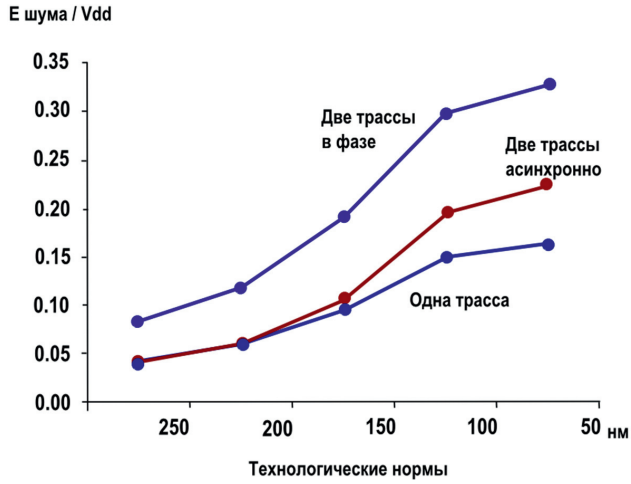


Рисунок 4 – Зависимость относительной величины напряжения помехи на шине питания от линий трассировки длиной 1 мм

На рисунке 4 показана зависимость относительной величины напряжения помехи на шине питания от фрагментов линий трассировки длиной 1 мм при топологически минимальном расстоянии между ними от проектных норм. Верхняя кривая – сигнал в источниках помех изменяется синфазно, средняя кривая – асинхронно, нижняя кривая соответствует наличию только одного проводника с помехой. Приняв во внимание реальное количество близко расположенных трасс на кристалле и их длину и посчитав вероятность пиковых значений для выбранной модели шума, получим ориентировочное количество превышений порогового уровня срабатывания вентилей и оценку сбойности конкретной архитектуры микропроцессора (разумеется, без учета схем компенсации ошибок). Даже такая грубая двумерная модель дает результаты, плохо совместимые с требованиями безопасности. Результаты 3D-моделирования конкретных фрагментов схем дают еще более удручающие результаты. Кроме того, в больших кристаллах значительно возрос ток утечки как дополнительный

дестабилизирующий фактор, также косвенно влияющий на вероятность сбоев.

Данные обстоятельства привели к тому, что помехоустойчивость упала так сильно, а сбойность так возросла, что это стало заметно в простых системах реального времени (не связанных с безопасностью). Изготовители вынужденно стали применять специальные меры компенсации сбоев, а именно: встраивать в кристаллы аппаратные блоки контроля данных и коррекции ошибок, дублировать ответственные сигналы и пр. Как результат, появились кристаллы, выполненные по технологии с нормами 65 нм, для которых гарантируется уровень SIL 2 (внимание, при идеальной ЭМС в аппаратуре!). Иными словами, к функциональной безопасности это не имеет отношения, поскольку достижением таких изделий считается ситуация, когда отдельные структуры на одном кристалле не очень мешают друг другу и могут хорошо работать при сбойности на уровне 10^{-6} час$^{-1}$. Но этого совершенно недостаточно для построения на их основе даже систем безопасности уровня SIL 2. При этом фактором, драматически влияющим на безопасность, будет, например, любое электромагнитное воздействие, имеющее соответствующую вероятность пикового уровня на рассматриваемом временном интервале.

Практикуемое обычно резервирование как способ повышения уровня безопасности для таких узлов также оказывается малоэффективным ввиду фундаментальной причины – большинство сбойных ошибок [8] при использовании данных технологий раскрываются как отказы по общей причине (ПОП). Так, внешнее электромагнитное воздействие даже небольшой энергетики, но хорошо совпавшее по спектру частот с «антеннами» кристаллов и разводки модуля, вызывает лавинообразные сбои, которые не могут быть отработаны стандартными средствами коррекции ошибок, рассчитанными на малочисленные или одиночные события. Тогда возникнет своего рода пороговый эффект воздействия, когда поведение системы становится непредсказуемым. Для систем безопасности это следует считать абсолютно

Рисунок 5 − Изменение соотношения вероятностей отказа и вероятностей сбоя в поколениях микропроцессоров

неприемлемым, а такие компоненты – непригодными. Областью их применения должны остаться бытовые и телекоммуникационные устройства, где уровень сбоев определяет доступность сервиса и качество сигнала, но никак не связан с риском для жизни.

Как результат, имеем необычную ситуацию (рисунок 5), когда надежность микропроцессорных компонентов стала многократно лучше их сбойности. Т.е. фактически самыми ненадежными компонентами современного электронного модуля являются PCB и разъемы; тогда как самым небезопасным – его процессорный элемент и чувствительные цифровые схемы. В пределе сбойность суперсовременной электроники достигает уровня, свойственного человеку-оператору (то есть мы достигли здесь совершенства и воспроизвели самих себя!). При этом данные о сбойности для большинства процессорных элементов практически отсутствуют в стандартной документации и доступны лишь после долгих и утомительных переговоров с изготовителем (если он вообще озаботился исследовать изделие и получить такие данные). В результате разработчики при оценке уровня полноты безопасности (УПБ) ошибочно используют вместо них цифры надежности микросхем, предоставляемые изготовителем, что абсолютно некорректно. Что же касается цифр сбойности – это является закрытой информацией, не обсуждаемой изготовителем.

У этой ситуации есть масса последствий: например, замена модификации микроконтроллера на другую, более новую и полностью совместимую по ПО, может драматически изменить УПБ изделия. Кроме того, помимо процессоров существуют дополнительные интерфейсные схемы, аналого-цифровые преобразователи (АЦП), тактовые генераторы и другие микросхемы, содержащие в себе цифровые блоки, выполненные по неизвестным разработчику технологиям и имеющие свой уровень сбойных ошибок. Некоторые из таких ошибок могут быть парированы алгоритмически тем же процессором. Но как быть, если источником сбоя становятся скачки фазы опорного сигнала – это приводит уже к абсолютно неконтролируемым последствиям для цифровых систем. Такое может возникнуть при простой замене одного компонента (генератора) в спецификации на другой, внешне и по спецификации – такой же (например, по инициативе снабжения).

На рисунке 6 в качестве примера показаны пять генераторов, выполненных по технологии поверхностного монтажа (SMD), одинакового применения, т.е. для одного и того же изделия, но от разных производителей, а рядом показаны результаты «вскрытия» после удаления резонаторов. Как видим, здесь присутствуют цифровые схемы с совершенно разными топологическими нормами, а сам монтаж кристаллов предполагает, как следствие, драматически разную помехоустойчивость.

Подытоживая вышесказанное, отметим, что создание микропроцессорных изделий для систем управления под требования SIL 3, и, тем более, SIL 4, является задачей,

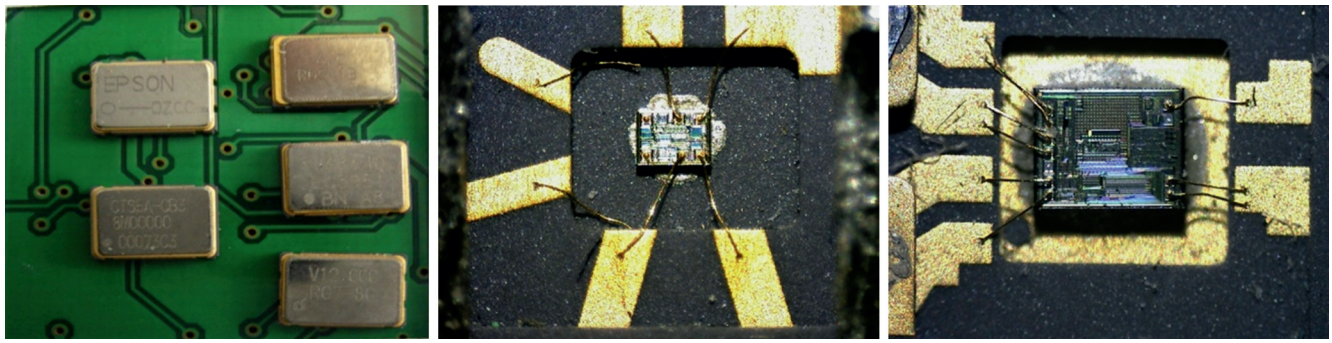


Рисунок 6 − Помехоустойчивость генераторов SMD. Слева направо: генераторы в корпусах SMD (5 типов); вариант исполнения с низкой помехоустойчивостью; приемлемый технологически и конструктивно вариант

едва ли легко выполнимой – особенно для современных коллективов разработчиков. Тем более что коллективы эти в большинстве своем состоят из IT специалистов, не видящих места для проявления физических и даже радиотехнических эффектов в своей работе. Для устройств критических приложений и безопасности это может оказаться фатальным…

Библиографический список

1. Васильев С.Н., Кирпичников А.П., Ботвинёнок А.А. Проблемы обеспечения безопасности в современных микропроцессорных системах управления подвижным составом, вызванные особенностями современной элементной базы, и их решение на примере блока безопасности «БАРС» вагонов 81–760 Московского метрополитена // Бюллетень Объединенного ученого совета ОАО «РЖД». 2016. № 5. С. 13 – 25.

2. Centre for Research on the Epidemiology of Disasters (CRED) www.emdat.be

3. Кирпичников А.П. Вопросы отказоустойчивости и безопасности в устройствах ЦОС критических приложений // Докл. 14-ой Междунар. конф. “Цифровая обработка сигналов и ее применение”. – Москва, 2012. – Т. 1. – С. III–V.

4. Кирпичников А.П. Новая роль микропроцессорных систем: обеспечение безопасности перед лицом катастроф // 16-ая Международная конференция «Цифровая обработка сигналов и ее применение – DSPA-2014». – Москва, 2014. Т.1, С.25-29.

5. Пат. №2439666 РФ. Блок безопасности с контролем достоверности входной информации / А.П. Кирпичников // Бюл. – 2010.

6. Пат. №2449900 РФ. Блок безопасности / А.П. Кирпичников // Бюл. – 2010.

7. Кирпичников А.П., Ботвинёнок А.А., Медуницин Н.Б. Многоканальная микропроцессорная система управления со сверхвысокой безопасностью для поездов Московского метрополитена //Датчики и Системы, 2014, №9, С.38-45.

8. И.Б.Шубинский «Функциональная надежность информационных систем» – М.:Надежность, 2012, 294с.

Сведения об авторах

Алексей П. Кирпичников – начальник отдела Института проблем управления им. В. А. Трапезникова РАН (ИПУ РАН), Россия, Москва, тел. +7 (495) 334-89-10, e-mail: abramo@ipu.ru

Станислав Н. Васильев – академик РАН, доктор физ.-мат. наук, главный научный сотрудник Института проблем управления им. В. А. Трапезникова РАН (ИПУ РАН), Россия, Москва, тел. +7 (495) 334-89-10, e-mail: snv@ipu.ru

Поступила 20.03.2017