ЗИ АКАДЕМИЯ СОВРЕМЕННЫХ ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

ЗИ Функциональная безопасность

ЗИ.16 Требования стандарта МЭК 61508. Терминология

Курс лекций (Лекция 2, число стр. - 16)

Москва, 2017

Академия Современных ИнфоКоммуникационных Технологий

Для того чтобы сделать еще один шаг в изучении функциональной безопасности, необходимо продолжить рассмотрение стандарта МЭК 61508 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью» (IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems). Дело в том, что функциональная безопасность – это достаточно формализованное свойство, поскольку системы, важные для безопасности, являются предметом государственного лицензирования во всех странах.

Изучение стандартов и заложенной в них терминологии – это не самое веселое занятие в мире, но, при прагматичном подходе, технический уровень специалиста может от этого повыситься. Толкование терминологии является своего рода «технической юриспруденцией», а хитросплетению сюжетных линий в изложении требований может позавидовать любой автор детектива.
Не станем уверять, что, изучая стандарты, все сразу станут техническими Шерлоками Холмсами. Хотя, знание основ стандартизации (то есть, технического законодательства), лежит в основе работы любого сыщика технического эксперта. Изучение стандартов – это скорее путь Дата Туташхиа из полузабытого ныне романа Чабуа Амирэджиби (а есть еще экранизация – «Берега»), путь не столько вперед, сколько в глубину, не столько в действие, сколько в осмысление.

Общие сведения о МЭК 61508

Стандарт оперирует термином электрическая/ электронная/ программируемая электронная (Э/Э/ПЭ) система (electrical/electronic/programmable electronic).

Особенностью стандарта является риск-ориентированный подход. В зависимости от риска, который техногенный объект создает для окружающей среды, жизни и здоровья людей, устанавливаются риски для отказов систем управления.

Например, обратим внимание на системы защиты атомных реакторов. Для них в режиме постоянной работы отказы должны происходить не чаще, чем один раз в 1000 лет эксплуатации (10

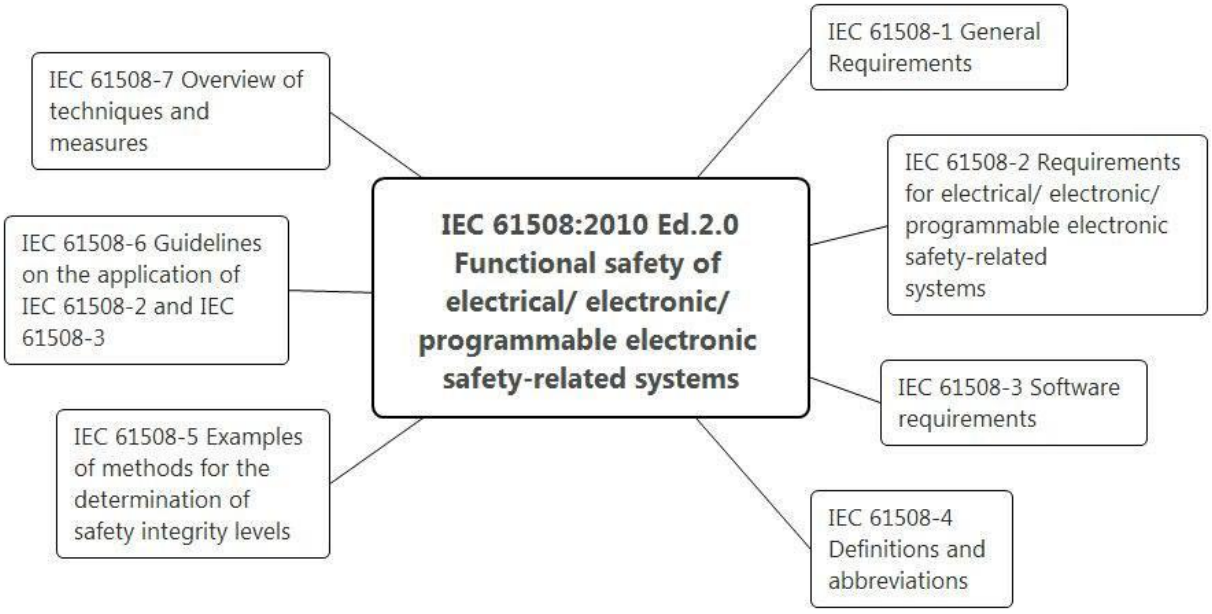
миллионов часов наработки на отказ). Такие показатели задаются не для единичного объекта, а для «флота», т.е. для множества однотипных объектов. Вроде бы, отказы являются достаточно редкими событиями, ведь ни одна атомная электростанция не проработает тысячу лет. Однако, если учесть, что в мире эксплуатируется более 400 атомных реакторов, то для «флота» мы уже получим цифру один отказ в 2,5 года, что звучит гораздо более удручающе. Во время Чернобыльской и Фукусимской ядерных катастроф системы аварийной защиты не сработали так, как ожидалось проектировщиками. Это еще один аргумент в пользу важности рассмотрения функциональной безопасности.

Для снижения значений рисков ниже заданных показателей реализуется комплекс организационно-технических мер, которые также регламентированы в МЭК 61508, в зависимости от допустимой величины риска отказа.

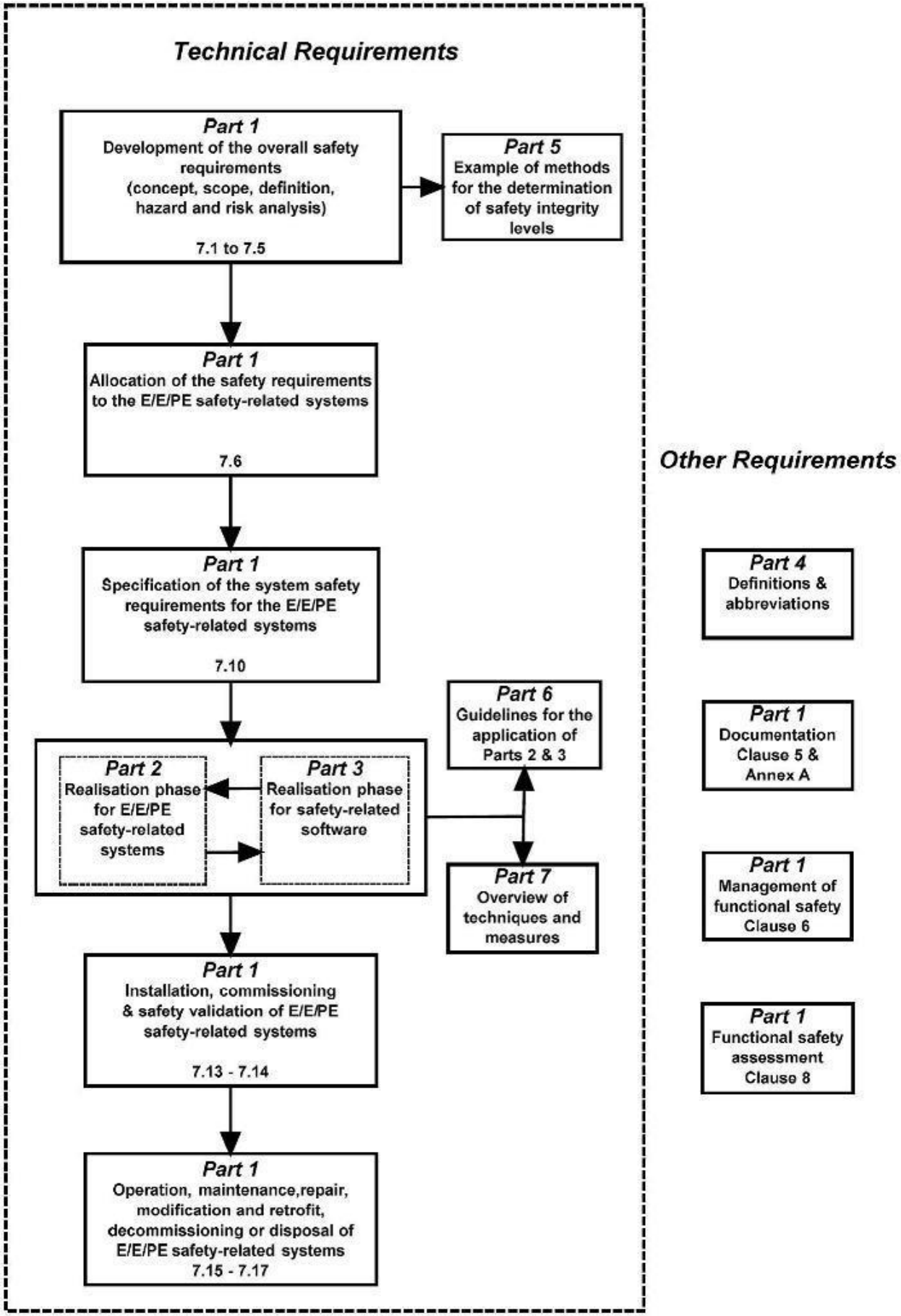
Кроме того, МЭК 61508 представляет собой верхний уровень целого семейства отраслевых стандартов, которые детализируют требования к функциональной безопасности для систем управления медицинским оборудованием, автомобильным и железнодорожного транспортом, АСУ ТП и т.д.

Первая редакция МЭК 61508 была разработана с 1998 по 2000 годы. В Российской Федерации первая редакция была принята в качестве государственного стандарта ГОСТ Р МЭК 61508 в 2007 году. В настоящее время в мире действует вторая редакция МЭК 61508, выпущенная в 2010. В Российской Федерации вторая редакция МЭК 61508 также является актуальной с 2012 года (ГОСТ Р МЭК 61508-2012).

Серия стандартов МЭК 61508 включает 7 частей, которые в сумме содержат около 600 страниц текста. О назначении частей легко догадаться по их названиям.

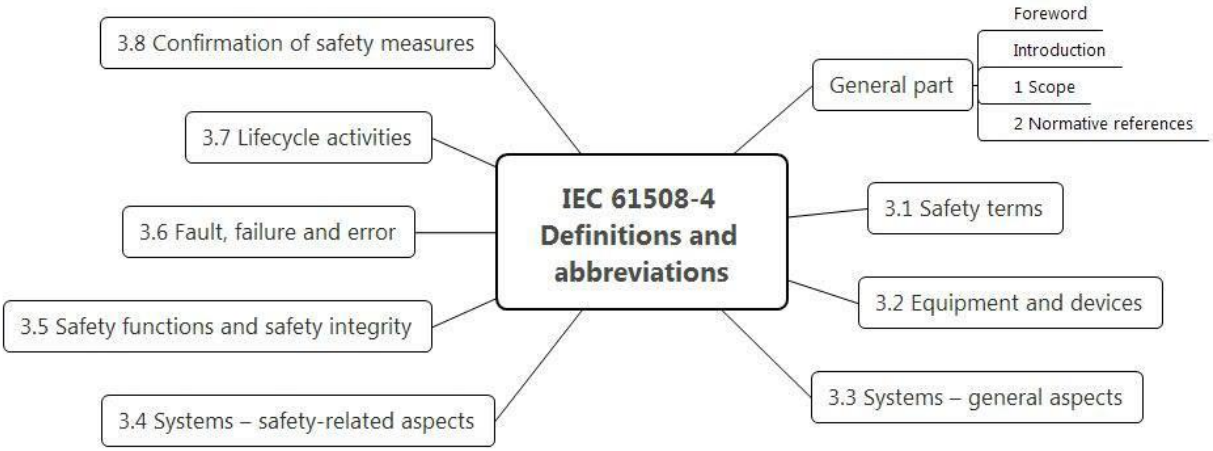


Конечно, между частями МЭК 61508 существуют довольно сложные связи, что отражено в рисунках самого стандарта: Overall framework of the IEC 61508 series (IEC 61508, Figure 1).


Technical Requirements
Part 1
Development of the overall safety requirements (concept, scope, definition, hazard and risk analysis)
7.1 to 7.5
Part 5
Example of methods for the determination of safety integrity levels
Part 1
Allocation of the safety requirements to the E/E/PE safety-related systems
7.6
Part 1
Specification of the system safety requirements for the E/E/PE safety-related systems
7.10
Part 6
Guidelines for the application of Parts 2 & 3
Part 2
Realisation phase for E/E/PE safety-related systems
Part 3
Realisation phase for safety-related software
Part 7
Overview of techniques and measures
Part 1
Installation, commissioning & safety validation of E/E/PE safety-related systems
7.13 - 7.14
Part 1
Operation, maintenance,repair, modification and retrofit, decommissioning or disposal of E/E/PE safety-related systems
7.15 - 7.17
Other Requirements
Part 4
Definitions & abbreviations
Part 1
Documentation Clause 5 & Annex A
Part 1
Management of functional safety Clause 6
Part 1
Functional safety assessment Clause 8

Терминология МЭК 61508: базовые термины по безопасности

Для того, чтобы разобраться с концепцией функциональной безопасности, пожалуй, начать надо, не с начала и не с конца, а с середины, а именно с четвертой части (МЭК 61508-4), где изложена основная терминология. Как видим, термины разделены на 8 групп (3.1-3.8). Эти группы логически связаны между собой. На мой взгляд, самыми важными являются группы 3.1 (Safety terms) и 3.5 (Safety functions and safety integrity).



Далее термины выборочно цитируются согласно русскоязычному тексту МЭК 61508-4, а затем дается их авторская интерпретация.

Итак, первый раздел по терминологии, 3.1 «Термины, относящиеся к безопасности».

3.1.1 вред (harm): Физическое повреждение или ущерб, причиняемый здоровью людей, имуществу или окружающей среде.

3.1.2 опасность (hazard): Потенциальный источник причинения вреда

3.1.6 риск (risk): Сочетание вероятности события причинения вреда P(t) и тяжести этого вреда C.

3.1.7 допустимый риск (tolerable risk): Риск, который приемлем при данных обстоятельствах на основании существующих в обществе ценностей.

3.1.11 безопасность (safety): Отсутствие неприемлемого риска.

3.1.12 функциональная безопасность (functional safety): Часть общей безопасности, обусловленная применением управляемого оборудования (УО) и системы управления УО, и зависящая от правильности функционирования систем, связанных с безопасностью, и других средств по снижению риска.

3.1.13 безопасное состояние (safe state): Состояние УО, в котором достигается безопасность.

Попытаемся связать все сущности в единое целое, и в результате получилась следующая схема (пожалуй, можно назвать ее онтологией). Важно отметить, что компьютерная система управления (КСУ) является лишь одной из многих мер по снижению рисков. Существует множество так называемых пассивных мер защиты, например, ремень безопасности в автомобиле или в самолете.

Риск является показателем безопасности, и на понятии риска необходимо будет обратить внимание в дальнейшем, при рассмотрении этих самых показателей. Пока приведём простой пример. Ходит зачем-то человек по краю крыши. Вероятность падения с крыши при прочих равных условиях не зависит от высоты здания. А вот степень ущерба зависит. Тогда и риск падения с крыши 10-этажного здания будет выше, чем риск падения с крыши одноэтажного здания. А вот риск падения с крыши 10-этажного здания практически равен риску падения с крыши 100-этажного здания, поскольку, если вероятность падения одинакова, то и последствия (ущерб) падения здесь, к сожалению, также одинаковы.

Интересным, на наш взгляд, является понятие допустимого (приемлемого) риска. Оно зависит от исторического и гуманитарного контекста. Правда ли, что наивысшими ценностями современного общества является человеческая жизнь и забота об окружающей среде, которая формирует и поддерживает эту самую жизнь? Реальное состояние техногенных объектов демонстрирует, насколько государство и общество реализуют провозглашенные ценности.

Еще одним принципиальным понятием является «безопасное состояние». Например, одна из важнейших систем безопасности, система противоаварийной защиты (ПАЗ), должна остановить функционирование управляемого объекта. Как это происходит? Как правило, путем разрыва электрических цепей (это уже зависит от технологических алгоритмов управления оборудованием), что происходит путем перевода выходных дискретных сигналов в состояние «логический 0» (так называемый принцип de-energize to trip, чтобы система могла отработать и при аварийной потере электроснабжения). При необходимости, «логический 0» может быть инвертирован в «логическую 1» через промежуточные реле.

Терминология МЭК 61508: термины, относящиеся к функциям безопасности и полноте безопасности (safety integrity)

В лекции №1 вкратце упомянуто, что понятие функциональной безопасности включает в себя реализуемые функции безопасности и полноту (интегрированность) выполнения этих функций.

В МЭК 61508-4, раздел 3.5 «Функции безопасности и полнота безопасности» приводятся соответствующие термины.

3.5.1 функция безопасности (safety function): Функция, реализуемая Э/Э/ПЭ системой, связанной с безопасностью, или другими мерами по снижению риска, предназначенная для достижения или поддержания безопасного состояния УО по отношению к конкретному опасному событию

3.5.4 полнота безопасности (safety integrity): Вероятность того, что система, связанная с безопасностью, будет удовлетворительно выполнять требуемые функции безопасности при всех оговоренных условиях в течении заданного интервала времени.

3.5.5 полнота безопасности программного обеспечения (software safety integrity): Составляющая полноты безопасности системы, связанной с безопасностью, касающаяся систематических отказов, проявляющихся в опасном режиме и относящихся к программному обеспечению.

3.5.6 полнота безопасности, касающаяся систематических отказов (systematic safety integrity): Составляющая полноты безопасности системы, связанной с безопасностью, касающаяся систематических отказов, проявляющихся в опасном режиме.

3.5.7 полнота безопасности аппаратных средств (hardware safety integrity): Составляющая полноты безопасности системы, связанной с безопасностью, касающаяся случайных отказов аппаратуры, проявляющихся в опасном режиме.

3.5.8 уровень полноты безопасности; УПБ [safety integrity level (SIL)]: Дискретный уровень (принимающий одно из четырех возможных значений), соответствующий диапазону значений полноты безопасности, при котором уровень полноты безопасности, равный 4, является наивысшим уровнем полноты безопасности, а уровень полноты безопасности, равный 1, соответствует наименьшей полноте безопасности.

3.5.9 стойкость к систематическим отказам (systematic capability): Мера уверенности (выраженная в диапазоне ССО 1 — ССО 4) в том. что систематическая полнота безопасности элемента соответствует требованиям заданного значения

уровня полноты безопасности (УПБ) для определенной функции безопасности элемента, если этот элемент применен в соответствии с указаниями, определенными для этого элемента в соответствующем руководстве по безопасности.

3.5.16 режим работы (mode of operation): Способ выполнения функции безопасности либо в режиме:

— с низкой частотой запросов (low demand mode), в котором функция безопасности выполняется только по запросу и переводит УО в определенное безопасное состояние, а частота запросов не превышает одного в год или

— с высокой частотой запросов (high demand mode), в котором функция безопасности выполняется только по запросу и переводит УО в определенное безопасное состояние, а частота запросов превышает один в год, или

— непрерывном режиме (continuous mode), в котором функция безопасности поддерживает УО в безопасном состоянии, как и при нормальном функционировании.

С точки зрения приводимого определения полноты безопасности (safety integrity), это свойство фактически сводится к безотказному выполнению функций безопасности, т.е. рассматривается, как часть безотказности, которая, в свою очередь, является составляющей классической надежности. На самом деле, из других положений МЭК 61508 следует, что полнота безопасности является более сложным свойством, связанным с такими атрибутами, как ремонтопригодность, готовность, долговечность, информационная безопасность. Терминологические и таксономические аспекты составляющих надежности и безопасности представляют собой смежную область знаний. В последующих публикациях есть смысл разобраться в этом подробней.

Еще одним центральным понятием в МЭК 61508 является уровень полноты безопасности (Safety Integrity Level, SIL). Значение SIL устанавливает в зависимости от того, насколько влияние управляемого оборудования создает риск для людей и окружающей среды.

Исходя из этого, установлен риск отказа и для самой

компьютерной системы управления. Например, в начале лекции уже говорилось, что для системы защиты атомного реактора наработка на отказ должна составлять не менее, чем 10 миллионов часов. Это соответствует SIL3. Вообще, принято считать, что SIL4 могут соответствовать лишь наиболее простые устройства. Для программируемых логических контроллеров (ПЛК), используемых в АСУ ТП, достижимым является SIL3.

Из структуры определений также следует, что полнота безопасности делится на две составляющие: полнота безопасности, касающаяся систематических отказов (сюда же попадает полнота безопасности программного обеспечения) и полнота безопасности аппаратных средств.

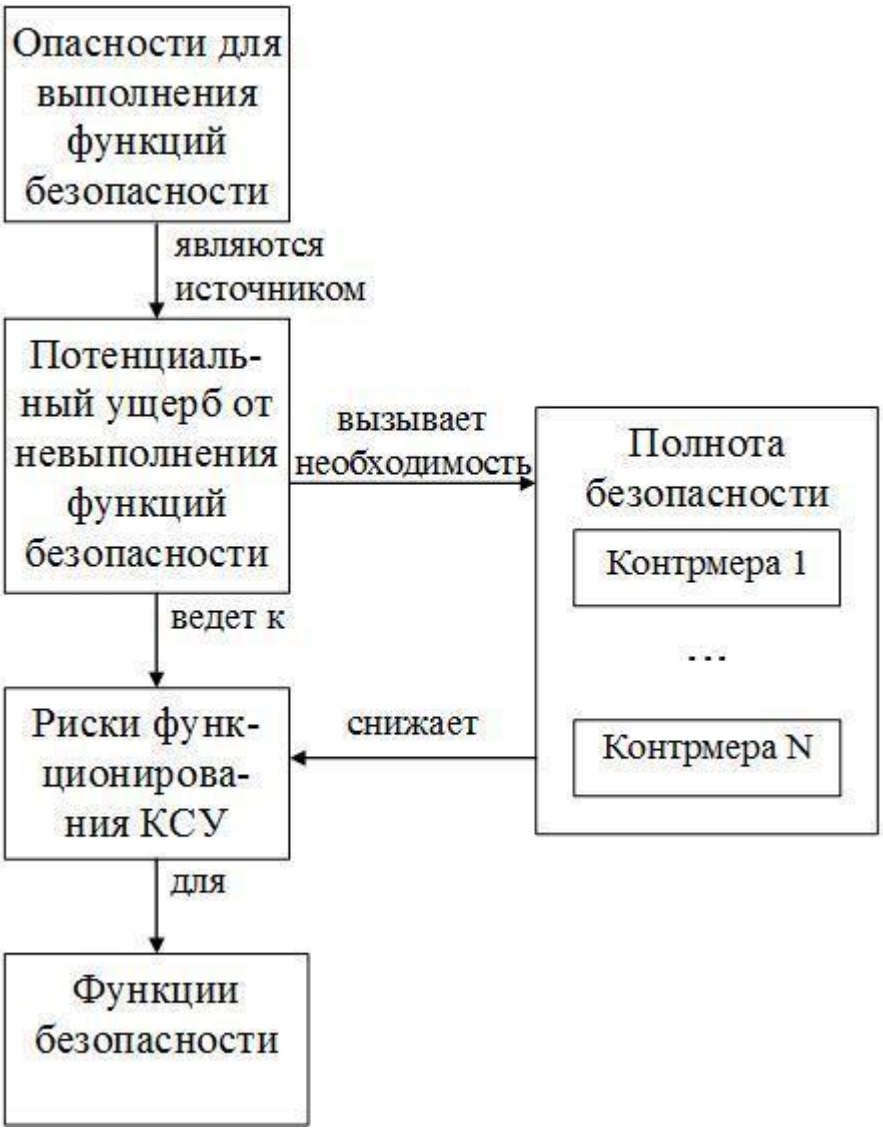
Первая составляющая требует применять меры защиты от систематических отказов, вызванных ошибками проектирования. Для этого необходимо совершенствовать процессы проектирования и разработки, тестирования, управления конфигурацией, проектного менеджмента и т.п. Это отдаленно напоминает уровни Capability Maturity Model Integration (CMMI), но напрямую к ним не трассируется. Для каждого из значений SIL определен набор методов защиты от систематических отказов, причем их количество и «строгость» возрастает с повышением SIL.

Полнота безопасности аппаратных средств связана с защитой от случайных отказов и обеспечивается применением компонентов с высоким уровнем безотказности и самодиагностики, и, конечно же, резервированием.

Здесь есть интересный фокус, который применяют многие разработчики ПЛК. Можно достичь уровня SIL2 при одноканальной конфигурации ПЛК. Тогда резервированная конфигурация даст SIL3. При этом процессы разработки (systematic capability), должны соответствовать SIL3.

Теперь, по аналогии с предыдущим разделом, попробуем применить структуру окружения (опасность, ущерб, риски, контмеры, управляемое оборудование) для компьютерной системы управления (КСУ). Здесь речь идет об опасностях для выполнения функций безопасности КСУ, поскольку их

невыполнение связано с риском. Для снижения этого риска применяются различные меры по обеспечению полноты безопасности. Как мы уже знаем, эти меры направлены на защиту от случайных и систематических отказов.



Попробуем теперь совместить полученную схему со схемой из предыдущего размера. Получается такая вот двухуровневая структура, демонстрирующая терминологическую среду функциональной безопасности «на пальцах».

Терминология МЭК 61508: еще несколько полезных терминов

Итак, согласно МЭК 61508-4, у нас еще осталось шесть из восьми разделов по терминологии.

Следующий терминологический раздел: 3.2 «Оборудование и

устройства». Здесь приводятся достаточно тривиальные определения, относящиеся к типам программного и аппаратного обеспечения, используемых в системах, важных для безопасности. Приведём лишь определение для упоминаемого выше управляемого оборудования.

3.2.1 управляемое оборудование; УО [equipment under control (EUC)]: Оборудование, машины, аппараты или установки, используемые для производства, обработки, транспортирования, в медицине или в других процессах.

В разделе 3.3 «Системы: общие аспекты» также содержать понятные технарям определения.

В разделе 3.4 «Системы: аспекты, связанные с безопасностью» содержится важное определение, отвечающее на вопрос: «а что именно подразумевается под системой, связанной с безопасностью?»

3.4.1 система, связанная с безопасностью (safety-related system): Система, которая:

— реализует необходимые функции безопасности, требующиеся для достижения и поддержки безопасного состояния УО и

— предназначена для достижения своими средствами или в сочетании с другими Э/Э/ПЭ системами, связанными с безопасностью, и другими средствами снижения риска необходимой полноты безопасности для требуемых функций безопасности.

Раздел 3.6 «Сбой, отказ и ошибка» дает определение этим досадным происшествиям. Кроме того, в данном разделе даются определения уже известным нам случайным и систематическим отказам, а также опасным и безопасным отказам. Далее следуют определение показателей безопасности, которые есть смысл рассмотреть в отдельной публикации.

3.6.1 сбой (fault): Ненормальный режим, который может вызвать снижение или потерю способности функционального блока выполнять требуемую функцию.

3.6.4 отказ (failure): Прекращение способности функционального блока выполнять необходимую функцию либо функционирование этого блока любым способом, отличным от требуемого.

3.6.5 случайный отказ аппаратуры (random hardware failure): Отказ, возникающий в случайный момент времени, который является результатом одного или нескольких возможных механизмов ухудшения характеристик аппаратных средств.

3.6.6 систематический отказ (systematic failure): Отказ, связанный детерминированным образом с некоторой причиной, который может быть исключен только путем модификации проекта, либо производственного процесса, операций, документации, либо других факторов.

3.6.7 опасный отказ (dangerous failure): Отказ элемента и/или подсистем и/или системы, которые принимают участие в реализации функций безопасности, в результате чего:

а) функция безопасности не выполняется, когда это требуется (для режимов с низкой или высокой частотой запросов) либо отказывает (для непрерывного режима), что приводит к переводу УО в опасное или потенциально опасное состояние;

б) снижается вероятность того, что функция безопасности при необходимости будет корректно выполнена.

3.6.8 безопасный отказ (safe failure): Отказ элемента и/или подсистем и/или системы, которые принимают участие в реализации функций безопасности, в результате чего:

а) приводят к выполнению функции безопасности по переводу УО (или его части) в безопасное состояние либо поддерживают безопасное состояние;

б) увеличивается вероятность выполнения функции безопасности по переводу УО (или его части) в безопасное состояние либо поддержке безопасного состояния.

3.6.10 отказ с общей причиной (common cause failure): Отказ, который является результатов одного или нескольких событий, вызвавших одновременные отказы двух или более отдельных каналов в многоканальной системе, ведущих к отказу системы.

3.6.11 ошибка (error): Расхождение между вычисленным, наблюдаемым или измеренным значением или условием и правильным, заданным или теоретически верным значением или условием.

Определения раздела 3.7 «Процессы жизненного цикла», как и сам жизненный цикл, являются темой отдельной публикации.

3.7.1 жизненный цикл систем безопасности (safety lifecycle): Необходимые процессы, относящиеся к реализации систем, связанных с безопасностью, проходящие в течение периода времени, начиная со стадии разработки концепции проекта и заканчивая стадией, когда все Э/Э/ПЭ системы, связанные с безопасностью, и другие средства снижения риска уже не используются.

В разделе 3.8 «Подтверждение мер по обеспечению безопасности» интерес представляют определения, даваемые для верификации и валидации. Сразу скажу, что обычно в жизненном цикле валидация и верификация (verification and validation, V&V) рассматривается как единый процесс. Непосредственно под валидацией понимаются испытания полностью интегрированной системы с физической симуляцией входных и выходных сигналов, а под верификацией – все остальные обзоры, анализы и тесты. Но из определений МЭК 61508 этого вовсе не следует.

Термины, относящиеся к подтверждению мер по обеспечению безопасности:

3.8.1 верификация (verification): Подтверждение выполнения требований путем исследования и сбора объективных свидетельств.

3.8.2 подтверждение соответствия (validation): Подтверждение, путем испытаний и представления объективных свидетельств, выполнения конкретных требований к предусмотренному конкретному использованию.

Выводы

МЭК 61508 представляет собой достаточно пространный, сложный, порой запутанный и противоречивый стандарт, включающий в себя 7 частей. «Распутать» его можно, только применяя на практике.

В основе МЭК 61508 лежит риск-ориентированный подход. Уровни риска для компьютерных систем управления назначаются в зависимости от влияния управляемого техногенного объекта на окружающую среду, а также на здоровье и жизнь людей.

Для этого в МЭК 61508 введено понятие уровня полноты безопасности (Safety Integrity Level, SIL), которые установлены по возрастающей, от 1 до 4. Для соответствия тому или иному SIL необходимо реализовать меры по защите от случайных отказов аппаратных средств, а также от систематических отказов, вызванных ошибками проектирования. Поэтому, для каждого из SIL заданы требования к продукту в виде значений показателей безопасности и требования к «строгости» реализации процессов жизненного цикла.

Терминология по функциональной безопасности изложена в четвертой части МЭК 61508 (МЭК 61508 4).

Разобравшись с терминологией, далее рассмотрим структуру и взаимосвязи для остальных частей МЭК 61508.

Трактовать законы и стандарты можно по-разному, но, в любом случае, трактующий обязан осмысливать их содержание, чтобы своевременно отличить добро от зла.

Автор: Владимир Скляр (Национальный аэрокосмический университет «Харьковский авиационный институт»), Project Manager, Functional Safety Expert, R&D

Материал взят с сайта Хабрахабр