СИСТЕМА ЭКСПЕРТ

от риска к безопасности

«Сравнительный анализ стандартов функциональной безопасности различных сфер деятельности:

- промышленные процессы,
- дорожные транспортные средства,
- железнодорожный транспорт,
- машины и механизмы»

В докладе выполнен анализ идентичных и отличающихся требований стандартов МЭК 61508, МЭК 61511, ИСО 26262, EN 50126...50129 и МЭК 62061 как с точки зрения сертификации компонентов, так и для выполнения прикладных проектов.

ООО «Система Эксперт» - независимая консалтинговая и инженерная компания

Основными видами деятельности являются работы в области **анализа рисков и функциональной безопасности:**

- Проведение сессий HAZOP / АОР
- Проведение сессий LOPA / АСЗ
- Расчет и анализ достигнутого SIL / УПБ систем ПАЗ
- Разработка спецификаций СТБ/SRS
- Разработка каталогов и мат.обеспечения СДКПБ
- Проведение обучающих семинаров по HAZOP и функциональной безопасности
- Консалтинг по системам ПАЗ

Эксперты обладают 20-летним опыта проектов в нефтепереработке,

газопереработке, химии, газодобычи, а так же в ЖД-транспорте и автомобильной индустрии

Рассматриваемые стандарты ФБ и их область распространения

СИСТЕМА ЭКСПЕРТ

ГОСТ Р МЭК 61508-1..7-2012 IEC 61508:2016	Функциональная безопасность **систем электрических, электронных, программируемых электронных**, связанных с безопасностью	Э/Э/ПЭ системы, выполняющее функции безопасности
ГОСТ Р МЭК 61511-1..3-2018 IEC 61511:2010	Безопасность функциональная. Системы безопасности приборные для **промышленных процессов**	Приборные системы безопасности, применяемые в промышленных процессах химических, нефтепереработывающих, нефтегазодобывающих, целлюлозно-бумажных производств, неядерной энергетики
ISO 26262-1:2018 ГОСТ Р ИСО 26262-1...10-2021*	**Дорожные транспортные средства**. Функциональная безопасность .	Э/Э системы связанные с безопасностью в серийно производимых дорожных транспортных средствах
CENELEC: EN 50126 (IEC 62278:2002) 1..4, ГОСТ Р МЭК 62278 - проект EN 50128 (IEC 62279:2015) ГОСТ Р МЭК 62279-2016 EN 5012 (IEC 62425:2024) ГОСТ Р МЭК 62280-2017	**Железные дороги.** -Определение и подтверждение надежности, эксплуатационной готовности, ремонтопригодности и безопасности (RAMS) на железных дорогах ч.1 – Basic, ч.2 – Safety Guide, ч.3 – Rolling Stock Guide -Системы связи, сигнализации и обработки данных. Программное обеспечение систем управления и защиты на ЖД. -Системы связи, сигнализации и обработки данных. Требования к обеспечению безопасной передачи информации.	- На железнодорожный транспорт в целом и относится к показателям RAMS - электронные системы управления и обеспечения безопасности (сигнализации. Подвижной состав – см. EN 50655, EN 50657)
IEC 62061:2021 ГОСТ Р МЭК 62061-2015 ISO 13849-1:2023 ГОСТ ISO 13849-1—2014	**Безопасность оборудования**. Функциональная безопасность систем управления Э/Э/ПЭ, связанных с безопасностью. **Безопасность оборудования.** Элементы систем управления связанные с ФБ Общие принципы конструирования	Э/Э/ПЭ системы выполняющие связанные с безопасностью функции управления (СБЭСУ), используемые в стационарно установленных промышленных машинах и механизмах

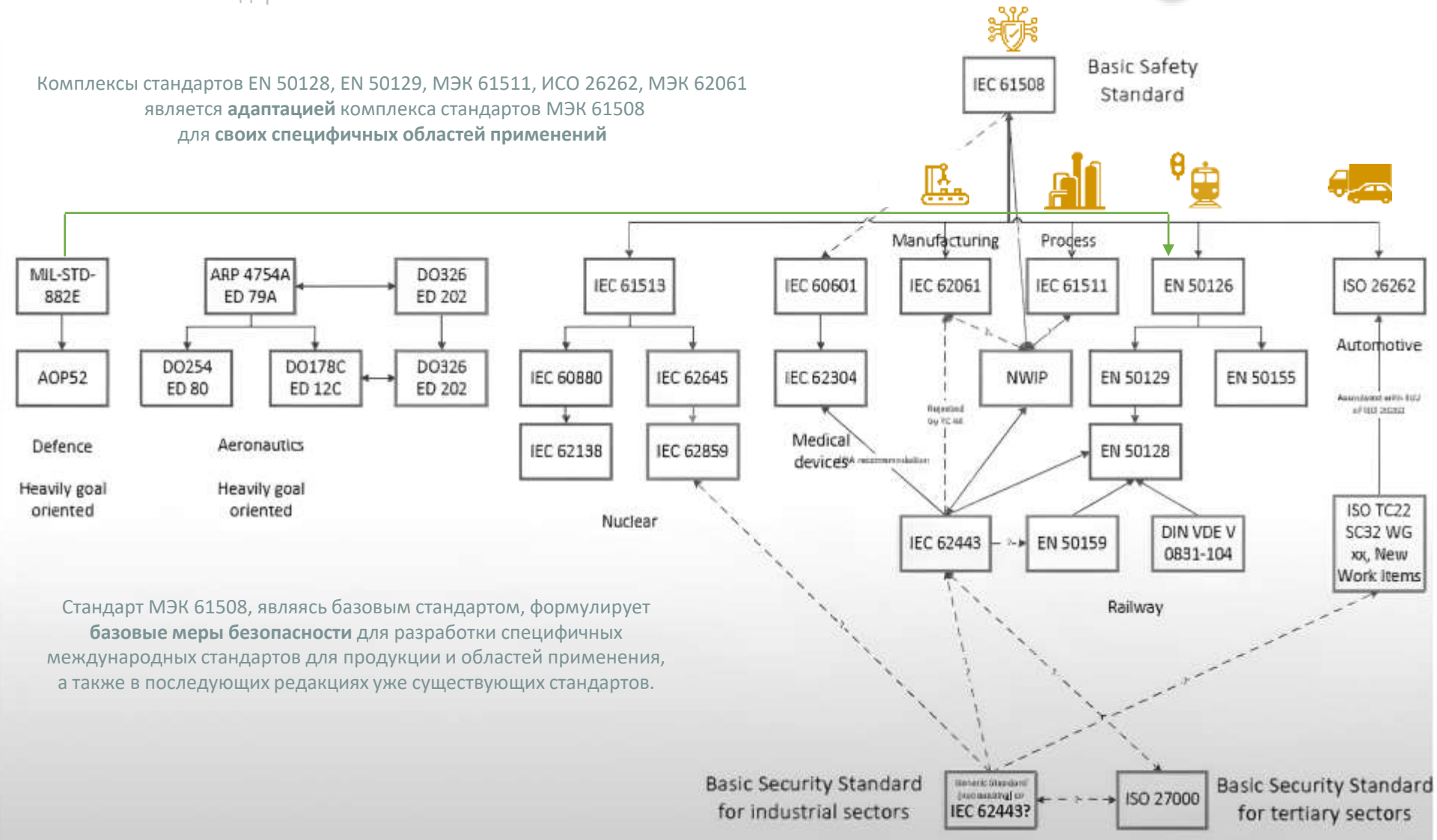
Приблизительное междоменное отображение уровней SIL





ч$^{-1}$	МЭК 61508	МЭК 61511	EN 5012x	ИСО 26262	МЭК 62061	ISO 13849
< 10^{-4}	SIL -	SIL -	SIL -	QM	SIL -	PL a
< $3 \cdot 10^{-4}$	SIL 1	SIL 1	SIL 1	ASIL A	SIL 1	PL b
< 10^{-5}						
< $3 \cdot 10^{-6}$	SIL 2	SIL 2	SIL 2	ASIL B	SIL 2	PL c
< 10^{-6}						PL d
< 10^{-7}	SIL 3	SIL 3	SIL 3	ASIL B	SIL 3	PL e
< 10^{-7}				ASIL C		
< 10^{-8}	SIL 4	-	SIL 4	ASIL D	-	-

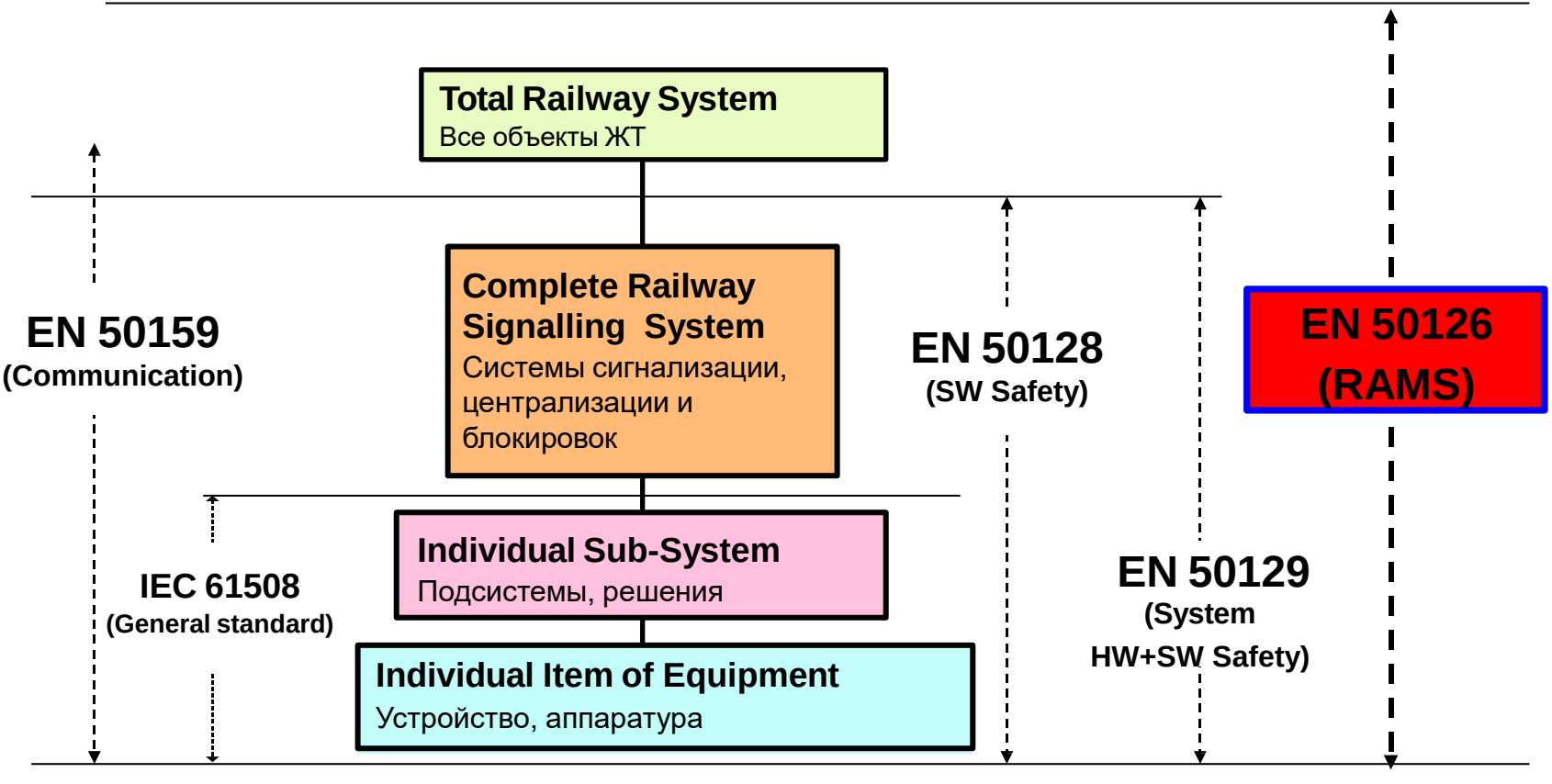
Комплексы стандартов EN 50128, EN 50129, МЭК 61511, ИСО 26262, МЭК 62061 является **адаптацией** комплекса стандартов МЭК 61508 для **своих специфичных областей применений**



Стандарт МЭК 61508, являясь базовым стандартом, формулирует **базовые меры безопасности** для разработки специфичных международных стандартов для продукции и областей применения, а также в последующих редакциях уже существующих стандартов.

ЖЕЛЕЗНЫЕ ДОРОГИ
EN 5012X

Диапазоны стандартов CENELEC



Термин **RAMS :**

Reliability – Безотказность,
Availability – Готовность,
Maintainability – Ремонтопригодность,
Safety – **Безопасность**

} Надежность (RAM+S)

был введен в комплексе стандартов, выпущенном Европейским комитетом электротехнической стандартизации CENELEC во второй половине 90-х годов прошлого века и предназначенных для применения на железных дорогах.

Фактически данная аббревиатура подразумевает сочетание перечисленных показателей, рассматриваемое в контексте методологии их обеспечения.

EN 50126-1

- **требует установить** (специфицировать) и подтвердить RAMS
- **не определяет** правила или процессы, относящиеся к сертификации железнодорожной продукции

Жизненный цикл RAMS

1. Концепция
2. Определение системы и условий применения
3. Анализ риска
4. Требования к системе
5. Пропорциональное распределение требований к системе
6. Проектирование и реализация
7. Производство
8. Установка
9. Валидация системы (включая аттестацию безопасности – safety acceptance, и ввод в эксплуатацию)
10. Приемка системы Acceptance
11. Эксплуатация и техническое обслуживание
12. Выполнение мониторинга
13. Модификация и переоборудование
14. Вывод из эксплуатации и утилизация

Повторный анализ риска (Анализ риска может быть повторен на нескольких этапах жизненного цикла)

- «Отчет оценки и приемлемости риска»
- «Журнал опасностей»
- «Программа RAM»
- «План безопасности»

* Журнал, программы, планы могут обновляться на каждом этапе

- «План аттестации/приемки» - критерии приемки
- «План валидации» - критерии валидации
- «План спецификации RAMS»

- Подготовка доказательства безопасности общего характера (Safety Case for Generic Product/Application)

- Сдача в эксплуатацию
- Испытательный период эксплуатации
- Обучение
- Верификация RAM
- Подготовка доказательства безопасности прикладной системы

* 9 и10 могут быть объединены

- Осуществление процедуры аттестации/приемки (Acceptance) на основании критериев приемки
- Оценка подтверждения RAM
- Оценка доказательства безопасности прикладной системы
- Ввод в эксплуатацию
- Продолжение испытательного периода эксплуатации (если необходимо)

Повторный жизненный цикл

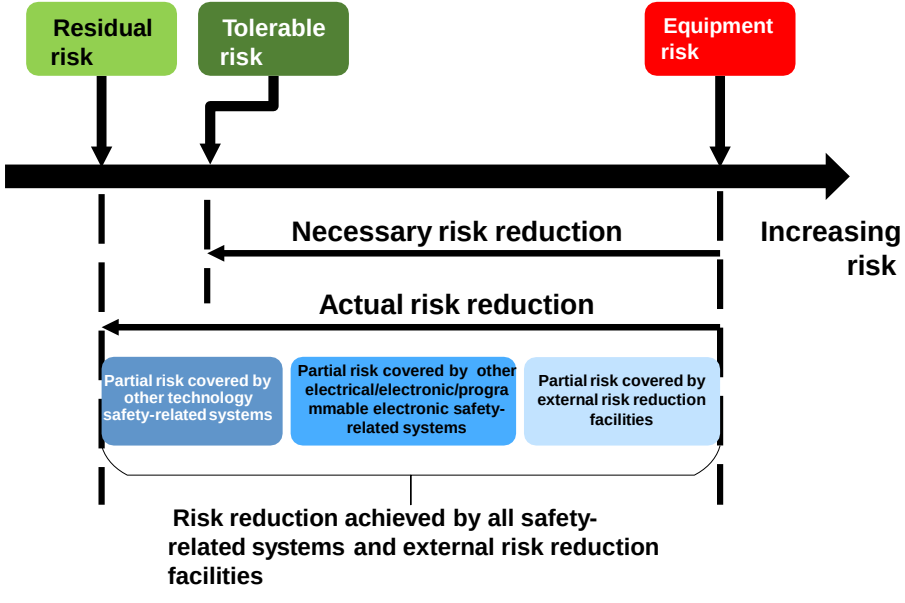
FRACAS
(Failure Reporting Analysis and Corrective Action System) – система создания отчетов об отказах и корректирующих воздействий;

- Сбор статистических данных по эксплуатационным показателям
- Получение, анализ и оценка данных

Принципы допустимого риска

GAMAB («Globalement Au Moins Aussi Bon» principle (practised in France) – («В целом, по крайней мере, такой же» принцип практикуется во Франции). Полная формулировка этого принципа: «Все новые управляемые транспортные системы должны, в целом, иметь степень риска, по крайней мере, такую же, что и равнозначная существующая система».

MEM («Minimum Endogenous Mortality» (MEM) principle (practised in Germany) – принцип не превышения уровня в 1/20 от минимальной эндогенной смертности.



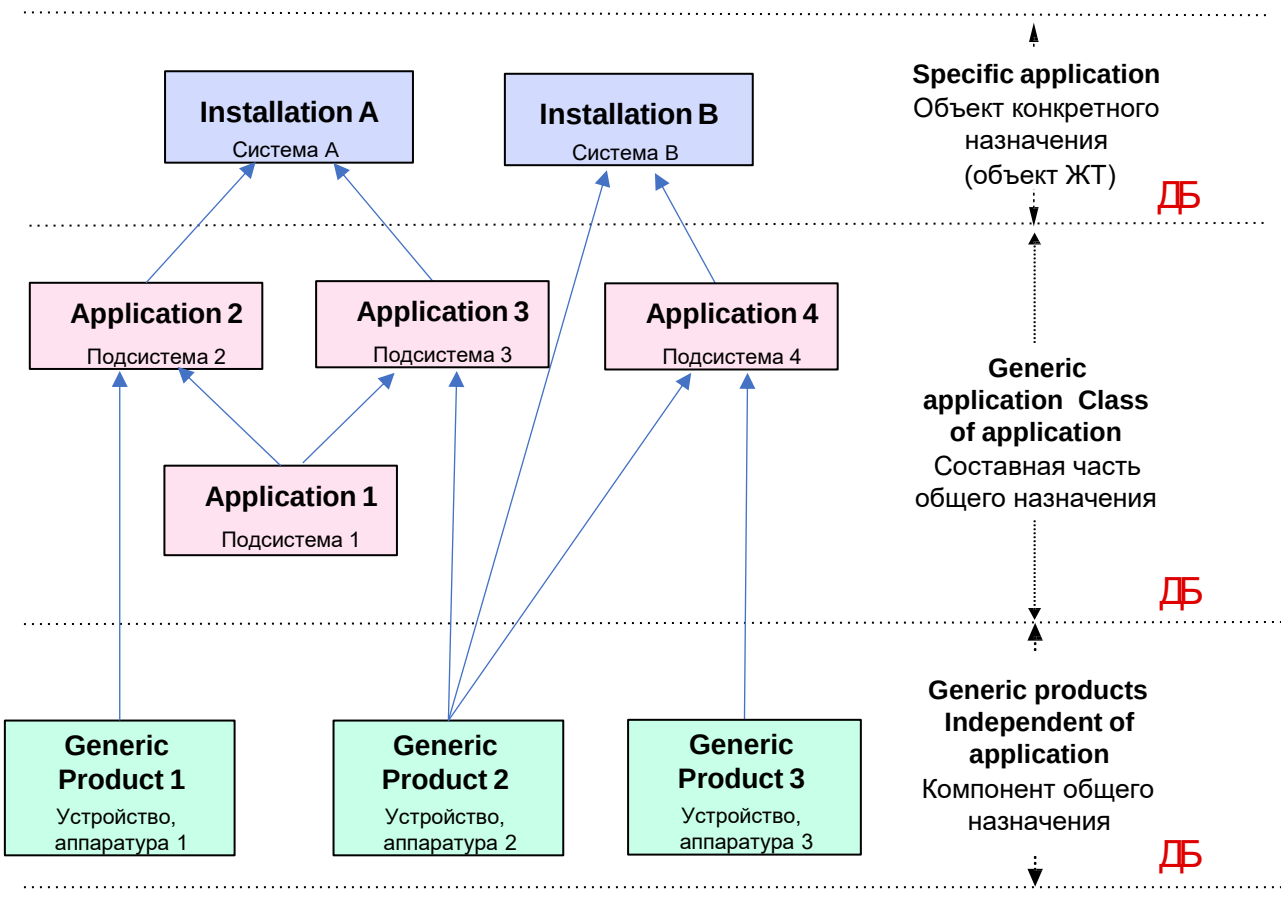
Приложение Е (справочное)
Распределение ответственности за RAMS на протяжении жизненного цикла

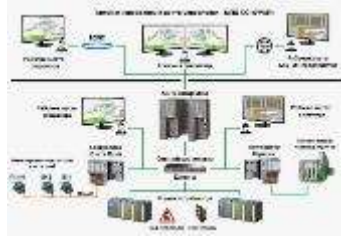
3.26 **административный орган железной дороги** (Railway Authority): Орган, несущий полную ответственность перед распорядительным органом за эксплуатацию железнодорожной системы *(владелец, оператор).*

3.40 **регулирующий орган по безопасности** (Safety regulatory authority): Обычно это национальный правительственный орган, занимающийся установлением или согласованием требований по безопасности для железных дорог и обеспечением соблюдения данных требований на железных дорогах.

	Потребитель/ эксплуатаци-онник	Утверждающий орган /Approval Authority	(Главный) подрядчик	Субподрядчик	Поставщики
Концепция	X				
Описание системы и условия применения	X				
Анализ риска	X		X		
Требования к системе	X	(X)			
Пропорциональное распределение требований к системе	(X)		X		
Проектирование и реализация			X	(X)	
Изготовление			X	(X)	
Установка			X	X	X
Валидация системы	X	X	X	(X)	
Приемка системы (acceptance/аттестация)	X	X			
Эксплуатация и техническое обслуживание	X		(X)	(X)	
Мониторинг эффективности	X		(X)	(X)	
Модификация и модернизация	X		X	X	
Вывод из эксплуатация и ликвидация	X		(X)		

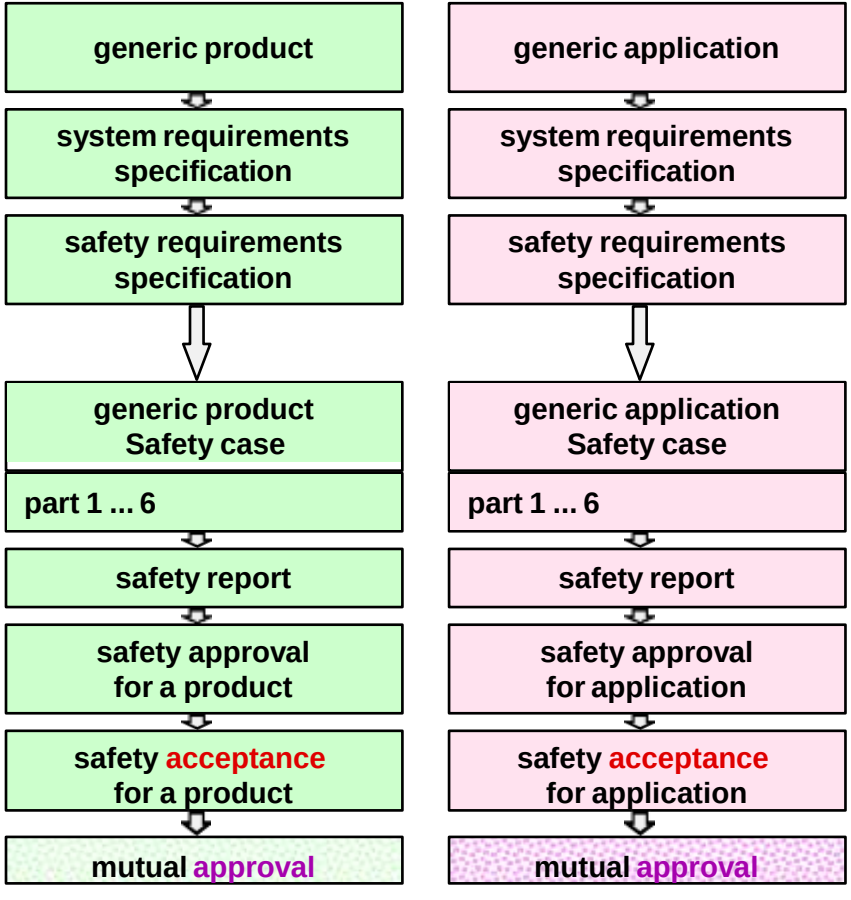
Зависимости ДБ объектов ЖТ и их составных частей (пример)

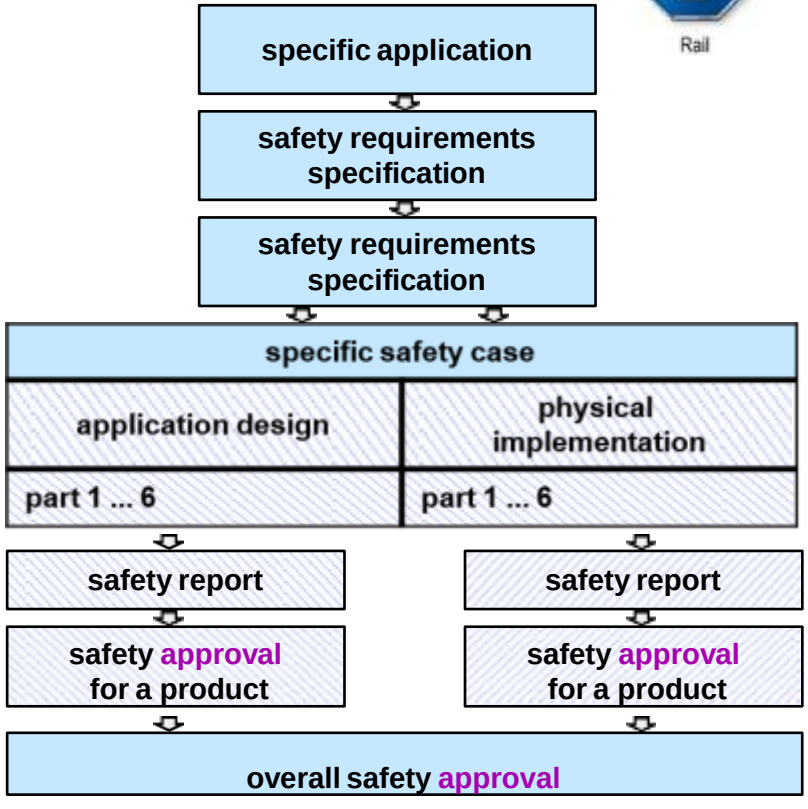




Safety Acceptance and Approval

Rail





Структура доказательства безопасности

- Заключение
- Доказательства безопасности составных частей
- Отчет о состоянии функциональной безопасности
- Отчет о мерах по управлению функциональной безопасностью
- Отчет о мерах по управлению качеством
- Характеристика объекта ЖТ

- Распоряжение ОАО "РЖД" от 8 декабря 2015 г. N 2855р "Об утверждении Стратегии обеспечения гарантированной безопасности и надежности перевозочного процесса в холдинге «РЖД»
- ГОСТ 33477-2015 «Система разработки и постановки продукции на производство. Технические средства железнодорожной инфраструктуры. Порядок разработки, постановки на производство и допуска к применению»

Пример жизненного цикла разработки ПО

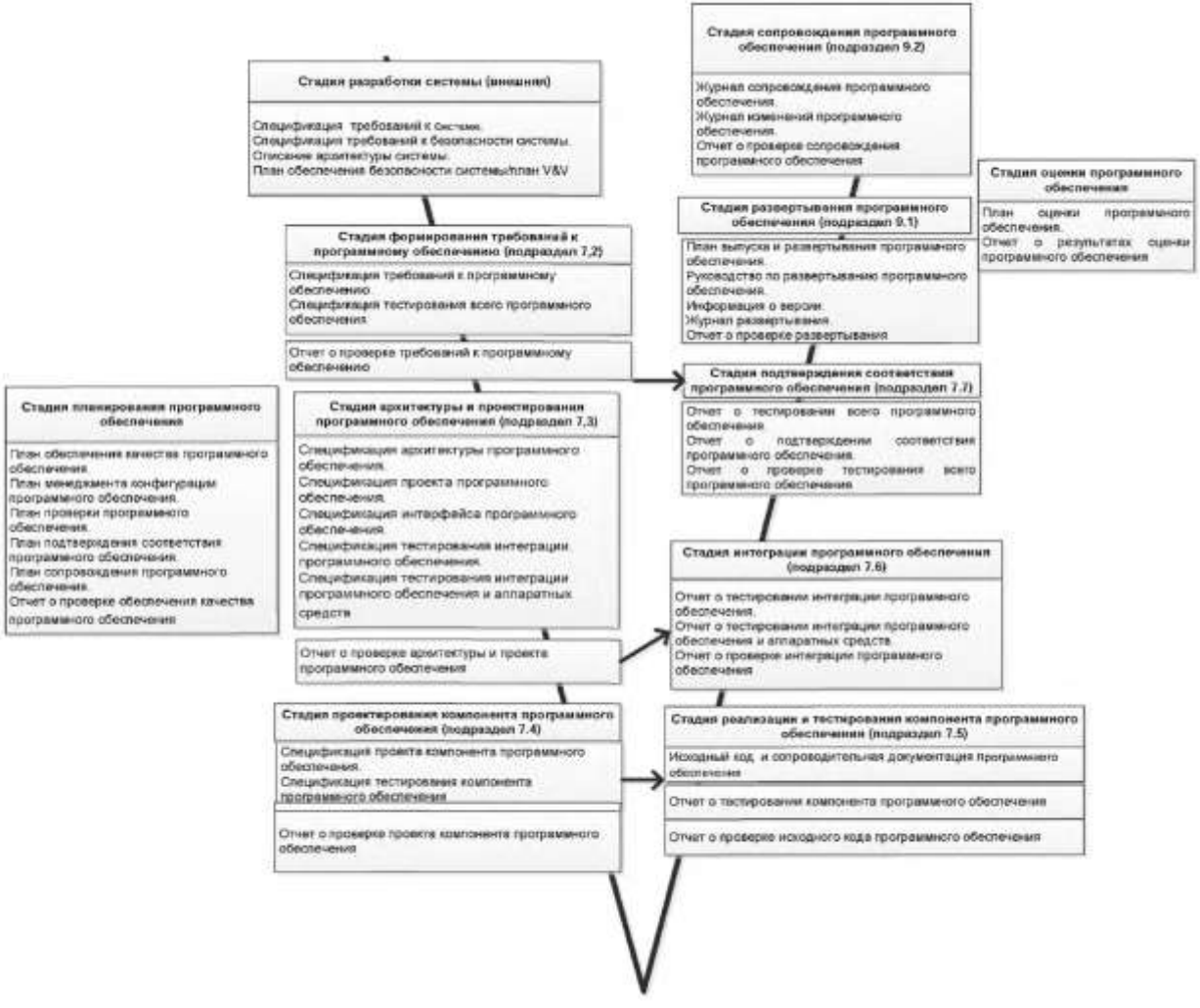
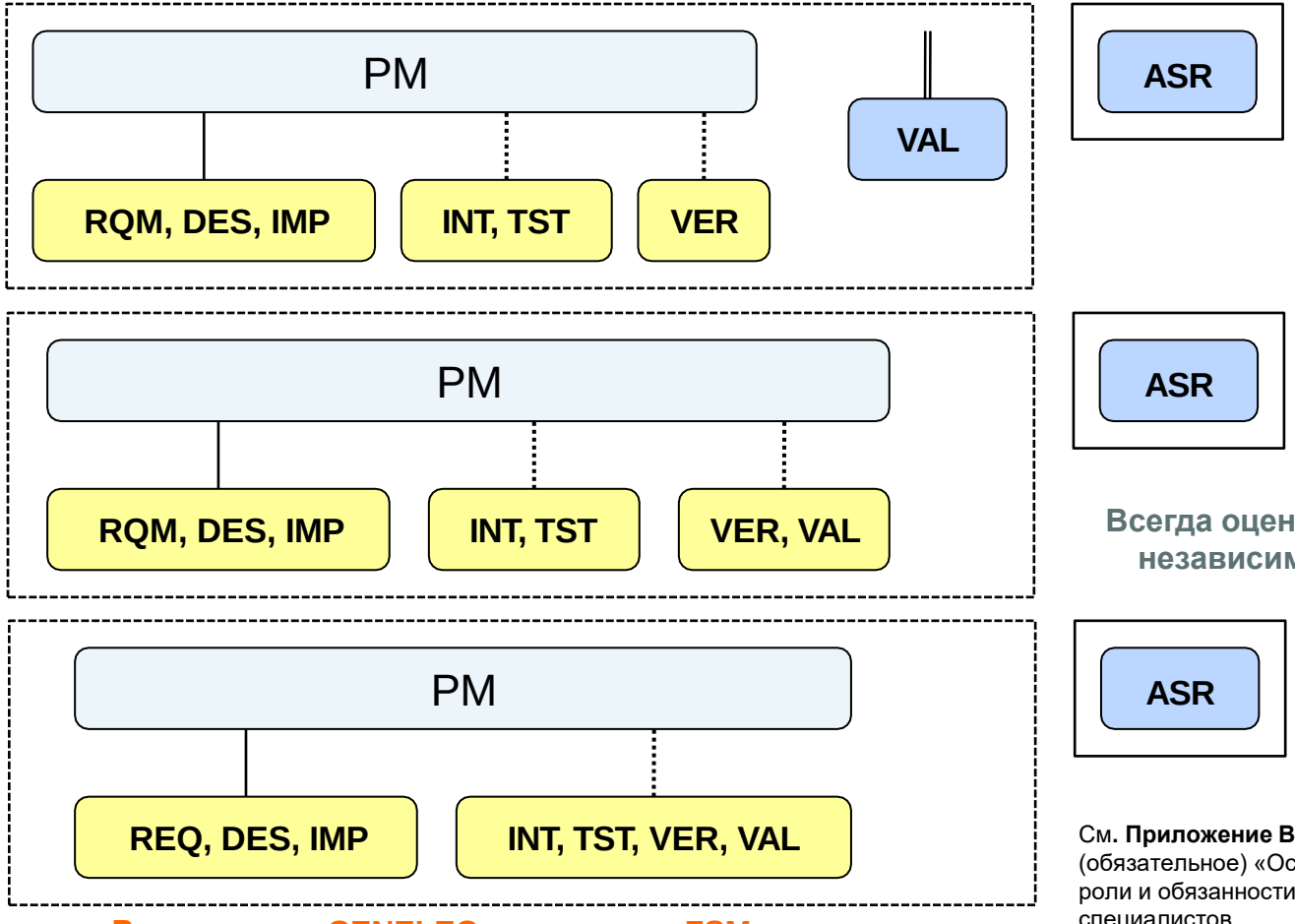


Иллюстрация предпочтительной организационной структуры для ПО



Всегда оценщик независим !

В стандартах CENELEC нет понятия FSM как такового – есть требования к ЖЦ, ролям и компетенциям.

См. **Приложение В** (обязательное) «Основные роли и обязанности специалистов в области программного обеспечения»

Accessor - оценщик

См. **Приложение В** (обязательное)
«Основные роли и обязанности специалистов в области программного обеспечения»

ASR

Таблица В.8 — Ролевая спецификация оценщика

Роль. Оценщик
Обязанности: 1) развивает системное понимание программного обеспечения в предполагаемом окружении приложения; • • • 10) выполняет аудиты безопасности и процедуры контроля для всего процесса разработки при необходимости на различных стадиях разработки; 11) высказывает профессиональное мнение о пригодности разработанного программного обеспечения для его надлежащего использования, детализируя любые ограничения, условия применения и соображения по управлению риском при необходимости; 12) разрабатывает отчет по результатам оценки и ведет формуляр процесса оценки.
Основные компетенции. Он должен: 1) быть компетентным в технологиях/предметной области, где выполняется оценка; 2) иметь разрешение/лицензию от признанного уполномоченного органа по безопасности; 3) иметь/стремиться постоянно повышать свой уровень в области реализации принципов обеспечения безопасности и применять эти принципы для приложений данной предметной области; 4) быть компетентным проверить, были ли применены подходящий метод или комбинация методов в данном контексте; 5) быть компетентным в понимании соответствующей безопасности, человеческих ресурсов, технических процессов и процессов управления качеством при выполнении требований настоящего стандарта; 6) быть компетентным в подходах/методологиях оценки; 7) иметь способность к аналитическому мышлению и хорошие навыки наблюдения; 8) быть способным объединять различные источники и типы доказательств и синтезировать общее представление об их пригодности для цели или условий и ограничений приложения; 9) иметь полное понимание и перспективу программного обеспечения, включая понимание окружения приложения; 10) быть в состоянии оценить соответствие всех процессов разработки (таких, как процессы управления качеством, управления конфигурацией, подтверждения соответствия и проверки); 11) понимать требования настоящего стандарта.

Универсальное программное обеспечение (generic software):

На универсальное ПО должны быть представлены документы, перечисленные в таблице А.1 .

Таблица А.1 — Проблемы жизненного цикла и документация (см. 5.3)

Документация	УПБ 0	УПБ 1	УПБ 2	УПБ 3	УПБ 4
Планирование					
1 План обеспечения качества программного обеспечения	HR	HR	HR	HR	HR
2 Отчет о проверке обеспечения качества программного обеспечения	HR	HR	HR	HR	HR
3 План управления конфигурацией программного обеспечения	HR	HR	HR	HR	HR
4 План проверки программного обеспечения	HR	HR	HR	HR	HR
5 План подтверждения соответствия программного обеспечения	HR	HR	HR	HR	HR
Требования к программному обеспечению					
6 Спецификация требований к программному обеспечению	HR	HR	HR	HR	HR
7 Спецификация тестирования всего программного обеспечения	HR	HR	HR	HR	HR
8 Отчет о проверке требований к программному обеспечению	HR	HR	HR	HR	HR
Архитектура и проект программного обеспечения					
9 Спецификация архитектуры программного обеспечения	HR	HR	HR	HR	HR
10 Спецификация проекта программного обеспечения	HR	HR	HR	HR	HR
11 Спецификации интерфейса программного обеспечения	HR	HR	HR	HR	HR
12 Спецификация тестирования интеграции программного обеспечения	HR	HR	HR	HR	HR
13 Спецификация тестирования интеграции программного обеспечения/ аппаратных средств	HR	HR	HR	HR	HR
14 Отчет о проверке архитектуры и проекта программного обеспечения	HR	HR	HR	HR	HR
Проект компонента программного обеспечения					
15 Спецификация проекта компонента программного обеспечения	R	HR	HR	HR	HR
16 Спецификация тестирования компонента программного обеспечения	R	HR	HR	HR	HR
17 Отчет о проверке проекта компонента программного обеспечения	R	HR	HR	HR	HR
Реализация и тестирование компонента					
18 Исходный код программного обеспечения и сопроводительная документация	HR	HR	HR	HR	HR
19 Отчет об испытаниях компонента программного обеспечения	R	HR	HR	HR	HR
20 Отчет о проверке исходного кода программного обеспечения	HR	HR	HR	HR	HR
Интеграция					
21 Отчет об испытаниях интеграции программного обеспечения	HR	HR	HR	HR	HR
22 Отчет об испытаниях интеграции программного обеспечения/аппаратных средств	HR	HR	HR	HR	HR
23 Отчет о проверке интеграции программного обеспечения	HR	HR	HR	HR	HR
Тестирование всего программного обеспечения/ заключительное подтверждение соответствия					
24 Отчет об испытаниях всего программного обеспечения	HR	HR	HR	HR	HR
25 Отчет о проверке испытаний всего программного обеспечения	HR	HR	HR	HR	HR
26 Отчет о подтверждении соответствия программного обеспечения	HR	HR	HR	HR	HR
27 Отчет о подтверждении соответствия инструментальных средств	R	HR	HR	HR	HR
28 Информация о версии	HR	HR	HR	HR	HR
Системы, сконфигурированные прикладными данными или алгоритмами					
29 Спецификация требований к приложению	HR	HR	HR	HR	HR
30 План подготовки приложения (см. примечание 2)	HR	HR	HR	HR	HR
31 Спецификация тестирования приложения (см. примечание 2)	HR	HR	HR	HR	HR
32 Архитектура и проект приложения (см. примечание 2)	HR	HR	HR	HR	HR
33 Отчет о проверке подготовки приложения	HR	HR	HR	HR	HR
34 Отчет об испытаниях приложения	HR	HR	HR	HR	HR
35 Исходный код данных/алгоритмов приложения	HR	HR	HR	HR	HR
36 Отчет о проверке данных/алгоритмов приложения	HR	HR	HR	HR	HR
Развертывание программного обеспечения					
37 План выпуска и развертывания программного обеспечения	R	HR	HR	HR	HR
38 Руководство по развертыванию программного обеспечения	R	HR	HR	HR	HR
39 Информация о версии	HR	HR	HR	HR	HR
40 Журнал развертывания	R	HR	HR	HR	HR
41 Отчет о проверке развертывания	R	HR	HR	HR	HR
Сопровождение программного обеспечения					
42 План сопровождения программного обеспечения	R	HR	HR	HR	HR
43 Журнал изменений программного обеспечения	HR	HR	HR	HR	HR
44 Журнал сопровождения программного обеспечения	R	HR	HR	HR	HR
45 Отчет о проверке сопровождения программного обеспечения	R	HR	HR	HR	HR
Оценка программного обеспечения					
46 План оценки программного обеспечения	R	HR	HR	HR	HR
47 Отчет по результатам оценки программного обеспечения	R	HR	HR	HR	HR

Требования для разработки прикладных алгоритмов совпадают с требованиями для разработки универсального ПО

Критерии выбора методов и мер

IEC 61508

Таблица А.9 — Верификация программного обеспечения (см. 7.9)

Метод/средство[1)]	Ссылка	SIL1	SIL2	SIL3	SIL4
1 Формальная проверка	C.5.13	—	R	R	HR
2 Вероятностное тестирование	C.5.1	—	R	R	HR
3 Статический анализ	B.6.4, таблица B.8	R	HR	HR	HR
4 Динамический анализ и тестирование	B.6.5, таблица B.2	R	HR	HR	HR
5 Метрики сложности программного обеспечения	C.5.14	R	R	R	R
Тестирование и интеграция программных модулей	См. таблицу А.5				
Проверка интеграции программируемых электронных устройств	См. таблицу А.6				
Тестирование программной системы (подтверждение соответствия)	См. таблицу А.7				

EN 50128

Таблица А.5 — Проверка и тестирование (см. 6.2, 7.3, 7.5)

Методы/меры	Ссылка	УПБ 0	УПБ 1	УПБ 2	УПБ 3	УПБ 4
1 Формальное доказательство	D.29	—	R	R	HR	HR
2 Статический анализ	Таблица А.19	—	HR	HR	HR	HR
3 Динамический анализ и тестирование	Таблица А.13	—	HR	HR	HR	HR
4 Метрики	D.37	—	R	R	R	R
5 Прослеживаемость	D.58	R	HR	HR	M	M
6 Анализ влияния ошибок в программном обеспечении	D.25	—	R	R	HR	HR
7 Тестовый охват для кода	Таблица А.21	R	HR	HR	HR	HR
8 Функциональное тестирование или тестирование методом «черного ящика»	Таблица А.14	HR	HR	HR	M	M
9 Тестирование производительности	Таблица А.18	—	HR	HR	HR	HR
10 Тестирование интерфейса	D.34	HR	HR	HR	HR	HR

Отношение между классом инструментальных средств и УПБ изделия:

Класс инструментальных средств	Методология обеспечения достоверности инструментального средства	УПБ разрабатываемого изделия
T2	1 Доказательство **успешного использования** в аналогичном окружении. или 2 Управление библиотекой **тестовых сценариев** с детерминированными результатами для установления функциональной полноты	**1 - 2**
T2 и T3	1 Выполнение **всех требований** настоящего стандарта, подходящих для конкретного УПБ применения к разработке или приобретению инструментального средства. или 2 Управление библиотекой **широко признанных тестовых случаев / наборов тестов** с детерминированными результатами для установления функциональной полноты. или 3 Применение **разнообразных инструментальных средств** к системе и сравнение производительности разрабатываемого изделия, проверка различий	**3 - 4**

Требования к обеспечению безопасной передачи информации

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61784-3— 2015

Промышленные сети

ПРОФИЛИ

Часть 3

Функциональная безопасность полевых шин. Общие правила и определения профилей

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 62280-2017

ЖЕЛЕЗНЫЕ ДОРОГИ

Системы связи, сигнализации и обработки данных. Требования к обеспечению безопасной передачи информации

(IEC 62280-2014, «Railway applications — Communication, signalling and processing systems —

Таблица 1 — Анализ эффективности применения различных мер к возможным ошибкам

Ошибка коммуникации	Меры безопасности							
	Номер последовательности (см. 5.4.2)	Временная метка (см. 5.4.3)	Время ожидания (см. 5.4.4)	Проверка подлинности соединения (см. 5.4.5)	Сообщение обратной связи (см. 5.4.6)	Обеспечение полноты данных (см. 5.4.7)	Избыточность с перекрестной проверкой (см. 5.4.8)	Различные системы обеспечения полноты данных (см. 5.4.9)
Искажение (см. 5.3.2)					x[d]	x	Только для последовательной шины[c]	
Непреднамеренный повтор (см. 5.3.3)	x	x					x	
Ошибочная последовательность (см. 5.3.4)	x	x					x	
Потеря (см. 5.3.5)	x				x		x	
Недопустимая задержка (см. 5.3.6)		x	x[b]					
Появление неизвестного сообщения (см. 5.3.7)	x			x[a]	x		x	
Подмена (см. 5.3.8)				x	x			x
Адресация (см. 5.3.9)				x				

Примечание — Таблица заимствована из МЭК 62280-2 [19] и [28].

[a] Только для идентификации отправителя. Обнаруживает только появление неверного источника.
[b] Необходимо для всех случаев.
[c] Данная мера сопоставима с механизмом обеспечения высокого качества данных, только если вычисление может показать, что частота появления остаточных ошибок Λ достигла значения, требующегося в 5.4.9, когда два сообщения посылаются через независимые передатчики.
[d] Эффективно, только если сообщение обратной связи содержит начальные данные или информацию о начальных данных.

Дорожные транспортные средства ISO 26262

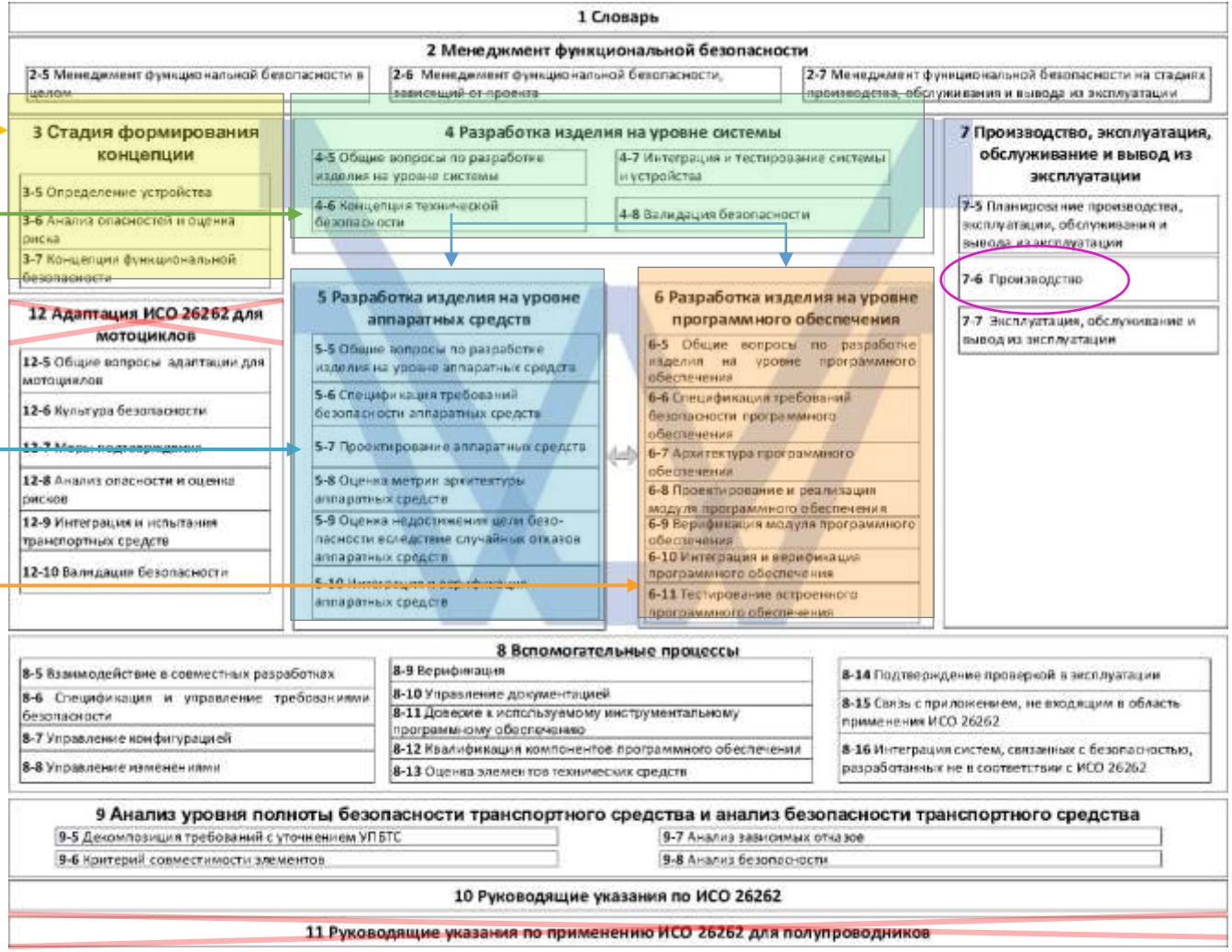
Общая структура ИСО 26262

Концепция

Уровень системы

Разработка HW

Разработка SW



Требования стандарта в части FSM

a) установить и поддерживать **культуру безопасности**, которая обеспечивает и содействует эффективному достижению функциональной безопасности;

b) установить и поддерживать систему **управления компетентностью**;

c) установить и поддерживать систему **менеджмента качества** для обеспечения функциональной безопасности.

Менеджмент функциональной безопасности в целом

a) определить и назначить **роли и ответственности**, связанные с действиями по обеспечению безопасности;

b) выполнить анализ влияния (новое, модификация, или другое применение) и определить действия по корректировке системы безопасности с целью обеспечения **соответствующих обоснований** и выполнения анализа полученного обоснования;

c) запланировать действия по обеспечению безопасности;

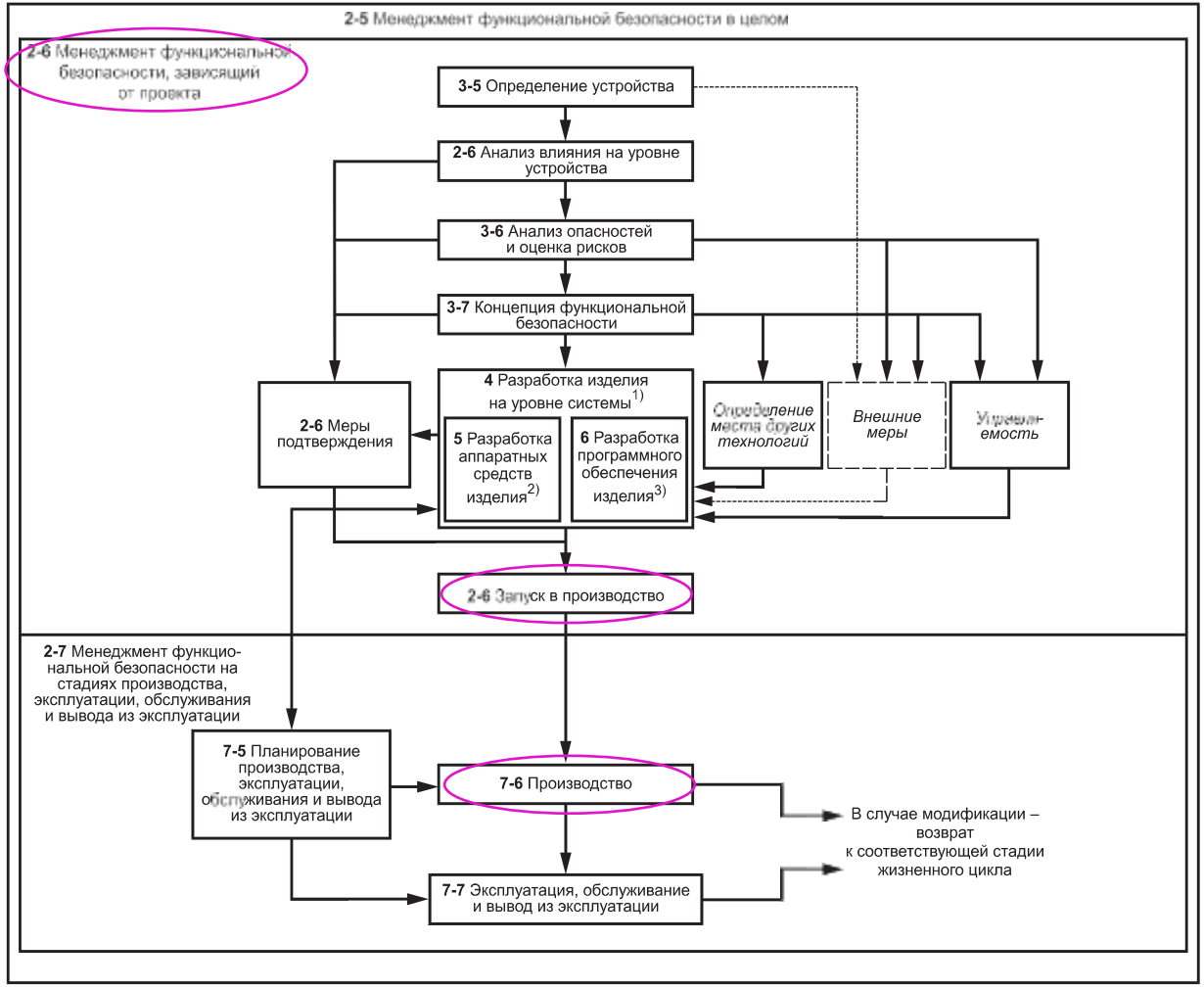
d) скоординировать и **отследить выполнение** действий по обеспечению безопасности в соответствии с планом обеспечения безопасности;

e) гарантировать установленную **последовательность** выполнения действий по обеспечению безопасности на всем **жизненном цикле** системы безопасности;

f) оценить, достигает ли устройство требуемый **уровень** функциональной безопасности и принять решение о запуске устройства или элемента(ов) в производство

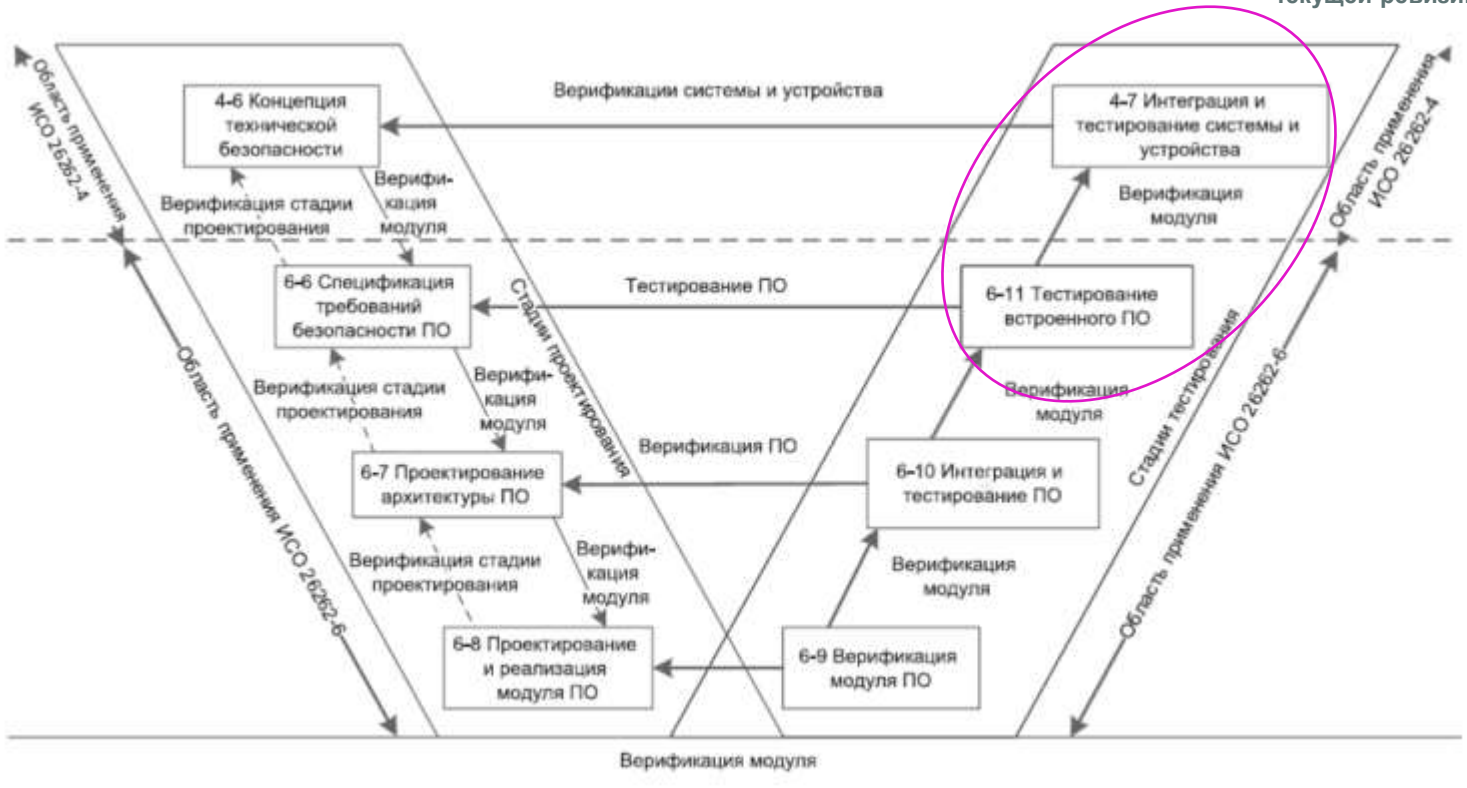
Менеджмент функциональной безопасности, зависящий от проекта

Требования стандарта в части FSM

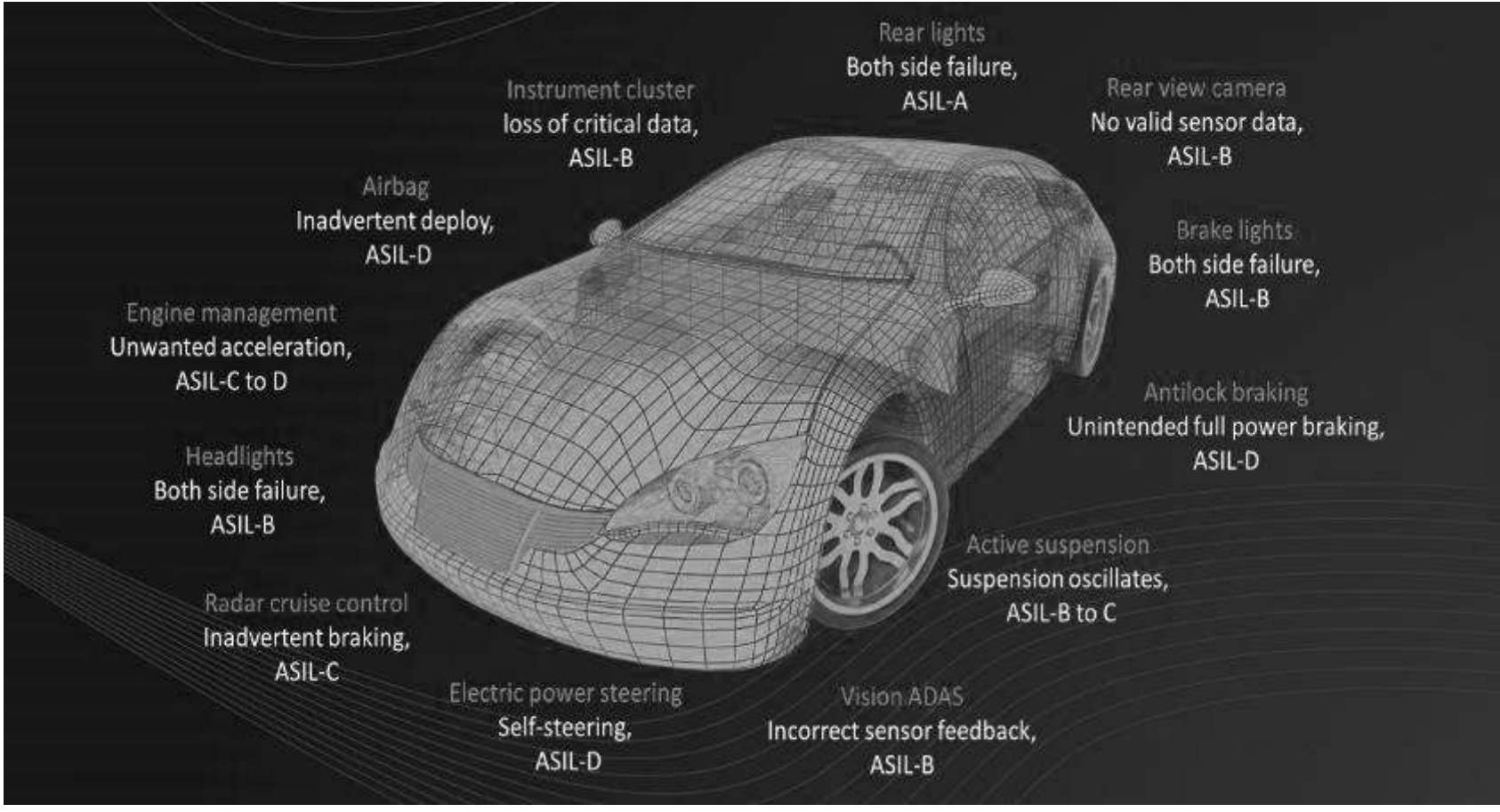


Базовая модель стадии разработки изделия на уровне программного обеспечения (ПО)

Не предусмотрено подтверждение соответствия ПО в текущей ревизии ГОСТ



Типовые классификации автомобильных систем



HARA – анализ опасностей и оценка рисков

Пример: устройство: **АБС** (Antilock breaking):
Цель безопасности: ослабление тормозного усилия в случае блокировки колёс для увеличения коэффициента сцепления
Идентифицированное опасное событие 1: непреднамеренное экстренное торможение, потеря курсовой устойчивости, наезд сзади

Классы тяжести последствий:

	Класс			
	S0	S1	S2	S3
Описание	Повреждения отсутствуют	Легкие и умеренные повреждения	Тяжелые и опасные для жизни повреждения (вероятное выживание)	Опасные для жизни повреждения (сомнительное выживание), повреждения со смертельным исходом

Классы вероятности воздействий эксплуатационных ситуаций:

	Класс				
	E0	E1	E2	E3	E4
Описание	Невероятное	Очень низкая вероятность	Низкая вероятность	Средняя вероятность	Высокая вероятность

Классы управляемости:

	Класс			
	C0	C1	C2	C3
Описание	Полностью управляемое	Легко управляемое	Обычно управляемое	Трудно управляемое или неконтролируемое

Определение УПБТС/ASIL:

Классы тяжести последствий	Класс вероятности воздействия	Класс управляемости		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A[a)]
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

АПБТС-**D**/
ASIL-**D**

Критерии выбора методов и мер

IEC 61508

Таблица А.9 — Верификация программного обеспечения (см. 7.9)

Метод/средство[1)]	Ссылка	SIL1	SIL2	SIL3	SIL4
1 Формальная проверка	C.5.13	—	R	R	HR
2 Вероятностное тестирование	C.5.1	—	R	R	HR
3 Статический анализ	B.6.4, таблица B.8	R	HR	HR	HR
4 Динамический анализ и тестирование	B.6.5, таблица B.2	R	HR	HR	HR
5 Метрики сложности программного обеспечения	C.5.14	R	R	R	R
Тестирование и интеграция программных модулей	См. таблицу A.5				
Проверка интеграции программируемых электронных устройств	См. таблицу A.6				
Тестирование программной системы (подтверждение соответствия)	См. таблицу A.7				

ISO 20262

Таблица 7 — Методы верификации модуля программного обеспечения

Методы		УПБТС			
		A	B	C	D
1a	Сквозной контроль проекта [a]	++	+	o	o
1b	Дублированное программирование [a]	+	+	+	+
1c	Ревизия [a]	+	++	++	++
1d	Полуформальная верификация	+	+	++	++
1e	Формальная верификация	o	o	+	+
1f	Анализ потока управления [b, c]	+	+	++	++
1g	Анализ потока данных [b, c]	+	+	++	++
1h	Статический анализ кода [d]	++	++	++	++
1i	Статический анализ, основанный на абстрактной интерпретации [e]	+	+	+	+
1j	Тестирование на основе требований [f]	++	++	++	++
1k	Тестирование интерфейса [g]	++	++	++	++
1l	Тестирование методом внесения дефектов [h]	+	+	+	++
1m	Оценка используемых ресурсов [i]	+	+	+	++
1n	Сравнительный тест между моделью и кодом, если он применим [j]	+	+	++	++

МЕТРИКИ АРХИТЕКТУРЫ АППАРАТНЫХ СРЕДСТВ

является важным показателем при оценке безопасности аппаратных средств

Согласно ГОСТ Р ИСО 26262 должна быть обоснована пригодность **архитектуры** аппаратных средств устройства с использованием метрики для выявления и управления связанными с безопасностью случайными отказами аппаратных средств.

Две метрики архитектуры HW

Метрика единичного сбоя

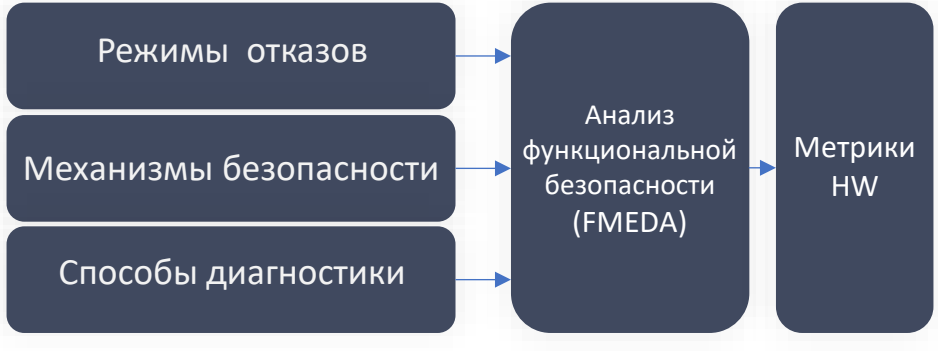
(фактически - доля безопасных отказов – SFF)

SPFM

Метрика скрытого сбоя

(аналог диагностического покрытия– DC)

LFM



ASIL	Интенсив-ность отказов	Метрика единичного сбоя (SPFM)	Метрика скрытого сбоя (LFM)
A	<1000 FIT	не нормир.	не нормир.
B	<100 FIT	≥90%	≥60%
C	<100 FIT	≥97%	≥80%
D	<10 FIT	≥99%	≥90%

Одиночный сбой (SPF)

Single point faiult

сбой в элементе аппаратных средств, который непосредственно приводит к недостижению цели безопасности, и ни один сбой в этом элементе не охвачен ни одним механизмом безопасности

(опасный недиагностируемый отказ в нерезервированном элементе)

Множественный сбой (MPF)

Multiple-point fault

отдельный сбой, который в сочетании с другими независимыми сбоями, если он не обнаружен и не воспринимается, может привести к множественному отказу к недостижению цели безопасности

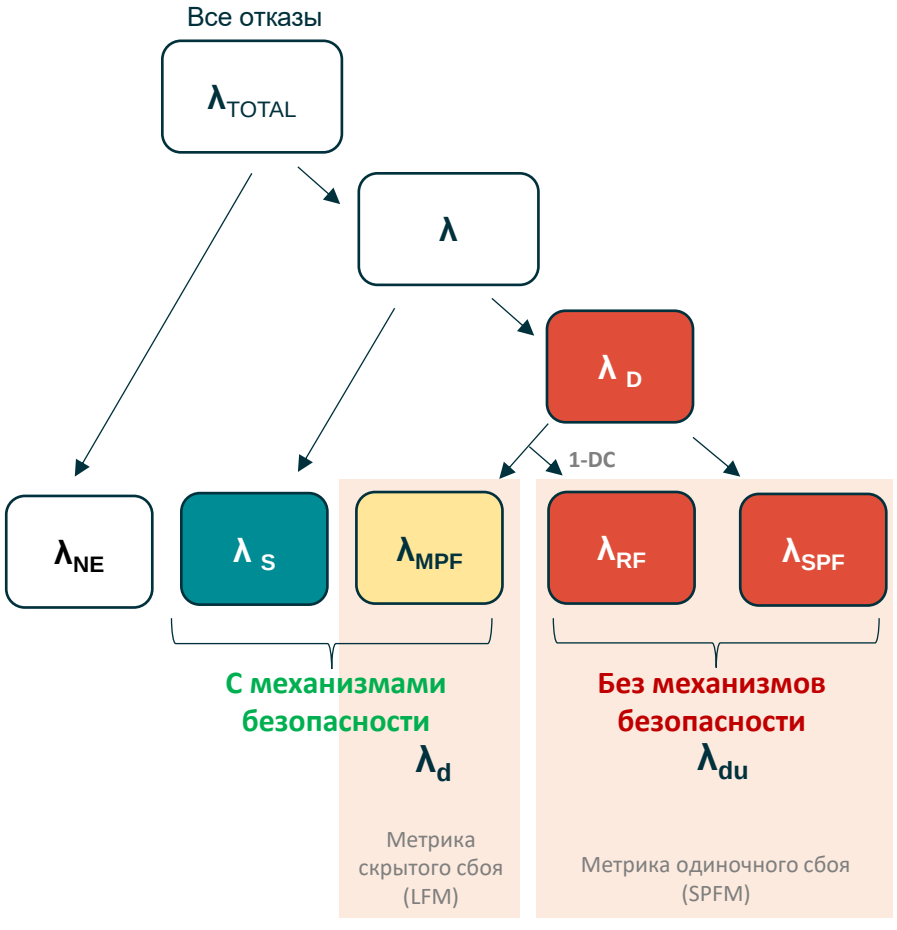
(опасный отказ одного из компонентов, для которого есть механизм безопасности – диагностика или резерв)

Остаточный сбой (RF)

Residual fault

часть случайных сбоев аппаратных средств, приводящих к не достижению цели безопасности, происходящих в элементе аппаратных средств, где эта часть случайных сбоев аппаратных средств не охвачена механизмами безопасности

(опасный отказ, не обеспеченный эффективной диагностикой)



ГОСТ Р ИСО 26262-5—2021 и ГОСТ Р ИСО 26262-10—2014 содержит примеры количественного анализа FMEA (FMEDA)

Уверенность в использовании инструментального программного обеспечения

Таблица 3 – Определение уровня доверия к инструменту (УДИ)

Класс инструмента		Инструменты, обнаруживающие ошибки		
		ООИ/TD 1	**ООИ/TD 2**	**ООИ/TD 3**
Влияние инструмента	**ВИ 1** (не может внести ошибку - Т1)	**УДИ/TCL 1**	**УДИ/TCL 1**	**УДИ/TCL 1**
	ВИ 2 (может внести ошибку - Т2, Т3)	**УДИ/TCL 1**	**УДИ/TCL 2**	**УДИ/TCL 3**

Таблица 4 – Квалификация инструментального программного обеспечения с УДИ 3

Методы		УПБА			
		A	B	C	D
1a	Рост доверия в результате использования в соответствии с 11.4.7	++	++	+	+
1b	Оценка процесса разработки инструмента в соответствии с требованиями 11.4.8	++	++	+	+
1c	Подтверждение соответствия инструментального программного обеспечения в соответствии с требованиями 11.4.8	+	+	++	++
1d	Разработка в соответствии со стандартом для системы безопасности [a]	+	+	++	++

[a] Не существует стандарта для системы безопасности, который в полной мере относится к разработке инструментального программного обеспечения. Вместо этого может быть выбрано соответствующее подмножество требований в стандарте для системы безопасности.

Пример – Разработка инструментального программного обеспечения в соответствии с требованиями ИСО 26262, МЭК 61508 или RTCA DO-178.

Таблица 5 – Квалификация инструментального программного обеспечения с УДИ 2

Методы		УПБА			
		A	B	C	D
1a	Рост доверия в результате использования в соответствии с 11.4.7	++	++	++	+
1b	Оценка процесса разработки инструмента в соответствии с требованиями 11.4.8	++	++	++	+
1c	Подтверждение соответствия инструментального программного обеспечения в соответствии с требованиями 11.4.8	+	+	+	++
1d	Разработка в соответствии со стандартом для системы безопасности [a]	+	+	+	++

[a] Не существует стандарта для системы безопасности, который в полной мере относится к разработке инструментального программного обеспечения. Вместо этого может быть выбрано соответствующее подмножество требований в стандарте для системы безопасности.

Пример – Разработка инструментального программного обеспечения в соответствии с требованиями ИСО 26262, МЭК 61508 или RTCA DO-178.

ООИ – обнаруживающий ошибки инструмент - Tool Error Detection (TD)
УДИ - уровня доверия к инструменту – Tool Confidence Level (TCL)
ВИ - класс влияния инструмента - Tool Impact (TI)

Сертификация существующего *(компилятора)*
или
Разработка инструментального средства в соответствии с МЭК 61508 или ИСО 26262
или применение широкого набора тестовых сценариев гарантирующих выявление ошибки

Квалификация компонентов и инструментов

План безопасности и требования проекта, ASIL

Информация о процессе разработки

Квалификация **инструментального ПО**

Отчет о критериях оценки

Отчет о квалификации ИПО

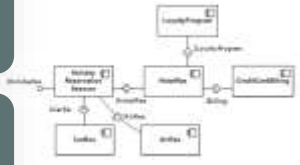
Спецификация компонента

Доказательства разработки на национальном стандарте

Квалификация **компонента ПО**

Документация на компонент

Отчет о квалификации ПО



Спецификация производителя

Данные об отказах

Требования и критерии

Квалификация **компонентов аппаратных средств**

План квалификации/теста

Результат теста или анализа

Отчет о квалификации ПО

- Полупроводники,
- Реле,
- Датчики,
- Приводы,
- ИС с заданной функциональностью (например, адаптер протокола).

Общеиспользуемый элемент безопасности (ОЭБ) – Элемент безопасности вне контекста (SEooC)

ОЭБ / SEooC - общеиспользуемые элементы для различных применений (ТС) и для различных заказчиков (проектов), например -

- системные контроллеры,
- электронные блоки управления,
- микроконтроллеры, программное обеспечение,
- реализующее коммуникационный протокол.

НЕ может быть устройством, так как разработка устройства всегда выполняется для конкретного ТС

ОЭБ разрабатывается на основе **предположений** в соответствии с настоящим стандартом.

На основе **предположений** разработчик ОЭБ определяет:

- цель, функционал и внешние интерфейсы ОЭБ
- требований безопасности к ОЭБ

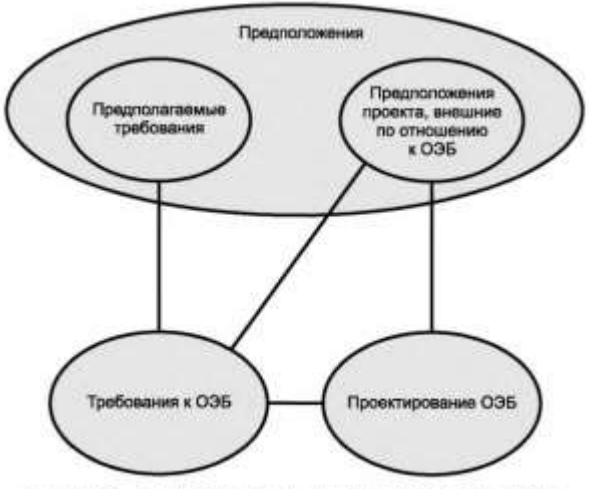


Рисунок 18 — Связь между предположениями и разработкой ОЭБ

Требуемые меры подтверждения с учетом требуемого уровня независимости

Меры подтверждения	Степень независимости[a] применятся к					Область применения
	QM	УПБТС A	УПБТС B	УПБТС C	УПБТС D	
Аудит функциональной безопасности в соответствии с 6.4.11. Выполняется независимо от разработчиков устройств и управления проектом	—	—	I0	I2	I3	Применяется к требованиям безопасности с самым высоким значением УПБТС
Оценка функциональной безопасности в соответствии с 6.4.12. Выполняется независимо от разработчиков устройств и управления проектом	—	—	I0	I2	I3	Применяется к требованиям безопасности с самым высоким значением УПБТС

[a] Обозначения определены следующим образом:

— — требования или рекомендации за или против данной меры подтверждения отсутствуют;

I0 — мера подтверждения должна быть выполнена; однако если данная мера подтверждения осуществляется, то она должна быть выполнена лицом, отличным от лиц(а), ответственных(ого) за создание рассматриваемого(ых) результата(ов) работы;

I1 — мера подтверждения должна быть выполнена лицом, отличным от лиц(а), ответственных(ого) за создание рассматриваемого(ых) результата(ов) работы;

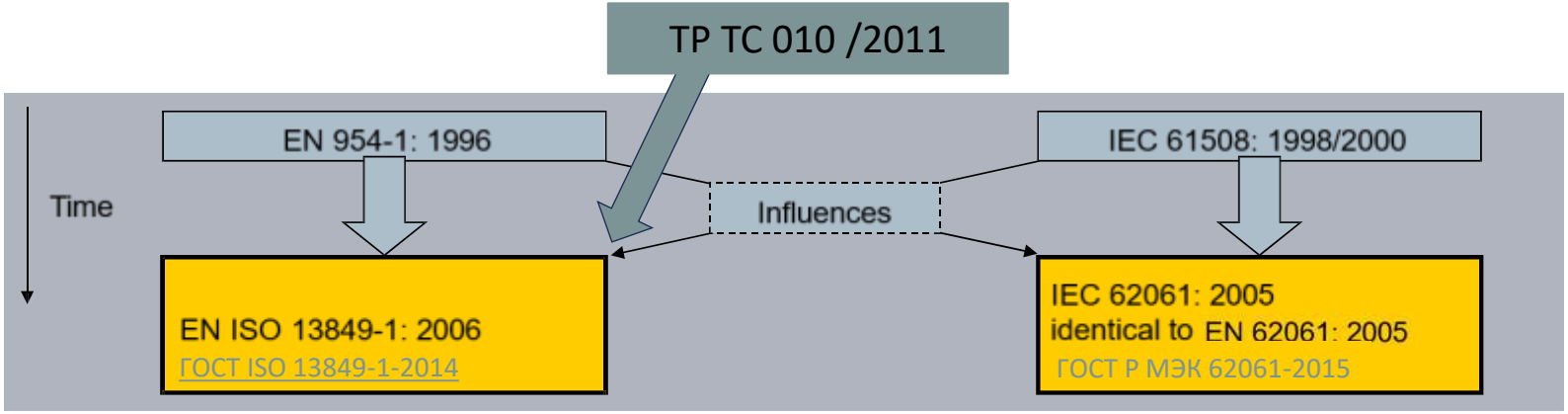
I2 — мера подтверждения должна быть выполнена лицом, не входящим в авторский коллектив, ответственный за создание рассматриваемого(ых) результата(ов) работы, то есть не подчиняющимся тому же непосредственному начальнику;

I3 — мера подтверждения должна быть выполнена лицом, независимым от отдела, отвечающего за рассматриваемые результаты работы, от организации их выполнения, используемых ресурсов и определения полномочий.

Безопасность оборудования ISO 13849 и IEC 62061

Безопасность оборудования

Два стандарта: ISO 13849 и IEC 62061 частично совпадают и могут использоваться в качестве альтернативы.
Новые концепции: Рабочий проект (Draft) 17305 - Объединение обоих стандартов ISO 13849 и IEC 62061



Feature	EN 954-1	EN ISO 13849-1	IEC 61508	EN 62061
For manufacturers of	Machinery	Machinery	Components	Machinery
Technology	Also non-electrical	Also non-electrical	Electrical	Electrical
Concept: Safety function Required safety level Probability of failure	 Parts Categories ---	 Total PL_r PFH_D	 Total SIL PFH_D	 Total SIL PFH_D
Use of programmable electronics (PLC, …)	No	Yes	Yes	Yes
Presumption of conformity, if applied	Yes	Yes	No	Yes

Область применения

Настоящий стандарт представляет собой руководство для тех. кто занимается проектированием и оценкой систем управления.

Цель разработки настоящего стандарта — предоставить четкую основу разработчикам стандартов типа С, на которой конструирование и функционирование любого элемента системы управления, связанного с обеспечением безопасности оборудования, может быть объективно **оценено, например, с помощью третьей стороны, собственных (внутренних) средств или независимого испытательного органа.**

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ ISO 13849-1— 2014

Безопасность оборудования

ЭЛЕМЕНТЫ СИСТЕМ УПРАВЛЕНИЯ, СВЯЗАННЫЕ С БЕЗОПАСНОСТЬЮ

Часть 1

Общие принципы конструирования

(ISO 13849-1:2006, IDT)

Охватывает требования как для разработчиков, так и для интеграторов.

3.1.1 **элемент системы управления**, связанный с безопасностью (safety-related part of a control system, SRP/CS): Часть системы управления, которая реагирует на входные сигналы и вырабатывает выходные сигналы, связанные с обеспечением безопасности.

Не выделяется независимая система безопасности!

Информация для расчета надежности элеметов

Приложение С (справочное)

Расчет и оценка среднего времени наработки на опасный отказ (MTTFd) для отдельных компонентов

С.3 Гидравлические компоненты

Таблица С.1 — Международные нормы, касающиеся $MTTF_d$ или $B10_d$ для компонентов

Компоненты	Основные принципы безопасности по ISO 13849-2	Соответствующие стандарты	Стандартные значения: $MTTF_d$ (годы) B_{10d} (циклы)
Механические компоненты	Таблицы А.1 и А.2	—	$MTTF_d$ = 150
Гидравлические компоненты	Таблицы С.1 и С.2	[24], [42]	$MTTF_d$ = 150

С.5 Значения MTTFd для электрических компонентов

С.5.2 Полупроводники
См. таблицы С.2 и С.3.

Таблица С.2 — Транзисторы (в режиме переключений)

Транзистор	Обозначение	MTTF для компонентов, лет	$MTTF_d$ для компонентов, лет		Примечания
			обычный	тяжелый	
Биполярный	TO18, TO92, SOT23	34 247	68 493	6 849	50 % опасных отказов
Биполярный, маломощный	TO5, TO39	5 708	11 416	1 142	50 % опасных отказов
Биполярный, мощный	TO3, TO220, D-Pack	1 941	3 881	388	50 % опасных отказов
ФЕТ	Junction MOS	22 831	45 662	4 566	50 % опасных отказов
МОС, силовой	TO3, TO220, D-Pack	1 142	2 283	228	50 % опасных отказов

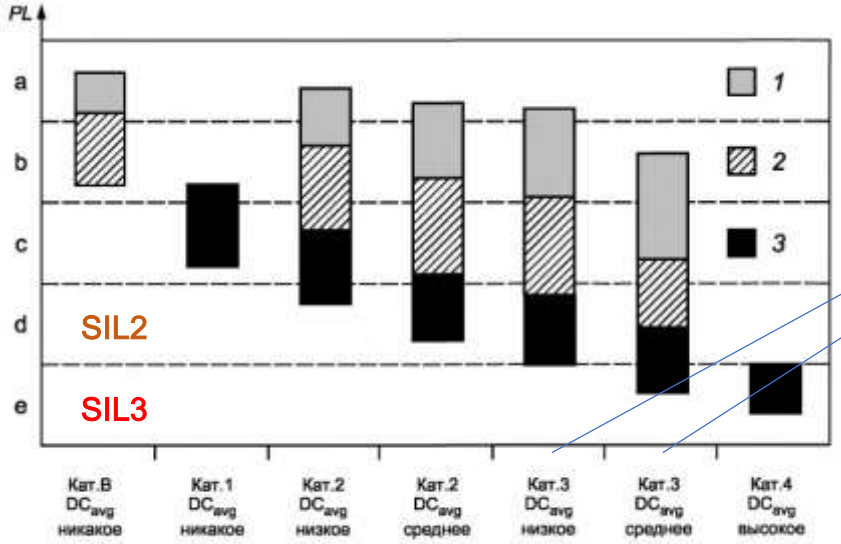
Таблица С.5 — Резисторы

Резистор	Обозначение	MTTF для компонентов, лет	$MTTF_d$ для компонентов, лет		Примечания
			обычный	тяжелый	
Карбон пленка	—	114 155	228 311	22 831	50 % опасных отказов
Металлопленка	—	570 776	1 141 552	114 155	50 % опасных отказов
Металлооксидные и проволочные	—	22 831	45 662	4 566	50 % опасных отказов
	—	3 767	7 534	753	50 % опасных отказов

Категории и требования к структурам

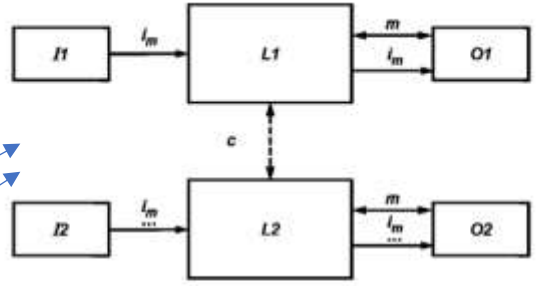
В случае применений PLr от **a до c** меры по избеганию неисправностей могут быть достаточными; при применении большего риска PLr — от **d до e** конструкция SRP/CS может обеспечить меры по избеганию, обнаружению или преодолению неисправностей. Практические меры включают **избыточность, разнообразие, контроль** (см. также ISO 12100, раздел 3 и IEC 60204-1).

6 Категории и их связь со средним временем наработки на опасный отказ ($MTTF_d$) каждого из каналов, средним диагностическим охватом (DC_{avg}) и отказом по общей причине (CCF)



PL — уровень эффективности защиты; *1* — $MTTF_d$ каждого канала — низкое; *2* — $MTTF_d$ каждого канала — среднее; *3* — $MTTF_d$ каждого канала — высокое

Рисунок 5 — Отношения между категориями DC_{avg}, $MTTF_d$ каждого канала и PL



Пунктирные линии означают обнаружение неисправности, целесообразное с практической точки зрения.

i_m — средства связи; *c* — перекрестный мониторинг; *I1, I2* — входное устройство, например, датчик; *L1, L2* — логический блок; *m* — контроль; *O1, O2* — выходное устройство, например, главный контактор

Рисунок 11 — Структурное построение для категории 3

Должны быть приняты меры, направленные на предотвращение CCF.

Область применения

Настоящий стандарт предназначен для использования разработчиками оборудования машин, производителями и интеграторами систем управления и другими специалистами, выполняющими спецификацию, проектирование и подтверждение соответствия СБЭСУ.

В настоящем стандарте представлена методология для применения, а не разработки подсистем и их элементов, являющихся частью СБЭСУ


НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 62061— 2015

Безопасность оборудования

ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ СИСТЕМ УПРАВЛЕНИЯ ЭЛЕКТРИЧЕСКИХ, ЭЛЕКТРОННЫХ И ПРОГРАММИРУЕМЫХ ЭЛЕКТРОННЫХ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ

IEC 62061:2005+A1:2012
Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems

В настоящем стандарте предполагается, что проектирование сложных программируемых электронных подсистем или их элементов удовлетворяет соответствующим требованиям МЭК 61508 и используется способ 1н (см. 7.4.4.2 МЭК 61508-2).

Подсистемы, включающие сложные компоненты, должны соответствовать МЭК 61508-2 и МЭК 61508-3 в зависимости от требуемого УПБ, и проект должен использовать Способ 1н.

Считается, что способ 2Н (см. 7.4.4.3 МЭК 61508-2) не подходит в общем случае для машинного оборудования, поэтому настоящий стандарт не рассматривает способ 2Н.

Определение уровня полноты безопасности

Пример: устройство: **АБС** (Antilock breaking):
Цель безопасности: ослабление тормозного усилия в случае блокировки колёс для увеличения коэффициента сцепления
Идентифицированное опасное событие 1: непреднамеренное экстренное торможение, потеря курсовой устойчивости, наезд сзади

Классификация серьезности (Se):

Последствия	Серьезность (Se)
Необратимые: смерть, потеря глаза или руки	4
Необратимые: сломанные конечности, потеря пальца(ев)	3
Обратимые: требующие участия врача	2
Обратимые: требующие оказания первой медицинской помощи	1

Классификация частоты и продолжительности воздействия (Fr):

Частота и продолжительность воздействия (Fr)	
Частота воздействия	Степень воздействия, Fr (см. A.2.4.1)
≥ 1 в ч	5
от < 1 в ч до ≥ 1 в день	5
от < 1 в день до ≥ 1 за 2 недели	4
от <1 за 2 недели до ≥ 1 в год	3
от < 1 в год	2

Определение УПБТ/SIL (PL по ISO 13849)

Последствия	Индекс серьезности (Se)	Класс Cl = Fr + Pr + Av												
		3	4	5	6	7	8	9	10	11	12	13	14	15
Летальный исход, потеря глаза или руки	4	SIL 1		SIL 2			SIL 2				SIL 3		SIL 3	
		PL,b	PL,c	PL,d			PL,d				PL,e		PL,e	
Необратимая травма, потеря пальцев руки	3			ПМ			SIL 1				SIL 2		SIL 3	
				PL,a		PL,b		PL,c			PL,d		PL,e	
Обратимая травма, медицинская помощь	2	SIL (или PL) не требуется					ПМ				SIL 1		SIL 2	
							PL,a			PL,b	PL,c		PL,d	
Обратимая травма, первая помощь	1	ПМ: прочие меры									ПМ		SIL 1	
											PL,a		PL,b	PL,c

Классификация вероятности возникновения опасного события (Pr):

Вероятность возникновения	Значение Pr
Очень высокая	5
Вероятно	4
Возможно	3
Редко	2
Незначительная	1

Классификация вероятности избежать или ограничить вред (Av):

Вероятность избежать или ограничить вред (Av)	
Невозможно	5
Редко	3
Вероятно	1

УПБ **3** /
SIL **3** (Pl **e**)

Программное обеспечение

IEC 62061

6.11 Проектирование и разработка программного обеспечения

6.11.1 Проектирование и разработка встроенного программного обеспечения

Встроенное программное обеспечение, включенное в подсистемы, должно соответствовать МЭК 61508-3 и требуемому УПБ.

Примечания

1 См. также 6.7.3.2.

2 В приложении С рассматривается проектирование и разработка встроенного программного обеспечения, используемого для реализации СБФУ для СБЭСУ.

ГОСТ Р МЭК 62061—2015

Приложение С
(справочное)

Руководство по проектированию и разработке встроенного программного обеспечения

Примечание — Данное приложение представляет основной подход, который удовлетворяет требованиям МЭК 61508-3. Сам по себе без применения дополнительных мер он не может обеспечить соответствие с МЭК 61508-3.

С.3.1 Процесс разработки. Жизненный цикл программного обеспечения

Жизненный цикл разработки программного обеспечения должен быть определен и документально оформлен (например, в плане качества программного обеспечения) и включать все технические мероприятия и стадии, необходимые и достаточные для разработки программного обеспечения.

ISO 13849

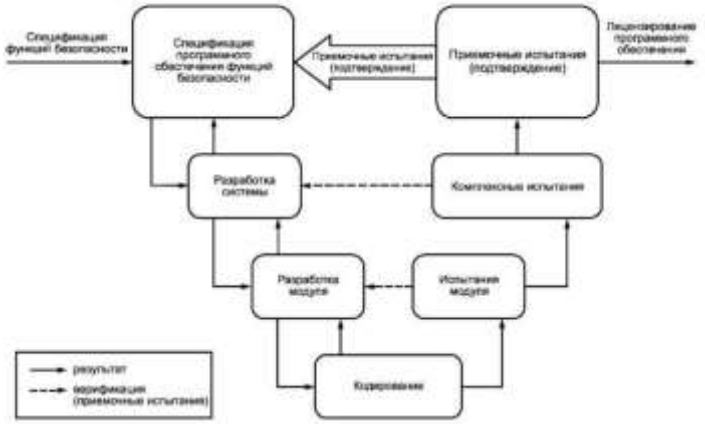
4.6.2 Встроенное программное обеспечение функций безопасности (SRESW)

Для компонентов SRESW с PL_r от *c* до *d* должны применяться следующие дополнительные меры:

- менеджмент качества сопоставляемых систем при конструировании, например, в соответствии с IEC 61508 или [18];

...

Компоненты SRESW с PL_r =e должны соответствовать IEC 61508, раздел 7, с подходящим SIL 3. С учетом отличий в области технических требований.



Нет никаких требований по сертификации или степени независимости при оценке ФБ

Заключение

Аспекты разработки и сертификации КОМПОНЕНТОВ





	МЭК 61508	МЭК 61511	EN 5012x	ИСО 26262	МЭК 62061	ISO 13849
Объем	7 частей	3 части	3 части + 3 стандарта	12 частей	1 часть + ссылки	2 части + ссылки
Аналог РФ	да	да	**не все стандарты и части**	да (10 частей, **не полностью актуален**)	да (предыдущая редакция)	да (**только 1 часть, предыдущая редакция**)
Концепция	SIL (1..4)	SIL (1..3)	**RAMS**	**ASIL** (A…D)	SIL (1..3)	**PLr**(a…e) / SIL
Типовые решения	SIL2-SIL3	SIL1-SIL3	SIL**4**	**ASIL B - ASIL D**	SIL3	PIe
Метрики	PFD_{avg}/PFH, SFF/DC, HFT, **SC**	PFD_{avg}/PFH, SFF/D, HFT, SC	**λ/MTTF/MDTF, A**, MTTR, SIL(1..4), (SC)	FIT, **SPFM, LFM**, DC, (SC)	PFH_D , SFF, HFT (1H), SC	$MTTF_D$, DC_{avg}, **Cat.(B,1…4)**
Управление ФБ (FSM)	**Выделение сотрудника**, политика и стратегия достижения функциональной безопасности, процедуры обеспечения безопасности	Политика и стратегия достижения функциональной безопасности, процедуры обеспечения безопасности	ИСО 9001, Управление RAMS: "Программа RAM", "План обеспечения безопасности" и ЖЦ	26262-2: **Выделение сотрудника, FSM в целом, FSM зависящий от проекта, FSM производства и эксплуатации (детально)**	только "План управления ФБ" (+ требования к ПО по IEC 61508)	**Менеджмент качества** и Управления документами в соотв. с **IEC 61508**
Требования к встроенному ПО	Оценка соответствия безопасности. Способы 1s (разработка по МЭК 61508-3); **2s "проверено в эксплуатации";** **3s (обоснование соответствия сущ.резработки)**	Выбор прошедшего оценку в соответствии с МЭК 61508 (т.к. обычно исп.ЯПИ)	**Оценка соответствия безопасности:** a) **разработка по МЭК 62279**; b) оценка требований к существующему ПО	a) **квалификация** сущ. встроенного ПО или b) разработка в соответствии с **26262-6**	**Оценка соответствия безопасности**: - должно соответствовать МЭК 61508-3 и требуемому УПБ	**Оценка соответствия безопасности:** **- для PL e - соответствие IEC 61508-3 SIL3;** - для PL c, PL d - соответствие менеджмента IEC 61508; - для PL a, PL b - соответствие п.4.6.2 ISO 13849
Основная выходная документация по ФБ для компонентов	План обеспечения безопасности (Safety/FSM plan). Спецификация требований безопасности (SRS) компонента. План V&V. План оценки ФБ. Отчеты V&V компонента. Отчет оценки ФБ компонента. Руководство по безопасности компонента.	- (не предусматривается для компонентов)	Журнал опасностей. Программа RAM. План безопасности. План спецификации RAMS. План аттестации/приемки. План V&V. **Доказательство безопасности устройства (GP Safety Case).** Обзорный отчет по RAMS.	План обеспечения безопасности (Safety/FSM plan). План V&V элемента. Обоснование безопасности (Safety Case) элемента. Отчеты о мерах подтверждения (V&V Report) элемента. Отчет об аудите ФБ элемента. Отчет об оценке ФБ элемента.	Для **сложных программируемых** электронных подсистем или их элементов - согласно **МЭК 61508**	**Спецификация безопасности для контроля машин.** План V&V. Отчет V&V PLr компонента (протоколы испытаний). **Отчет оценки PLr компонента.**

Аспекты разработки ПРИКЛАДНЫХ ПРОЕКТОВ





	МЭК 61508	МЭК 61511	EN 5012x	ИСО 26262	МЭК 62061	ISO 13849
Идентификация рисков	ГОСТ Р 27.012-2019 (IEC 61882) -HAZOP, IEC 60300-3-1	Контрольные листы (HAZID), HAZOP, FMEA и т.д.	**Анализ RAMS** и опасных факторов системы (**нет примеров**)	FMEA, HAZOP (**нет примеров**)	**Опросный лист в ГОСТ ISO 12100 (HAZID)**	**Типовые функции SRP/CS и ГОСТ ISO 12100**
Назначение SIL	Risk Graph, LOPA, Risk Matrix, QRA	FTA/ETA, Risk Graph, LOPA, Risk Matrix, QRA	Численный или **матрица** «Частота / Последствие»	**Таблицы** факторов риска	**Таблицы** факторов риска или методы из МЭК 61508-5	Risk **Graph**
Архитектурные ограничения	Способы 1H, 2H (с опытом применения). На практике - избыточность для SIL3	Способы 1H, 2H (с опытом применения). На практике - избыточность для SIL3	**Нет прямых ограничений**, разработка в соответствии с RAMS и IEC 61508 (обычно 2x(1oo2) или 2oo3)	**Нет прямых ограничений**, ограничение через SPFM и как мера оценки DC	Способ 1H, все подсистемы **типа B**	Категории систем Cat.(B,1…4), **избыточность для Cat.3, Cat.4**
Требования к выбору компонентов	Разработка. Нет выделения элементов прошедших оценку, есть способ 2s - "проверено в эксплуатации"	Выбираемые компоненты и подсистемы должны либо соответствовать требованиям **МЭК 61508-2 и МЭК 61508-3, либо иметь успешный опыт предшествующего применения**	**Аттестация + ДБ:** - Составная часть общего назначения; - Компонент общего назначения.	**"Квалификация" всех компонентов**, использование "элементов безопасности вне контекста" (SEooC)	Разработка или выбор существующих (предварительно спроектированных) подсистем. **Для сложных программируемых** электронных подсистем или их элементов - подтверждение соответствия требованиям **МЭК 61508**	**Отбор** успешно испытанных компонентов, и/или применение хорошо проверенных принципов безопасности (**ISO 13849-2**)
Требования к прикладному ПО	Идентичные встроенному ПО: Оценка соответствия безопасности. Способы 1s (разработка по МЭК 61508-3); 2s "проверено в эксплуатации"; 3s (обоснование соответствия сущ.резработки)	Раздел 12 МЭК 61511-1: **Разрабатывается на языках ЯОИ и ФЯП (МЭК 61131-3), сертифицированные или верифицированные библиотеки, сертифицированный компилятор, проектирование, валидация.**	Раздел 8 МЭК 62279: разработка на основании спецификации и проекта.	Идентичные встроенному ПО: квалификация сущ.прикладного ПО или разработка в соответствии с 26262-6	В соответствии с МЭК 61508-3 для языков ЯПИ, МЭК 61511 - для языков **ЯОИ и ФЯП**	Для ЯПИ - требования как для встроенного ПО. Для **ЯОИ и ФЯП**- разработка на основании спецификации и проекта.
Основная выходная документация по ФБ для конкретных систем	План обеспечения безопасности (Safety/FSM plan). Отчеты по анализу рисков. Спецификация требований безопасности (SRS) E/E/PE. План V&V E/E/PE Отчеты V&V E/E/PE Отчет оценки ФБ E/E/PE	План обеспечения безопасности (Safety/FSM plan). Отчеты по анализу рисков. Спецификация требований безопасности (SRS) ПСБ. План V&V. Отчеты V&V ПСБ. Отчет оценки ФБ ПСБ.	Журнал опасностей объекта ЖТ. Программа RAM. План безопасности. План спецификации RAMS. План аттестации/приемки. План V&V объекта ЖТ. **Доказательство безопасности объекта ЖТ (SA Safety Case).** Обзорный отчет по RAMS объекта ЖТ.	**Отчет об анализе опасностей и оценке рисков** План обеспечения безопасности (Safety/FSM plan). План V&V системы. **Обоснование безопасности (Safety Case) системы.** Отчеты о мерах подтверждения (V&V Report) системы. Отчет об аудите ФБ системы. Отчет об оценке ФБ системы.	План обеспечения безопасности (Safety/FSM plan). План V&V. Спецификация требований безопасности (SRS). Отчеты V&V.	**Спецификация безопасности для контроля машин.** Спецификация компонентов. Руководство пользователя. Протоколы испытаний.

Выводы

Стандарты **функциональной безопасности разных отраслей:**

- **не полностью введены в действие в РФ (даже для наиболее широких областей применения)**
- **устанавливают схожие, но отличные требования к элементам и системам**

- **схожие требования позволяют выполнять сертификацию (оценку) элементов одновременно на соответствие разным (нескольким) стандартам**

- **сертификация на соответствие базового МЭК 61508 позволяет часто использовать оборудование в проектах для различных отраслей**
- **при подборе оборудования необходимо учитывать требования «отраслевых» стандартов ФБ**

- **для реализации проектов в разных отраслях необходимо использование соответствующих «отраслевых» стандартов ФБ**

СИСТЕМА ЭКСПЕРТ

от риска к безопасности

ОСТАЛИСЬ ВОПРОСЫ?

СВЯЖИТЕСЬ С НАМИ

сайт компании
https://www.systema-expert.ru

e-mail
dablokhin @ systema-expert.ru

телефон
+7 916 965 9301