# Многоуровневая защита электронной аппаратуры от воздействия электростатических разрядов: от схемного до системного уровня

**Почти каждый из нас в детстве экспериментировал со статическим электричеством, разделяя заряды трением натуральной шерсти о синтетические материалы. Когда мы стали разработчиками, настройщиками или специалистами по обслуживанию полупроводниковой техники, стало ясно, что электростатические разряды — жестокий враг, безжалостно повреждающий электронные приборы. Ущерб, наносимый электростатическими разрядами электронной промышленности в мире, измеряется миллиардами долларов в год.**

**Антон ЕРЕМИН**
ant@s-erp.ru

Выбросы электромагнитной энергии, к которым относятся электростатические разряды, могут приводить к временному нарушению работы оборудования или его повреждению. Этим они отличаются от обычных помех, которые, несмотря на более длительное воздействие, чаще всего только нарушают нормальную работу приемника помехи. После прекращения воздействия шума работоспособность устройств, как правило, восстанавливается. В соответствии с ГОСТ Р 53734.1-2014 (МЭК 61340-1:2012) электростатический разряд (ЭСР) — это перенос заряда непосредственным прикосновением или пробоем при разности потенциалов между объектом и окружающей средой при непосредственном соприкосновении или пробое.

При рассмотрении последствий электростатических разрядов используют следующую классификацию:

- электростатический разряд на электронный компонент (дискретный или в интегральном исполнении);
- электростатический разряд на корпус оборудования;
- непрямой электростатический разряд, при котором нарушение работы электронной схемы является результатом электромагнитного импульса токов ЭСР, протекающих вблизи приемника помехи.

Стандарт ГОСТ 30804.4.2-2013 устанавливает регламенты испытаний на устойчивость к электростатическим разрядам. В документе приведены требования как к испытаниям на прямое воздействие электростатическими разрядами (методы воздушного разряда и контактного разряда), так и непрямое воздействие.

Электростатический разряд на электронный компонент — наиболее грозное явление, приносящее убытки как за счет явного повреждения компонентов, так и неявного повреждения, выражающегося в снижении ресурса компонента при эксплуатации. Интересно, что в отдельных случаях «поврежденные» партии компонентов имели увеличенный срок службы по сравнению с референтной группой, демонстрируя свойства самовосстановления.

Оператор может даже не ощутить факт разряда, если электростатическое напряжение не превышает порог чувствительности человека, определенный на уровне 1,5–2 кВ. Поэтому оператор должен носить антистатический браслет или, как минимум, прикоснуться к «мягко заземленным» конструкциям, прежде чем касаться компонента. Рабочие поверхности и окружающие конструкции должны быть «мягко заземлены» через резистор номиналом несколько сотен килоом. «Жесткое», низкоимпедансное заземление конструкций приводит к возникновению в них больших токов ЭСР, что становится причиной излучаемых помех высокого уровня. В этом случае оборудование в пластиковом корпусе оказывается более уязвимым для таких помех, чем оборудование в металлическом корпусе.

Электростатический разряд вызывает в электронных компонентах три основных вида повреждения:

- Пробой изолирующего слоя $SiO_2$. Например, в металлооксидных полупроводниках типовая толщина оксидного слоя составляет 0,1 мкм, поэтому при прочности такой изоляции 7 МВ/см она может быть повреждена напряжением выше 70 В.
- Прожиг дорожек металлизации. Прожиг металлических проводников для типового времени электростатического разряда начинается уже при значениях тока 2 кА/мм$^2$, при которых происходит миграция частиц алюминия. Полное размягчение или отслоение происходит при токах порядка 30 кА/мм$^2$. Ток прожига медных проводников примерно в 2,5 раза превышает эти значения.
- Повреждение пассивных или активных элементов интегральной микросхемы. Например, поликремниевые резисторы КМОП-логики могут быть повреждены при электростатическом разряде с напряжением выше 2,5–3 кВ. При этом отказ элементов (например, биполярных транзисторов) может быть и параметрическим, что выражается в снижении коэффициента передачи или увеличении уровня шума. Другой частый вид отказа активных элементов интегральных микросхем — тиристорный эффект, которому подвержена КМОП-логика с поданным питанием, если на нее поступил входной сигнал выше напряжения питания или ниже 0 В [1].

Ступенчатый принцип ослабления помехи в случае ЭСР реализуют следующим образом:

- необходимо создать условия, предотвращающие накопление зарядов, обеспечить рассеяние и нейтрализацию накопленных зарядов;

- снизить вероятность воздействия ЭСР на токопроводящие части аппаратуры;
- предотвратить передачу импульсной помехи с токопроводящих частей в чувствительные элементы схемы;
- использовать схемные, конструктивные и программные решения, повышающие устойчивость аппаратуры к воздействию ЭСР.

## Предотвращение накопления, нейтрализация и рассеяние зарядов

Для предотвращения накопления зарядов, нейтрализации и рассеяния уже накопленных зарядов на предприятии, использующем чувствительные к ЭСР компоненты, должна быть разработана программа ЭСР-управления в соответствии с ГОСТ IEC 61340-5-1-2019. Эта программа должна предусматривать организационные и технические мероприятия, направленные на снижение риска повреждения компонентов статическим электричеством. К организационным мероприятиям относят проведение обучения и аудиты. Технические мероприятия в соответствии с этим стандартом предусматривают:

- использование материалов с повышенной проводимостью, обеспечивающих стекание зарядов;
- повышение влажности воздуха;
- рассеивающие напольные покрытия;
- ионизаторы воздуха;
- индивидуальную антистатическую защиту персонала;
- антистатическую упаковку оборудования [2].

## Снижение вероятности воздействия ЭСР на токопроводящие элементы

Снижение вероятности проникновения ЭСР внутрь экранированного объема обеспечивают изоляцией этого объема от внешней среды с использованием следующих приемов, описанных в [3].

Для пластиковых или композитных непроводящих корпусов:

- используйте соединения деталей, аналогичные столярным методам «паз и гребень» или «в четверть», не образующие «прямого пути» для ЭСР внутрь экранированного объема (рис. 1);
- для защиты от ЭСР с напряжением до 20 кВ обеспечьте воздушный зазор не менее 20 мм между электронными элементами и любым незаземленным токоведущим элементом, которого может коснуться оператор (включая органы управления, индикаторы или винтовые крепления). Базовое правило обеспечения зазоров — 1 мм на 1 кВ напряжения ЭСР. При этом воздушный зазор должен быть обеспечен не только между поверхностью корпуса и элементами схемы (печатными проводниками, выводами микросхем, транзисторов), но и любыми токопроводящими деталями (например, кронштейнами, стойками). Если создать такой зазор невозможно из-за габаритных ограничений, используйте метод организации лабиринтов для увеличения пути распространения ЭСР.

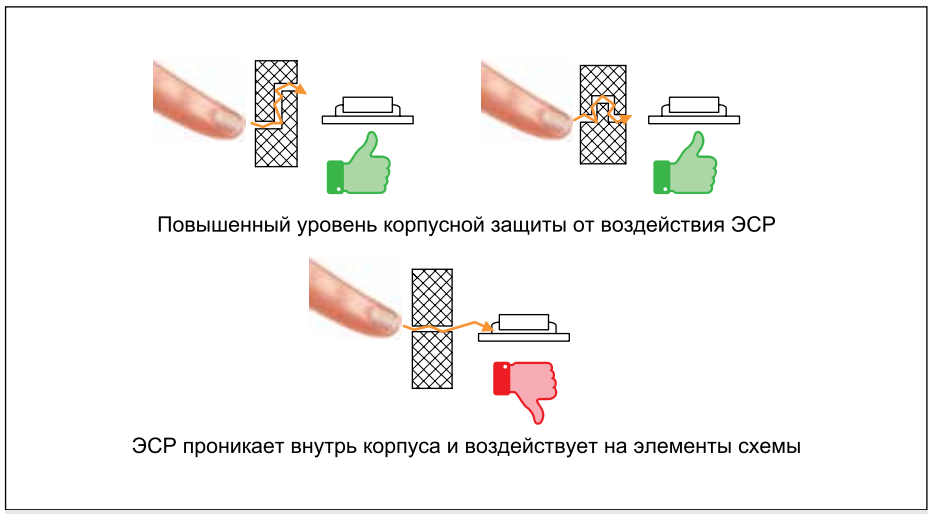


**Рис. 1.** Методы увеличения пути для электростатического разряда от точки воздействия до электронной схемы

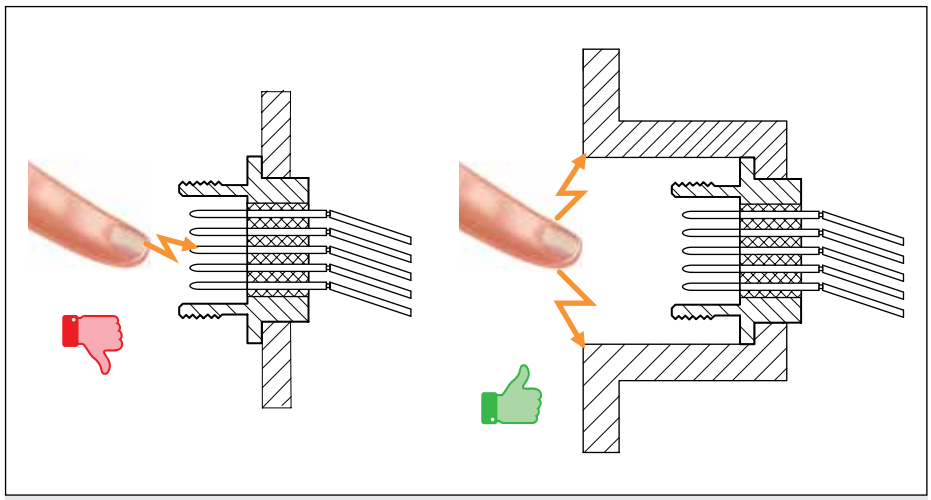

**Рис. 2.** Заглубление соединителей для целей перехвата электростатического разряда

Другая особенность непроводящих поверхностей — наличие на них грязи, потожировых следов от пальцев оператора и т. д. Для мембранных и бесконтактных клавиатур это наиболее актуально. Поэтому ЭСР может распространяться по такой поверхности на несколько десятков миллиметров, прежде чем найдет проводник с меньшим потенциалом, чем у источника. Обычно для поверхностного разряда расстояние «точка воздействия — сигнальный проводник» выбирают исходя из правила «не менее 20 мм для ЭСР с напряжением 8 кВ». Для снижения вероятности проникновения такого разряда внутрь оборудования через воздушный зазор между клавиатурой и пластиковой корпусной деталью зазор должен быть тщательно (без пор и промежутков) заполнен герметиком или уплотнен силиконовыми прокладками. Для проводящих корпусных деталей клавиатура должна иметь с ними непосредственный контакт по всему периметру, что образует так называемый перехватывающий экран для ЭСР.

Для внешних соединителей:

- не подключайте внутренний проводной монтаж от печатной платы к внешнему соединителю, если в данной конфигурации не предусмотрено его использование;
- заглубите соединители таким образом, чтобы ЭСР от руки оператора или инструмента в первую очередь был направлен на корпус оборудования или корпус соединителя (рис. 2);
- обеспечьте неиспользуемые соединители заглушками (металлическими или, в крайнем случае, пластиковыми с напряжением пробоя не ниже 20 кВ);
- в случае опасности воздействия ЭСР на контакты соединителей обеспечьте эти линии устройствами подавления переходных процессов (TVS);

- используйте заглушки с пружинными контактами, обеспечивающими электрическое соединение контактов незадействованных входных соединителей с корпусом этого соединителя;
- для защиты электронной схемы от ЭСР выше 2 кВ можно использовать зазор-разрядник между сигнальной линией и системой заземления.

Для органов управления:

- используйте переключатели и регуляторы с пластиковыми рычагами или ручками (или пластиковыми рукоятками на металлическом валу, если расположение винтов крепления рукоятки исключает их касание рукой);
- обеспечьте расстояние не менее 12 мм между доступной поверхностью мембранной клавиатуры и сигнальными проводниками, изолируйте сигнальные проводники или добавьте защитный контур по краю клавиатуры (рис. 3);
- обеспечьте дополнительную изоляцию индикаторов или светодиодов с помощью прозрачных пленок, стекол или световодов;
- скруглите углы и грани дополнительных радиаторов, расположенных вблизи отверстий или щелей в корпусе.

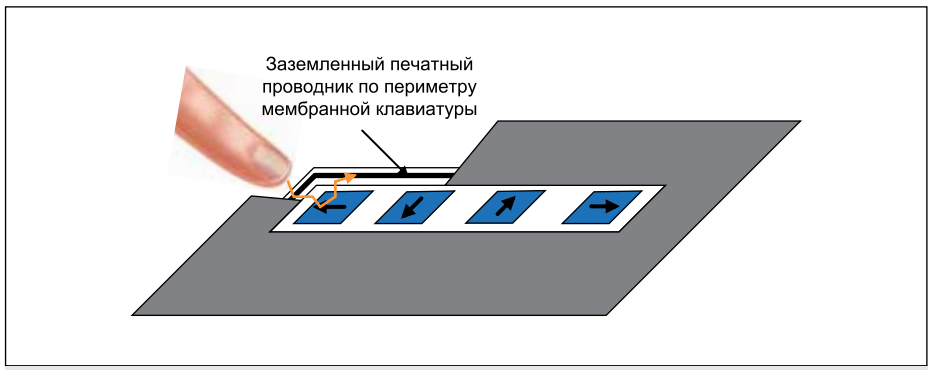


**Рис. 3.** Печатный проводник по периметру печатной платы для перехвата ЭСР

## Предотвращение передачи импульсной помехи в чувствительные элементы схемы

### *Экранирование*

Основной поражающий фактор ЭСР — это высокие амплитуды и скорости изменения электрического и магнитного полей, более характерные для радиолокационных станций: токи в десятки ампер с временем нарастания менее 1 нс, электрические поля с напряженностью порядка киловольт на метр, магнитные поля в килоамперы на метр. Эти воздействия предъявляют соответствующие требования к однородности корпусных экранов, размерам отверстий и качеству соединения в зоне стыковки деталей. Если на пути протекания токов ЭСР возникает неоднородность, имеющая на данной частоте значительный импеданс, то в этой точке может возникнуть вторичный ЭСР, что означает новый источник помеховой активности.

Если вы используете металлический корпус для разрабатываемого изделия, то с точки зрения ЭСР для вас есть две новости. Хорошая новость в том, что металлический корпус обеспечивает путь для токов ЭСР в обход электронной схемы. Плохая новость — металлический корпус в силу своей природы стимулирует ЭСР. Как мы говорили ранее, после воздействия ЭСР потенциал металлического корпуса из-за ненулевой индуктивности в системе заземления может составлять 1500–2000 В. Если система базово-возвратного заземления прибора отключена от системы экранирующе-защитного заземления (так называемая плавающая система заземления), то между корпусом и электронной схемой возникает электрическое поле высокой напряженности. Это может вызвать помехи в электронной схеме или привести к вторичному ЭСР между корпусом и токопроводящими элементами схемы. Как мы упоминали, для предотвращения повреждения схемы вторичным ЭСР необходимо соблюдать минимальные воздушные зазоры или использовать вторичное экранирование. Если система базово-возвратного заземления (то есть «сигнальный общий») соединена с системой экранирующе-защитного заземления (то есть «корпус»), то в случае ЭСР потенциал схемы повышается до потенциала корпуса и вероятность вторичного разряда снижается практически до 0. Соединение сигнального общего с корпусом возле интерфейсных соединителей также помогает снизить излучение помехи от кабелей, поэтому подобный прием может одновременно иметь два положительных эффекта. К сожалению, в этом случае повышенный потенциал сигнального общего транслируется через соединительные кабели в другое оборудование как помеха общего вида (то есть между «землей» системы и сигнальным проводником).

Все доступные для касания токопроводящие детали должны быть заземлены для предотвращения вторичного ЭСР. Элементы электронной схемы должны быть отделены от таких незаземленных деталей на расстояние не менее 10 мм, а от заземленных — не менее 1 мм. Примером такой токопроводящей детали может служить шильдик прибора, установленный на окрашенную поверхность посредством винтов или заклепок. Электрический контакт в этом случае может отсутствовать изначально (из-за изолирующих свойств краски) или быть утрачен при эксплуатации (поскольку эти соединения обычно не рассматриваются конструктором как критические с точки зрения долговечности низкоимпедансного контакта). При прикосновении к шильдику оператором — носителем заряда потенциал детали изменяется скачкообразно. Разность потенциалов между винтом крепления шильдика с внутренней стороны и окружающими проводниками приводит к возникновению электрического поля с высокой напряженностью, что может привести к вторичному ЭСР. Вторичный ЭСР более опасен для аппаратуры, поскольку характеризуется большей амплитудой тока из-за гораздо более низкого внутреннего сопротивления металлической детали по сравнению с человеческим телом. Потенциал человеческого тела может достигать 25 кВ, и этот потенциал может полностью быть передан на незаземленную деталь. Электрическая прочность воздуха (до пробоя) составляет около 3 кВ/мм, поэтому для разности потенциалов 25 кВ расстояние между проводниками не должно быть менее 1 см (с небольшим запасом). Однако необходимо помнить, что при повышении влажности электрическая прочность воздуха может быть существенно ниже. Если деталь заземлена, то индуктивность всего пути заземления для типичного для ЭСР времени нарастания токового импульса может привести к возникновению разности потенциалов между заземленной деталью и элементом схемы порядка 1,5 кВ, поэтому расстояния в 1 мм (опять же, с небольшим запасом) в данном случае достаточно.

### *Фильтрация*

В отдельных случаях у конструктора нет возможности защитить сигнальный проводник, гальванически связанный со схемой, от воздействия ЭСР. Это, например, может быть наружная телескопическая антенна прибора. Практически все выпускаемые в настоящее время микросхемы имеют на входах и выходах встроенные диоды защиты от перенапряжений, предназначенные для шунтирования положительных и отрицательных выбросов напряжения. Однако с переходом на более малоразмерные технологии подобные элементы тоже становятся все более маломощными. Помочь защитным диодам можно, если добавить последовательно включенное в сигнальную линию сопротивление (активное или реактивное), как показано на рис. 4. В качестве таких последовательных элементов могут выступать высоковольтные резисторы, катушки индуктивности или обычные ферритовые фильтры или резисторы поверхностного монтажа. При использовании резисторов или ферри-

товых фильтров для поверхностного монтажа необходимо принимать меры для предотвращения поверхностного разряда (как по поверхности корпуса этих элементов, так и через возможные загрязнения на поверхности печатной платы). Для этого необходимо увеличить длину защитного резистора, использовав набор из 10–20 последовательно включенных сопротивлений, разделенных промежутками. Параметры резисторов или ферритовых фильтров должны быть выбраны исходя из необходимости ограничить максимально возможный ток ЭСР до уровня, который могут шунтировать внутренние защитные устройства микросхемы. Значения токов можно найти в технических описаниях на микросхемы.

Более эффективная фильтрация может быть обеспечена при использовании двухэлементных фильтров, состоящих из блокирующего шумовые токи элемента (резистора/резисторов или ферритового фильтра) и шунтирующего шумовые токи элемента (конденсатора). Для эффективной защиты фильтр должен обеспечивать подавление сигнала помехи не менее 40 дБ в диапазоне 100–500 МГц, в котором сосредоточена большая часть энергии ЭСР. Номинал шунтирующего элемента обычно выбирают в диапазоне 100–1000 пФ, а блокирующего элемента — в пределах 50–100 Ом. Эти мероприятия могут обеспечить сохранность чувствительных элементов схемы, но обычно не предотвращают сбоев в работе схемы.

### *Подавление амплитуды переходных процессов*

К сожалению, описанный выше прием ограничения токов ЭСР, поступающих на вывод микросхемы, не всегда применим. Для высокоскоростных интерфейсов внесение дополнительного импеданса в линию может привести к недопустимому сглаживанию фронтов и срезов импульса (вплоть до смыкания глазковой диаграммы). Кроме того, множество простых полупроводниковых устройств вовсе не имеют встроенной защиты от перенапряжений, и описанный прием ограничения токов в таком случае неэффективен. Устройства подавления переходных процессов должны (аналогично фильтрам) обеспечивать подавление как минимум 40 дБ для переходных процессов со временем нарастания 0,7 нс, что обеспечивает снижение амплитуды импульса с 8 кВ до 80 В. Эквивалентная верхняя граница частотного диапазона при этом будет на уровне 460 МГц. В идеальном случае такие устройства должны характеризоваться подавлением в 70 дБ для переходных процессов со временем нарастания 0,2 нс, что подразумевает снижение амплитуды импульса с 24 кВ до 8 В. Эквивалентная верхняя граница рабочего диапазона частот — 1,6 ГГц.

Аналогично случаю фильтрации помех эти элементы должны вносить минимальные искажения в полезный сигнал, то есть не изменять его напряжение, ток и форму фронта цифрового сигнала. Принцип работы параллельно включенных ограничителей состоит в том, что при превышении входным напряжением определенного уровня сопротивление ограничителя становится существенно меньше, чем входное сопротивление защищаемого элемента. В этом случае важнейшим параметром является время срабатывания ограничителя, то есть его перехода в проводящее состояние. Кроме времени срабатывания, большое значение имеют паразитная емкость, которая аналогично конденсатору сглаживает фронт цифрового сигнала, и паразитная индуктивность корпуса и выводов, повышающие импеданс ограничителя для высокочастотных токов помехи. Низкоимпедансное подключение к системе заземления для ограничителей напряжения так же важно, как и для емкостных фильтров.

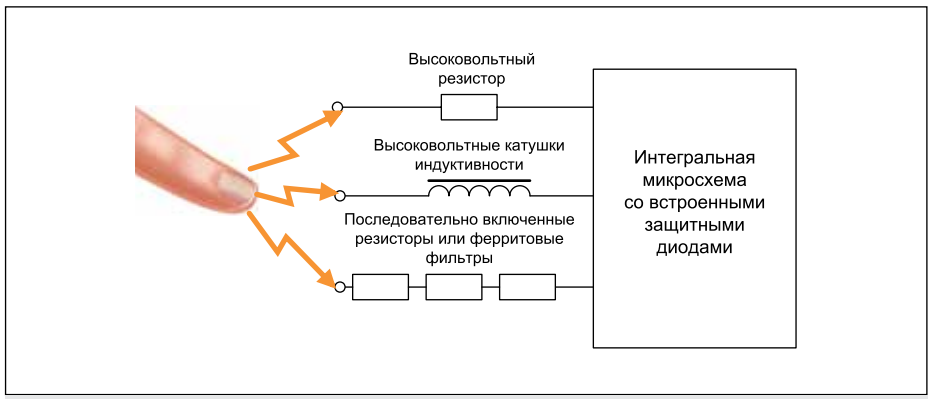


**Рис. 4.** Последовательно включаемые элементы защиты от воздействия ЭСР

В самом простом случае в качестве ограничителей напряжения используют диоды или стабилитроны. Более эффективными ограничителями являются диоды с обратным смещением и варисторы [4].

## Схемные и конструктивные решения для повышения устойчивости аппаратуры к воздействию ЭСР

Повышения устойчивости аппаратуры к воздействию ЭСР можно достигнуть путем выбора элементов, допускающих выбросы напряжения с большей амплитудой и соблюдения ряда правил при проектировании печатной платы.

Остановимся подробнее на правилах проектирования печатных плат. Одно- и двухсторонние печатные платы наиболее подвержены воздействиям ЭСР как в части нарушения нормальной работы, так и повреждения элементов. Однако даже в этом случае знание основ электромагнитных взаимодействий может помочь повысить устойчивость схемы. Система сигнального заземления на одно- и двухсторонних печатных платах имеет чрезвычайно высокий импеданс на частоте ЭСР. Одним из возможных методов снижения импеданса системы заземления становится использование дополнительной, внешней поверхности заземления. Конструктивно такая поверхность может быть выполнена в виде листа алюминиевой или медной фольги с изоляционным покрытием, расположенной на минимально возможном расстоянии от печатной платы. Основной критерий в данном случае — минимизировать импеданс соединения «проводник заземления — поверхность», не допуская при этом давления токоведущих элементов платы на изоляционный слой. Вот почему такую поверхность обычно располагают со стороны монтажа, соединяя ее с системой заземления на печатной плате в как можно большем количестве точек. Больше точек соединения — меньше выбросы напряжения в системе заземления печатной платы при воздействии ЭСР. Большее количество соединений рекомендуют для критических зон на печатной плате, таких как зона расположения процессора, микросхем памяти, интерфейсных соединителей печатной платы, чувствительных к тиристорному эффекту микросхем КМОП и т. д. На практике при добавлении внешней поверхности заземления удается повысить стойкость двухсторонней печатной платы к повреждению при непосредственном воздействии ЭСР с 2 до 15 кВ [5].

Многослойные печатные платы обеспечивают повышение стойкости к ЭСР до 100 раз. Для снижения влияния ЭСР на такие платы необходимо применять следующие приемы:

- Располагайте поверхности питания и заземления как можно ближе к внешним сигнальным слоям. Это снижает размер контура для магнитного поля и реализует отклоняющее экранирование для электрического поля помехи.
- По возможности выделите для токов ЭСР отдельную поверхность экранирующего заземления. Фильтрующие конденсаторы и устройства защиты от выбросов напряжения генерируют сильные токи в системе заземления в момент воздействия ЭСР. Эти токи могут вызвать выбросы напряжения даже в низкоимпедансной системе сигнального заземления.

- Обеспечьте минимальное расстояние между поверхностью питания и поверхностью заземления, по возможности используйте две пары таких поверхностей. Распределенная емкость имеет очень низкую паразитную индуктивность и в том числе обеспечивает эффективную фильтрацию помехи по питанию в диапазоне частот от нескольких сотен мегагерц до нескольких гигагерц.
- Минимизируйте длину сигнальных проводников, особенно во внешних сигнальных слоях. Используйте полосковые линии для чувствительных сигналов.
- Организуйте дополнительные защитные электромагнитные зоны вокруг чувствительных элементов: экранируйте их, применяйте дополнительные фильтры перед вводом проводников в экранированное пространство.

## Программные методы повышения устойчивости аппаратуры к воздействию ЭСР

Разработчики электроники давно убедились, что применение микроконтроллеров обеспечивает как повышение текущих характеристик приборов, так и расширение функционала аппаратуры в целом. Однако использование микроконтроллеров не только несет ощутимые преимущества, но и ставит новые, неизвестные ранее вопросы при обеспечении ЭМС. В частности, было установлено, что микропроцессорные системы особенно чувствительны к нестационарным процессам, то есть воздействиям ЭСР, перенапряжениям, импульсным помехам и вариациям напряжения питания.

Разработчики программного обеспечения для микроконтроллеров часто считают, что обеспечение ЭМС — это забота инженеров-схемотехников или, на крайний случай, разработчиков корпусов и компоновки прибора. И уж во всяком случае не инженеров-программистов. Действительно, основная нагрузка по обеспечению ЭМС ложится на разработчиков аппаратных средств, и их задача — максимальное ослабление сигнала кондуктивной и излучаемой помехи перед его поступлением в приемник и обеспечение устойчивости к внешнему электромагнитному воздействию. Однако последним рубежом защиты на пути помех всех типов (в том числе и от ЭСР) для микропроцессорных систем является должным образом разработанное программное обеспечение. Дополнительное преимущество программных методов в том, что доработка кода программы на любых стадиях проектирования стоит приблизительно одинаково, в то время как внесение изменений в схему или конструктив прибора часто приводит к значительным затратам. В особенности это относится к поздним стадиям разработки, например к этапу испытаний. Поэтому приемы программирования для обеспечения ЭМС не являются средством штопанья дыр, оставленных разработчиками аппаратных средств, а одним из средств борьбы с помехами на пути ее следования в приемник.

Основное условие помехоустойчивости ПО — выполнение правильных команд в правильной последовательности. Ошибки при выполнении программы могут возникать из-за нарушения порядка выполнения программы (например, при повреждении содержимого счетчика команд процессора) или выполнения ошибочной команды (например, при повреждении содержимого области, где хранилась команда). Более безопасный исход наступает, если помеха приводит к переходу в начало другой команды, расположенной ближе к концу или началу программы (так как команды могут быть как однобайтными, так и многобайтными). Хуже, если происходит переход к ячейке, содержащей, например, второй байт команды или данные. Результатом такой ошибки может стать выполнение программой бесконечного цикла, или зависание. Для обнаружения такого типа ошибок ПО система должна периодически контролировать длительность выполнения операций микропроцессором и функционирование программы в заданной для процедуры области памяти. Контроль таких состояний незначительно влияет на длину программного кода, добавляя обычно лишь несколько строк [6].

Кратко рассмотрим наиболее часто используемые для контроля корректности исполнения программы инструменты:

- сторожевые таймеры;
- программные контрольные точки;
- блоки пустых команд;
- обнаружение и блокирование неиспользуемых векторов прерываний.

Строго говоря, эти инструменты не повышают непосредственно стойкость к электромагнитным воздействиям, но обеспечивают контролируемые процедуры обработки обнаруженных ошибок.

Теме повышения эффективности сторожевых таймеров посвящено множество статей и научных работ, например [7, 8]. Основное правило в этом случае: сторожевой таймер должен стать средством контроля не только активности программы, но еще в большей мере контроля выполнения команд в правильной последовательности. Для этого разработчики программного обеспечения должны использовать в составе разрабатываемого ПО специальные блоки, выдающие сигнал сброса сторожевого процессора только в том случае, если фактическая последовательность выполнения командных блоков совпадает с заданной.

Более широкие возможности могут быть обеспечены при использовании многоступенчатых сторожевых таймеров. Эти устройства способны поддерживать автоматическое выполнение следующих шагов:

- перевод системы в безопасное состояние;
- сохранение отладочной информации в энергонезависимой памяти;
- выдачу сигнала «сброс» на микроконтроллер.

Самым мощным на сегодня сторожевым устройством можно по праву считать сторожевой процессор, способный взять на себя часть вычислительной нагрузки микроконтроллера при контроле хода выполнения программы. Последние исследования показывают, что сигнатурный анализ, выполняемый сторожевым процессором, — один из самых эффективных инструментов повышения надежности систем на основе микроконтроллеров [9].

Использование программных контрольных признаков — токенов, являющихся индикатором передачи управления определенному блоку команд, — особенно эффективно при реализации модульного подхода при разработке программ для микроконтроллеров. Этот метод обнаруживает факт повреждения содержимого счетчика команд как результат воздействия электромагнитных помех. При передаче управления любому модулю программа присваивает одной или нескольким глобальным переменным признак модуля, который должен быть проверен на выходе из него. Если полученный на входе в модуль признак не совпадает с контрольным значением на выходе, значит, воздействие помехи на счетчик команд при исполнении модуля привело к переходу в другой модуль (например, из процедуры X в процедуру Y, как показано на рис. 5). Проверка идентификатора может быть проведена и в ходе исполнения программного модуля несколько раз для того, чтобы минимизировать негативные последствия неконтролируемого перехода.

Блоки пустых команд используют, если программный код занимает только часть общего объема памяти программ. В этом случае обращение к неиспользуемому сегменту памяти программ приведет к исполнению ошибочного кода. Неиспользуемая область памяти обычно заполнена байтами FFH, что, например, для микроконтроллера 8051 соответствует команде MOV R7, A (то есть переместить содержимое аккумулятора в регистр R7). Таким образом, программа, переброшенная при воздействии помехи в такую область, будет исполнять команду перемещения данных до тех пор, пока не достигнет предела области памяти программ. Затем программа перейдет к исполнению команды по адресу 0000H, что аналогично поступлению сигнала «сброс». Описанный эффект может быть признан наиболее безопасным, поскольку для других приложений считывание FFh как программного кода или данных может привести к более тяжелым последствиям. Чтобы избежать негативных последствий такого перехода, неиспользуе-

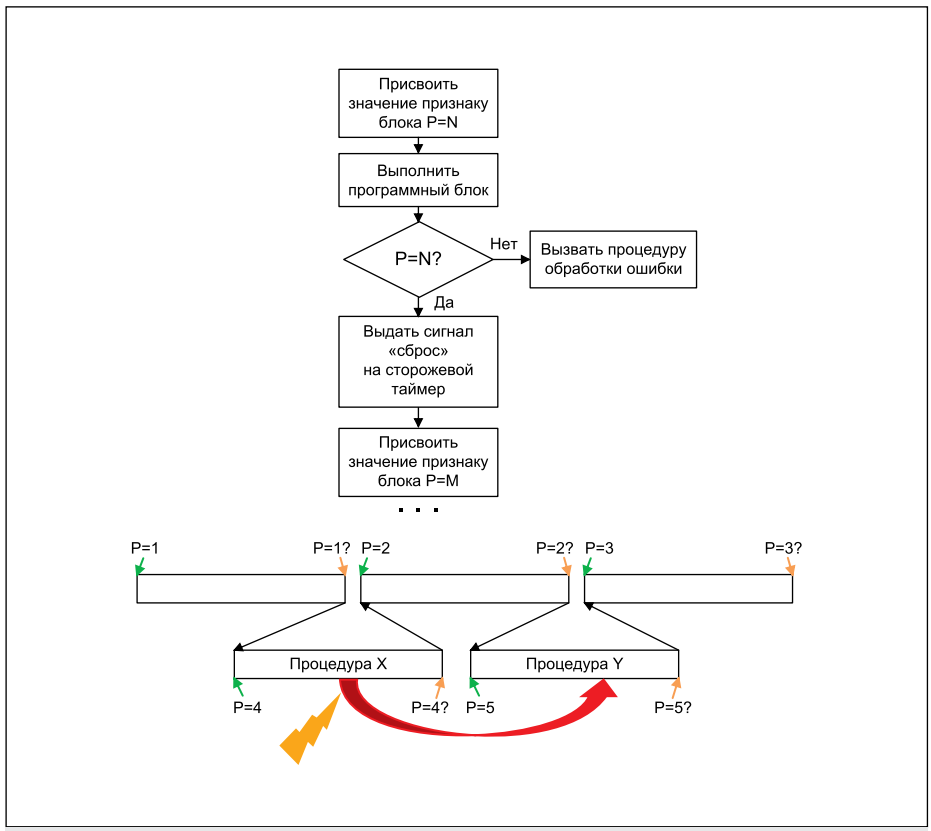


**Рис. 5.** Алгоритм контроля хода выполнения программы с использованием признаков-токенов

мая область памяти программ должна быть принудительно заполнена блоками команд «NOP — нет операции» (или аналогичными командами, не предусматривающими активных действий), завершающимися передачей управления модулю обработки ошибок или срабатыванием сторожевого таймера по истечении тайм-аута.

Неиспользуемые векторы аппаратных прерываний также могут быть причиной ошибок при исполнении программного кода. Поступление помехового импульса на вывод незадействованного прерывания способно привести к считыванию вектора этого прерывания и исполнению ошибочного кода. Самое простое в случае активации неиспользуемого вектора прерывания — выполнение команды «выход из прерывания» или передача управления модулю обработки ошибок. Прерывания по фронту сигнала часто становятся необходимостью, однако при этом следует принимать меры для защиты линии прерываний от импульсных помех. Поэтому если имеется возможность использовать прерывания по уровню, то выбор должен быть сделан в пользу этого варианта.

## Заключение

Как мы убедились, высокий уровень защиты электронной аппаратуры от воздействия электростатических разрядов не может быть обеспечен с помощью только одного инструмента. Поэтапное ступенчатое ослабление уровня воздействия — эффективный метод, который должен быть взят на вооружение разработчиками высоконадежной техники.

Очевидно, в этой статье, в силу ее ограниченного объема, приведен только общий перечень мер повышения устойчивости техники к воздействию ЭСР. Детально изучить эту тему, в том числе и на конкретных примерах, можно на одном из семинаров, проводимых ООО «КРЭЛС» в Москве и Санкт-Петербурге (см. стр. 112).

## Литература

1. Mardiguian M. Electrostatic Discharge. Understand, Simulate, and Fix ESD Problems. John Wiley & Sons, Inc, 2009.
2. Кечиев Л. Н., Пожидаев Е. Д. Защита электронных средств от воздействия статического электричества. М.: Технологии, 2005.
3. Barnes J. R. Designing Electronic Systems For ESD Immunity. Conformity, February 2005.
4. Joffe E. B., Sang K. Lock, Grounds for Grounding. A Circuit-to-System Handbook John Wiley & Sons, Inc, 2010.
5. Montrose M. I. Printed Circuit Board Design Techniqies For EMC Compliance. A Handbook for Designers. The Institute of Electrical and Electronics, 2000.
6. Ott H. Electromagnetic Compatibility Engineering. John Wiley & Sons, Inc, 2009.
7. Zlatanov N. Architecture and Operation of a Watchdog Timer, DOI: 10.13140/RG.2.1.1149.1605.
8. Murphy N. Watchdog Timers. Embedded Systems Programming. 2000.
9. Платунов А. Е., Стерхов А. С. Сторожевые механизмы во встраиваемых вычислительных системах. Научно-технический вестник информационных технологий, механики и оптики, 2017.