ЗИ

АКАДЕМИЯ
СОВРЕМЕННЫХ
ИНФОКОММУНИКАЦИОННЫХ
ТЕХНОЛОГИЙ

ЗИ Функциональная безопасность

ЗИ.17 Стандарт МЭК 61508: структура требований

Курс лекций (Лекция 3, число стр. - 12)

Москва, 2017

Академия Современных ИнфоКоммуникационных Технологий

Как разобраться в структуре требований МЭК 61508?

Обратимся к структуре и взаимосвязям между всеми семью частями МЭК 61508 (повтор рисунка из лекции 2). Сейчас для нас важно то, что непосредственно требования содержатся в первых трех частях, а остальные четыре части носят справочный характер.

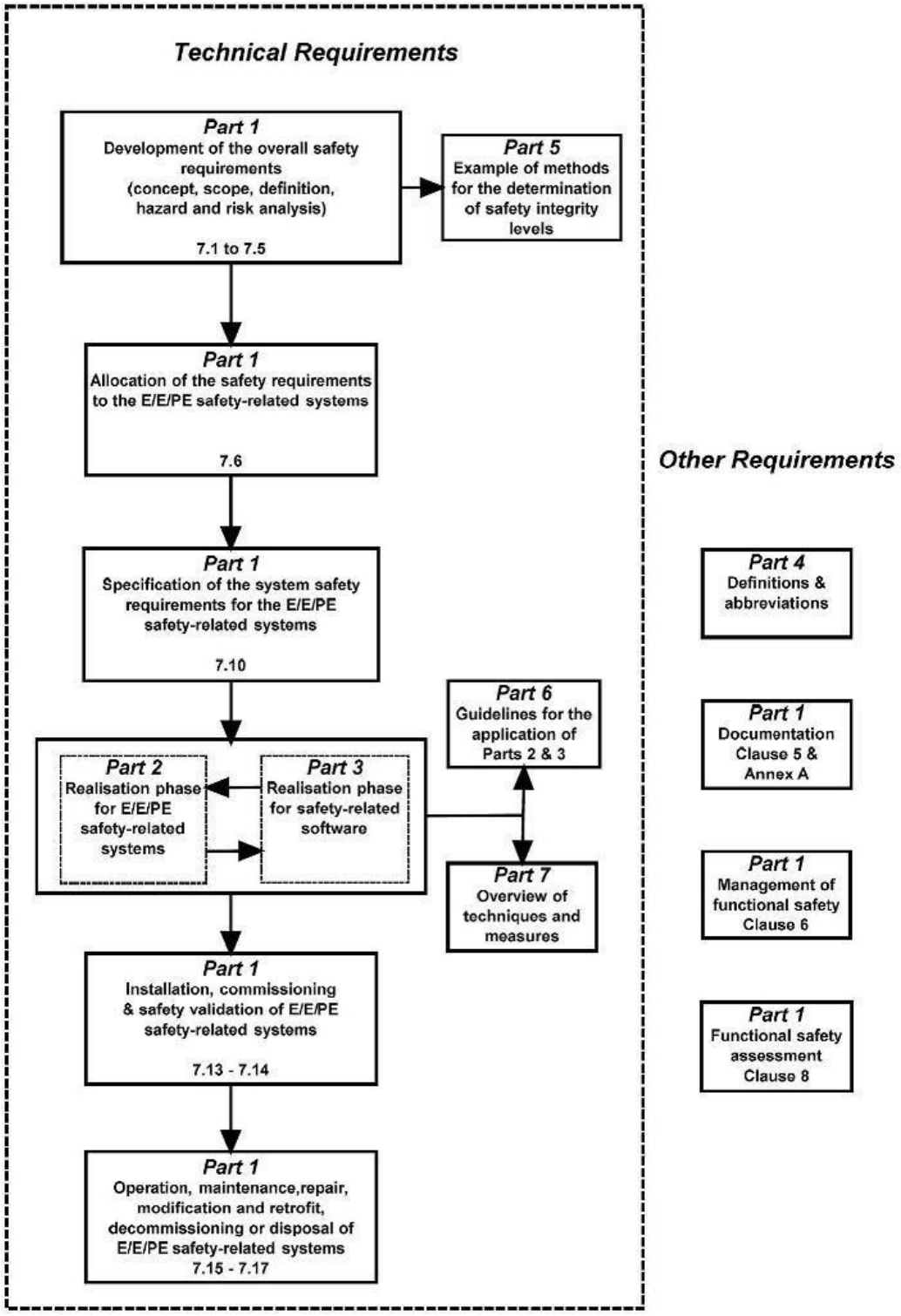

Рисунок 1. Overall framework of the IEC 61508 series (IEC 61508, Figure 1)

Давайте подумаем, на основе чего можно анализировать требования, чтобы разложить их «по полочкам»? Нужна классификация (таксономия), а где ее взять? Для начала можно взглянуть на содержание стандарта.

Действительно, части МЭК 61508-1,2,3 имеют типовое содержание, поскольку во всех трех частях:

— в разделе 5 изложены требования к документации;

— в разделе 6 приведены требования к управлению функциональной безопасностью;

— в разделе 7 описана структура жизненного цикла;

— в разделе 8 изложены требования к оцениванию функциональной безопасности.

Однако, только простого взгляда на содержание стандартов недостаточно для того, чтобы систематизировать их требования. Необходимо вспомнить, что функциональная безопасность, а вместе с ней и уровень полноты безопасности, который нам надо достичь, зависят от наличия либо отсутствия двух типов отказов:

1) случайные отказы аппаратных средств, для которых можно определить вероятность возникновения;

2) систематические отказы вызванные ошибками проектирования.

Для обозначения способности противостоять первым и вторым введены специальные термины: Random Capability & Systematic Capability (стойкость к случайным и систематическим отказам). По поводу Random Capability понятно, что надо защищать систему от случайных отказов (например, методами резервирования, устойчивости к помехам и другим экстремальным воздействиям и т.п.). Systematic Capability зависит, как от реализации процессов разработки, так и от механизмов защиты от отказов, и включает в себя:

— управление функциональной безопасностью (Functional Safety Management);

— реализацию жизненного цикла функциональной безопасности (Functional Safety Life Cycle);

— защиту от систематических отказов проектирования системы и аппаратных средств (Systematic Failures Avoidance);

— защиту от систематических отказов проектирования программного обеспечения (Software Failures Avoidance).

Кроме того, необходимо выполнять оценку функциональной безопасности (Functional Safety Assessment) путем определения соответствия продуктов (оборудования, программного обеспечения и документации) и процессов разработки продуктов указанным выше требованиям.

Такая вот структура требований к функциональной безопасности приведена на рисунке ниже, и именно такую структуру предлагается использовать при анализе требований отдельных частей МЭК 61508. Дальше в статье поочередно проводится краткий разбор содержания каждой из частей МЭК 61508, представленных в виде Mind Map.

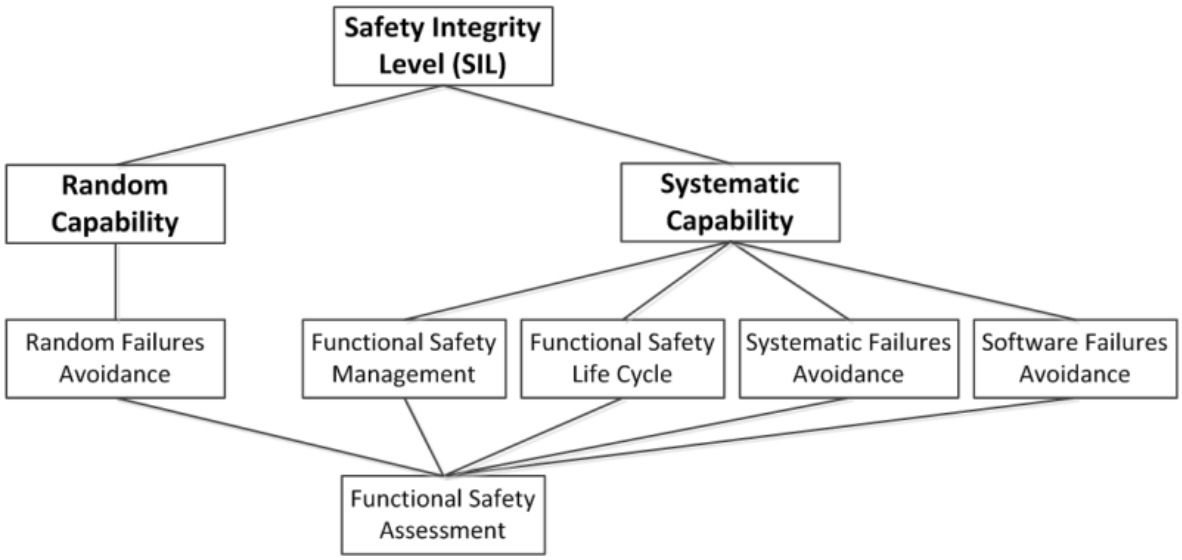

Рисунок 2. Структура требований МЭК 61508

МЭК 61508-1, Общие требования

Первая часть, МЭК 61508-1, задает тон всему стандарту. Некоторая сложность для понимания состоит в том, что эта часть во многом описывает уровень объекта контроля и управления, не очень привычный для IT-специалистов. Здесь подход даже шире, чем уровень АСУ ТП, и гораздо шире, чем уровень контроллера и софта. Что с этим делать? Выбирать только те требования,

которые относятся непосредственно к разрабатываемой или оцениваемой системе.

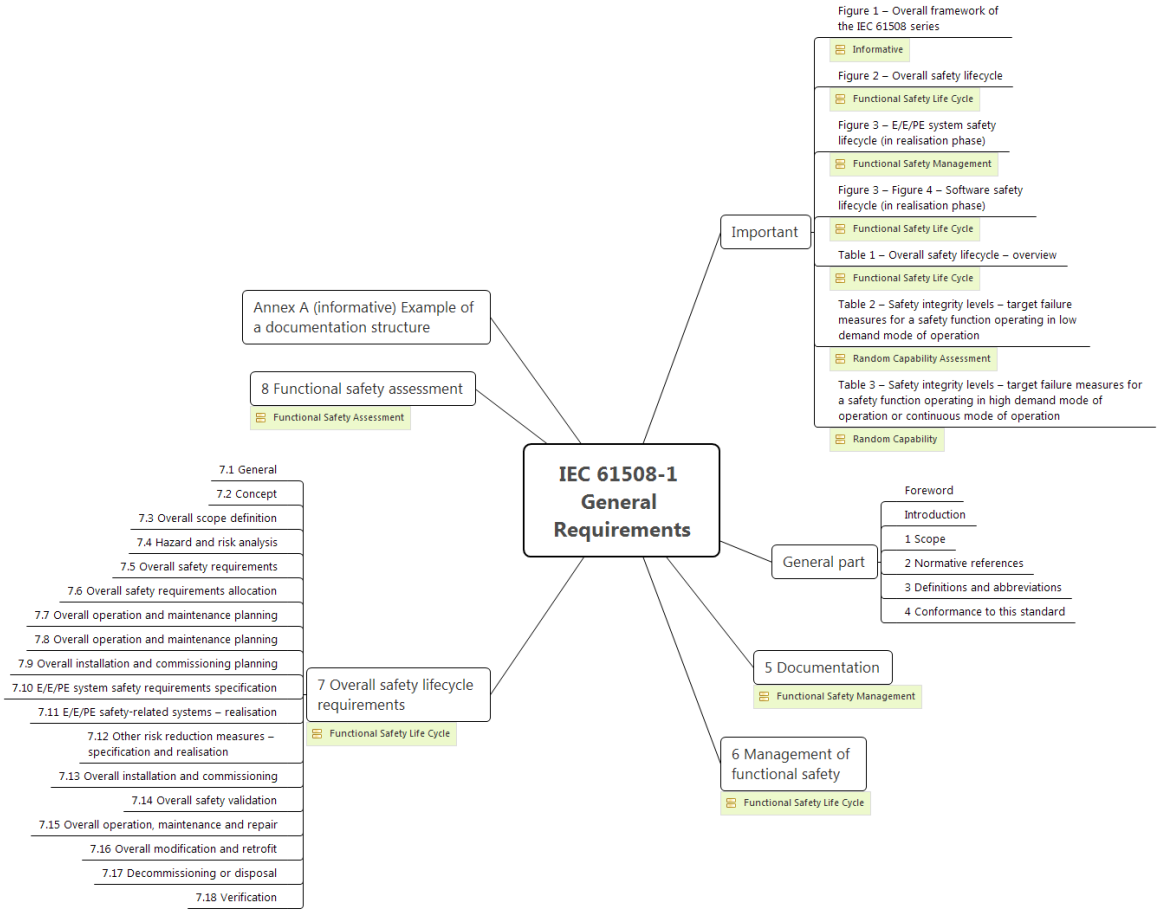

Рисунок 3. Содержание МЭК 61508-1

Здесь и далее на Mind Map разделы и приложения размечены снизу ярлыками, которые указывают на то, какой группе требований соответствует тот или иной раздел или приложение. Кроме того, на Mind Map создана ветвь Important, подчеркивающая важные таблицы и рисунки, которые без этого «теряются» в тексте стандарта.

Требования к документации (раздел 5) отнесем к группе Functional Safety Management. МЭК 61508-1 содержит еще и приложение А, относящееся к документации, но оно, на мой взгляд, не особенно полезно. Рекомендуемую структуру документации (исходя из опыта сертификации) рассмотрим в последующих публикациях. Структура документов во многом определяет и структуру

жизненного цикла, а он у нас, как и для всех приложений, связанных с безопасностью – V-образный.

МЭК 61508-2, Требования к системам

Вторая часть, МЭК 61508-2, как следует из названия, относится к управляющей системе. Как было определено во вводной публикации по функциональной безопасности, мы рассматриваем три типа архитектур управляющих систем: встроенные системы (Embedded Systems), АСУ ТП на базе ПЛК (Industrial Control Systems) и Device Layer интернета вещей. Важно отметить, что, кроме системных требований, МЭК 61508-2 определяет также требования к аппаратной (hardware) составляющей систем. Разделы 5, 6 и 8 содержат лишь ссылки на МЭК 61508-1.

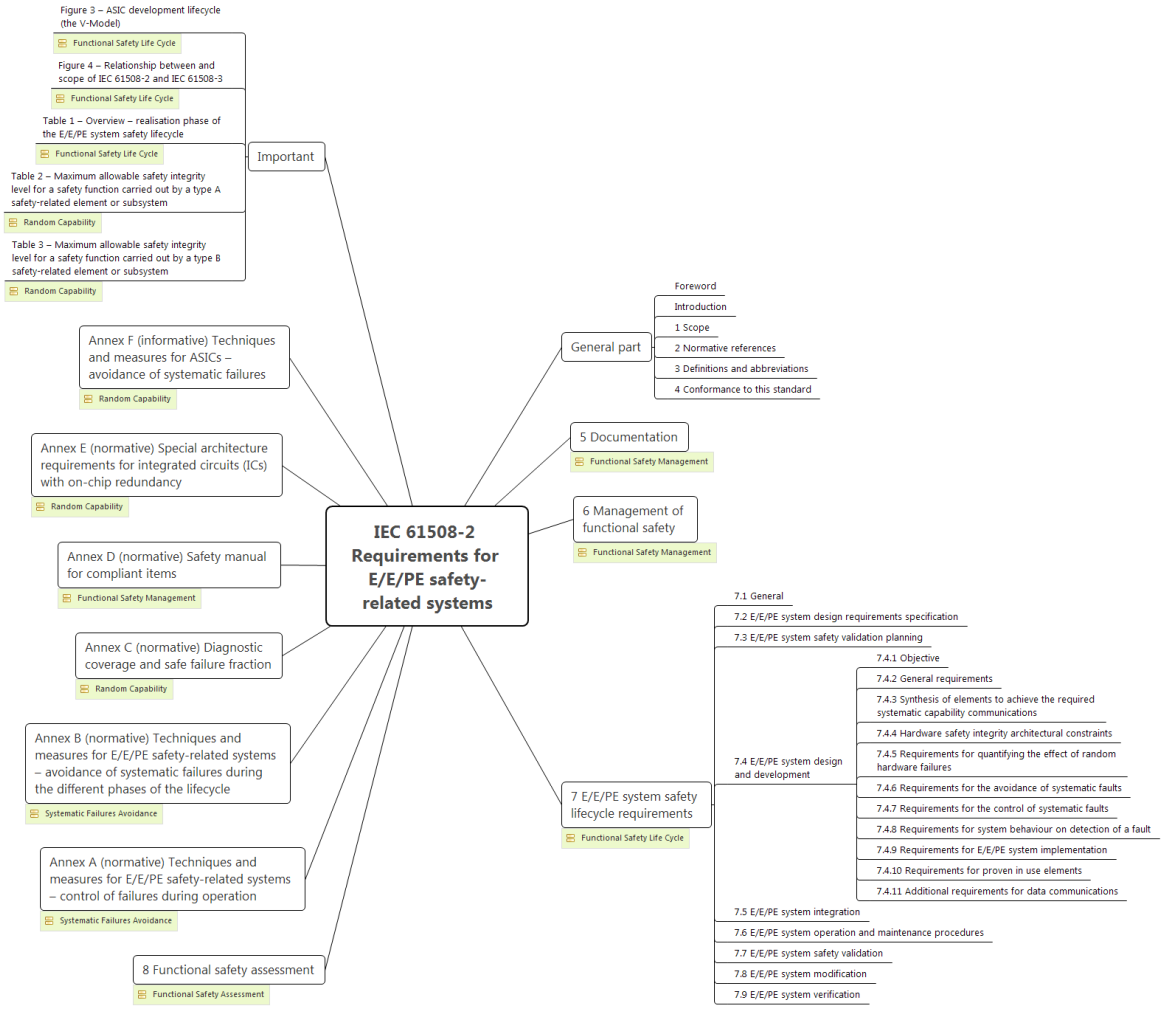

Рисунок 4. Содержание МЭК 61508-2

В составе МЭК 61508-2 мы найдем ряд важных приложений, которые носят нормативный, т.е. обязательный к выполнению характер:

— в приложении A предложен подход к реализации самодиагностики, а также к защите от систематических отказов;

— в приложении B меры защиты от систематических отказов дополнены требованиями к их реализации на различных этапах жизненного цикла системы;

— в приложении C показано, как рассчитывать диагностическое покрытие в целях обеспечения того или иного уровня полноты безопасности (SIL);

— в приложении D сформулированы требования к содержанию руководства по эксплуатации, которое с учетом требований к безопасности носит название Safety Manual;

— в приложение E описаны подходы к внутрикристальному резервированию при реализации управляющих функций с использованием интегральных схем;

— приложение F формально является информативным, т.е. как бы необязательным к выполнению, но, тем не менее, де-факто его надо рассматривать, если в системах применяются заказные интегральные схемы (ASIC) или программируемые логические интегральные схемы (FPGA & CPLD).

МЭК 61508-3, Требования к программному обеспечению

Третья часть, МЭК 61508-3, определяет требования к программному обеспечению, которое может быть, как компонентом системы, так и отдельным объектом оценивания и сертификации.

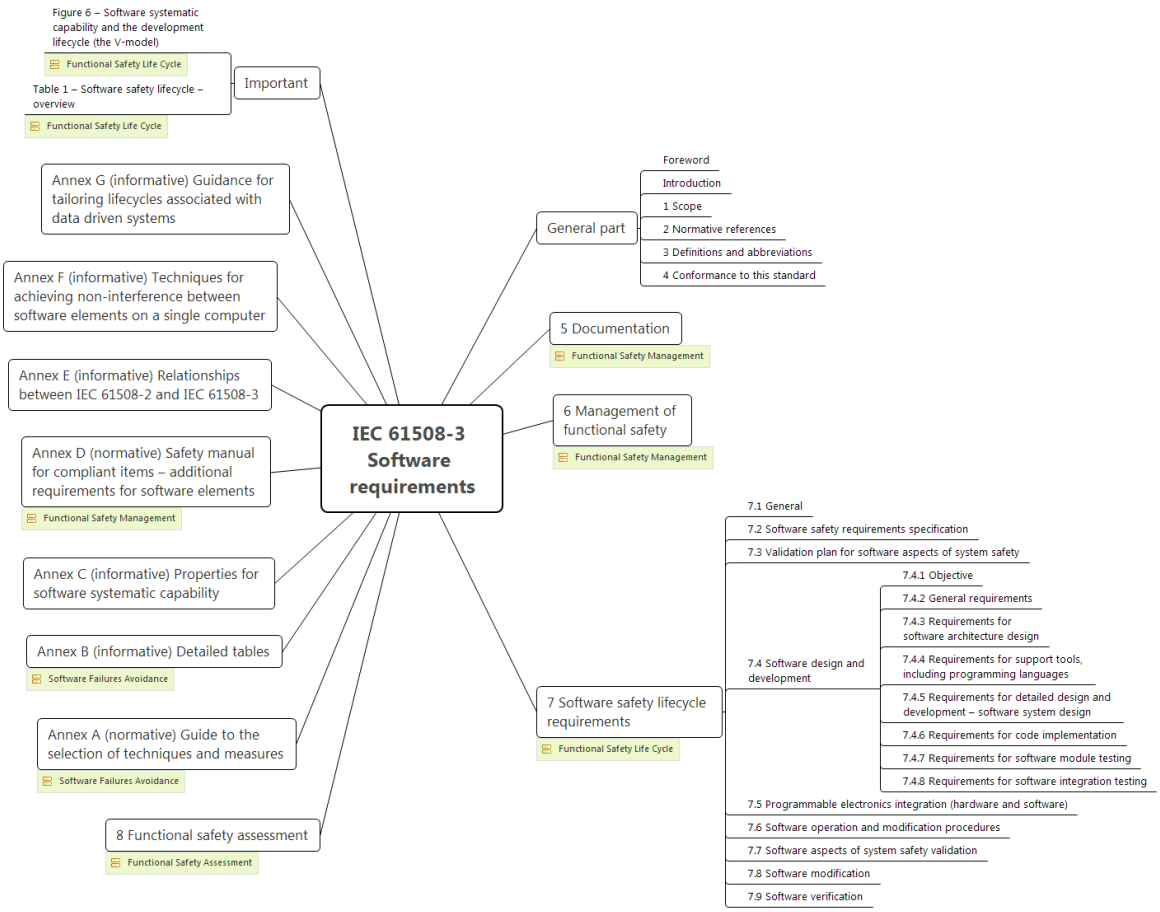

Рисунок 5. Содержание МЭК 61508-3

Разделы 5, 6 и 8 традиционно ссылаются на МЭК 61508 1, но есть небольшие дополнения, учитывающие особенности программного обеспечения.

Из приложений важны A и B, содержащие требования к защите от отказов программного обеспечения. В приложении D содержатся требования к руководству по эксплуатации (Safety Manual) в части особенностей ПО.

МЭК 61508-4, Термины и определения

МЭК 61508-4 содержит структурированный перечень используемых терминов, что подробно рассмотрено в лекции 2 публикации.

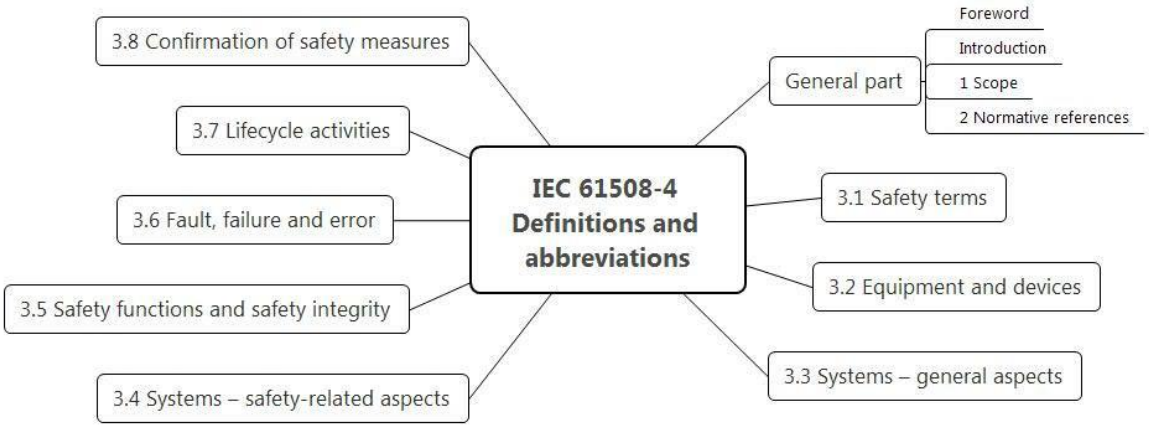

Рисунок 6. Содержание МЭК 61508-4

МЭК 61508-5, Рекомендации по применению методов определения уровней полноты безопасности

МЭК 61508-5 приводит достаточно абстрактные примеры того, как определять уровень полноты безопасности (safety integrity level, SIL). Я бы рассматривал эту часть просто, как иллюстративный материал для изучения, тем более, что, когда мы получаем исходные данные для разработки системы или ПО, то уровень полноты безопасности (SIL), как правило, там уже задан.

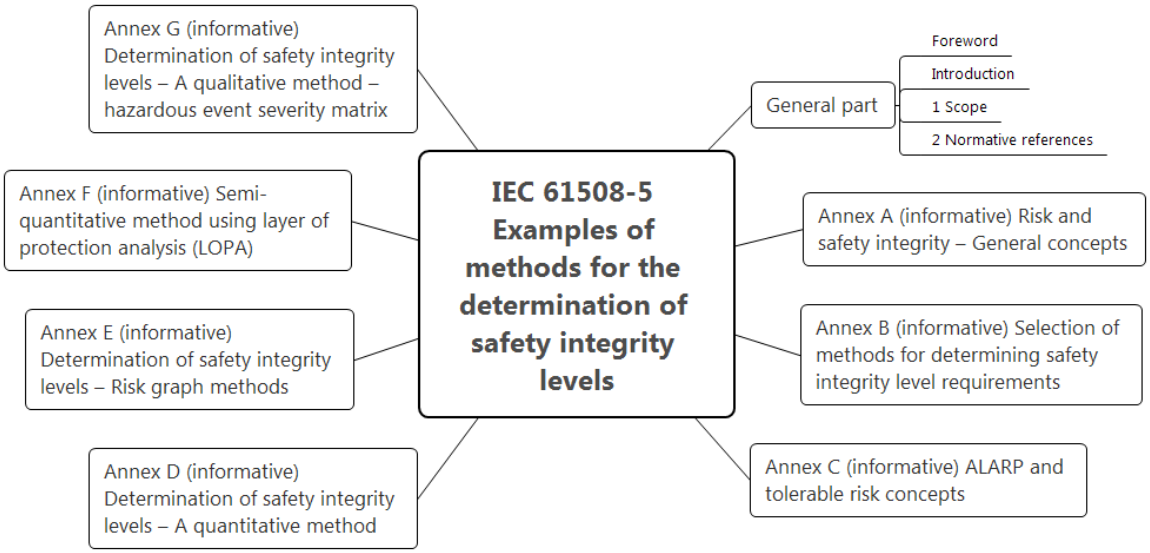

Рисунок 7. Содержание МЭК 61508-5

МЭК 61508-6, Руководство по применению МЭК 61508-2 и МЭК 61508-3

МЭК 61508-6 громко заявляет о том, что он содержит руководство по применению частей 2 и 3 МЭК 61508, т.е. требований к системе, аппаратному и программному обеспечению. На самом деле, в приложении А содержится достаточно тривиальное описание этапов выполнения проекта (на уровне «разработайте требования», «спланируйте работу» и т.д.). Что действительно представляет интерес, так это подробные примеры расчета показателей надежности и безопасности (приложения B, C, D), а также пример того, как внедрять методы обеспечения полноты безопасности (safety integrity) для программного обеспечения (приложение E). Последнее иллюстрирует применение приложений A и B из МЭК 61508-3.

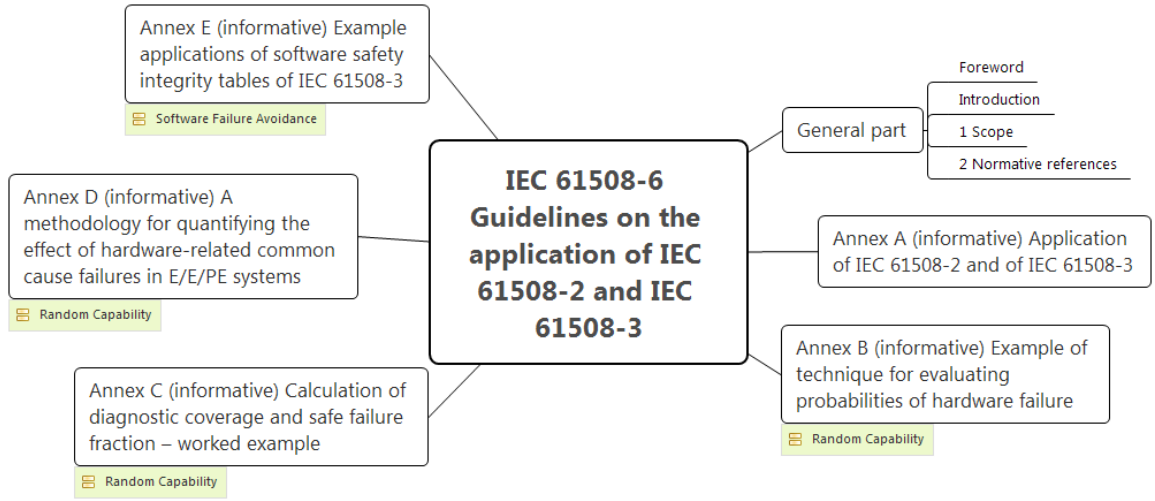

Рисунок 8. Содержание МЭК 61508-6

МЭК 61508-7, Методы и средства

МЭК 61508-7 содержит перечень методов защиты от случайных отказов аппаратных средств и от систематических ошибок проектирования (как системы и аппаратных средств, так и программного обеспечения). Похоже, что авторы стандарта постарались опубликовать все, что они когда-либо слышали об этих методах. Поэтому, там много теоретических вещей, которые вряд ли могут быть эффективно применены на практике. Тем не

менее, применение основных подходов в части диагностирования, тестирования, организации управления проектом и т.п. является обязательными нормативными требованиями. Таким образом, изучать МЭК 61508-7 следует на основе МЭК 61508-2 и МЭК 61508-3, где как раз и описан прагматичный подход к внедрению защиты от отказов и ошибок.

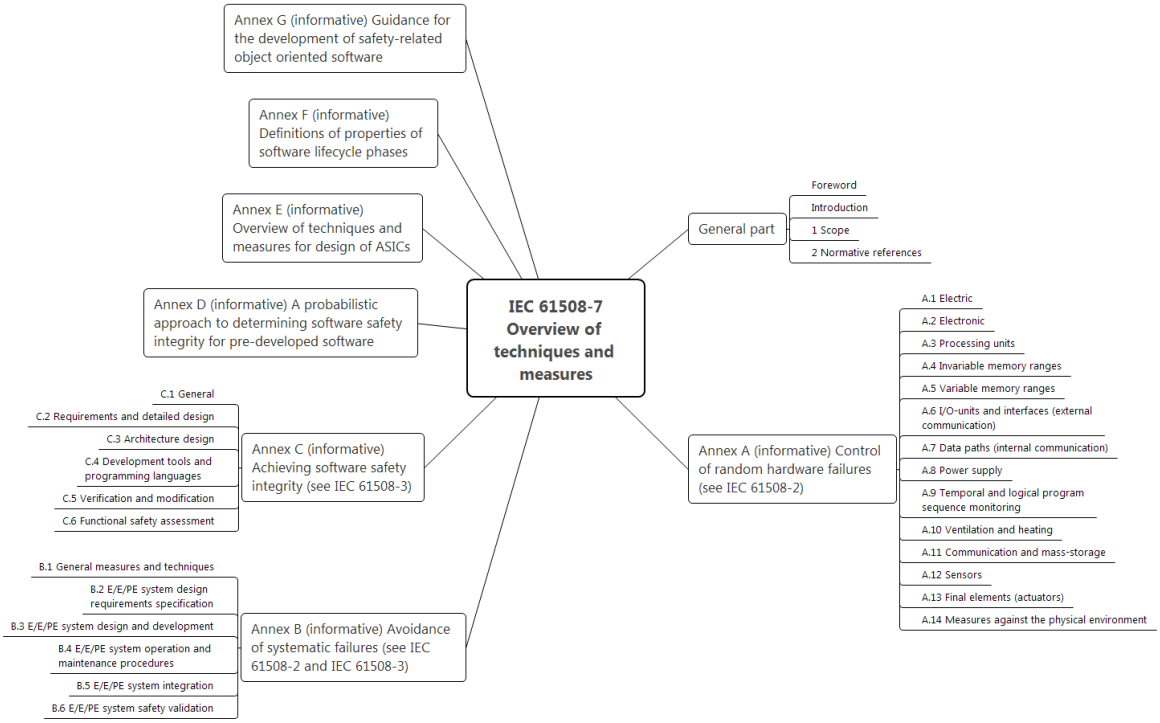

Рисунок 9. Содержание МЭК 61508-7

Выводы

Рассмотрение МЭК 61508 на основе классификации и структурирования требований позволило разложить «по полочкам» этот серьезный документ из семи частей и 700 страниц.

Классификационные признаки требований позволяют выделить аспекты функциональной безопасности, которые надо будет рассмотреть для полноты картины в планируемом цикле статей, а именно:

— управление функциональной безопасностью (Functional Safety Management) и оценивание функциональной безопасности (Functional Safety Assessment);

— реализацию жизненного цикла функциональной безопасности (Functional Safety Life Cycle), включая тестирование;

— оценивание вероятности случайных отказов и обеспечение защиты от таких отказов (Random Capability) через призму теории надежности и безопасности;

— методы защиты от систематических отказов проектирования системы и аппаратных средств (Systematic Failures Avoidance) и от систематических отказов проектирования программного обеспечения (Software Failures Avoidance).

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

Материал взят с сайта Хабрахабр