



МЭК 61508 - стандарт для многих ситуаций

Доктор Йозеф Бёрчек

МЭК 61508 – стандарт для многих ситуаций

Йозеф Бёрчек, HIMA GmbH + Co KG

Аннотация

Вплоть до 90-х годов прошлого века использование сложной микроэлектроники и микроконтроллеров в системах обеспечения безопасности считалось если не совсем невозможным, то по крайней мере сопряженным с необходимостью выполнения большого объема контрольных испытаний. Причины лежали и в большом количестве норм и стандартов, которые содержали действовавшие в то время правила, предписывавшие исключительное применение традиционных решений с использованием релейных устройств защиты. Тем самым изначально исключалось применение современного, экономичного и высокотехнологического с точки зрения безопасности оборудования.

Стандарт МЭК 61508 охватывает семь частей, описывающих классификацию, аппаратное и программное обеспечение безопасных электрических / электронных / программируемых электронных систем. В ходе разработки стандарта была специально поставлена цель не закреплять в нем положений, могущих в дальнейшем воспрепятствовать применению будущих, сегодня еще неизвестных технологий. Стандарт МЭК 61508 формулирует поэтому свои требования на очень высоком уровне абстрагирования и поэтому не всегда легкодоступен для понимания.

1 Введение

В настоящее время на мировом рынке широко предлагаются безопасные системы противоаварийной защиты и контроля для критических в отношении безопасности производств. Для их правильной эксплуатации необходимы хорошее знание и правильное применение положенных в основу работы этих систем международных стандартов в области функциональной безопасности.

Рис. 1 показывает общепризнанное распределение отказов в жизненном цикле оборудования. При этом неважно, идет ли речь о простой системе управления или о сложной установке в целом.

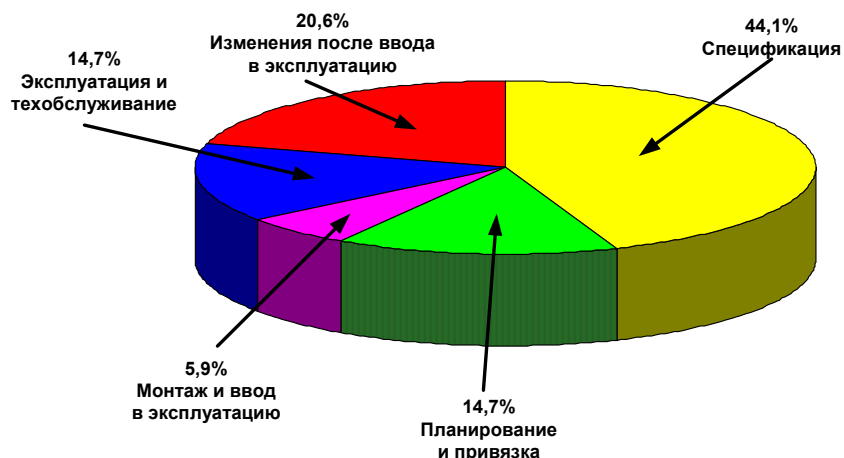


Рис. 1. Интенсивность отказов на различных стадиях жизненного цикла оборудования

При анализе видов отказов их делят в принципе на опасные и безопасные. В свою очередь безопасные отказы делятся на

- безопасные обнаруживаемые и
- безопасные необнаруживаемые.

О безопасных отказах речь идет в тех случаях, когда такие отказы, обнаруженные или необнаруженные, не влияют на надёжное функционирование системы. При опасных отказах все наоборот. Возникая, такие отказы приводят к опасным ситуациям в системе, которые в зависимости от стечения обстоятельств способны создать существенную угрозу для человеческих жизней.

Эти отказы также делятся на

- опасные обнаруживаемые и
- опасные необнаруживаемые.

При опасных обнаруживаемых отказах система обеспечения безопасности может при соответствующей настройке перевести весь агрегат или установку в безопасное состояние. Весьма критичную ситуацию представляют собой необнаруживаемые опасные отказы. Ни одна система обеспечения безопасности не сможет их обнаружить в случае их возникновения. Они могут сохраняться в системе до ее выключения, или в худшем случае, до ее опасного отказа, при полном неведении пользователя об их наличии.

Само собой разумеется, что представленная на рис. 2 структура распределения отказов носит исключительно демонстрационный характер. Доля опасных отказов, как представлено на этом рисунке, ни в коем случае не может являться приемлемой для реальной системы обеспечения безопасности.

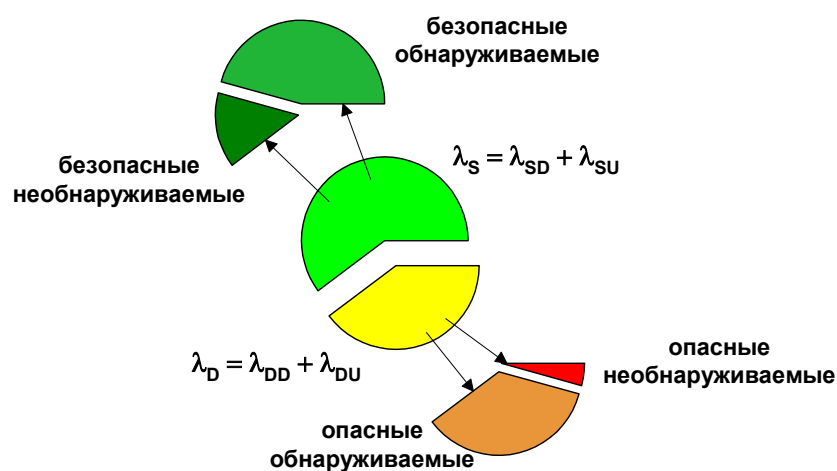


Рис. 2. Структура распределения интенсивностей отказов по типам

Для проектирования и эксплуатации систем или устройств, обеспечивающих безопасность, необходимы обширные мероприятия по их сертификации. Они служат для предотвращения описанных выше опасных ситуаций или, если это невозможно, перевода оборудования в безопасное состояние.

Стандарт МЭК 61508 описывает в своих семи частях полный жизненный цикл оборудования. Часть 1 определяет жизненный цикл оборудования, обеспечивающего безопасность, требования к нему и значения параметров PFD и PFH. В части 2 определены остальные требования к системам, обеспечивающим безопасность, и их архитектуре. В части 3 подробно описывается полный жизненный цикл аппаратуры и ПО, а также методы для достижения и поддержания безопасности. В части 4 разъясняются используемые термины и сокращения, причем эта часть является неоценимым источником информации для изучения самой нормы.

В части 5 приводятся методы анализа использования систем по обеспечению безопасности. Часть 6 описывает применение частей 2 и 3. Часть 7 посвящена методам, используемым во всех остальных частях.

Принципиальная последовательность действий при применении стандарта показана на рис. 3. Стандарт, как уже упоминалось, носит общий характер и применим для всех безопасных электрических / электронных / программируемых электронных систем (сокращенно E/E/PES) независимо от сфер их применения. В него были интегрированы различные другие стандарты по безопасности. Отсюда следует, что МЭК 61508 можно рассматривать как в узком смысле, в виде отдельного стандарта, так и в широком смысле, как основополагающий документ.

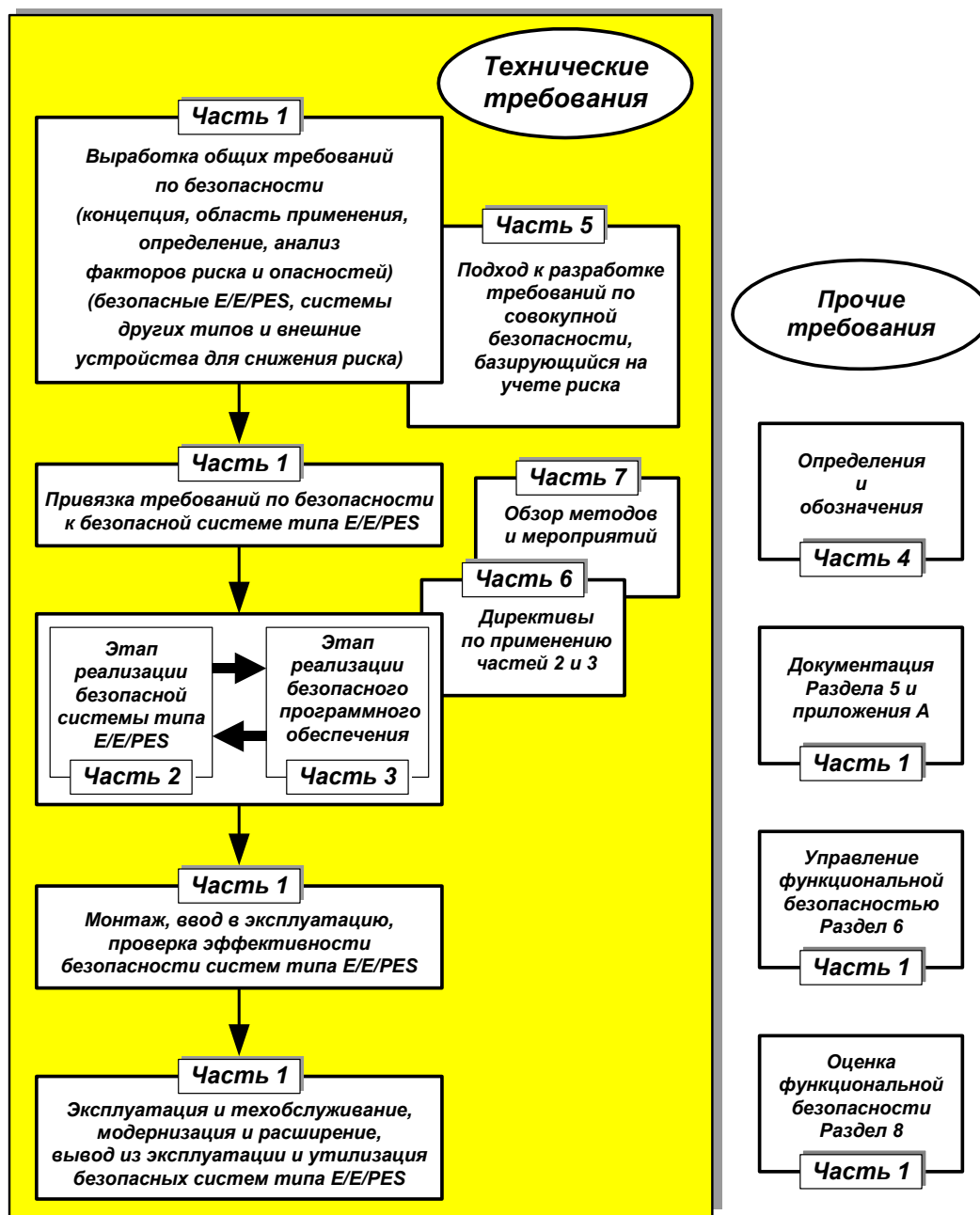


Рис. 3. Принципиальное построение МЭК 61508

Для достижения соответствия этому стандарту необходимо доказать, что выполнены требования заложенных в ней критериев. Исключения допускаются только для систем невысокой сложности, для которых имеются достоверные результаты их применения.

2 Общие пояснения к МЭК 61508

В части 1 МЭК 61508 устанавливается область применения стандарта и излагаются все аспекты, связанные с использованием E/E/PES систем в оборудовании, обеспечивающем безопасность. Здесь также раскрывается понятие «Управление Функциональной Безопасностью» (Functional Safety Management) и дано планирование всех этапов жизненного цикла безопасности.

Рассмотрение жизненного цикла безопасности позволяет реализовать системный подход к проблеме функциональной безопасности, состоящий в основном из трех составных частей:

- Определение требований к безопасности
- Реализация системы или устройства, обеспечивающего безопасность
- Ввод в эксплуатацию, проверка эффективности всех функций безопасности, эксплуатация, техническое обслуживание и вывод из эксплуатации.

Для подробного рассмотрения обратимся к отдельным этапам, представленным на рис. 4.

На этапе 1 выработки концепции устройства следует добиться удовлетворительного понимания объекта контроля (EUC, Equipment Under Control) и его окружения. Это требование включает в себя также необходимость рассмотреть возможных источников опасности и предписаний законодательства. На следующем этапе 2 следует определить всю охватываемую область применения, включая ее границы и возможные внешние источники опасности. На основании этого в этапе 3 проводится анализ источников риска и опасностей. В нем должны учитываться в разумных пределах все предсказуемые ситуации, опасности и потенциально опасные происшествия. Для них должны быть определены вероятности наступления и возможные последствия. На обоих следующих этапах 4 и 5 формулируются общие требования к обеспечению безопасности и их распределение. На первом из них определяются в совокупности функции обеспечения безопасности, необходимые для достижения требуемой функциональной безопасности. Далее следует определить степень возможного снижения риска при помощи внешних систем. Только после этого имеется возможность установить на следующем этапе, какие безопасные системы необходимо будет использовать для достижения требуемой функциональной безопасности. Здесь также определяется, какой уровень SIL (см. [1]) должна иметь каждая отдельная функция безопасности (Таблица 1).

Уровень совокупной безопасности (SIL)	Режим с низким уровнем требований по требованию функции безопасности (средняя вероятность отказа в выполнении заданной функции безопасности по требованию)	Режим с высоким уровнем требований по требованию функции безопасности (вероятность опасного отказа в течении одного часа в режиме непрерывной работы)
4	$\geq 10^{-5} \text{ bis } < 10^{-4}$	$\geq 10^{-9} \text{ bis } < 10^{-8}$
3	$\geq 10^{-4} \text{ bis } < 10^{-3}$	$\geq 10^{-8} \text{ bis } < 10^{-7}$
2	$\geq 10^{-3} \text{ bis } < 10^{-2}$	$\geq 10^{-7} \text{ bis } < 10^{-6}$
1	$\geq 10^{-2} \text{ bis } < 10^{-1}$	$\geq 10^{-6} \text{ bis } < 10^{-5}$

Таблица 1. SIL с низким и высоким уровнем требований

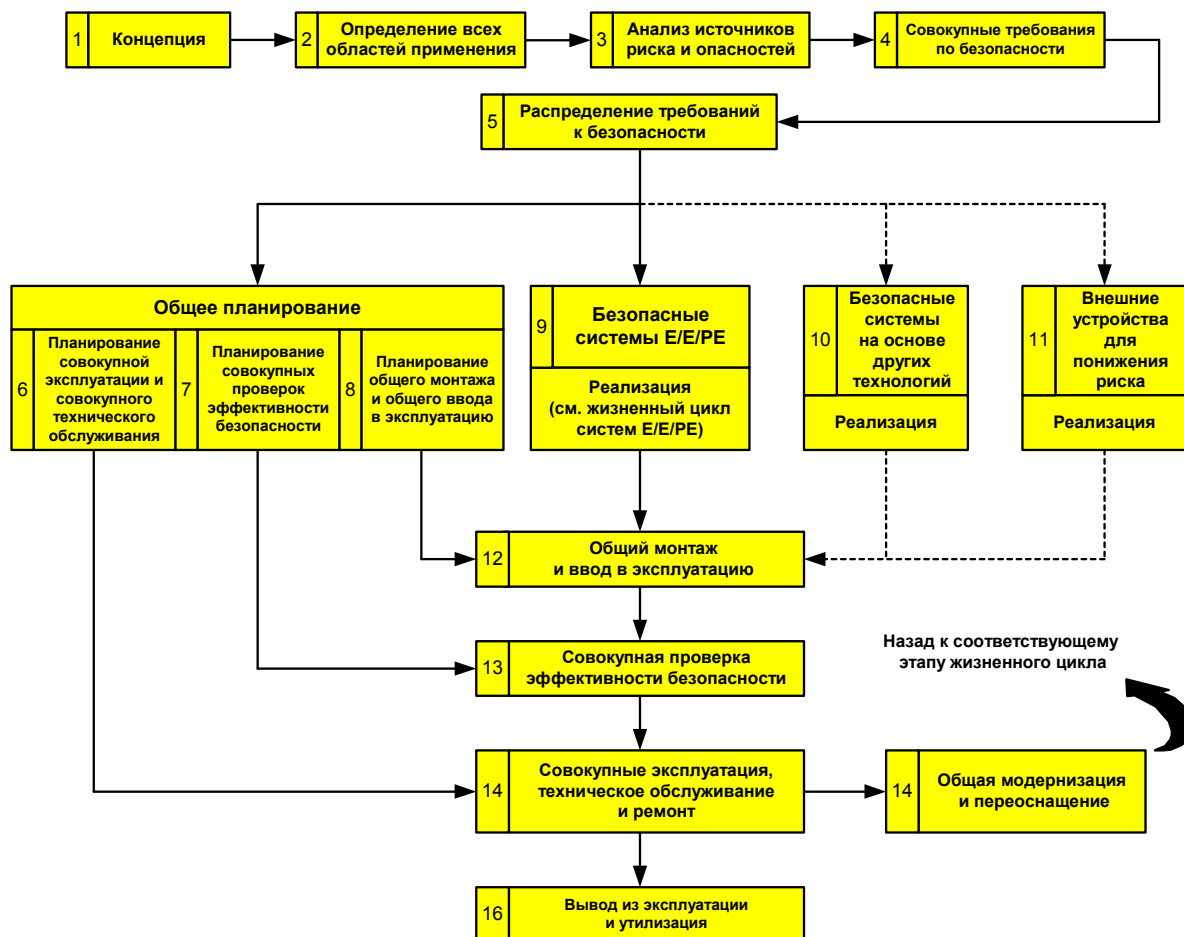


Рис. 4. Жизненный цикл безопасности

Наряду с описанием этапов выработки концепции и проектирования МЭК 61508 устанавливает также действия после начала эксплуатации. Здесь предусмотрены фазы планирования всего процесса эксплуатации, включая техобслуживание (этап 6). Эти планы должны, по необходимости, содержать стандартные операции по техобслуживанию для поддержания функциональной безопасности. Для самого процесса техобслуживания также должны быть запланированы мероприятия по поддержанию уровня обеспечения безопасности во время его проведения. На рис. 4 упоминается также совокупная проверка эффективности всех функций безопасности (этап 13). Для этого на этапе 7 создается план проверки, в котором рассматриваются все возможные режимы работы. Здесь также должна быть принята стратегия проверки и критерии ее удовлетворения. Следующими этапами общего планирования являются планирование общего монтажа (этап 8) с контролем качества его исполнения и ввод в эксплуатацию. Здесь следует обращать особое внимание на планирование временного графика, распределения ответственности и соблюдения последовательности действий. Кроме того, должны быть определены критерии завершения монтажа системы или установки.

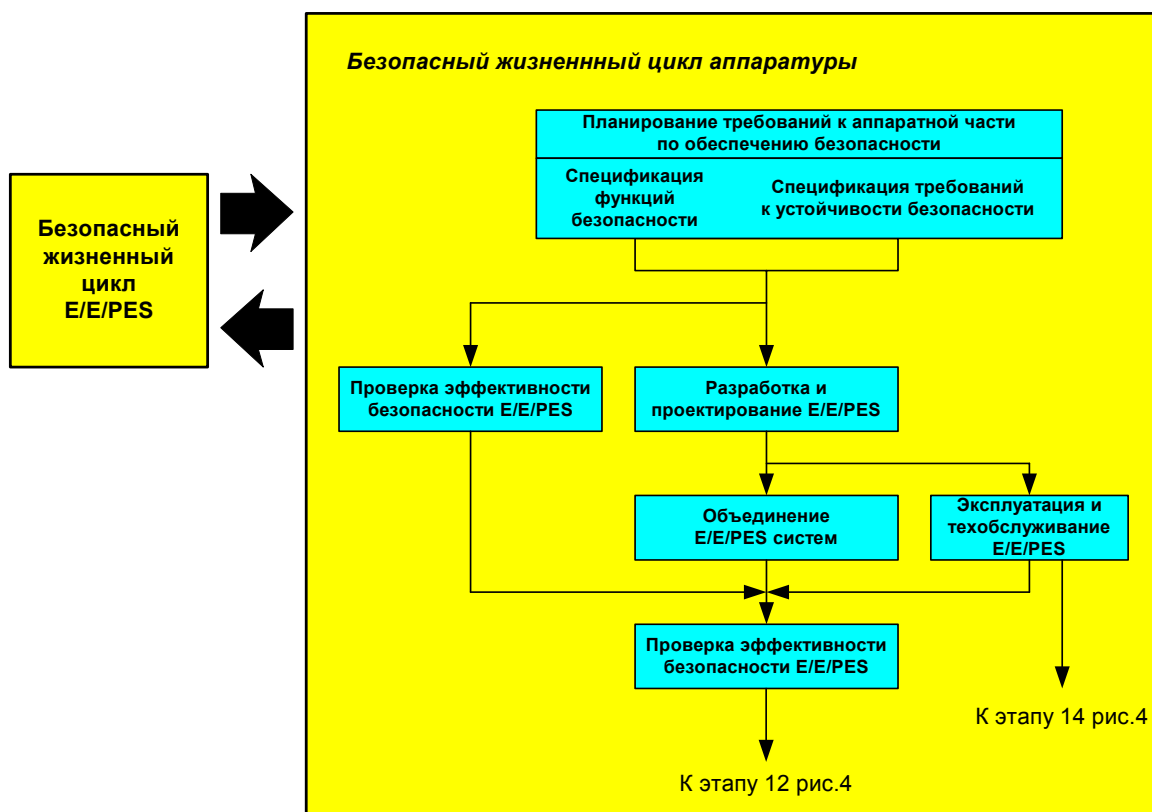


Рис. 5: Схема безопасного жизненного цикла аппаратуры

Одной из важнейших сторон общего планирования является реализация (этапы с 9 по 11). На этом этапе планируется реальное воплощение разработанной концепции, для чего необходимы специальные проекты. Поэтому должны также привлекаться части 2 и 3 стандарта МЭК 61508, касающиеся разработки и реализации требований к аппаратуре и программному обеспечению.

После завершения планирования и реализации следуют предусмотренные генеральным планом общий монтаж и ввод в эксплуатацию (этап 12), а также проверка эффективности всех функций обеспечения безопасности в соответствии с планом (этап 13). Стандарт также устанавливает процесс общей модернизации и переоснащения (этап 15). При этом необходимо обеспечить сохранение уровня функциональной безопасности как во время, так и после модернизации. Важно, чтобы все действия при этом были тщательно спланированы и все их последствия учтены и приняты во внимание. Важно также отрегулировать вопросы вывода из эксплуатации и утилизации (этап 16). Здесь анализируется и прогнозируется влияние вывода из эксплуатации на функциональную безопасность других систем, находящихся в контакте с выводимой. Только после такого анализа можно выдать распоряжение о выводе из эксплуатации.

3 Требования к аппаратной части

Часть 2 МЭК 61508 описывает требования к аппаратуре. Здесь определяются жизненный цикл безопасности оборудования, требования к архитектуре, а также типы подсистем А (поведение подсистемы в аварийных ситуациях полностью предсказуемо) и Б (поведение подсистемы в аварийных ситуациях не может быть полностью предсказано) и соответствующие им значения SFF (Safe Failure Fraction). Кроме того разъясняется необходимая информация и действия по системной разработке аппаратуры. Предлагаемые для этого методы, мероприятия и приемы собраны в таблицах в приложении к норме. Обязательным является составление

спецификации функции безопасности, содержащей точные сведения о том, каким образом предполагается достичь и сохранить необходимый уровень безопасности. При ее составлении следует учитывать все возможные режимы эксплуатации. Далее следует составить также общую спецификацию безопасности, которая содержит данные об уровне совокупной безопасности каждой функции, влияющей на безопасность.

При планировании проверки эффективности обеспечения безопасности должны быть приняты во внимание все требования к тестовым процедурам относительно порядка и условий их проведения, а также критериев их выполнения или невыполнения.

Доля неопасных отказов	Подсистема типа А			Подсистема типа В		
	Число допускаемых дефектов в аппаратуре			Число допускаемых дефектов в аппаратуре		
	0 отказов	1 отказ	2 отказа	0 отказов	1 отказ	2 отказа
< 60 %	SIL 1	SIL 2	SIL 3	Не допустимо	SIL 1	SIL 2
От 60 % до 90 %	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
От 90 % до 99 %	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
> 99 %	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

Таблица 2. Подсистемы типов А и В

Разработка безопасных систем должна осуществляться в полном соответствии с созданной спецификацией безопасности. При этом требования к архитектуре аппаратной части должны соответствовать требуемому уровню SIL [1]. Этот уровень определяется через отказоустойчивость аппаратного обеспечения и долю неопасных отказов (Таблица 2).

Следующей важной составляющей нормированного процесса конструирования и разработки являются расчеты оценок вероятности отказа функций безопасности узлов оборудования вследствие случайных отказов компонентов. Здесь особое внимание необходимо обратить на оценку интенсивности отказов подсистем с вероятностью обнаружения отказов при помощи диагностирующих устройств, а также время, затрачиваемое на устранение обнаруженного отказа. Для каждого уровня совокупной безопасности рекомендуются методы и мероприятия для обуздания случайных отказов компонентов, систематических отказов, а также отказов, вызванных влиянием окружающей среды и условий эксплуатации.

Нормативная проверка эффективности всех функций безопасности должна осуществляться по заранее составленному плану. При этом необходимо проверить эффективность каждой специфицированной функции обеспечения безопасности путем испытаний или анализа при строгом документировании результатов. Очевидно, что поступая таким образом, необходимо также тщательно перепроверять и документировать все последующие модернизации.

МЭК 61508 предписывает обязательную проверку правильности всех действий каждого этапа всего цикла разработки.

4 Требования к программному обеспечению

Часть 3 МЭК 61508 определяет требования к программному обеспечению систем. Как и в части 2 стандарта здесь описывается безопасный жизненный цикл и управление качеством программного обеспечения на всех стадиях его разработки вплоть до модернизации и проверки эффективности. Исходя из результатов частей 1 и 2 здесь предписывается порядок действий при разработке безопасного программного обеспечения. При помощи этой информации, а также табличных материалов из приложения к стандарту можно сформулировать последовательность действий для разработки безопасного программного обеспечения.

Требования к безопасности программного обеспечения должны быть детально проработаны и тщательно проверены программистом-разработчиком при выполнении контрольной проверки (Review), дабы убедиться, что все предъявляемые требования к программному обеспечению достаточно специфицированы для возможности быть выполненными. Спецификация должна содержать положения для самоконтроля программного обеспечения и данные для контроля аппаратуры. После составления спецификации предусмотрено планирование проверки эффективности безопасности. Здесь, как это было сделано в части 2 в отношении аппаратуры, излагаются все требования к методам тестирования, а также критерии оценки выполнения или невыполнения. На следующем этапе происходит непосредственно разработка программного обеспечения. Созданное программное обеспечение должно быть пригодным для анализа и проверки для получения уверенности, что проверка требований по обеспечению уровня совокупной безопасности может быть надежно проведена. Создаваемое программное обеспечение следует, по возможности, разделять на отдельные модули. Преимущество этого состоит в том, что сложность отдельных модулей гораздо ниже, чем одной большой программы. При проектировании каждого модуля необходимо следить за тем, чтобы он был достаточно точно специфицирован и проверен. МЭК 61508 рекомендует тщательный выбор средств программирования и компиляторов.

При интеграции программного обеспечения в аппаратуру необходимо путем тестирования проверить их совместимость для уверенности, что требуемый уровень совокупной безопасности может быть достигнут. Тестами, к примеру, могут являться циклические тесты памяти или Walking-Bit тест для проверки шин системы. Интегрированная система из аппаратуры и программного обеспечения должна удовлетворять специфицированным требованиям. При этом следует действовать в соответствии с созданными планами проверки эффективности безопасности и проверять их выполнение путем тестирования.

При последующих модификациях программного обеспечения следует убедиться в том, что они не влияют на выполнение предписанных требований безопасности. Для этого необходимо каждый раз проводить анализ влияния запланированной модификации.

Как и в случае с аппаратурой, при контроле программ на каждом этапе жизненного цикла программного обеспечения должна проверяться правильность результатов. Поэтому верификацию программ необходимо планировать одновременно с их разработкой. Каждый отдельный компонент, как например программный код, данные, программные модули и архитектура программного обеспечения, должен быть верифицирован отдельно.

5 Примеры методов для определения SIL

В части 5 МЭК 61508 предлагаются методы для определения уровня SIL. Здесь для каждой функции обеспечения безопасности приведены методы, с помощью которых может быть проверена система. Принципиально различают два метода: качественный и количественный.

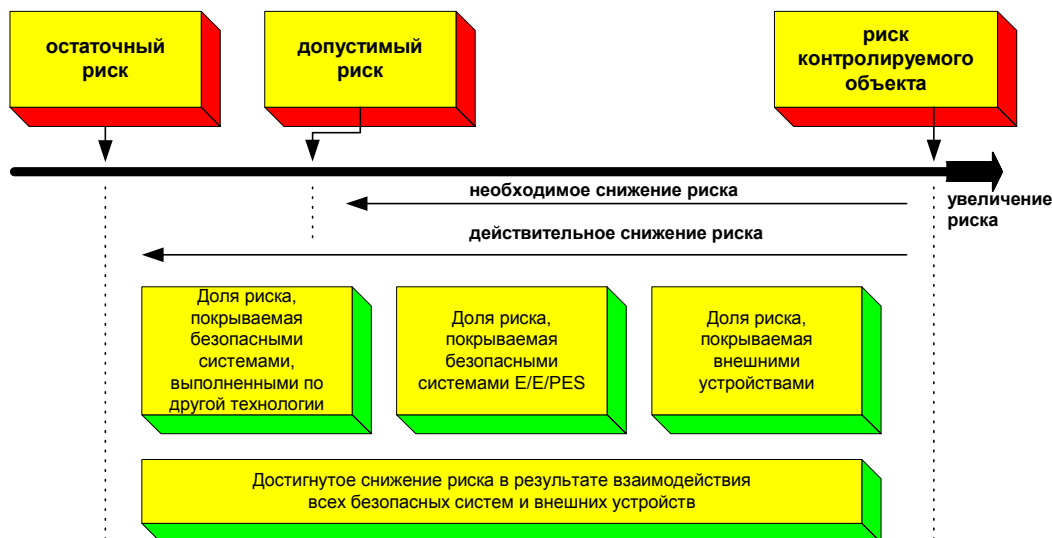


Рис. 6. Общие концепции снижения риска

При рассмотрении риска часто идет речь о допустимом риске. Это понятие зависит от различных факторов, таких как: тяжесть полученных повреждений, количество человек, которые могут пострадать, частота и длительность подверженности опасности. В общем смысле для этого применяется понятие ALARP риска (ALARP, As Low As Reasonable Practicable, минимальный разумно оправданный, целесообразный). При этом определены следующие группы риска:

- Недопустимый риск
- Нежелательный но еще допустимый риск
- Допустимый риск
- Незначительный риск

Помимо этого определения при классификации групп риска для оценки несчастных случаев оцениваются также вероятность возникновения и последствия аварийных ситуаций. С учетом этих параметров составлена таблица 3 классификации групп риска:

Степень риска	Интерпретация	Оценка
Класс I	Недопустимый риск	существенно
Класс II	Нежелательный риск, допустим только если уменьшение риска не является возможным или если расходы на уменьшение риска непропорционально превышают достигаемый эффект	существенно
Класс III	Допустимый риск, когда расходы на уменьшение риска превосходят достигаемое его уменьшение	существенно
Класс IV	Пренебрегаемый риск	существенно

Таблица 3. Классификация степени риска

Для определения уровня SIL привлекаются также количественные методы. В МЭК 61508 изложено, как с помощью графов риска и со знанием факторов риска может быть определен уровень SIL. Эти методы были заимствованы из стандарта ФРГ DIN V 19250 [7].

Количественная методика для определения уровня SIL демонстрируется в МЭК 61508 с помощью следующего порядка действий. Для этого допустимый риск методически связывается с риском контролируемого оборудования EUC для определения степени необходимого снижения риска:

$$PFD_{avg} \leq \frac{F_t}{F_{np}} = \Delta R \quad (1)$$

где

PFD_{avg} средняя вероятность возникновения отказа (average probability of failure on demand)

F_t частота возникновения допустимого риска

F_{np} интенсивность использования системы

ΔR необходимое снижение риска

Этот подход легко можно изобразить графически.

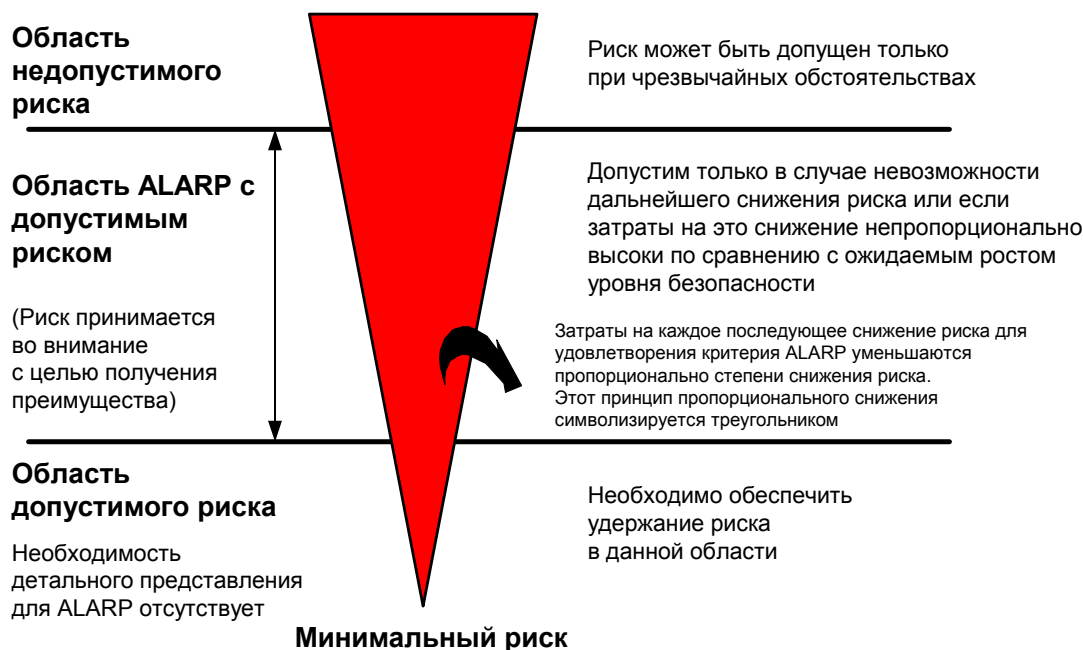


Рис. 7. Допустимый риск с точки зрения ALARP принципа

6 Замечания по применению частей 2 и 3

Часть 6 МЭК 61508 представляет для разработки безопасных систем (как и части 2 и 3) один из центральных разделов стандарта. Здесь приводятся подробные указания для количественного расчёта безопасных систем. Среди прочего здесь даны блок-схемы, диаграммы и формулы для расчёта значений PFD и PFH, а также таблицы для определения коэффициента β и для оценки степени охвата системы диагностикой. Таблицы с рассчитанными значениями PFD и PFH приведены для всех указанных в стандарте вариантов конфигураций систем со всеми существенными параметрами.

В качестве примера можно привести здесь уравнение для расчёта коэффициента PFD для 1oo2 – системы:

$$PFD_{G,1oo2} = 2 \cdot ((1 - \beta_D) \cdot \lambda_{DD} + (1 - \beta) \cdot \lambda_{DU})^2 \cdot t_{CE} \cdot t_{GE} + \beta_D \cdot \lambda_{DD} \cdot MTTR + \beta \cdot \lambda_{DU} \cdot \left(\frac{T_I}{2} + MTTR \right) \quad (2)$$

где

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_I}{2} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \quad (3)$$

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_I}{3} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \quad (4)$$

Уравнение (2) состоит из трёх слагаемых. Первое слагаемое с квадратной частью описывает простые отказы (normal cause failure). Второе и третье слагаемые определяют вероятность возникновения опасных отказов, имеющих общую причину возникновения, причём в системе могут происходить как опасные обнаруживаемые отказы с интенсивностью отказов λ_{DD} , так и опасные необнаруживаемые отказы с интенсивностью отказов λ_{DU} . Присутствующий в уравнении (2) коэффициент β вводится как отношение вероятности отказов, имеющих общую причину возникновения, к вероятности случайного отказа для согласования влияния отдельных частей выражения.

Двумя следующими важными для безопасных систем коэффициентами являются коэффициенты SFF (Safe Failure Fraction, доля безопасных и опасных обнаруживаемых отказов в общем количестве отказов системы) и DC (Diagnostic Coverage Factor, эффективность системы диагностики). Вычисление коэффициента SFF может производиться при помощи уравнения:

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_{DD} + \lambda_{DU}} \quad (5)$$

Коэффициент DC можно определить при помощи следующего уравнения

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_D} \quad (6)$$

Параметры и коэффициенты, встречающиеся в уравнениях, имеют следующие значения:

- β Коэффициент влияния опасных необнаруживаемых отказов, имеющих общую причину возникновения (dangerous undetected common-cause failure)
- β_D Коэффициент влияния опасных обнаруживаемых отказов, имеющих общую причину возникновения (dangerous detected common-cause failure)
- λ_D Интенсивность отказов вследствие опасных неисправностей (dangerous failure)
- λ_{DD} Интенсивность отказов вследствие опасных обнаруживаемых неисправностей (dangerous detected failure)
- λ_{DU} Интенсивность отказов вследствие опасных необнаруживаемых неисправностей (dangerous undetected failure)

$MTTR$	Среднее время выполнения ремонта (восстановления) (Mean Time To Repair)
PFD_G	Средняя вероятность отказа (Average Probability of Failure on Demand)
T_1	Среднее время между диагностикой (proof-test interval)
t_{CE}	Среднее время простоя одного канала (channel equivalent mean down time)
t_{GE}	Среднее время простоя системы (voted group equivalent mean down time)

МЭК 61508 описывает образцовый подход при определении отказов оборудования. Сначала приводятся основные положения и гипотезы, на которых будут базироваться расчёты. Существует большое количество методов для анализа совокупной безопасности в безопасных системах. К числу наиболее часто используемых относятся диаграммы надёжности и марковские модели. Оба метода дают при их правильном применении почти одинаковые результаты. Более точными, но одновременно и более сложными, являются марковские модели [1], которые при их применении даже в сложных системах позволяют получить точные результаты. Для нахождения значений PFD безопасной системы в целом необходимо сложить величины средней вероятности отдельных подсистем, таких как подсистемы датчиков, средств обработки сигнала и исполнительных устройств:

$$PFD_{sys} = PFD_{датчики} + PFD_{обработка} + PFD_{исполнение} \quad (17)$$

Для определения средней вероятности отказа каждой подсистемы должны быть известны следующие данные:

- архитектура построения,
- охват (покрытие) диагностикой каждого канала,
- интенсивность отказов для каждого канала в час,
- коэффициенты β и β_D для отказов, имеющих общую причину.

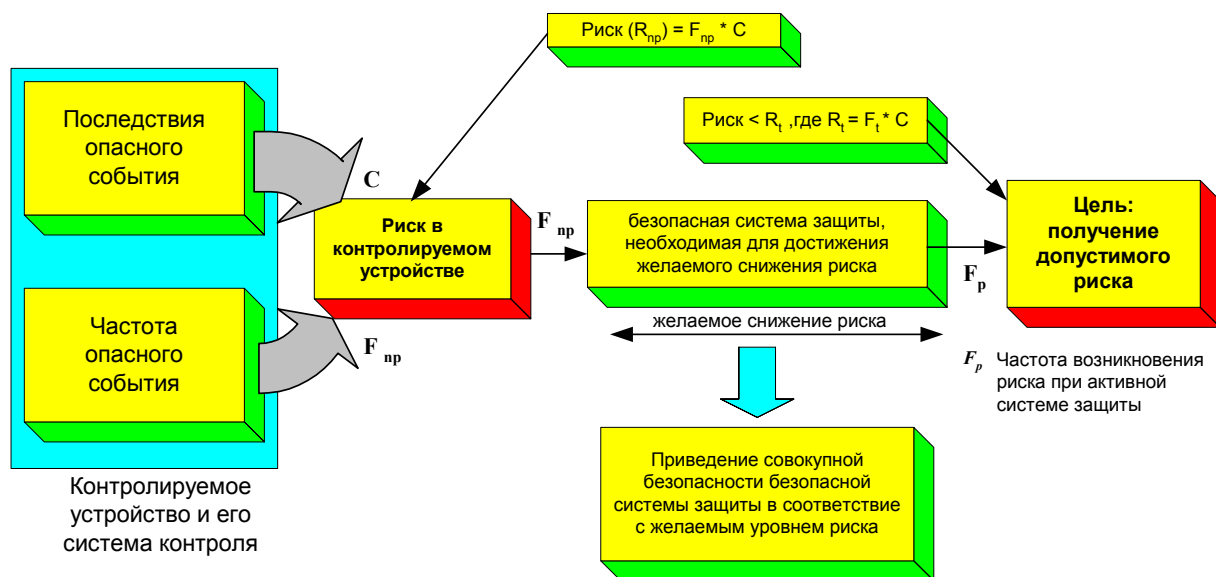


Рис. 8. Порядок действий при определении уровня SIL системы

7 Обзор методов и приемов

В заключительной части МЭК 61508 подробно разъясняются указания, сделанные в таблицах в частях 2 и 3. Здесь даны упорядоченные по темам необходимые указания по всем используемым в стандарте методам и приемам. Данная часть стандарта может использоваться как справочное пособие. Часть 7 состоит из четырех больших тематических разделов:

1. Обзор методов и приемов предупреждения случайных отказов аппаратуры
2. Обзор методов и приемов предупреждения систематических отказов аппаратуры
3. Обзор методов и приемов достижения совокупной безопасности программного обеспечения
4. Обзор методов и приемов достижения совокупной безопасности так называемого прототипа программного обеспечения (pre-developed software)

8 Заключение

Данное краткое обобщение МЭК 61508 показывает универсальность применения стандарта для техники обеспечения безопасности. Поставленное намерение создать универсальный стандарт было по мнению автора статьи полностью достигнуто. Стандарт рассматривает не только отдельные выделенные аспекты безопасных систем, как PFD или MTTF, но и описывает рациональный подход для всего жизненного цикла этих систем или устройств. Такая методика упрощает наряду с проектированием также сертификацию и техобслуживание систем обеспечения безопасности и стимулирует строгое документирование отдельных процессов. Дальнейшим положением, освещаемым стандартом, является тот факт, что не каждая система, применяемая для обеспечения безопасности, автоматически получает присвоение уровня SIL в соответствии со стандартом. Особо подчеркивается, что исключительно системы незначительной сложности (под это определение микропроцессорные устройства не подпадают) могут быть сертифицированы вдобавок только на основе опыта их эксплуатации. Для сертификации уже используемых сложных систем необходимо подтверждение их соответствия стандарту. Стандарт однако тоже, как и все нормы, допускает определенную свободу выбора в пределах каждого уровня SIL. Кроме того сертификация только безопасной системы по уровню SIL 3 не должна автоматически являться критерием решения в пользу всего устройства. Хотя выбранная система и удовлетворяет данному совокупному уровню, необходимо учитывать ограничения, отраженные в так называемых «certification reports» (отчеты по сертификации). В них в общих чертах документируются ограничения сертифицированной по МЭК 61508 системы (устройства). Можно уверенно предсказать, что благодаря заложенной универсальности МЭК 61508 найдет широкое применение во всем мире в качестве стандарта по безопасности.

Литература

- [1] IEC/EN 61508: International Standard 61508 Functional Safety: Safety-Related System. Geneva, International Electrotechnical Commission.
- [2] *Börçsök, J.*: Internationale-/Europa Norm 61508, Vortrag bei der VD-Tagung der HIMA GmbH + Co KG, 2002.
- [3] *Börçsök, J.*: Konzepte zur methodischen Untersuchung von Hardwarearchitekturen in sicherheitsgerichteten Anwendungen, Universität Kassel (noch nicht veröffentlicht).
- [4] *Börçsök, J.*: Sicherheits-Rechnerarchitekturen Teil 1 und 2, Vorlesung Universität Kassel; 2000 / 2001.
- [5] *Börçsök, J.*: Echtzeit-Betriebssysteme für sicherheitsgerichtete Realzeitrechner, Vorlesung Universität Kassel, 2001.
- [6] DIN VDE 0801: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme (E/E/PES), (IEC 65A/255/CDV:1998), S. 27f., August 1998.
- [7] DIN V 19250: Grundlegende Sicherheitsbetrachtungen für MSR - Schutzeinrichtungen, Beuth Verlag, Berlin 1998.
- [8] DIN VDE 0801/A1: Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben, Beuth Verlag, Berlin 1994.
- [9] IEC 60880-2: Software für Rechner mit sicherheitskritischer Bedeutung, Beuth Verlag, Berlin 2001.

Об авторе



Приват-доцент д-р Йозеф Бёрчек (44) руководит департаментом проектирования фирмы HIMA GmbH + Co KG, производящей системы автоматизации промышленности. Более 9 лет он специализируется в области безопасной вычислительной техники и участвует в работе различных комитетов Немецкой комиссии по стандартизации в электротехнике, электронике и информационной технике (составной части DIN и VDE). С 1992 он читает лекции в университетах и институтах на темы автоматизации, микропроцессоров, систем реального времени, ЭВМ и архитектур безопасных ЭВМ.

Адрес: HIMA Paul Hildebrandt GmbH + Co KG, Albert-Bassermann-Str. 28, D-68782 Brühl bei Mannheim, тел. +49-6202-709-270, адрес электронной почты: j.boercsoek@hima.com