УДК 621.37/.39.001.12/.18; 621.396.6:621.391.827

А.Г. Бурутин, Н.В. Балюк, Л.Н. Кечиев

Электромагнитные эффекты среды и функциональная безопасность радиоэлектронных систем вооружения

Рассматривается проблема функциональной безопасности, определяемой ЭМС. Показана ее комплексность, приводится расширенная классификация и характеристика электромагнитных эффектов, формирующих электромагнитную среду. Отмечаются опасности, вызванные неадекватно функционирующими системами и оборудованием в оперативной электромагнитной среде. Обосновывается необходимость развития более совершенных методов теории и практики создания радиотехнических и электронных систем, которые обеспечат целостность функциональной безопасности на всем жизненном цикле систем.

Формулируются требования к методам и средствам испытаний и измерений, экспериментально-исследовательской базе, которые должны соответствовать реальным электромагнитным эффектам, отвечающих требованиям функциональной безопасности.

Выдвигаются требования к компетентности персонала, связанного с оборудованием и системами в течение всего жизненного цикла, что является важнейшим фактором обеспечения целостности функциональной безопасности.

функциональная безопасность, электромагнитная совместимость, электромагнитный эффект, вооружение, военная техника, программа, испытание

Введение

Развитие систем вооружения [1, 2] идет по направлению расширенного применения электронных систем, построения комплексов по принципу «система в системе», применения роботизированных систем, замены гидравлических систем на электромеханические. Электронные системы вооружения на основе микроэлектроники позволяют с одной стороны снизить энергопотребление систем, уменьшить уровни полезных сигналов, повысить быстродействие при обработке и передаче информации, а с другой стороны – обладают относительно низкой помехозащищенностью. Этот фактор становиться все более актуальным, поскольку наличия широкого спектра электронных средств усложняет электромагнитную обстановку, в которой приходится функционировать электронным системам, увеличивает вероятность деструктивных воздействий на среду передачи и обработки информации, что может привести к нарушениям функциональной безопасности.

Ситуация усложняется с появлением новых технических средств мощных преднамеренных электромагнитных воздействий [3, 4], которые могут быть использованы в качестве оружия [5, 6, 7] или средств электромагнитного терроризма [8].

Многонациональные военные операции, быстрое увеличение систем электромагнитного оружия, расширенное использование радиочастотного ресурса во всем мире привели к рабочей электромагнитной обстановке, с которой разработчики систем ранее не сталкивались. Растущее присутствие преднамеренных излучателей, расположенных по всему миру, – существенные вызовы вооруженным силам. Подобные условия заставляют рассматривать традиционную проблему электромагнитной совместимости (ЭМС) применительно к системам вооружения шире, включая в единый комплекс вопросы и задачи обеспечения функциональной безопасности, связанные с электромагнитными эффектами.

ЭМС и функциональная безопасность

Информационные технологии все более широко используются в приложениях, связанных с безопасностью. Ошибки в работе и сбои электронного оборудования в результате нарушений требований ЭМС могут вести к опасным ситуациям и риску нанесения вреда здоровью людей, оборудованию и окружающей среде.

Исторически складывалось так, что подразделения, которые занимались ЭМС и безопасностью, в пределах одной организации работали в значительной степени независимо друг от друга. В этом случае, безопасность, определяемая ЭМС (ЭМС-безопасность), оказалась вне поля зрения специалистов. Для гражданских приложений, которые опираются, например, на Директиву ЕС по ЭМС [9], требования по функциональной безопасности не определены. Наличие знака соответствия «CE», отмечающего соответствие требованиям Директивы ЭМС (или ее гармонизированным стандартам), не могут гарантировать, что вопросы ЭМС-безопасности правильно идентифицированы и законодательно решены.

Различные электронные технологии имеют отличающийся потенциал сохранения качественных показателей при воздействии электромагнитных возмущений (ЭМВ). Многие традиционные информационные технологии, которые на определенном этапе своего развития были не восприимчивы к ЭМВ, при усложнении электромагнитной обстановки и увеличении уровня возмущений, стали чувствительны к ним. Кроме этого, современная элементная база имеет тенденцию к увеличению восприимчивости ЭМВ.

Для того, чтобы корректно управлять ЭМС-безопасностью, необходима оценка последствий опасности и оценка риска. При этом следует принимать во внимание следующее [10]:

- электромагнитные возмущения, которыми может быть подвергнута аппаратура;
- разумно обозримые результаты воздействия таких возмущений;
- эффект воздействия ЭМВ от одного аппарата на другой;
- разумно обозримые параметры безопасности (серьезность, масштаб риска, уровень целостности безопасности), которые могут быть нарушены ЭМВ;
- уровень требований, которые необходимо выполнить, чтобы обеспечить желаемый уровень ЭМС-безопасности.

Такие опасности и оценки рисков вместе с законченными решениями, техническими требованиями, проектными решениями и тестами должны формировать часть из требований обеспечения функциональной безопасности и должны быть документированы. Проектные решения и связанная с ними документация существенно отличаются между организациями и между проектами, но там, где опасности и риски выше (то есть применяются более высокие уровни целостности безопасности), требуются более высокие уровни деятельности и документации.

Безопасность – термин, использованный, чтобы обозначить понятие согласованного понимания опасностей и их рисков, которые являются приемлемыми для данного общества в конкретной ситуации. Законы о безопасности вообще требуют, чтобы продукты были разработаны и произведены настолько безопасными, насколько люди «имеют право ожидать».

Функциональная безопасность – термин, использованный, чтобы охватить опасности и риски, связанные с ошибками или сбоями при *функционировании* систем, устройств или аппаратов. Это отлично от безопасности, которая определяет потенциал устройства противостоять таким опасностям как возгорание, удар током и образование ядовитых паров. Базовыми документами в области функциональной безопасности следует считать стандарты [11–17], которые гармонизированы с международным стандартом МЭК 61508. Он соотносится с гражданскими системами и в явном виде не затрагивает взаимоувязанные вопросы ЭМС и функциональной безопасности.

При проектировании связанных с безопасностью систем необходимо включать анализ опасностей и исследования рисков, которые принимают во внимание, по крайней мере, в следующих направлениях:

- ошибки применения – или случайные (такие, как ошибки при инсталляции оборудования или ошибки оператора) или преднамеренные (перегрузка или использование для непредусмотренных целей),
- обозримые ошибки проекта,
- применение в экстремальной среде, включая, среди других, электромагнитные эффекты, высокие температуры, вибрации и т.п.,

- последствия (опасности) с их вероятностями (рисками), которые вызваны отмеченными выше факторами.

Весь персонал, ответственный за управление ЭМС и безопасностью в организации должен понимать значения этого и должен быть знаком с соответствующей нормативной документацией, быть компетентным исполнить ее требований и правильно применять руководящие принципы на практике. Возможны случаи, когда потребуется помощь специалиста.

Терминология

Базовая терминология в области функциональной безопасности приведена в [14], но она ориентирована в первую очередь на трактовку с позиций вероятностных подходов. В контексте рассматриваемой проблемы представляется, что основные термины должны носить более выраженную смысловую нагрузку. Используя материалы [18–22] дадим определение некоторым терминам.

Опасность. Любое реальное или потенциальное условие, которое может вызвать ранение, болезнь или смерть персонала; повреждение или потерю системы, оборудования или собственности; или ухудшение окружающей среды.

Жизненный цикл. Все фазы существования системы, включая проектирование, исследование, разработку, тестирование, производство, развертывание, функционирование, поддержку (обслуживание) и утилизацию.

Сбой. Незапланированный случай или последовательность событий, приводящих к ранению, болезни или смерти персонала; повреждению или потере системы, оборудования или собственности; или ухудшению окружающей среды.

Риск сбоя. Выражение воздействия и возможности сбоя в терминах потенциальной серьезности сбоя и вероятности его возникновения.

Остаточный риск сбоя. Остающийся риск сбоя, который существует после применения всех методик его снижения, которые были осуществлены или исчерпаны в соответствии с системным порядком очередности проекта безопасности.

Безопасность. Отсутствие условий, которые могут вызвать ранение, болезнь или смерть персонала; повреждение или потерю системы, оборудования или собственности; или ухудшение окружающей среды.

Подсистема. Группировка элементов, выполняющих логическую группу функций в пределах специфической системы.

Система. Интегрированный составной объект людей, продуктов и процессов, которые обеспечивают возможность удовлетворить установленную потребность или цель.

Функциональная безопасность. Приложение разработки и принципов управления, критериев и методик для достижения приемлемого риска сбоя в пределах ограничений функциональной эффективности и пригодности, времени и стоимости по всем фазам жизненного цикла.

Отказоустойчивость. Особенность проекта, которая гарантирует, что система остается безопасной в случае отказа, и заставляет систему возвращаться к состоянию, которое не будет вызывать сбой.

Термин «безопасная система» обычно используется для описания таких систем, которые требуют наличия специальных функций, чтобы уменьшить риски до допустимого уровня. Система, требующая решения вопросов безопасности, может быть реализована в любой технологии, но в контексте ЭМС, интерес представляют электротехнические и электронные системы (включая программируемую электронику). Можно привести некоторые примеры нарушения безопасности подобных систем:

- выгорание или повреждение компонентов, антенн, и т.д.,
- деградация производительности цепей обработки сигналов спецвычислителей,
- ошибочная работа электромеханического оборудования, электронных цепей, компонентов, оружия и т.д.,
- преждевременный взрыв или воспламенение оружия и огнеопасных материалов,
- потеря связи,
- потерю управления и трекинга радара,
- погрешности показателей индикаторов и т.п.,
- нанесение вреда здоровью персонала.

Безопасная система выполняет функции безопасности и, таким образом, функция безопасности должна быть определена как в терминах функциональных возможностей (что функция делает) и целостности безопасности (вероятность выполнения функции безопасности удовлетворительно, когда это требуется).

Технические требования для целостности безопасности могут быть получены, анализируя опасности и риски и определяя степень снижения риска, которую вызывает специфическая функция безопасности. Общий принцип, – чем выше уровень требуемой целостности безопасности, тем более жесткие требования предъявляются к разработке систем, чтобы достичь более низких интенсивностей сбоев и отказов, которые требуются для достижения допустимого риска.

Требования безопасности для электрического или электронного оборудования, используемого в безопасных системах, должны быть специфицированы и определены в контексте опасности системы и оценка риска на возможно более ранней стадии ее жизненного цикла. Аспект безопасности должен быть учтен даже в процессе обслуживания и эксплуатационных процедур, поэтому и на этих этапах следует рассматривать доминирующие электромагнитные эффекты. Программные изменения и обновления могут также негативно затрагивать ЭМС систем и оборудования и, следовательно, функциональную безопасность, так что к ним нужно относиться так же, как и к аппаратно-техническим компонентам систем.

Оборудование может излучать электромагнитные поля, которые могут заметно ухудшать локальную электромагнитную обстановку, возможно вызывая деградацию функциональных возможностей в другом оборудовании. Например, аудио- или системы радиосвязи могут быть очень восприимчивы к ЭМВ, что может привести к рискам безопасности в том случае, если они используются для передачи экстренной информации и команд. Таким образом, когда планируется применить новое оборудование, должны быть предприняты шаги, гарантирующие одновременную совместную работу этого оборудования и ранее установленного таким образом, чтобы имеющие место электромагнитные возмущения не вызывали уход функциональных параметров оборудования за пределы установленных границ.

Стандартные испытания на соответствие требованиям ЭМС не всегда дают полное представление о функциональной безопасности оборудования, работающего в реальной электромагнитной обстановке. Поэтому обеспечение ЭМС в контексте функциональной безопасности требует специальных программ испытаний.

Особенно важно, чтобы вопросы обеспечения ЭМС рассматривались на возможно ранних стадиях проектирования оборудования, поскольку именно тогда могут быть приняты наиболее эффективные меры (это вероятно будут и наиболее рентабельные способы гарантировать ЭМС).

В некоторых случаях следует рассмотреть возможность нарушения требований ЭМС при электромагнитных возмущениях одновременно для ряда компонентов некоторой системы. Это особенно важно тогда, когда система спроектирована с некоторой избыточностью для обеспечения резервирования и повышения надежности работы. Важно, что меры, принятые для повышения надежности системы, могут в этом случае оказаться бесполезными в условиях ЭМВ. Очевидно, что нарушение функционирования всех параллельных компонентов системы в этом случае сведет на нет принятые меры повышения функциональной надежности оборудования.

Там, где используются защитные устройства (например, устройства амплитудного ограничения – варисторы) для достижения требуемого уровня помехоустойчивости, отказ такого устройства может вызвать снижение этого уровня и привести к нарушению ЭМС-безопасности. В этом случае отказ защитного устройства должен обнаруживаться автоматически (например, действием диагностических подсистем) или путем регулярных проверок с целью выявления любых отказов. Периодичность таких испытаний должна быть определена на основе приемлемой вероятности отказа защитного элемента в конкретном специфическом приложении.

Необходимо, чтобы информация о методах и способах обеспечения ЭМС была доступной для проектировщиков, изготовителей, наладчиков, операторов и инсталляторов, чтобы гарантировать осуществление и поддержку предпринятых в проекте мер. Это необходимо для сохранения уровней эмиссии и восприимчивости оборудования в предусмотренных проектом пределах.

Кроме этого можно отметить следующие особенности построения безопасных систем:

- не всегда признается, что система управления связана с безопасностью. Системы диагностики микропроцессорной системы должны учитывать критические ситуации, ведущие к нарушению

безопасности, и должны быть поддержаны аппаратными и программными методами проектирования;

- блокирующая функция для обеспечения безопасности должна быть выполнена схемами доказанной целостности. Блокирующая функции для обеспечения безопасности не должна быть поручена микроконтроллерам, микропроцессорам и т.д. до тех пор, пока целостность таких управляющих цепей не будет формально утверждена как адекватная относительно рисков, связанных с приложением;
- устойчивость к электромагнитным возмущениям может быть достигнута и аппаратными и программными средствами.

При модернизации оборудования необходимо провести анализ рисков и опасностей, и разработать технические задания по обеспечению целостности безопасности после внесенных изменений.

Учет электромагнитной обстановки

Одна из основных целей создания безопасной системы – оговорить для нее электромагнитную обстановку (ЭМО), чтобы технические средства не были неблагоприятно затронуты электромагнитными эффектами (ЭМЭ) во время всех фаз жизненного цикла. Эффекты могут привести к потере работоспособности системы или их уровень может быть снижен до приемлемого.

Воздействие на рецептор в определенной электромагнитной среде зависит от особенностей восприимчивости рецептора, амплитуды и частоты ЭМВ, особенностей среды и т.д. Чтобы предотвратить эти проблемы, обязательно при разработке новой системы должны быть учтены возможные электромагнитные эффекты среды. Требования к ЭМО должны быть включено в спецификацию оборудования, чтобы гарантировать удовлетворительную работу в определенной среде.

В разработке требований работоспособности и безопасности технических средств, которые предъявляются к электромагнитной среде, рассматриваются следующие основные аспекты [21, 23, 24]:

- конфигурация среды,
- конфигурация системы,
- требования к живучести,
- восприимчивость,
- перспективы применения.

Конфигурация среды. Любое оборудование, подсистема и система будут подвержены влиянию нескольких различных электромагнитных эффектов в течение их жизненного цикла. Необходимо определить каждую ЭМО. Например, ракета будет находиться в различных электромагнитных средах во время отгрузки, хранения, контроля, запуска и во время подхода к цели.

Конфигурация системы. Конфигурация оборудования, подсистемы и системы может измениться в зависимости от местоположения и в течение жизненного цикла. В итоге ее восприимчивость к электромагнитной среде может также измениться. Поэтому, в разработке требований к работоспособности должны быть идентифицированы для каждой из определенных сред режимы работы, экранирование и т.д.

Требования к живучести. Важно определить различие между условиями работоспособности и живучести. Обычно есть существенное различие между уровнями среды, которые ухудшат работоспособность и уровнями, которые постоянно приводят к отказам. Надо иметь в виду, что есть много мер и средств, которые могут быть использованы, чтобы защитить оборудование от повреждения, когда оно не работает, но которые невыполнимы, когда оно работает.

Воспримчивость. Восприимчивость оборудования, подсистемы или системы может быть различной в зависимости от особенностей проекта. Эти особенности, так же как целостность экранирования, выбор компонентов и использование фильтрации нужно учитывать, оценивая воздействие электромагнитной среды на оборудование. Кроме того, для использования на новых платформах перспективно применение неметаллических материалов. Поскольку они обеспечивают слабое экранирование или его отсутствие, система, подсистема или оборудование могут быть подвергнуты воздействию ЭМЭ среды более интенсивно, чем на платформе с

обычными металлическими материалами.

Перспективы применения. Определение ЭМЭ, которые могут воздействовать на оборудование, подсистемы или системы, должно также включать рассмотрение любых возможных будущих приложений и изменений в среде. Оборудование, которое проектировалось для работы в одной среде, со временем может быть установлено в другой, или использоваться для выполнения функций, которые не были запланированы при первоначальной разработке. Даже при неизменном местоположении со временем интенсивность ЭМЭ возрастает, что следует учитывать при создании систем с длительным сроком эксплуатации. Например [2], уровни уязвимости для авионики (США) поднялись для напряженности поля с 1 В/м (1968 г) до 200 В/м (1986 г), а частотный диапазон воздействий расширился за тот же период с 10 ГГц до 40 ГГц. Преднамеренные электромагнитные воздействия и оружие направленной энергии обеспечивают еще более высокие показатели электромагнитных воздействий. Поэтому, когда прогнозируются экстремальные ЭМЭ с учетом перспектив применения, важно понять, что в этом случае стоимость оборудования, подсистем или систем увеличиться, но это увеличение будет компенсировано в будущих приложениях.

Определяя электромагнитную среду, в пределах которой система должна функционировать во время ее жизненного цикла, необходимо принимать во внимание любые условия, которые могут препятствовать незащищенности относительно ЭМЭ, и любую дополнительную информацию относительно среды, которая поможет правильно оценить уровни воздействия в настоящий период и в перспективе. Например, установка дополнительных излучателей на платформе создаст новые эффекты, которые следует учитывать. Кроме того, из-за ограничения размеров подсистема или оборудование может работать непосредственно в поле излучающей антенны. Другие факторы, которые должны быть рассмотрены: учет конкретных для данной системы параметров излучателей и ЭМЭ, а не усредненных; учет конкретного местоположения системы; учет рабочих процедур для более точного определения ЭМЭ (например, резервное оборудование может не подвергаться предельным уровням ЭМЭ).

Уровни, которые следует использовать для тестирования военной техники, являются трудными для воспроизведения и требуют тщательного рассмотрения пригодности испытательного оборудования и типа тестирования. Многочисленные альтернативы доступны для выполнения оценки, включая лабораторные исследования, воспроизведение ЭМЭ в безэховой камере, полномасштабные испытания в полевых условиях.

Параметры ЭМЭ должны быть включены в документацию заказа, чтобы подтвердить, что электромагнитная среда рассматривается во всех случаях согласно контракту. Должны быть описаны испытательные методы и оборудование, которые будут использоваться при тестировании, а результаты должны быть зарегистрированы и проанализированы.

Электромагнитная среда

Электромагнитная среда (Electromagnetic Environment – EME[1]) – результирующий продукт мощностного и временного распределения в различных частотных диапазонах излученных или кондуктивных электромагнитных помех, с которыми может встретиться вооружение, система или платформа, выполняя определенную задачу в предусмотренной оперативной среде.

Электромагнитные эффекты окружающей среды (Electromagnetic Environmental Effects – E3) определяют воздействие EME на функциональную возможность вооружения, оборудования, систем и платформ. Это явление охватывает все электромагнитные факторы, включая:

- электромагнитную совместимость (ЭМС) (electromagnetic compatibility – EMC),
- электромагнитные помехи (электромагнитные шумы) (electromagnetic interference – EMI),
- электромагнитную уязвимость (electromagnetic vulnerability – EMV),
- электромагнитный импульс (electromagnetic pulse – EMP),
- электростатический разряд (ЭСР) (electrostatic discharge – ESD),
- молнии (lightning),
- накопления статического электричества (precipitation static – p-static),

а также, как результат воздействия, опасности электромагнитного излучения для:

- персонала (hazards of electromagnetic radiation to personnel – HERP),

[1] Здесь и далее использованы отдельные англоязычные термины и аббревиатуры соответствующие военным стандартам зарубежных стран.

- вооружения (hazards of electromagnetic radiation to ordnance – HERO),
- летучих материалов типа топлива (hazards of electromagnetic radiation to fuel – HERF).

EME является результатом распределения мощности по времени, в пределах различных частотных диапазонов, и включает излученные и кондуктивные уровни ЭМ-эмиссии, с которыми можно встретиться. Это общее количество ЭМ-энергии от техногенных и естественных источников, в которой платформа, система, подсистема или оборудование (обобщенно – объекты) будут находиться в пределах любого пространственного домена (земля, воздух, космическое пространство, море), выполняя намеченную задачу в течение жизненного цикла. Электромагнитная среда соответствует специфическому времени и местоположению. Определенные особенности оборудования (такие как уровни мощности передатчика, рабочие частоты и чувствительность рецептора), оперативные факторы (такие, как расстояние между платформами, системами и т.д.) и распределение частот – аспекты определяющие EME. Кроме того, обстановку определяют переходные процессы и длительности их фронтов и спадов (например, электромагнитный импульс – EMP, молнии и p-static).

Воздействие ЭМ-энергии на объекты, которые работают в определенной среде, зависит от восприимчивости элемента (или помехозащищенности), амплитуды, частоты и особенностей EME. Чтобы препятствовать негативному влиянию ЕЗ, нужно рассмотреть возможные нежелательные последствия воздействия ЭМ-энергии на каждый элемент, работающий в намеченной для него обстановке. Эти оценки должны выполняться для потенциально опасных условий EME на персонал, вооружение и сферу заправки топливом.

Электромагнитная обстановка, в которой должны работать военные объекты, состоит из множества естественных и техногенных источников. Естественные источники состоят из галактических, атмосферных, солнечных шумов, накопления статического электричества, молнии и ЭСР.

Техногенные источники создают в окружающей среде преднамеренные, непреднамеренные и паразитные эмиссии. Преднамеренные эмиттеры включают, например, следующие типы подсистем/оборудования: связь, метеорология, радары, вооружение, средства радиоэлектронной война (EW) и электромагнитное оружие.

Непреднамеренные эмиттеры охватывают подсистемы и оборудование, которые используют, преобразовывают или генерируют нежелательную ЭМ-энергию как побочный продукт выполнения их задач. Поэтому любое электрическое, электронное, электромеханическое или электрооптическое устройство может быть непреднамеренным эмиттером.

Уровни мощности и исходные местоположения относительно объекта – два основных параметра, используемые для того, чтобы определить, какие источники являются доминирующими в электромагнитной обстановке. Например, во время нормальных условий не боевые первичные источники ЭМ-энергии определяют обстановку. В боевых условиях специальные источники помех могут быть доминирующим фактором в формировании электромагнитной обстановки. Следовательно, EME, в пределах которого объект должен функционировать, зависит от выполняемой функции и сценария действий.

EME, в которой, наиболее вероятно, будет работать элемент, должна быть определена на возможно более ранних этапах процесса разработки. Начальный шаг должен идентифицировать главные географические области, в которых система будет работать, то есть, США, Атлантика, Тихий океан, Европа, Ближний Восток, или возможно, во всем мире. Следующий шаг должен идентифицировать определенные страны в каждой главной области, в которой, вероятно, будет развернута система. Как только это сделано, должны быть определены театр действий и задачи системы. Это определит состав системы и ее окружение при развертывании. Следующий шаг – идентификация типов и особенностей любого (созданного или запланированного) зависимого от спектра объекта, который возможно будет взаимодействовать с системой. Эта идентификация обращается к источникам и рецепторам помех как военного назначения, так и коммерческого. Информация относительно взаимодействующих объектов должна использоваться как начальный фактор для распределения частот и исследований ЕЗ.

Хотя EME определяется на ранних этапах, необходимо учитывать непрерывное обновление EME в течение всего жизненного цикла, потому что среда не является статической. Появляются новые и модернизируются используемые объекты, которые будут работать в пределах той же самой EME. Данные относительно этих «новых» объектов должны быть определены и добавлены к определенной EME. Кроме того, начальная задача действующего объекта может быть изменена, могут быть охвачены дополнительные географические области, страны. Появление

новых данных должно использоваться, чтобы усовершенствовать исследования ЕЗ и вопросы распределения частоты. Одна из главных трудностей, с которой можно столкнуться, когда определяются требования к параметрам системы –это отсутствие количественных данных о рабочей ЕМЕ.

Каждый объект, вероятно, будет находиться в нескольких различных уровнях ЕМЕ во время его жизненного цикла. Определение уровня ЕМЕ, который является слишком жестким, может привести к увеличению стоимости системы, которая вряд ли будет оправданной. Каждая из различных ЕМЕ, в которых объект будет функционировать во время его жизненного цикла, должна быть определена прежде, чем определены показатели объекта. Следует гарантировать, что ни один из уровней ЕМЕ, в которых находиться объект, не будет отрицательно влиять на показатели системы и ее функциональную безопасность.

Система должна быть электромагнитно совместимой со всеми подсистемами и оборудованием в пределах системы и со средами, вызванными электромагнитными эффектами, внешними к системе. Проверка должна быть проведена на промышленных представительных системах. Безопасность критических функций должна быть проверена на ЭМС в пределах системы и с условиями эксплуатации до использования. Тестирование должно относиться ко всем аспектам жизненного цикла системы, включая штатные операции, контроль, хранение, транспортировку, обработку, упаковку, загрузку, разгрузку, запуск.

Границы показателей объектов должны быть основаны на системных требованиях функционирования, допусках для системных аппаратных средств и неопределенностях, которые присутствуют при проверках требований к проекту системного уровня. У важных параметров безопасности и функции систем непрерывного действия должен быть запас, по крайней мере, 6 дБ [19, 21, 24]. У вооружения (электрически инициируемые устройства) запас должен быть не менее 16,5 дБ. Это требование должно быть проверено тестом, анализом или их комбинацией.

Электромагнитные эффекты (ЕЗ)

Выше были перечислены электромагнитные эффекты, которые формируют электромагнитную обстановку и определяют спектр электромагнитных воздействий на объекты. В зависимости от показателей помехозащищенности и функциональной безопасности объектов эти эффекты могут проявляться в виде опасностей для персонала, оборудования, вооружения и летучих материалов (топлива). Рассмотрим электромагнитные эффекты более детально.

Электромагнитные шумы – любое ЭМ-возмущение, которое прерывает, затрудняет, или иначе, ухудшает или ограничивает эффективность функционирования электроники и электрического оборудования. Эти ЭМВ могут быть вызваны преднамеренно, как в некоторых формах радиоэлектронной войны, или непреднамеренно, в результате паразитной эмиссии или продуктов взаимной модуляции и т.п. Связанная с электромагнитными шумами «восприимчивость» является мерой неспособности объекта выполнять свою функцию без деградации при наличии ЭМ-возмущения.

ЭМ-возмущения могут быть в форме излученной или кондуктивной эмиссии (помехи электромагнитной энергии). Особенностями электромагнитных шумов объектов нужно управлять, чтобы получить высокую степень гарантии, что эти элементы будут функционировать в намеченных инсталляциях без неумышленных ЭМ-взаимодействий с другим оборудованием, подсистемами или внешней ЕМЕ. ЕМЕ в пределах системы является сложной и переменной в зависимости от операционных режимов и частот встроенного оборудования. Кроме того, конфигурации систем непрерывно изменяются, поскольку устанавливается новое или модернизированное оборудование, а элементы, разработанные для одной платформы, могут использоваться для других платформ.

Электромагнитный импульс (EMP) [4, 25–29], является неионизированным ЭМ-излучением (EMR) от ядерного взрыва (ЯВ). Электрические и магнитные поля ЯВ могут взаимодействовать с электрическими или электронными системами и связанными с ними интерфейсами, генерируя разрушительный ток и выбросы напряжения. В ядерном конфликте большинство военных систем будут подвержены EMP. Результирующее ЭМ-поле EMP характеризуется большой амплитудой, малой продолжительностью и коротким фронтом импульса. В любом случае эффекты от воздействия EMP могут быть разрушительными для работы многих электрических и электронных систем [4]. Уровни ЕМЕ, сгенерированные при нормальной работе систем, подсистем или оборудования (такими, как ЭМ-пусковыми установками или электронными пушками), в настоящее время в военных стандартах США не

оговорены.

Контроль эмиссии (Emission control – EMCON). Для сухопутных и военно-морских сил США непреднамеренная электромагнитная эмиссия излучения не должна превышать –105 дБм/м^2 на расстоянии одного километра от источника по частотному диапазону от 500 кГц до 40 ГГц [21].

Опасности электромагнитного излучения (RADHAZ) – могут иметь вредное воздействие на персонал, топливо и вооружение, если они не контролируются. Эти эффекты обсуждаются ниже.

HERP [18, 21] – потенциальная опасность, которая существует для персонала, который подвергнут влиянию ЭМ-поля достаточной интенсивности, чтобы нагреть человеческое тело. Факт, что нагревание связано с поглощением радиочастотной (РЧ) энергии людьми, был известен почти 50 лет назад и привел к внедрению РЧ-диатермии в медицинских и хирургических целях. Если теплота тела превышает его способность избавиться от лишней теплоты, то температура тела растет. Поэтому, если поглощена существенная мощность, может произойти увеличение температуры тела, что может оказать воздействие на метаболические процессы с потенциально вредными последствиями. Радары и системы электромагнитного оружия представляют самую большую потенциальную угрозу для персонала из-за их высоких выходных мощностей передатчиков и особенностей антенн. Персонал, назначенный для ремонта и обслуживания, имеет большую вероятность попасть под значительные опасные уровни излучения из-за его нахождения вблизи к излучающим элементам и необходимости ускоренного проведения работ.

HERF [18, 21, 23] – потенциальная опасность, которая возникает, когда летучее горючее, такое как топливо, подвергается воздействию ЭМ-полей, энергии которых достаточно для того, чтобы вызвать воспламенение. Для того, чтобы топливные пары воспламенились, должна присутствовать огнеопасная смесь паров топлива и воздуха в дополнение к интенсивному ЭМ-полю. Излучение может вызвать токи в любом металлическом объекте. Интенсивность тока, и, таким образом, сила искры через промежуток между двумя проводниками, зависит от интенсивности энергии поля и от того, насколько эффективны проводники в качестве приемной антенны. Многие части системы заправляющегося горючим транспортного средства, или статический проводник заземления, могут действовать как приемные антенны. Индуцированный ток зависит, главным образом, от длины проводника относительно длины волны РЧ-поля и ориентации поля. Ни прогнозировать, ни управлять этими факторами невозможно. Критерии опасности должны в этом случае базироваться на условии, что идеальная приемная антенна с необходимым искровым промежутком может быть создана случайно. Существование и степень топливной опасности определяются, сравнивая фактическую плотность потока мощности излучения с установленным критерием безопасности.

HERO [19] – потенциальная опасность, которая существует, когда на вооружение, которое содержит электрически инициализируемые взрывные устройства (EID), неблагоприятно воздействует электромагнитная среда. Вооружение включает ракеты, взрывчатые вещества, непосредственно EID, петарды, воспламенители, пиротехнические болты, электрические заправленные картриджи, разрушительные устройства и т.п. Современные передатчики могут излучать высокий уровень EME, который может быть опасным для вооружения. Эти уровни EME могут вызвать преждевременное приведение в действие взрывных устройств. РЧ-энергия достаточной интенсивности для стрельбы или приведения в действие EID может быть получена от внешнего EME или по проводам взрывных подсистем или посредством индуктивно-емкостной связи от соседних источников излучения. Возможные последствия включают опасности: деградацию свойств и безопасность. EID должно быть выбрано таким образом, чтобы быть наименее чувствительным к системным требования. Каждый EID должен быть категоризирован относительно того, привела ли его случайная инициализация к нарушению безопасности или к проблемам деградации функционирования. Проектировщик должен определить эту классификацию.

Подсистемы вооружения не должны быть инициализированы электростатическими разрядами 25 кВ, вызванными персоналом. Тестирование проводится непосредственным разрядом через конденсатор 500 пФ и резистор 500 Ом на подсистему (электрические интерфейсы, корпуса, точки операционной работы).

EMV [21] – электромагнитная уязвимость – особенность объекта, которая вызывает ухудшение его качества функционирования, или соотносится с неспособностью выполнить требуемую задачу в рабочей ЭМО. Элемент уязвим, если его параметры стали хуже допустимого уровня из-за незащищенности к рабочей ЭМО или переходному процессу. Во время жизненного

цикла объект будет находиться в различных электромагнитных средах. Многие угрозы отмечаются достаточно редко. Однако если объект эксплуатируется в ЭМО, которая соответствует его спецификации и проверялась в лабораторном испытании, то он может или перенести деградацию работоспособности, или не будет в состоянии выполнить требуемую задачу вообще в оперативной среде. Анализ EMV обычно требует определения связи восприимчивости, наблюдаемой в лаборатории, и фактических рабочих характеристик. Результаты анализа EMV покажут возможные направления в аппаратной модификации, дополнительных исследованиях или тестировании.

Молния [4, 30, 31] – электрический разряд, который происходит в атмосфере между облаками или между облаками и Землей. ЭМ-излучение, связанное с разрядом молнии, производит электрическое и магнитное поля, которые могут воздействовать на электрические или электронные элементы, что приводит к разрушительным токам и выбросам напряжения. Эффекты молнии могут быть разделены на прямой и косвенный.

Прямое разряд молнии может вызвать физическое повреждение в системной структуре или оборудовании из-за прямого приложения канала молнии. Эти эффекты включают разрыв, изгиб, горение, испарение или взрывы аппаратных средств, а так же ударные волны с высоким давлением и магнитные силы, вызванные мощными разрядными токами.

Косвенные воздействия вызваны электрическими переходными процессами в электрических цепях из-за ЭМ-полей, связанных с молнией, и взаимодействием этих полей с оборудованием в системе.

Например, удар молнии в антенну может вызвать физическое повреждение и наведенные разрушительные напряжения в передатчике или приемнике, которые подключены к этой антенне. Кроме того, токи и напряжения, в кабельных линиях самолета, могут вызвать серьезное поражение электрическим током.

Поверхностное заряжение (p-static) [32, 33] – ЭМ-возмущение, вызванное случайным заряжением статическим электричеством в результате движения потока воздуха, влаги или частиц пыли по структуре или компонентам транспортных средств, двигающихся в атмосфере, таких как самолет или космический корабль. Когда системы движется в пыли, дожде, снеге и льде, электростатический заряд на ее поверхности растет. Это наращивание статического электричества определяет наличие существенного напряжения, которое может привести к воздействию на оборудование и определит опасность шока для персонала. Экипаж самолета может быть подвергнут ЭСР во время полета, а обслуживающий персонал на земле может быть подвергнут воздействию ЭСР после приземления. P-static заслуживает особого внимания из-за увеличенной чувствительности электронного оборудования, более широкого спектра частоты для новых систем связи и расширенного использования композиционных материалов.

Система должна управлять и рассеивать электростатические заряды [33], чтобы избежать воспламенения топлива и опасностей для вооружения, защитить персонал от опасностей шока и предотвратить деградацию производительности или повреждение электроники.

ЭСР происходит, когда статическое электрическое поле между двумя объектами превышает пробивное напряжение воздуха между ними. Разряд – сложный случай, при котором заряд концентрируется около точки разряда, а ЭМ-поля от разряда вызывают наведенные токи в объекте. Все эти явления способны к порождению сбоев и в некоторых случаях приводят к повреждению электронного оборудования. Примерами чувствительных компонентов, которые могут быть повреждены ЭСР, являются микросхемы, дискретные полупроводники, толстопленочные резисторы, гибридные устройства и пьезоэлектрические кристаллы и т.п. ЭСР может вызвать неустойчивые или триггерные (переходные) отказы, а так же аппаратные отказы. Неустойчивые отказы происходят, когда оборудование находится в работе, и обычно характеризуется потерей информации или временным искажением ее функций. В этом случае отсутствуют видимые аппаратные повреждения, и надлежащая работа восстанавливается после перезагруки. Катастрофические (аппаратные) отказы от ЭСР могут быть результатом электрического перенапряжения электронных цепей, вызванных разрядом от человека или объекта, электростатического поля, или искрового разряда высокого напряжения.

Движение топлива в баках и в трубопроводах может благоприятствовать росту заряда, что может привести к возможной топливной опасности из-за воспламенения. Любая другая жидкость или газ, текущие в системе (например, жидкостного или воздушного охлаждения), могут аналогично внести заряд с потенциально опасными последствиями.

Вооружение потенциально восприимчиво к случайному воспламенению от ЭСР, особенно

при разряде через детонаторы «bridgewire» (пережигание проволочной перемычки) EID, используемые для инициализации взрывчатого вещества.

Во время обслуживания контакт персонала с оборудованием и различными материалами может создать электростатический заряд на персонале и оборудовании (особенно на непроводящих поверхностях), что создаст проблему безопасности персонала, опасности для топлива и электроники.

Проектирование и тестирование

Электромагнитные эффекты должны учитываться на всем жизненном цикле системы. Технические решения должны быть проверены тестами, анализом, осмотрами или их комбинацией.

Проект по учету параметров ЭМС должен быть комплексным, основанным на архитектуре системного уровня, соответствующих требованиях повышения стойкости, которые должны быть распределены между уровнями систем, подсистемам и оборудования.

Учет электромагнитных эффектов может быть выполнен в следующей последовательности:

1. Установление внешней электромагнитной среды, в которой система обязана нормально функционировать.
2. Идентификация электрического и электронного оборудования, выполняющего заданные операции при наличии внешней угрозы. Все функции, существенные для выполнения задач, должны быть защищены от внешних электромагнитных эффектов.
3. Определение внутренней электромагнитной среды, вызванной внешними электромагнитными эффектами для каждого вида оборудования. Все среды, внешние к системе, должны быть увязаны с внутренней средой системы. Уровень этой внутренней среды будет результатом многих факторов, зависящих от особенностей конструкции объекта, проникновение поля через апертуры и швы, системных и кабельных резонансов т.п. Внутренняя среда для каждой угрозы должна быть установлена анализом, подобием с ранее проверенными системами или тестированием. Внутренняя среда обычно выражается как уровень наведенных токов и напряжений, появляющихся на интерфейсах и портах оборудования, или напряженности поля внутри системы. Эти параметры связываются со стандартизированными требованиями для оборудования. Если наведенные сигналы превышают стандартные требования, разрабатываются меры дополнительной защиты: экранирование, фильтрация, установка ограничителей, рационализация монтажа, зонирование и повышение качества электрических соединений [4, 31–36].
4. Проектирование методов и средств защиты оборудования и система. Системные меры разрабатываются для того, чтобы параметры внутренней среды привести к уровням, определенным соответствующими ограничениями, наложенными на электрическое и электронное оборудование. Уровни помехозащищенности оборудования должны быть заданы с определенным запасом, который учитывает погрешности изготовления оборудования и неопределенности при проверке. Проект системы должен быть жизнеспособным во всем ее жизненном цикле. Этот аспект требует понимания: 1) надлежащего контроля коррозии [36] и 2) проблем, связанных с обслуживанием, которые могут затронуть ЭМС, например, гарантий того, что параметры электрических соединений не ухудшены.
5. Проверка адекватности защиты. Система и проект защиты оборудования должны быть проверены на соответствие договорным требованиям. Проверка адекватности проекта защиты включает демонстрацию, что фактические уровни внутренних сред, появляющиеся на интерфейсах и портах оборудования, не превышают пределов квалификационных испытательных уровней для оборудования для каждой среды. Эти действия проверки должны быть подробно зарегистрированы в процедурах проверки и отчетах.

Ранняя реализация требований защиты от электромагнитных эффектов способствует предотвращению проблемы на последующих этапах.

Важно, чтобы все условия эксплуатации были проработаны в едином объединенном подходе. Дублирование усилий для решения задач, связанных с различными электромагнитными явлениями, характерно для прошлого. Например, методы защиты от воздействия электромагнитного импульса и переходных процессов, вызванных молнией, разрабатывались независимо, а не как общая угроза с соответствующими мерами защиты. Эта задача должна решаться организационно-техническими мерами.

Выбор теста, метода анализа, натурного эксперимента или некоторой их комбинации для демонстрации специфических требований зависит от степени желаемой достоверности результатов, технических возможностей, стоимости и т.п. Анализ и тестирование часто дополняют друг друга. До создания аппаратных средств анализ будет первичным инструментом, используемым для получения гарантий в том, что проект включает адекватные условия. Тогда тестирование может быть ориентировано на проверку достоверности и точности используемых моделей. В ряде случаев построение модели весьма сложная задача, тогда натурный эксперимент должен подтвердить правильность принятых решений. Например, проект защиты самолета от воздействия электромагнитных импульсов или косвенных воздействий молнии сложно оценить на этапе анализа.

Требования ЕЗ должны быть проверены через *возрастающий* процесс проверки. Термин «возрастающий» подразумевает, что проверка согласия с требованиями ЕЗ – продолжающийся процесс в течение разработки, т.е. процесс идет от компонента до системы. Начальный технический проект должен быть основан на анализе и моделях. По мере того, как аппаратные средства становятся доступными, может использоваться тестирование компонентов подсистемы для проверки качества решений, развития методов анализа и моделей. Поскольку получена дополнительная информация, проект уточняется и получает дополнительное развитие. Когда система физически воплощена, то осмотр, конечное тестирование и последующий анализ завершает «возрастающий» процесс проверки. Важно отметить, что тестирование часто необходимо, чтобы получить информацию, которая не поддается определению анализом.

Ниже приведены факторы, которые следует учитывать при анализе электромагнитных эффектов:

- системы, используемые для проверки, должны быть промышленной конфигурации,
- система должна включать все одобренные предложения по конструктивным изменениям (аппаратные средства и программное обеспечение),
- классификация электромагнитных помех должна быть завершена на подсистемах и оборудовании,
- подсистемы и оборудование должны быть помещены в условия, которые соответствуют реальным условиям эксплуатации, включая электромагнитные эффекты и совместно работающие системы,
- электроэнергия, используемая для работы системы, должна соответствовать стандарту качества электропитания системы,
- любые зафиксированные аномалии должны быть оценены, чтобы определить, являются ли они действительно проблемой ЕЗ или некоторым другим типом сбоя или отказа,
- любые системные модификации, вытекающие из результатов тестирования, должны включаться в проект и проходить утверждение в установленном порядке,
- предельные параметры должны быть использованы везде, где они применимы.

Следующий список дает представление по дополнительным проблемам, которые должны быть учтены для внутрисистемного тестирования ЭМС:

- потенциальный источник помех и соответствующий критический рецептор должны быть оценены для подсистем и оборудования при различных режимах и функциях, при контроле деградации остающихся элементов. Нужно рассмотреть для критических элементов различные комбинации источников помех: одиночный и множественные,
- план выбора частот должен быть разработан для обеспечения межсистемной ЭМС, и он должен включать:
    - взаимодействие между передатчиками и рецептором с учетом гармоник, продуктов взаимной модуляции, перекрестной модуляции и т.п.,
    - оценка передатчиков и рецепторов во всем рабочем частотном диапазоне, включая чрезвычайные частоты,
    - оценка эмиссии электромагнитных помех и восприимчивости подсистем,
- предельные уровни должны быть определены для взрывчатых подсистем,
- должна быть подтверждена оценка работы системы на натурных испытаниях в случае предварительного тестирования в лабораторной среде (например, тестирование самолета в полете для проверки тестов, проведенных на земле),
- тестирование должно быть проведено в условиях, в которых электромагнитная среда не влияет на результаты испытаний; худший аспект – загруженность радиочастотного ресурса, что

может препятствовать оценке работоспособности оборудования рецептора из-за шумовой эмиссии стороннего оборудования, установленного в системе,

- тестирование должно включать все соответствующие внешние системные аппаратные средства, такие как оружие, обслуживающее оборудование (элементы, установленные в системе пользователем) и оборудование поддержки.

Испытание систем в реальных условиях часто начинается прежде, чем полный тест внутрисистемной ЭМС выполнен. Кроме того, система, используемая для начального тестирования, редко находится в промышленной конфигурации. Как правило, она будет оснащена разнообразной испытательной аппаратурой, будет иметь некоторые макетные узлы, определенные недоработки конструкции. Некоторые системы, такие как бортовые системы посадки по приборам и идентификация «свой-чужой», требуют, чтобы базовый входной сигнал был эффективно оценен. Другое оборудование, которое излучает энергию и оценивает отраженный сигнал, например, радары или высотомеры, нуждается в фактическом или моделируемом отраженном сигнале, который должен быть полностью оценен для потенциальных эффектов.
Тестирование должно включать осуществление и оценку всех функций, которые могут затронуть безопасность.

Управление ЭМС для достижения функциональной безопасности

Чтобы корректно управлять ЭМС для достижения функциональной безопасности, необходимо принимать во внимание опасность и оценки риска, параметры электромагнитной обстановки, уровни эмиссий, характеристики помехоустойчивости, а именно:

- электромагнитные эффекты, которым может быть подвергнуто оборудование, но частота появления их невелика,
- обозримые эффекты проявления подобных возмущений при функционировании оборудования,
- оценка влияния излучения от оборудования на другое оборудование, которое уже установлено или которое планируется установить,
- обозримые параметры безопасности, изменения которых возможны при наличии вышеупомянутых возмущений (серьезность опасности, размер риска и соответствующий уровень целостности безопасности),
- некоторый уровень уверенности в том, что рассмотрены все необходимые аспекты проблемы и намеченные действия приведут к достижению желательного уровня безопасности.

Какие функциональные значения безопасности могли бы быть разумно предсказаны? Этот анализ должен принимать во внимание серьезность любой возможной опасности и масштаб риска [10].

Электромагнитная обстановка. При анализе ЭМО следует квалифицировать и определить количество и параметры электромагнитных эффектов в предназначенной для эксплуатации среде, принимая во внимание вероятные (или возможные) изменения в будущем. Это должно включить все разумно обозримые электромагнитные возмущения *любого вида*.

Также необходимо определить параметры электромагнитных излучений от аппаратуры, последствия их обозримых воздействий на другую аппаратуру, функционирование которой может влиять на безопасность.

Технические требования. Необходимо определить приемлемую помехоустойчивость и критерии параметров эмиссии для каждой функции аппарата, связанной с безопасностью. Для каждого из возмущений, идентифицированных выше, следует определить желательные коэффициенты безопасности для соответствующих уровней ее целостности.

Результаты часто наиболее удобно выражаются как таблица (матрица) «функция – электромагнитное явление» с критериями, отмеченными в ячейках [37]. Оценки опасностей и рисков может приводить к функциональным критериям, которые отличны от требований Директивы ЭМС.

Разработка-создание-верификация-поддержка. Следует гарантировать, что все необходимые шаги приняты на всех этапах полного цикла жизни аппарата (включая техническое обслуживание, обновление или восстановление), чтобы выполнить определенные критерии функционирования. Это должно контролироваться перед поставкой и после технического обслуживания, модификации, обновления и восстановления.

Верификация должна гарантировать, что требования к функциональным параметрам аппаратуры отвечают его эксплуатационной среде и что их безопасность отвечает требованиям действующего законодательства и разумными ожиданиями ее пользователей и других людей, которые имеют к ней отношение. Некоторые клиенты или пользователи могут иметь собственные требования для проверки правильности принятых решений.

Тестирование. Проблемы тестирования рассмотрены выше.

Информирование и предупреждение. Необходимо информировать предполагаемых и фактических покупателей и пользователей о параметрах ЭМС аппаратуры и любых ограничениях при работе, требованиях к квалификации операторов и обслуживающего персонала, а также возможных ухудшениях рабочих характеристик в процессе эксплуатации. Также следует предупреждать относительно любых потенциальных рисков, связанных с необычными или особо мощными эмиссиями. При разработке проектов эти предупреждения, ограничения и технические требования включаются во все предложения и контракты.

Предупреждение об опасностях не рассматривается как замена принятия мер защиты от возможного нарушения безопасности. В свою очередь – защита не рассматривается как замена проектных решений обеспечения функциональной безопасности, которые стоят на первом месте.

Инструкции пользователя. На всех этапах инсталляции, использования и обслуживания соответствующие инструкции должны определить ЭМО, при которой достигается заданное качество функционирования.

Необходимо указать, каким образом ЭМО может касаться пользователя, и какие методы и приемы уменьшения негативного действия ЭМО доступны для него.

Маркетинг и поставки. Следует иметь гарантии в том, что рекламируется и поставляется аппаратура, предназначенная для работы в заданной ЭМО, а ограничения и сведения о квалификации персонала и деградации характеристик не будут умалчиваться или искажаться.

Это часто очень трудно достичь практически, но не должно игнорироваться, потому что несоответствующая продажа может свести на нет всю тщательность подготовки и выполнения проекта. Кроме этого, некомпетентная торговая сделка может привести к наказанию производителя законным штрафам даже притом, что никакой инцидент нарушения безопасности не произошел.

Процедуры, документация и доказательство. Системное планирование безопасности. Прежде формально документировать системный подход безопасности, диспетчер программ, совместно с системным проектированием и связанной системной безопасностью профессионалы, должен определить, какое системное усилие по обеспечению безопасности необходимо, чтобы выполнить программу и регулирующие требования. Это усилие будет сформировано вокруг требований, которые включают разработку плана для выполнения задачи безопасности, обеспечения компетентности людей, участвующих в этом процессе, установление требований для того, чтобы осуществить задачи безопасности через все уровни управления, и распределить соответствующие ресурсы, чтобы гарантировать, что задачи безопасности завершены.

Обеспечение функциональной безопасности должно планироваться с учетом подзадач, основные из которых следующие:

1. Установление определенных требований к безопасности, основанных на требованиях к функционированию системы в заданной обстановке.
2. Установление системных требований, функций и взаимодействия с правительственными и подрядными организациями, от которых зависит выполнение проекта. Следует определить связь между функциональной безопасностью, которая определяется электромагнитными эффектами, и другими функциональными элементами программы, а также с безопасностью, которая определяется другими факторами (например, ионизирующим излучением, наличием взрывчатых веществ, химическими и биологическими воздействиями).
3. Разработка плана реализации по обеспечению безопасности с указанием связи со стратегической программой создания и развития систем.
4. Установление контроля и отчетности за выполнением программы.
5. Установление приемлемого уровня риска неудачи, вероятности неудачи и порогов серьезности.
6. Установление подходов и методологии, обеспечивающих безопасность в критических приложениях, требования к обслуживанию и модернизации, управление приобретением опасных материалов.

7. Формирование требований к итоговой документации, значением остаточного риска и информировании об этом конечного пользователя.

Требования к безопасности. Безопасность определяются уровнями риска, которые приемлемы для системы. Приемлемые уровни риска могут быть определены в терминах: категории. Количественные требования обычно выражаются как частота события, в результате которого нанесен ущерб. В [16, 37] описан количественный метод определения полноты безопасности.

Управление требованиями. Команда разработчиков, включающая проектировщиков систем, конструкторов, специалистов по ЭМС и безопасности, должна установить определенные требования к полноте безопасности проекта для системы. Цель требований проекта безопасности состоит в том, чтобы достигнуть приемлемого риска ущерба через систематическое использование руководств по проектированию, стандартов, спецификаций, инструкций, контрольных списков и других источников и нормативно-технической документации. При этом должны быть приняты следующие решения:

- устранены технические решения, потенциально приводящие к опасности, а связанные риски уменьшены. Применяя потенциально опасные материалы, следует выбирать те материалы, которые представляют наименьшую угрозу на протяжении всего жизненного цикла;
- опасные вещества, компоненты и операции изолированы от персонала и несовместимых материалов;
- оборудование расположено так, чтобы доступ к нему во время работы, обслуживания, ремонта или регулировок не снижал защищенность персонала к опасностям (например, к опасным веществам, высокому напряжению, электромагнитному излучению и т.п.);
- источники питания, средства управления и критические компоненты должны быть физически разнесены или экранированы;
- необходимо рассмотреть устройства обеспечения безопасности, которые снизят риск ущерба (например, блокировки, избыточность, системная защита, система пожаротушения и т.п.) для опасностей, которые не могут быть устранены. Эти устройства должны периодически проверяться;
- должны быть предусмотрены предупреждающие сигналы, которые минимизируют вероятность неправильной реакции персонала на сигналы; они стандартизируются в пределах подобных типов систем;
- следует обеспечить предупреждения и наличие предостерегающих примечаний в монтаже, операциях и командах обслуживания, включая отличительные маркировки на опасных компонентах, оборудовании и средствах, чтобы гарантировать защиту персонала и оборудования, когда никакие дополнительные меры не могут устранить опасность. Нельзя рассматривать эти предупреждения, предостережения или другую письменную информацию как единственный метод сокращения риска для опасностей, представляющих катастрофическую или критическую категорию опасности;
- безопасность в критических задачах может потребовать профессионального мастерства персонала; в этом случае разработчик должен предложить процесс освидетельствования мастерства, который будет использоваться;
- все изменения в проекте, системе, условиях эксплуатации должны быть проанализированы с позиций безопасности.

Недопустимые условия. Следующие критические условия безопасности считаются недопустимыми при разработке систем. Необходимы позитивные действия, направленные на снижение риска, связанного с этими ситуациями, до приемлемого уровня.

1. Единственный отказ, ошибка персонала или особенность проекта может вызвать катастрофический или критический ущерб.
2. Двойные независимые отказы, двойные независимые ошибки персонала или комбинация отказа и человеческой ошибки, связанные с критическими командами безопасности и функциями управления, которые могут вызвать катастрофический или критический ущерб.
3. Наличие опасных уровней электромагнитных эффектов или энергии, при которых не были предприняты меры адекватной защиты систем, подсистем, оборудования и персонала.
4. Категории опасности, которые в техническом задании определены как «недопустимые».

Приемлемые условия. Следующие подходы при проектировании систем считаются приемлемыми для того, чтобы предотвратить появление недопустимых условий.

1. Для обеспечения безопасности критическая команда и функция управления требует два и больше независимых отказа, две или больше независимых человеческих ошибки, или комбинация независимого отказа и человеческой ошибки.
2. Для обеспечения безопасности критическая команда и функции управления требует минимум три независимых отказа, или три независимых человеческих ошибки, или комбинация трех независимые отказов и человеческих ошибок.
3. Необходимо предусмотреть меры, которые предотвращают ошибки в монтаже, инсталляции или подключениях, которые могут привести к нарушению безопасности.
4. Применение мер, которые предотвращают распространение повреждения от одного компонента к другому или предотвращают распространение энергии, достаточной чтобы вызвать неудачу.
5. Обеспечение запасов прочности и пределов, минимизирующих вероятность отказов.
6. Наличие систем, управляющих наращиванием энергии, что может потенциально вызвать ущерб (например, плавкие предохранители, вспомогательные клапаны и т.п.).
7. Проектирования систем, в которых безопасный отказ может быть временно допущен, но при этом операции могли быть продолжены с уменьшенной, но приемлемой целостностью безопасности.
8. Проектирования систем, которые позволяют персоналу перейти в состояние готовности при наличии опасной ситуации, основанных на учете реакции операторов.
9. Проектирования систем, в которых ограничено или управляемо использование опасных материалов.

Элементы эффективного системного подхода. Элементы эффективного системного подхода по безопасности систем включают:

1. Разработчик всегда знает о рисках, связанных с системой, и формально документирует это понимание. Опасности, связанные с системой, идентифицированы, оценены, прослежены, проверены и связанные риски или устранены, или снижены до приемлемого уровня во всем жизненном цикле. Необходимо идентифицировать и документировать действия, предпринятые для устранения или уменьшения рисков, с целью последующего изучения.
2. Следует изучать исторический опыт построения других безопасных систем.
3. Защита окружающей среды, безопасность и профессиональное здоровье, совместимые с техническими требованиями, учитываются при проектировании наиболее рентабельным способом. Включение особенностей безопасности достигается во время соответствующих фаз жизненного цикла системы.
4. Минимизируются риски, следующие из вредных условий окружающей среды (например, электромагнитные эффекты, температура, давление, токсичность, ускорение и вибрация) и человеческой ошибки.
5. Пользователи систем включаются в рассмотрение проблемы и процесса обеспечения безопасности системы.

Документация должна обеспечить выполнение инструкций и процедур, предписание действий и их ясные результаты. Если действие должным образом не документировано, может быть законным образом доказано в суде, что это имело место. Это может быть серьезной проблемой для любой организации, которая подвергается контролю в области обеспечения безопасности.

Идентификация опасностей

В настоящее время разработаны и используются многочисленные подходы, чтобы идентифицировать системные опасности. Ключевой аспект многих из этих подходов заключается в идентификации опасностей для последующего управления разработкой и сопровождением программ обеспечения безопасности, связанных с проектом [18].

Оценка риска. Следует оценить серьезность и вероятность риска причинения ущерба, связанного с каждой идентифицированной опасностью, то есть, определить потенциальное воздействие опасности на персонал, технические средства, оборудование, топливо, выполняемые операции или окружающую среду. Чтобы оценить риск могут также использоваться другие факторы, например, число людей, которым нанесен ущерб здоровью.

Категории последствий. Категории последствий нанесения ущерба определяются для обеспечения качественной меры самого разумного вероятного ущерба, следующего из ошибки персонала, влияния условий окружающей среды, погрешностей проекта, процедурных

неточностей, ошибок в работе системы и подсистем. Принятые категории даны в табл. 1. Стоимость, показанная в этой таблице, должна быть установлена в зависимости от размера системы, и отражать материальную сторону ущерба.

Адаптация отмеченных категорий к специфической программе обеспечивается взаимодействием между разработчиками относительно трактовки терминов, использованных для определений категорий. Другие методики оценки риска могут применяться при условии, что пользователь одобряет их.

Вероятность опасного события. Вероятность опасного события – вероятность, что событие произойдет в течение запланированного срока службы системы. Определение количественной вероятности события для проекта невозможно на ранних стадиях проекта. Здесь качественная вероятность опасного события может быть получена из результатов исследований, анализа и оценки исторических данных безопасности подобных систем. Качественные уровни вероятности опасного события представлены в табл. 2.

Таблица 1

Категории последствий причинения ущерба

Описание последствий	Категория	Ущерб для персонала, среды
Катастрофические	I	Мог привести к смерти, постоянной полной нетрудоспособности, превышение потери $1M, или необратимое серьезное нарушение экологии, которое нарушает закон или регулирование.
Критические	II	Мог привести к постоянной частичной нетрудоспособности, ранению или профессиональной болезни, которая может привести к госпитализации по крайней мере трех людей, ущерб более $200 К, но меньше чем $1M, или обратимое нарушение экологии, вызывающее нарушение закона или регулирования.
Граничные	III	Мог привести к ранению или профессиональной болезни, приводящей к одному или более потерянные рабочим дням, ущерб более $10 К, но меньше чем $200 К, или незначительное нарушение экологии без нарушения закона или регулирования, где действия восстановления могут быть достигнуты.
Незначительные	IV	Мог привести к ранентю или болезни, не приводящей к потере трудоспособности, ущерб более $2 К, но меньше чем $10 К, или минимальное нарушение экологии, не нарушающее закон или регулирование.

Примечание: М – миллион, К – тысяча.

Таблица 2

Уровни вероятности опасного события

Описание	Уровень	Характеристика	Частота возникновения
Частый	A	Происходить часто в жизни элемента, с вероятностью больше, чем 10^{-1} за период жизни.	Непрерывно
Вероятный	B	Произойдет несколько раз за период жизни элемента, с вероятностью меньше, чем 10^{-1}, но больше чем 10^{-2}.	Происходит часто
Случайный	C	Произойдет несколько раз за период жизни элемента, с вероятностью меньше, чем 10^{-2}, но больше чем 10^{-3}.	Произойдет несколько раз
Редкий	D	Маловероятно, но возможно, что произойдет за период жизни элемента, с вероятностью меньше,	Вряд ли, но, как можно разумно ожидать, произойдет

		чем 10^{-3}, но больше, чем 10^{-6}.	
Невероятный	E	Настолько маловероятно, что может вообще не произойти; вероятность меньше, чем 10^{-6} за период жизни.	Вряд ли произойти, но возможно

Оценка риска опасного события. Классификация риска опасного события, последствий события и вероятность опасного события может быть выполнена с помощью матрицы оценки риска. Эта оценка позволяет назначать значение оценки риска в зависимости от опасности, основанной на последствиях опасного события и вероятности события. Это значение часто используется, чтобы ранжировать различные опасности относительно связанных с ними рисков. Пример матрицы оценки рисков показан в табл. 3.

Таблица 3

Пример классификации рисков по частоте опасных случаев

Частота	Последствия			
	катастрофические	важные	граничные	незначительные
Частые	1	3	7	13
Вероятные	2	5	9	16
Случайные	4	6	11	18
Отдаленные	8	10	14	19
Невероятные	12	15	17	20

Категории риска опасного события. Значения оценки риска часто используются в группировании индивидуальных опасностей в категории риска, которые используются для генерирования определенных действий, такое как мер по предотвращению опасностей или формального принятия риска. В табл. 4 показаны примеры категорий риска опасного события и связанных значений оценки. В данном случае оценка риска 1–5 соответствует «высокий» риск, а оценка 6–9 соответствует «серьезному» риску.

Таблица 4

Категории риска

Класс рисков	Оценка риска	Категория риска	Интерпретация
Класс I	1–5	Высокая	Недопустимый риск
Класс II	6–9	Серьезная	Нежелательный риск может быть допустим, только если снижение риска невозможно или если затраты на снижение существенно непропорциональны достигаемому результату
Класс III	10–17	Средняя	Риск допустим, если цена снижения риска превосходит достигаемый выигрыш.
Класс IV	18–20	Низкая	Незначительный риск.

Оценка риска может быть выполнена по мере необходимости, используя другие коэффициенты, чтобы различить опасности, имеющие одинаковую оценку риска. Можно было бы различить опасности с тем же самым значением оценки риска в терминах возможностей систем или коэффициентами, учитывающими социальные, экономические и политические последствия. При разработке и сопровождении программ обеспечения безопасности в этом случае необходимо консультироваться со специалистами относительно приоритетов решений.

Опасности должны быть расположены по приоритетам так, чтобы корректирующие усилия могли быть сосредоточены сначала на самых серьезных опасностях. Классификация опасностей может быть проведена согласно потенциалу риска, который они представляют.

Окончательная цель программы безопасности состоит в том, чтобы проектировать системы, которые не содержат опасностей. Однако природа большинства сложных систем не позволяет или делает экономически неприемлемым их проектирование полностью без опасностей. Однако успешная программа обеспечения безопасности позволяет проектировать системы, в которых не существуют опасности, приводящие к недопустимому уровню риска.

Функциональная безопасность и стандарты ЭМС

Имеется распространенное представление, что применение оборудования, отмеченного знаком соответствия, например, знаком соответствия «CE» для Европейской Директивы по ЭМС 204/108/ЕС [10], обеспечивает надежное функционирование в условиях электромагнитных возмущений. Однако имеются причины, по которым это представление не всегда правильно, а именно:

- стандарты ЭМС не использует в тексте термин «безопасность»;
- стандарты ЭМС только охватывает некоторую усредненную ситуацию и не затрагивает разумно обозримые предельные отклонения параметров окружающей среды, ошибок операторов, непредсказуемы эксплуатационные ситуации или использование не по назначению, т.е. ряд факторов, которые являются существенными для функциональной безопасности;
- почти все стандарты в области ЭМС, в том числе и те, которые гармонизированы с Директивой ЭМС, явно или неявно исключают рассмотрение аспектов безопасности;
- упомянутые стандарты охватывают ограниченное число возможных электромагнитных возмущений, и их конечное число определяет и конечную вероятность несовместимости;
- технические условия, как правило, дают минимальные требования по обеспечению ЭМС и не затрагивают вопросы безопасности; органы по сертификации обычно не принимают во внимание вопросы безопасности.

Директива заинтересована исключительно в удалении технических барьеров при торговле в пределах рынка ЕС и не может, по его ограниченной природе, должным образом иметь дело с проблемами функциональной безопасности связанными с ЭМС. Она принимает во внимание только нормальную работу и типичные электромагнитные среды. В отличие от этого, требования безопасности учитывает разумно обозримые события низкой вероятности, человеческие ошибки и неправильную эксплуатацию, перегрузки и экстремальные значения окружающей среды, в том числе критичные электромагнитные эффекты.

Таким образом, соответствие Директиве ЭМС не гарантирует ЭМС оборудования в реальной жизни и отсутствия рисков безопасности из-за нарушения ЭМС.

Требования компетентности для персонала

Персонал, вовлеченный в процедуру обеспечения ЭМС и функциональной безопасности, должен иметь соответствующую квалификацию и обладать комплексом знаний и умений, который не может быть поделен между отдельными работниками. Эти специалисты должны видеть проблему в целом и координировать ее решение на всех этапах – от концепции создания до вывода оборудования из эксплуатации.

Все люди, имеющие дело со связанными с безопасностью системами (включая заказчиков, операторов, инсталляторов, также как и проектировщиков и конструкторов) должны быть компетентны исполнить назначенные им задачи. Компетентность требует квалификации, опыта и качеств, соответствующих сфере деятельности. Она включают:

- такое обучение, которое гарантировало бы приобретение необходимого знания в сфере задач, требующих решения;
- адекватное знание опасностей и отказов оборудования, которые они вызывают;
- знание и понимание сферы действия организации, где они работают;
- способность эффективно сотрудничать с равными по положению сотрудниками, с любым штатом подчиненных и руководителями;
- трезвая оценка собственных ограничений (знаний, опыта, средств, ресурсов и т.д.) и готовность к совершенствованию.

Профессионалы, ответственные за проект или за управление персоналом, вовлеченного в действия, связанные с безопасностью, должны, кроме отмеченного выше, иметь:

- детальное знание всех установленных законом условий, одобренных практических руководств и другой информации, относящейся к их сфере деятельности;
- понимание нормативных актов других организаций, которые могли бы затрагивать их работу;
- общее знание ситуации в других учреждениях подобного типа;
- понимание текущих и перспективных разработок в сфере их деятельности.

Степень компетентности может быть классифицирована на четыре уровня:

- технические навыки, например, анализ опасности, запись сообщения, и т.д.;
- поведенческие навыки; например, аккуратность, способность системно рассматривать проблему, внимание к деталям и т.д.;
- расширенные знания; например, человек, выполняющий идентификацию опасности должен знать специфические приложения, чтобы быть способным идентифицировать вероятные опасности, которые существуют;
- расширенное понимание; например, маловероятно, что кто-то мог устанавливать граничные уровни риск для специфической проблемы без понимания основных принципов безопасности и риска.

Специалисты, работающие в сфере ЭМС-безопасности, должны быть аккредитованы на выполнение основных функции на одном из трех уровней: контролируемый практик; практик; эксперт. В настоящее время с особой остротой встает вопрос подготовки кадров в области ЭМС и функциональной безопасности, которая практически отсутствует в вузах страны.

Заключение

1. Функциональная безопасность, связанная с ЭМС, – сложная междисциплинарная область технической экспертизы и практики создания сложных радиотехнических и электронных систем, требующая внимания и развития методов и средств обеспечения ее целостности.
2. Электромагнитная среда и формирующие ее электромагнитные эффекты непрерывно усложняется: повышается интенсивность электромагнитных полей, расширяется частотный диапазон, что увеличивает круг опасностей, вызванных неадекватно функционирующими системами и оборудованием.
3. Необходимы более совершенные методы теории и практики создания радиотехнических и электронных систем, которые обеспечат целостность функциональной безопасности на всем жизненном цикле систем.
4. Методы испытаний и измерений, экспериментально-исследовательская база должна соответствовать реальным электромагнитным эффектам, которые воспроизводятся при проведении исследований и сертификации продукции, отвечающих требованиям функциональной безопасности.
5. Инженерно-технические кадры, участвующие в создании и эксплуатации систем и оборудования должны быть осведомлены о проблеме функциональной безопасности и хорошо сведущим во всех делах, имеющих отношение к электромагнитной среде и ее влияние на функционирование систем. Компетентность персонала, связанного с оборудованием и системами в течение всего жизненного цикла, важнейший фактор обеспечения целостности функциональной безопасности.

Список литературы

1. Лифанов Ю.С., Саблин В.Н., Салтан М.И. Направления развития зарубежных средств наблюдения за полем боя. – Успехи современной радиоэлектроники. – 2004. – № 7. – С. 5–37.
2. Газизов Т.Р. Преднамеренные электромагнитные помехи и авионика. – Успехи современной радиоэлектроники. – 2004. – № 2. – С. 37–51.
3. Кечиев Л.Н., Степанов П.В., Арчаков О.Н. Предотвращение катастроф электромагнитного характера в информационных системах. – Технологии ЭМС. – 2005. – № 4 (15). – С. 7–19.
4. Балюк Н.В., Кечиев Л.Н., Степанов П.В. Мощный электромагнитный импульс: воздействие на электронные средства и методы защиты. – М.: ООО «Группа ИДТ», 2008. – 478 с.
5. Walling Eileen M., High Power Microwaves: Strategic and Operational Implications for Warfare/ Occasional Paper No. 11. Center for Strategy and TechnologyAir War. CollegeAir UniversityMaxwell. Air Force Base, Alabama – February 2000. – 52 p.
6. Geis II J. P. Directed Energy Weapons on the Battlefield: a New Vision for 2025/ Occasional Paper No. 32. Center for Strategy and Technology. Air War College Air University. Maxwell Air Force Base, Alabama. – April 2003. – 73 p.
7. Nielsen Ph. E. Effects of Directed Energy Weapons. – VG93.B36, 1994. – 347 p.

8. Газизов Т.Р. Электромагнитный терроризм. Электромагнитный терроризм на рубеже тысячелетий / Под ред. Т.Р. Газизова. – Томск: Томский государственный университет, 2002. – 206 с.
9. Directive 2004/108/EC of the European Parliament and of the Council. – 2004. – 14 p.
10. Armstrong Keith. EMC-Related Functional Safety of Electronically Controlled Equipment. Compliance Engineering, 2001. [Электронный ресурс]. www.ce-mag.com.
11. ГОСТ Р МЭК 61508-1–2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования. – М.: Стандартинформ, 2008. – 50 с.
12. ГОСТ Р МЭК 61508-2–2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам. – М.: Стандартинформ, 2008. – 22 с.
13. ГОСТ Р МЭК 61508-3–2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению. – М.: Стандартинформ, 2008. – 42 с.
14. ГОСТ Р МЭК 61508-4–2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения. – М.: Стандартинформ, 2008. – 22 с.
15. ГОСТ Р МЭК 61508-5–2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности. – М.: Стандартинформ, 2008. – 27 с.
16. ГОСТ Р МЭК 61508-6–2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Рекомендации по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р МЭК 61508-3. – М.: Стандартинформ, 2008. – 22 с.
17. ГОСТ Р МЭК 61508-7–2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства. – М.: Стандартинформ, 2008. – 73 с.
18. MIL-STD-882D, DoD. Standard Practice for System Safety. – 2000. – 31 p.
19. MIL-HDBK-240, DoD Handbook. Hazards of Electromagnetic Radiation to Ordnance (HERO) Test Guide. – 2002. – 121 p.
20. MIL-HDBK-764(MI), Military Handbook. System Safety Engineering Design Guide for Army Material. – 1990. – 346 p.
21. MIL-HDBK-237D. DoD Handbook. Electromagnetic Environmental Effects and Spectrum Supportability Guidance for Acquisition Process. – 2005. –172 p.
22. Electromagnetic Compatibility & Functional Safety. A Factfile provided by The Institution of Engineering and Technology, 2006, 69 p.
23. E3 and SM Assessment Guide for Operational Testing. Director Operational Test & Evaluation, 2001. – 86 p.
24. MIL-HDBK-235-1B. Military Handbook. Electromagnetic (Radiated) Environment Considerations for Design and Procurement of Electrical and Electronic Equipment, Subsystems and Systems. General Guidance. – 1993. – 36 p.
25. МЭК 61000-5-3. Электромагнитная совместимость (ЭМС). "Устойчивость к электромагнитному импульсу высотного ядерного взрыва (ЭМИ ВЯВ). Концепция (классы) защиты оборудования",1999.
26. МЭК 61000-5-4. Электромагнитная совместимость (ЭМС). "Устойчивость к электромагнитному импульсу высотного ядерного взрыва (ЭМИ ВЯВ). Общие технические требования к средствам защиты. Излученные помехи",1995.
27. МЭК 61000-5-5. Электромагнитная совместимость (ЭМС). "Устойчивость к электромагнитному импульсу высотного ядерного взрыва (ЭМИ ВЯВ). Общие технические требования к средствам защиты. Наведенные помехи",1995.
28. МЭК 61000-5-6. Электромагнитная совместимость (ЭМС). "Устойчивость к электромагнитному импульсу высотного ядерного взрыва (ЭМИ ВЯВ). Уменьшение уровней внешних электромагнитных воздействий", 2002.

29. МЭК 61000-5-7. Электромагнитная совместимость (ЭМС). "Устойчивость к электромагнитному импульсу высотного ядерного взрыва (ЭМИ ВЯВ). Степени защиты от электромагнитных помех. Методы расчета защищенности", 1997.
30. Кравченко В.И., Болотов Е.А., Латунова Н.И. Радиоэлектронные средства и мощные электромагнитные помехи. – М., Радио и связь, 1987. – 256 с.
31. Кравченко В.И. Грозозащита радиоэлектронных средств. Справочник. – М.: Радио и связь, 1991 – 264 с.
32. Уильямс Т. ЭМС для разработчиков продукции. – М.: Издательский Дом «Технологии», 2003. – 540 с.
33. Кечиев Л.Н., Пожидаев Е.Д. Защита электронных средств от воздействия статического электричества/ Учеб. пособие для вузов. – М.: Издательский Дом «Технологии», 2005. – 352 с.
34. Кечиев Л.Н. Проектирование печатных плат для цифровой быстродействующей аппаратуры. – М.: ООО «Группа ИДТ», 2007. – 616 с.
35. Кечиев Л.Н., Степанов П.В. ЭМС и информационная безопасность в системах телекоммуникаций. – М.: Издательский Дом «Технологии», 2005. – 320 с.
36. Кечиев Л.Н., Акбашев Б.Б., Степанов П.В. Экранирование технических средств и экранирующие системы. – М.: ООО «Группа ИДТ», 2010. – 470 с.
37. Смит Д.Д. Функциональная безопасность. Простое руководство по применению стандарта МЭК 61508 и связанных с ним стандартов/ Дэвид Дж. Смит, Кеннет Дж. Л. Симпсон – М. Издательский Дом «Технологии», 2004. – 208 с.

Генеральный штаб Вооруженных сил Российской Федерации,
ФГУ «12 ЦНИИ Минобороны России»,
Московский государственный институт электроники и математики (МИЭМ).
Статья поступила 10.01.2010.

Burutin A.G., Baljuk N.V., Kechiev L.N.

Electromagnetic Effects of Environment and
Functional Safety Radio-electronic Systems of Arms

The problem of the functional safety, defined EMC is considered. Its integrated approach is shown, the expanded classification and the characteristic of the electromagnetic effects forming the electromagnetic environment is resulted. The dangers caused by inadequately functioning systems and the equipment in the operative electromagnetic environment are marked. Necessity of development of more perfect methods of the theory and practice of creation of radio engineering and electronic systems which will provide integrity of functional safety on all life cycle of systems is proved.

Requirements to methods and means of tests and measurements, experimentally-research base which should correspond to the real electromagnetic effects, meeting the requirements of functional safety are formulated.

Demands to competence of the personnel connected with the equipment and systems during all life cycle that is the major factor of maintenance of integrity of functional safety are made.

functional safety, electromagnetic compatibility, electromagnetic effect, arms, the military technics, the program, test

The Joint Staff of Armed forces of the Russian Federation,
12 CR&DI of the Ministry of Defense of Russia,
The Moscow State Institute of Electronics and Mathematics.