



ENDURANCE
TEST & CERTIFICATION

ОСОБЕННОСТИ СЕРТИФИКАЦИИ ОБОРУДОВАНИЯ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ



ЗУБРЕВ ЕВГЕНИЙ

Эксперт по сертификации

СЕРТИФИКАЦИОННЫЙ ЦЕНТР ЭНДЮРЕНС – ЭТО:



9 лет на рынке



20 экспертов в команде



наши сотрудники входят
в различные рабочие группы



аккредитованы
по ГОСТ Р МЭК 61508



аккредитованы по всем
техническим регламентам
ТР ТС 004, 010, 012, 020, 032



собственная испытательная
лаборатория



НАША ДЕЯТЕЛЬНОСТЬ И УСЛУГИ

1

ВЗРЫВОЗАЩИТА

- Сертификация ТР ТС 012/2011
- Испытания взрывозащищенного оборудования
- Консалтинг взрывозащиты
- Ех-инспекции
- Внедрение систем качества

2

ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ

- Сертификация 61508
- Анализ рисков HAZOP
- Назначение уровней УПБ
- Верификация контуров безопасности
- Консалтинг функциональной безопасности

3

ОБУЧЕНИЕ

- Образовательная лицензия
- Курс Функциональная безопасность ГОСТ Р МЭК 61508 для разработчиков оборудования.
- Курс Анализ рисков, hazop. Функциональная безопасность. Разработка и эксплуатация СПАЗ (МЭК 61511)
- Разработчик внутреннего курса по системам ПАЗ для Сибур

«ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ»

Для чего создана:

для осуществления подтверждения соответствия продукции и услуг в соответствии со стандартами функциональной безопасности ГОСТ Р МЭК 62061, ГОСТ Р МЭК 61511, ГОСТ ISO 13849, ГОСТ Р МЭК 61508, ISO 26262

№ РОСС RU.32383.04ЕДРО

Система Зарегистрирована Федеральным агентством по техническому регулированию и метрологии (Росстандарт) от 18.03.2021 г.

ЧТО ПРОХОДИТ ПОДТВЕРЖДЕНИЕ

ДАТЧИКИ

КОНТРОЛЛЕРЫ

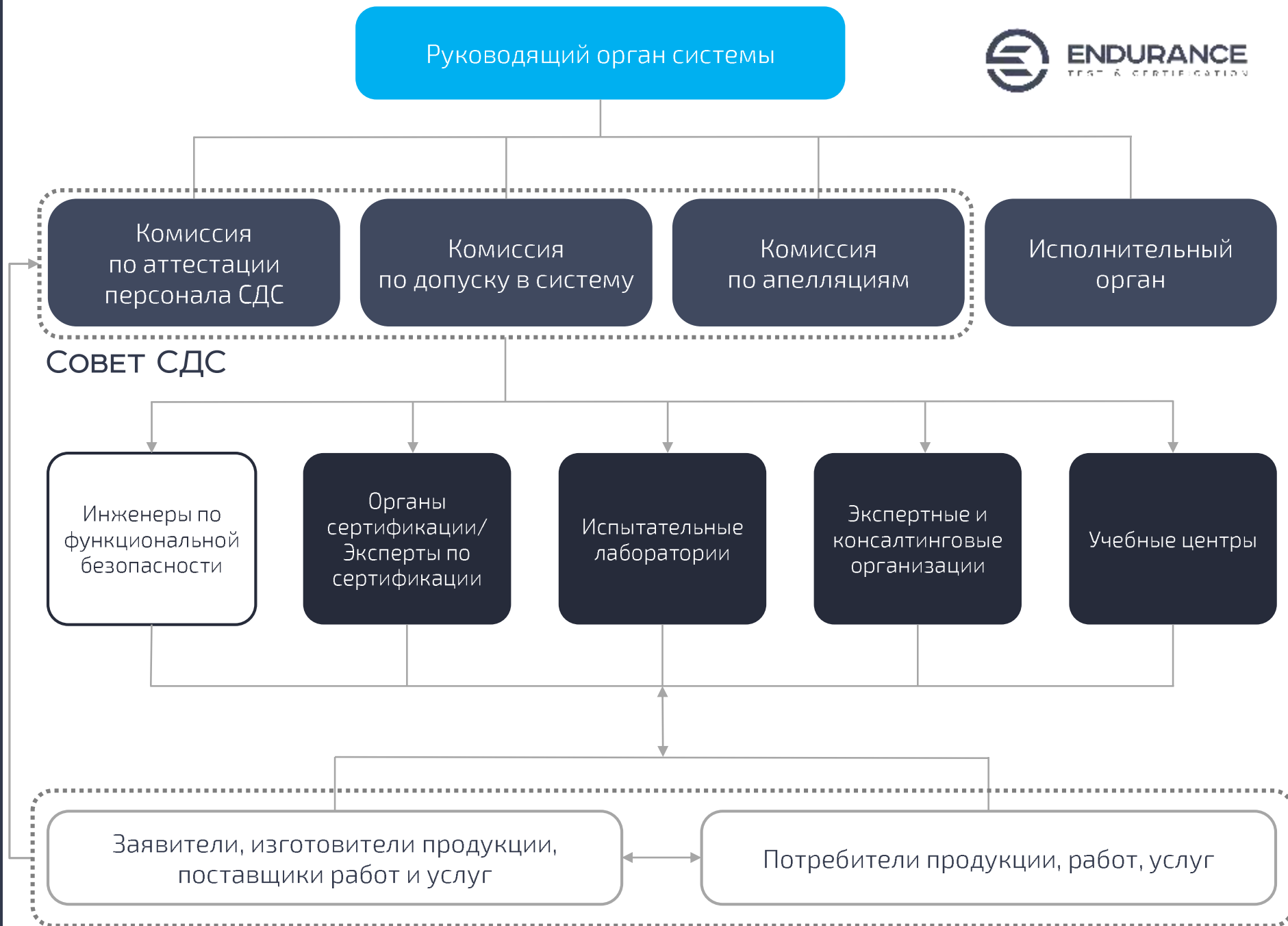
ИСПОЛНИТЕЛЬНЫЕ ЭЛЕМЕНТЫ

РЕЛЕ

БАРЬЕРЫ ИСКРОЗАЩИТЫ

ДРУГОЕ ОБОРУДОВАНИЕ

НАЦИОНАЛЬНАЯ
СИСТЕМА ОЦЕНКИ
СООТВЕТСТВИЯ
ЭТО НЕ ТОЛЬКО
СЕРТИФИКАЦИЯ



ГОСТ 61508-1 (раздел 8) обязывает проводить периодическую оценку функциональной безопасности

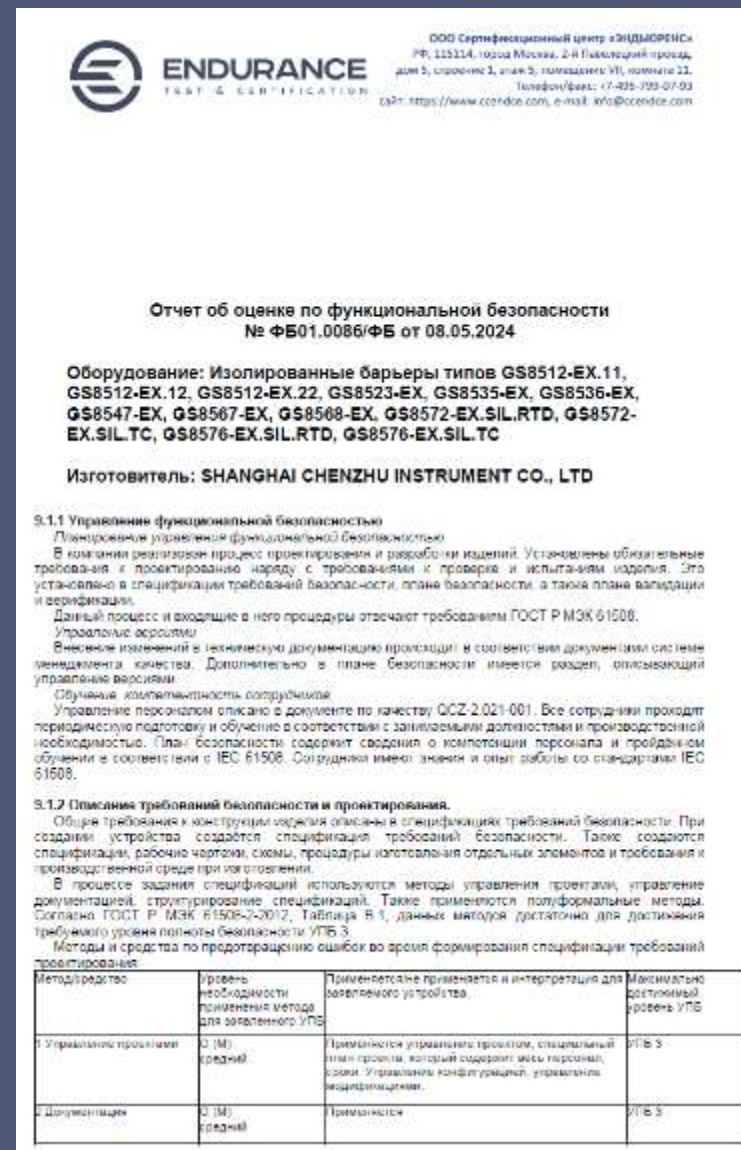
Минимальный уровень независимости	Уровень полноты безопасности/Стойкость к систематическим отказам				
	УПБ 1	УПБ 2	УПБ 3	УПБ 4	УПБ 1
Независимое лицо	X	X1	Y	Y	X
Независимое подразделение	-	X2	X1	Y	-
Независимая организация	-	-	X2	X	-

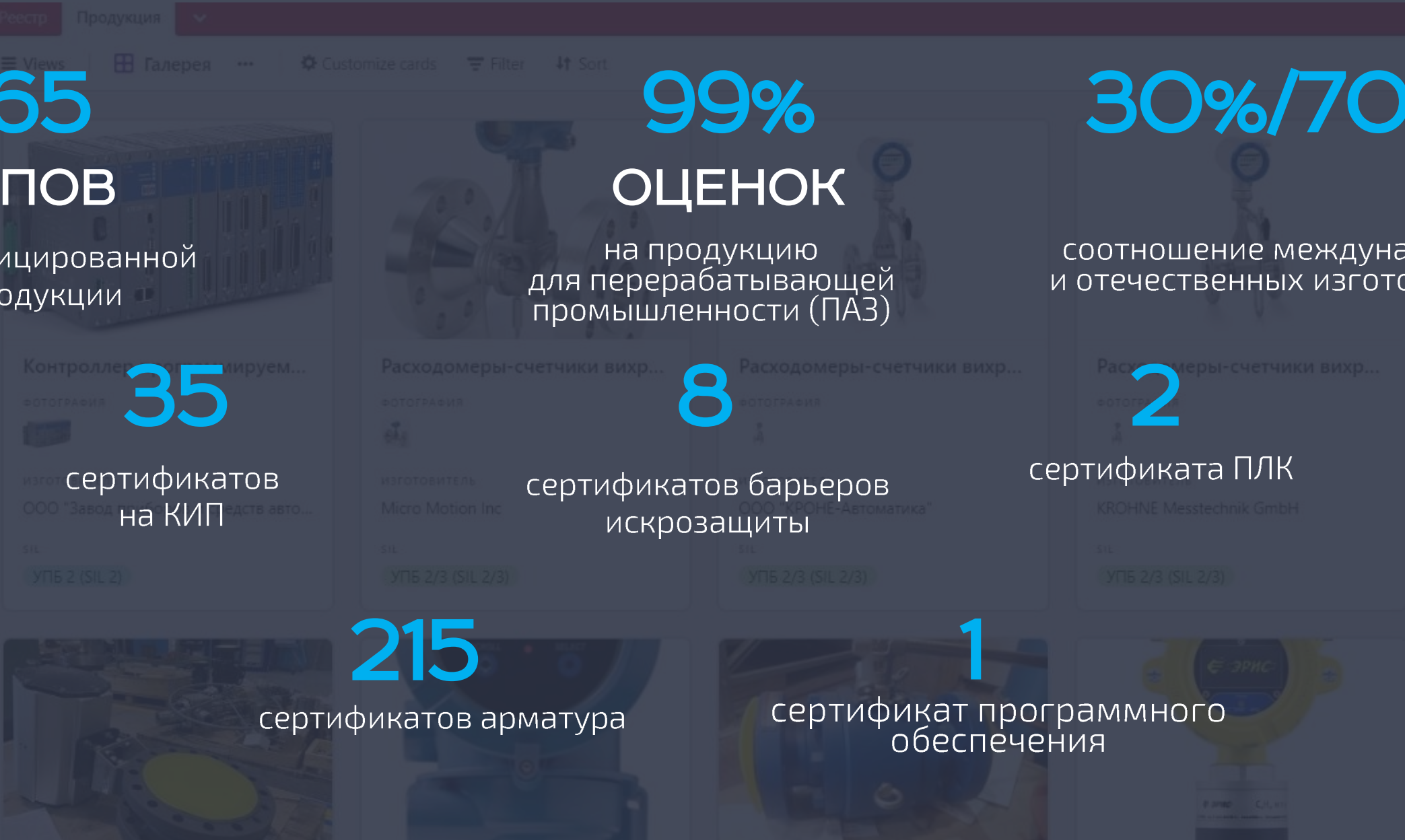
X – минимальный уровень независимости

Y – не рекомендуется для данного уровня риска

Документальное оформление результатов, включающее:

-  выполненные действия;
-  полученные результаты;
-  выводы;
-  суждение об адекватности функциональной безопасности требованиям стандарта;
-  рекомендации, вытекающие из оценки, в т.ч. рекомендации по принятию, условному принятию или отклонению.



 СТАТИСТИКА СЕРТИФИКАЦИИ

~65

ТИПОВ

сертифицированной
продукции

99%

ОЦЕНОК

на продукцию
для перерабатывающей
промышленности (ПАЗ)

30%/70%

соотношение международных
и отечественных изготовителей

35

сертификатов
на КИП

8

сертификатов барьеров
искрозащиты

2

сертификата ПЛК

215

сертификатов арматура

1

сертификат программного
обеспечения

РЕЗУЛЬТАТЫ ОЦЕНКИ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Среднее количество замечаний
по результатам оценки
функциональной безопасности

Тип оценки	Количество замечаний
Аудит существующей разработки (не закладывались требования ФБ)	~100
Аудит разработки с учетом требований ФБ	~30
Повторный аудит (международные отчеты/сертификаты)	~5

14	10.1.9	Провести испытания на воздействие климатических факторов	Необходимо	Высокий
15	10.1.9	Провести испытания на ЭМС	Необходимо	Высокий
16	10.1.10	Внести изменения в действующие документы СМК или разработать обособленный документ, поддерживающий внесение изменений в изделия с учетом влияния данных изменений на функциональную безопасность	Рекомендуется	Низкий
Систематическая полнота безопасности аппаратных средств				
17	10.1.11	Разработать Спецификацию требований по безопасности контроллера (SRS)	Необходимо	Высокий
18	10.1.11	Разработать план валидации и верификации контроллера (V&V)	Необходимо	Высокий
19	10.1.11	Разработать Руководство по безопасности пользователя (Safety manual). В руководстве по безопасности требования по выделению системы безопасности и по допустимым безопасным конфигурациям	Необходимо	Высокий
20	10.1.11	В качестве мониторинга выполнения программ применить аппаратные или программные средства защиты. Например, watchdog таймеры	Необходимо	Высокий
21	10.1.11	Провести и задокументировать испытания контроллера, функциональные тесты, климатические испытания, ЭМС	Необходимо	Высокий
22	10.1.11	Выполнять разработку (модификацию) контроллера на основании ГОСТ Р МЭК 61508.	Необходимо	Низкий
Результаты оценки случайных отказов аппаратной части устройства (Hardware)				
23	10.2.2	Для соответствия уровню УПБ2 (SIL2) требуется (как минимум, по структурным ограничениям): применение избыточных архитектур (1oo2 с HFT = 1) для модулей ПЛК	Необходимо	Высокий
24	10.2.2	Альтернативным способом достижения целевого уровня полноты безопасности (без избыточных архитектур) является повышение уровня охвата диагностикой. В качестве "уязвимого места" всех модулей контроллера является микроконтроллер.	Рекомендуется	Низкий

НЕДОБРОСОВЕСТНЫЕ ИГРОКИ РЫНКА

НЕЛЕГИТИМНЫЕ СЕРТИФИКАТЫ

На рынке существуют недобросовестные организации, выдающие сертификаты без оценки оборудования.

В ЧЕМ ПРИЧИНА?

1. Отсутствует регулирование добровольных сертификатов соответствия со стороны Росстандарта и ФСА
2. Отсутствует единый реестр сертификатов
3. Сотрудники не обладают соответствующими компетенциями

ОШИБКИ

Нет никаких данных по функциональной безопасности

Система сертификации не относится к функциональной безопасности

Сертификат выдан на основании протокола, в котором, скорее всего, нет никаких данных



ВАЖНО ПРОВОДИТЬ СОВМЕСТНУЮ РАБОТУ ПО КОНТРОЛЮ СЕРТИФИКАТОВ

ТОЛЬКО ТАКИМ ОБРАЗОМ
МЫ СМОЖЕМ ФИЛЬТРОВАТЬ
НЕДОБРОСОВЕСТНЫЕ
СЕРТИФИКАТЫ

КОНТРОЛЬ
ДОБРОВОЛЬНЫХ
СИСТЕМ
СЕРТИФИКАЦИИ
В ОБЛАСТИ ФБ

Росстандарт

СОЗДАНИЕ ЕДИНОГО
РЕЕСТРА ПРОДУКЦИИ
В ОБЛАСТИ ФБ

Заинтересованные лица

ПРОВЕРКА
СЕРТИФИКАТОВ
НА НАЛИЧИЕ
НЕОБХОДИМОЙ
ИНФОРМАЦИИ

Эксплуатирующие организации

СОЗДАНИЕ РЕЕСТРА
ПЕРСОНАЛА И ЭКСПЕРТОВ
В ОБЛАСТИ ФБ

Учебные центры

ВАЖНОСТЬ ТЕХНИЧЕСКОГО ЗАДАНИЯ

Требования к сертификатам необходимо отражать в тех.заданиях и тендерах на поставку оборудования

**СТОЙКОСТЬ
К СИСТЕМАТИЧЕСКИМ
ОТКАЗАМ**

Отражается в сертификате

**ПОЛНОТА
БЕЗОПАСНОСТИ
АППАРАТНЫХ СРЕДСТВ**
включая частоты отказов, долю
безопасных отказов

Отражается в сертификате

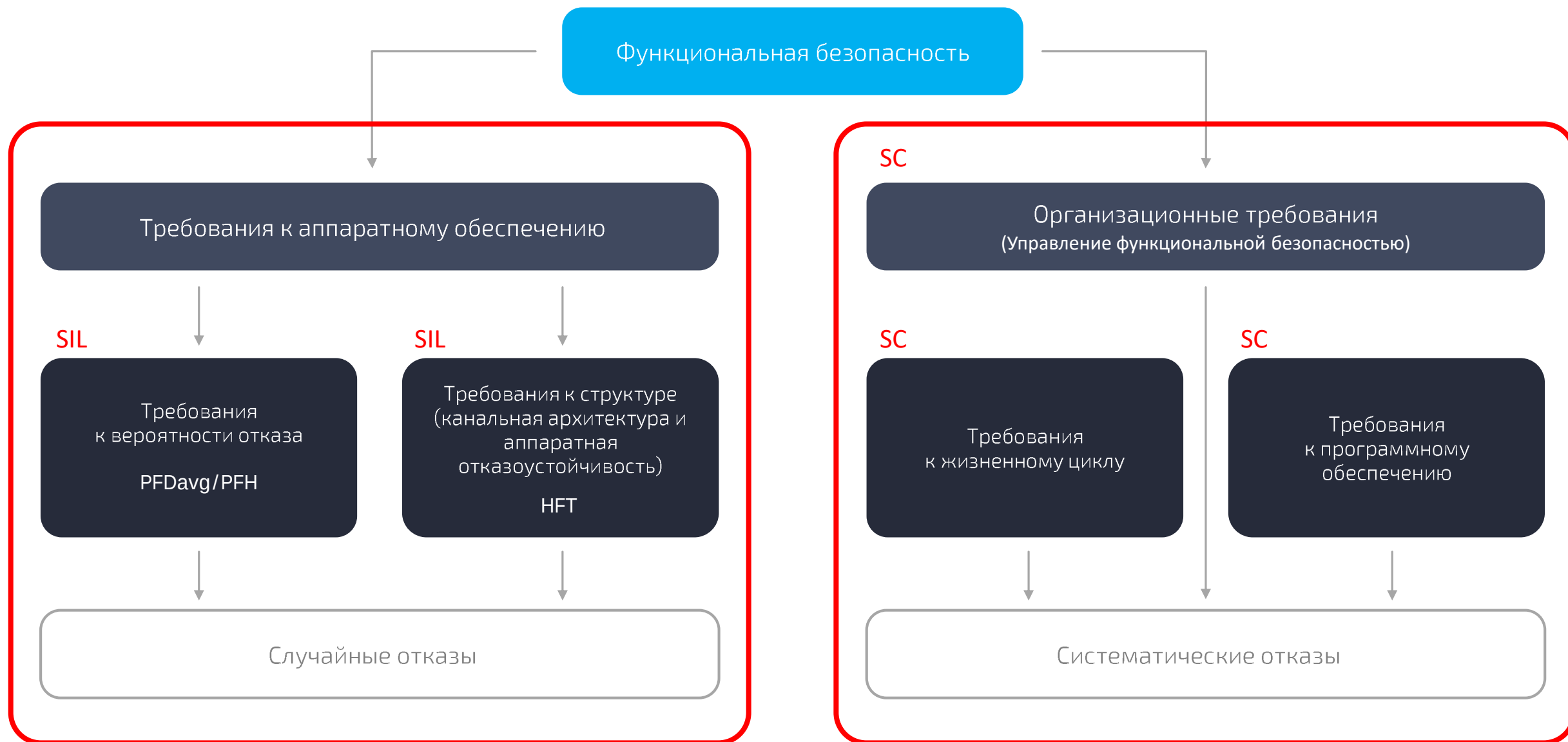
**ОТЧЁТ ИЛИ
ПРОТОКОЛ**
с подробным описанием
оценки изделия и ПО

Прилагается к сертификату

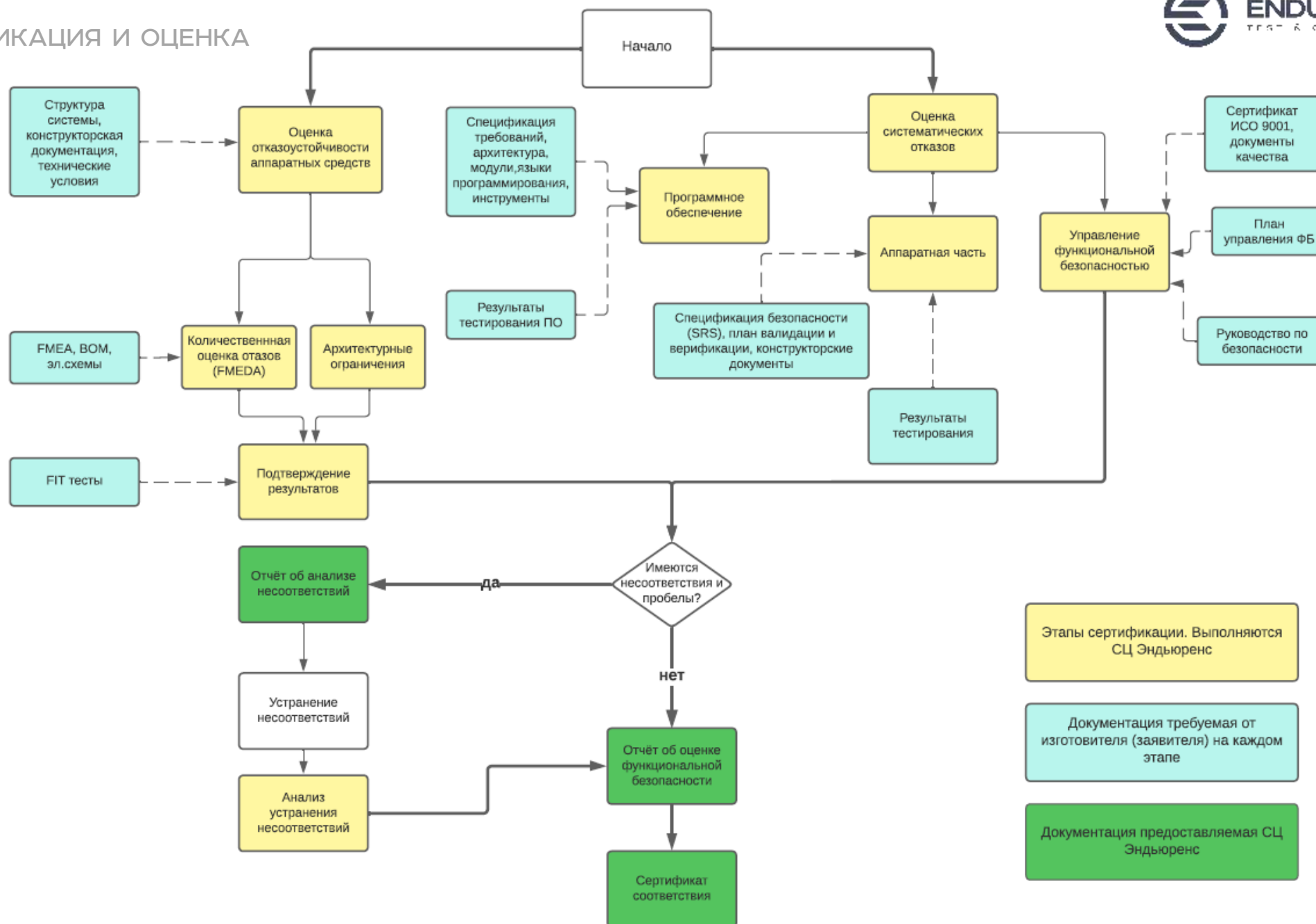
**РУКОВОДСТВО
ПО ФУНКЦИОНАЛЬНОЙ
БЕЗОПАСНОСТИ**
safety manual, требуемый ГОСТ
Р МЭК 61508

Должно быть у изготовителя

ТИПЫ ОТКАЗОВ И ОТКАЗОУСТОЙЧИВОСТЬ ОБОРУДОВАНИЯ



СЕРТИФИКАЦИЯ И ОЦЕНКА



СТОЙКОСТЬ К СИСТЕМАТИЧЕСКИМ ОТКАЗАМ

Что это?

это демонстрация всех этапов процесса проектирования и разработки технического устройства в соответствии с требованиями, предъявляемым к заявляемому уровню полноты безопасности.

Особенность ГОСТ Р МЭК 61508

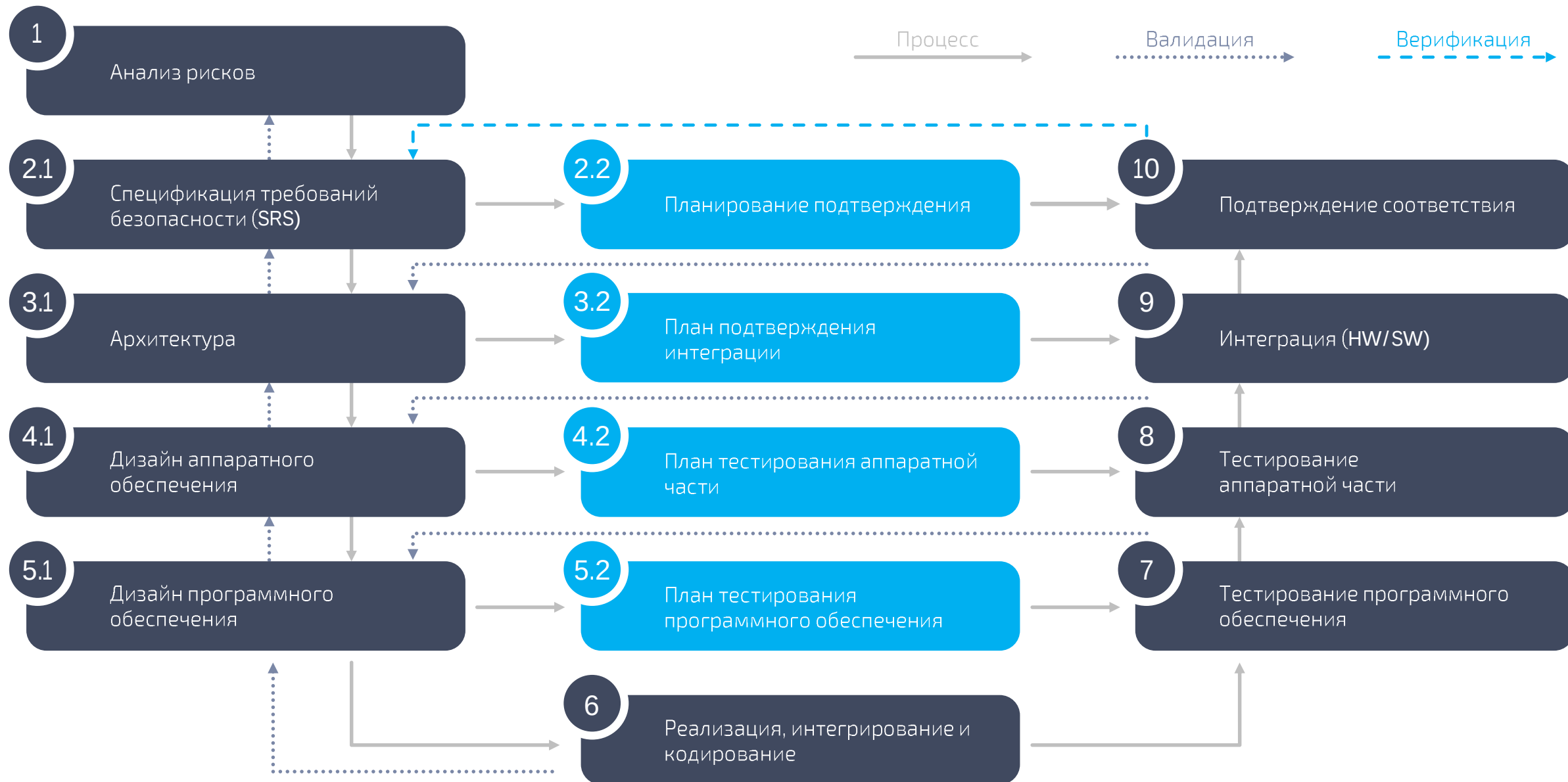
ориентирован на разработку и процесс проектирования, в отличие от ISO 9001 или других стандартов качества

ЦЕЛЬ

Предотвращение внесения систематических ошибок во время разработки и создания аппаратных средств и программного обеспечения в ходе жизненного цикла изделия

С каждым уровнем полноты безопасности требования к предотвращению систематических отказов возрастают

СТРУКТУРА ЖИЗНЕННОГО ЦИКЛА ИЗДЕЛИЯ (HW+SW)



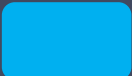
ПРИМЕР

ТРЕБОВАНИЯ ПО ПРЕДОТВРАЩЕНИЮ ОШИБОК

во время формирования спецификации
требований проектирования

ОБОЗНАЧЕНИЯ:

 - низкий

 - средний

 - высокий

Методы/меры, средства	См. МЭК 61508-7	УПБ 1	УПБ 2	УПБ 3	УПБ 4
1. Управление проектами	B.1.1	О (М)	О (М)	О (М)	О (М)
2. Документация	B.1.2	О (М)	О (М)	О (М)	О (М)
3. Разделение Э/Э/ПЭ систем (связаны/не связаны с безопасностью)	B.1.3	КР (HR)	КР (HR)	КР (HR)	КР (HR)
4. Структурирование спецификации	B.2.1	КР (HR)	КР (HR)	КР (HR)	КР (HR)
5. Экспертиза спецификации	B.2.6.	-	КР (HR)	КР (HR)	КР (HR)
6. Полуформальные методы	B.2.3, B7 МЭК 61508-3	Р (R)	Р (R)	КР (HR)	КР (HR)
7. Таблица контрольных проверок	B.2.5	Р (R)	Р (R)	Р (R)	Р (R)
8. Автоматизированные средства разработки спецификаций	B.2.4	-	Р (R)	Р (R)	Р (R)
9. Формальные методы	B.2.2	-	-	Р (R)	Р (R)

ИСПЫТАНИЯ ИЗДЕЛИЙ (Валидация)

СТАНДАРТЫ СЕРИИ ГОСТ Р МЭК 61508 В ЗАВИСИМОСТИ ОТ УРОВНЯ ПОЛНОТЫ БЕЗОПАСНОСТИ ТРЕБУЮТ ПОДТВЕРЖДЕНИЯ БЕЗОПАСНОСТИ (ВАЛИДАЦИИ) ИЗДЕЛИЯ ОПРЕДЕЛЁННЫМИ МЕТОДАМИ (ИСПЫТАНИЯМИ).

К ОСНОВНЫМ ИСПЫТАНИЯМ ОТНОСЯТСЯ:



Функциональное тестирование



Испытание с введением неисправностей



Функциональные испытания в условиях окружающей среды (климатические испытания, вибрация)



Испытания на устойчивость к пиковым выбросам внешних воздействий (ЭМС)

СООТВЕТСТВИЕ ПО

ПО – программное обеспечение

ОБОЗНАЧЕНИЕ РЕКОМЕНДАЦИЙ

HR

Настоятельно рекомендуется применять этот метод/средство для данного уровня полноты безопасности. Если этот метод/средство не используется, то на этапе планирования системы безопасности должно быть дано подробное объяснение со ссылкой на приложение С. Объяснение должно быть согласовано с экспертом.

R

Метод или средство рекомендуется применять для данного уровня полноты безопасности, но степень обязательности рекомендации ниже, чем в случае рекомендации HR.

-

Для данного метода или средства рекомендации ни за ни против не приводятся.

NR

Данный метод/средство не рекомендуется для этого уровня полноты безопасности. Если данный метод/средство применяют, то на стадии планирования системы безопасности этому должно быть дано подробное объяснение со ссылкой на приложение С. Объяснение должно быть согласовано с экспертом.

Разработка, испытание, верификация и подтверждение соответствия программного обеспечения проводится в соответствии с ГОСТ Р МЭК 61508-3-2018

Перечень методов и средств, используемых для разработки ПО для достижения SIL программным обеспечением, приведен в приложениях А и В ГОСТ Р МЭК 61508-3 и в ГОСТ Р МЭК 61508-7.

V-МОДЕЛЬ



— ПРИМЕР ТРЕБОВАНИЙ

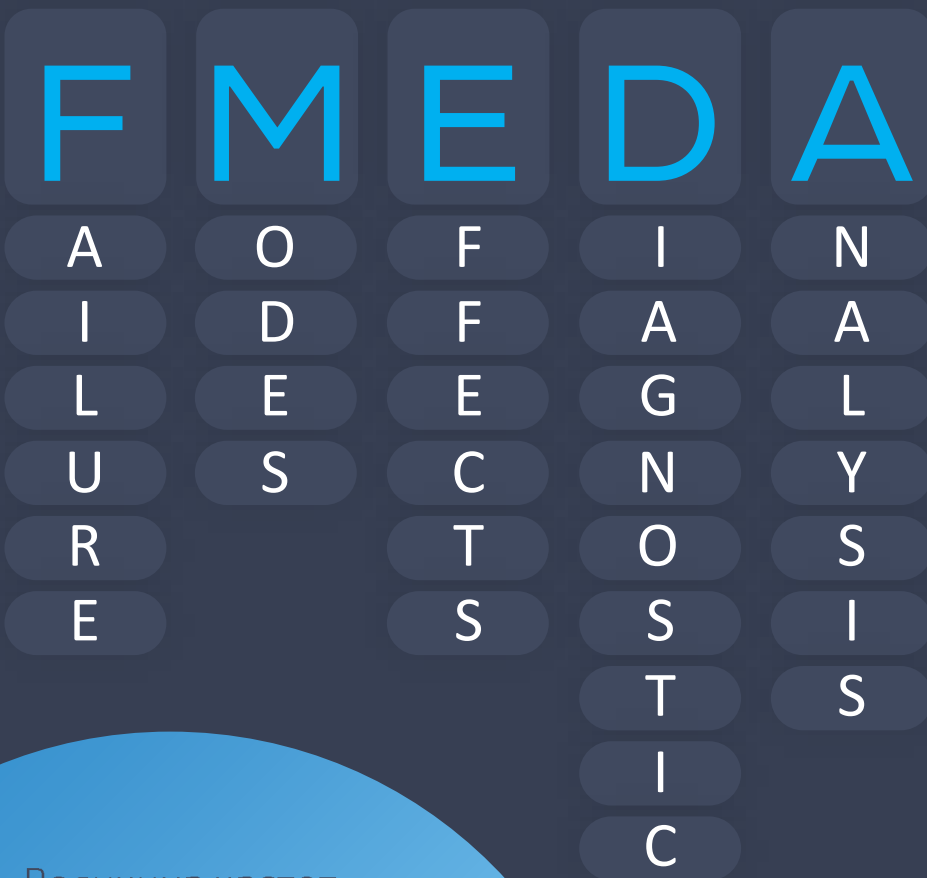
ВЫБОР И ИСПОЛЬЗОВАНИЕ ЯЗЫКОВ ПРОГРАММИРОВАНИЯ

Метод/средство	Ссылка	УПБ 1	УПБ 2	УПБ 3	УПБ 4
1. Выбор соответствующего языка программирования	Таблица В.7	HR	HR	HR	HR
2. Строго типизированные языки программирования	В.2.2, С.2.4	HR	HR	HR	HR
3. Подмножество языка	С.2.11	-	-	HR	HR
4а Сертифицированные средства и сертифицированные трансляторы	С.2.11	R	HR	HR	HR
4б Инструментальные средства, заслуживающие доверия на основании опыта использования	В.2.4.	HR	HR	HR	HR

ПОЛНОТА БЕЗОПАСНОСТИ АППАРАТНЫХ СРЕДСТВ



Количественная оценка случайных отказов



Величина частот отказов и, как следствие, ДБО (SFF), PFDavg, PFH определяются по результатам FMEDA

FMЕА

Анализ режимов отказов и их последствий

это системный способ определения и оценки влияния разных типов отказов компонентов, позволяющий понять, каким образом можно устранить или снизить вероятность отказа, а также документального описания архитектуры устройства.

FMEDA

Анализ режимов отказов, их последствий и диагностики

объединяет стандартные методы FMEA с дополнительными, чтобы определить способы диагностики и режимы отказов, относящиеся к выполнению функции безопасности устройства.

FMEDA АНАЛИЗ

проводимый в процессе сертификации

Обозначение компонента на схеме	Описание компонента	Количество	Режимы отказа	Критичность отказа	Диагностика отказа	Λ	Pct_Lb	Коэфф. каждого отказа	Охват диагностики	Поведение	SD	SU	DD	DU	#
Конденсаторы							100%	20%	0%	S	0,0E+00	0,0E+00	0,0E+00	0,0E+00	0,0E+00
C1, C5	Танталовый Тип A-10B-10мкф±20%	2	К.З	опасный	диагностируемый	2,00E-09	100%	50%	90%	D	0,0E+00	0,0E+00	9E-10	1E-10	0,0E+00
		2	Обрыв	не влияющий	не диагностируемый	2,00E-09	100%	30%	0%	#	0,0E+00	0,0E+00	0,0E+00	0,0E+00	6E-10
		2	Изменение ёмкости до 0,5x	не влияющий	не диагностируемый	2,00E-09	100%	10%	0%	#	0,0E+00	0,0E+00	0,0E+00	0,0E+00	2E-10
		2	Изменение ёмкости до 2x	не влияющий	не диагностируемый	2,00E-09	100%	10%	0%	#	0,0E+00	0,0E+00	0,0E+00	0,0E+00	2E-10

Обозначение компонента на схеме	Описание компонента	Количество	Режимы отказа	Критичность отказа	Диагностика отказа	Пояснение разработчика
Конденсаторы						
C1, C5	Танталовый Тип A-10B-10мкф±20%	2	К.З	опасный	диагностируемый	1.1. C1, C5 – конденсаторы на выходе стабилизаторов, формирующих напряжение +2.5В для питания микроконтроллера и пироприемников (ПП). При К.З напряжение питания уменьшается до 0, что приводит к отказу ИК-датчика. Отказ ИК-датчика выявляется при самодиагностике, соответствующее сообщение выдается по каналам связи (цифровым или аналоговым).
		2	Обрыв	не влияющий	-	1.2. При обрыве C1 (или C5) помехи по цепи питания фильтруются двумя соединенными параллельно керамическими конденсаторами C2 C3 (или C6 C7), т.о. обрыв C1 (или C5) не приводит к изменению показаний.
		2	Изменение ёмкости до 0,5x	не влияющий	-	1.3. Аналогично п. 1.2
		2	Изменение ёмкости до 2x	не влияющий	-	1.4. Аналогично п. 1.3

УВЕЛИЧЕНИЕ ДИАГНОСТИЧЕСКОГО ОХВАТА ЯВЛЯЕТСЯ ОДНИМ ИЗ ОСНОВНЫХ МЕТОДОВ ПОВЫШЕНИЯ УРОВНЯ ПОЛНОТЫ БЕЗОПАСНОСТИ АППАРАТНОЙ ЧАСТИ

Ошибка постоянной памяти
Метод диагностики: контрольная сумма CRC16

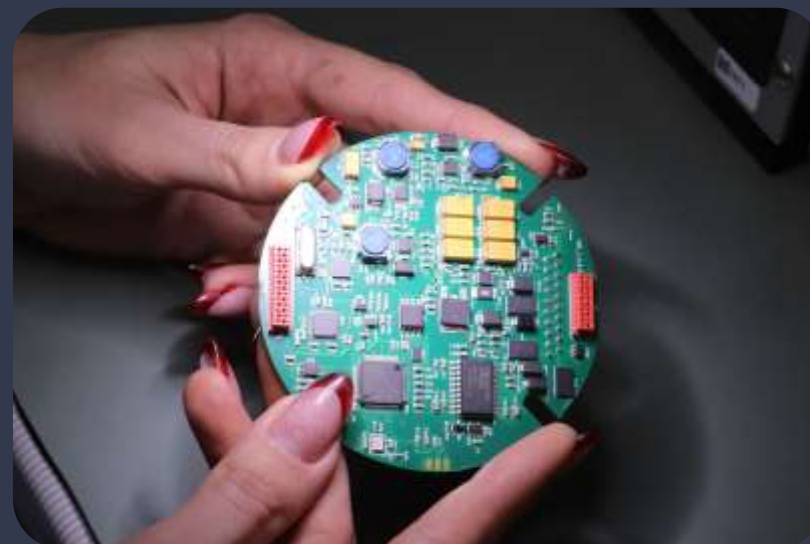


Аварийный сигнал в систему безопасности
о неисправности прибора.
Например, Namur NE43: $\leq 3,6 \text{ mA}$ или $\geq 21,0 \text{ mA}$

ПОДТВЕРЖДЕНИЕ FMEDA

FIT ТЕСТЫ – ПОДТВЕРЖДЕНИЕ FMEDA

В изделие вносятся неисправности и документируется реакция изделия на неисправность. Входными данными являются результаты FMEDA



РЕЗУЛЬТАТЫ АНАЛИЗА УКАЗЫВАЮТСЯ В СЕРТИФИКАТЕ СООТВЕТСТВИЯ И РУКОВОДСТВЕ ПО БЕЗОПАСНОСТИ (SAFETY MANUAL)

для того, что бы конечный пользователь мог применить данное оборудование и рассчитать показатели безопасности приборной системы безопасности

6 Данные по функциональной безопасности

Проведена количественная оценка случайных отказов, согласно которой преобразователи давления измерительные PC и PR модификаций APC-2000.Safety/ALW, APC-2000.Safety/ALW/Ex, APR-2000.Safety/ALW, APR-2000.Safety/ALW/Ex соответствуют:

- Уровню полноты безопасности УПБ 2 (SIL 2) при отказоустойчивости аппаратных средств HFT = 0;
- Уровню полноты безопасности УПБ 3 (SIL 3) при отказоустойчивости аппаратных средств HFT = 1.

Интенсивности отказов преобразователей давления приведены в таблице 1.

Исполнение преобразователя	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	ДБО (SFF)
APC-2000.Safety/ALW, APC-2000.Safety/ALW/Ex	0 FIT ¹⁾	138 FIT	452 FIT	49 FIT	92 %
APR-2000.Safety/ALW, APR-2000.Safety/ALW/Ex	0 FIT	138 FIT	453 FIT	62 FIT	90 %

¹⁾ FIT = 1отказ/10⁹ часов - единица измерения интенсивности отказов.

Изделие	λ_{total}	λ_{SE}	λ_{SD}	λ_{DET}	λ_{DD}	λ_{DU}	SFF %	DC %	MTBF
APC-2000.Safety/ALW	905,321	265,723	0	138,208	451,857	49,533	92,256	90,121	1,105 x 10 ⁶ ч 126,094 лет
APR-2000.Safety/ALW	919,621	265,723	0	138,208	453,387	62,303	90,472	89,919	1,087 x 10 ⁶ ч 124,133 лет

Изделие	T [Proof] - 1 год	T [Proof] - 2 года	T [Proof] - 5 лет	T [Proof] - 10 лет
APC-2000.Safety/ALW	$PFD_{avg} = 2,17 \times 10^{-4}$	$PFD_{avg} = 4,34 \times 10^{-4}$	$PFD_{avg} = 1,08 \times 10^{-3}$	$PFD_{avg} = 2,17 \times 10^{-3}$
APR-2000.Safety/ALW	$PFD_{avg} = 2,73 \times 10^{-4}$	$PFD_{avg} = 5,46 \times 10^{-4}$	$PFD_{avg} = 1,36 \times 10^{-3}$	$PFD_{avg} = 2,73 \times 10^{-3}$

Систематическая полнота безопасности	SC 3 (SIL 3 Capable)
Случайные отказы	Type B Element SIL2@HFT=0; SIL3@HFT=1; Route 1n



ПРИМЕР СЕРТИФИКАТА

Одна из задач системы

ВЕДЕНИЕ ОТКРЫТОГО РЕЕСТРА ПРОДУКЦИИ

По реестру потребители смогут подобрать оборудование

Реестр Продукция					
Views Таблица 1 hidden field Filtered by Продукция Group Sort					
	Но...	Дата окончания действия	Заявитель	Продукция	Изготовитель
1	8	27/6/2024	ООО «ЭРИС»	Газоанализатор стационарный ДГС ЭРИС-ФИД М	ООО «ЭРИС»

Подбор газоанализатора

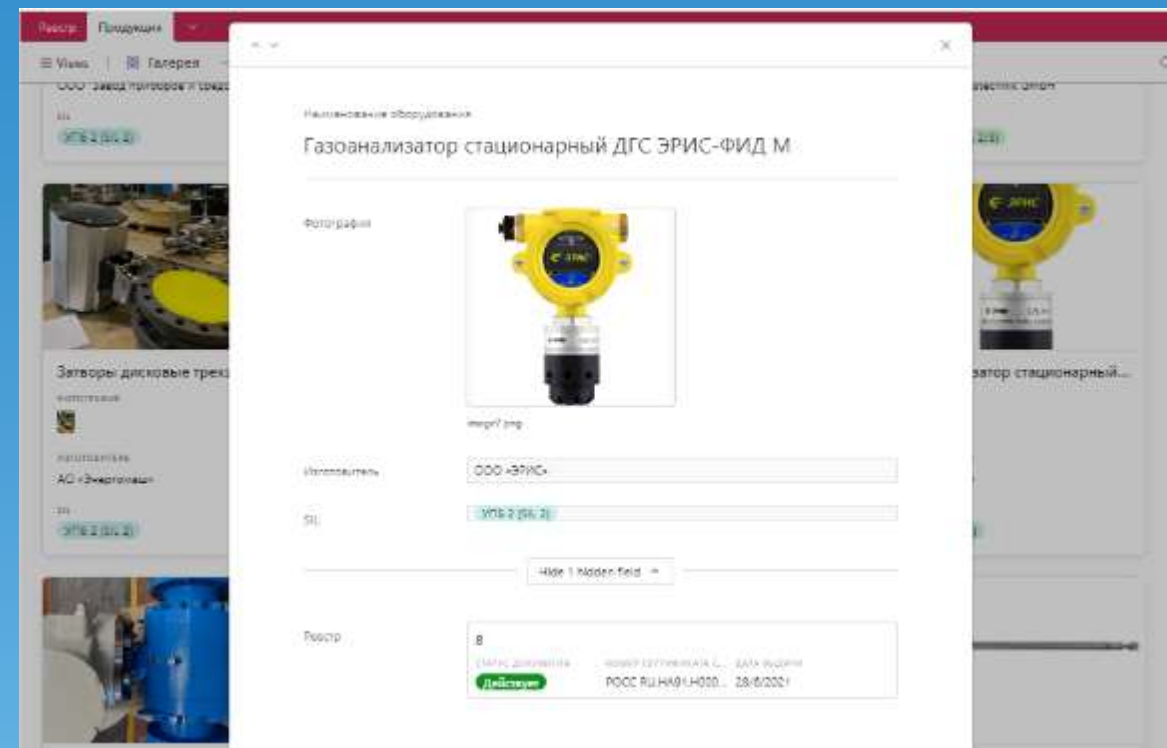
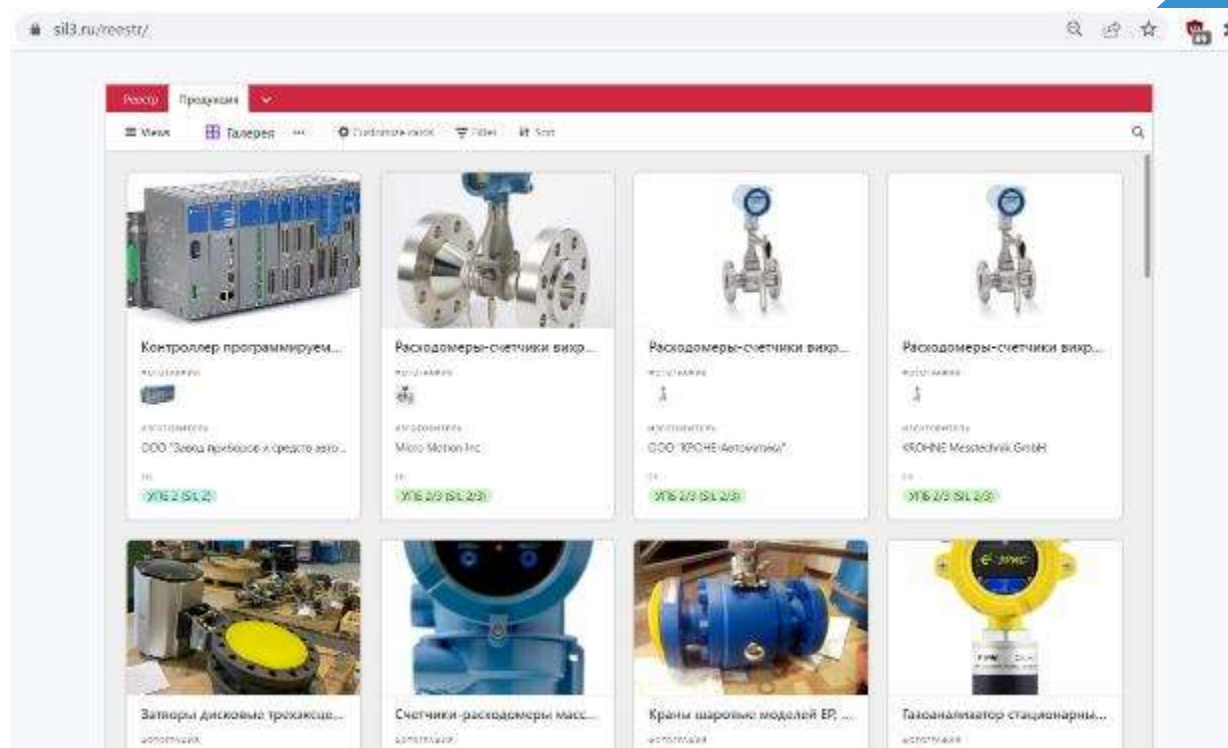


2	2	Расходомеры-счетчики вихревые 8800 (серия 88)	Micro Motion Inc	Контрольно-измерительные приборы
3	3	Расходомеры-счетчики вихревые OPTISWIRL 4200	ООО "КРОНЕ-Автоматика"	Контрольно-измерительные приборы
4	4	Расходомеры-счетчики вихревые OPTISWIRL 4200	KROHNE Messtechnik GmbH	Контрольно-измерительные приборы

Подбор КИП



ОТОБРАЖЕНИЕ ИНФОРМАЦИИ



ОСТАЛИСЬ ВОПРОСЫ?

СВЯЖИТЕСЬ С НАМИ



сайт компании

<https://www.endce.ru>



сайт по функциональной безопасности

<https://sil3.ru/>



e-mail

info@endce.ru



телефон

+7 495 799-07-93



telegram

https://t.me/endurance_msc



@ENDURANCE_MSC