ENDURANCE
TEST & CERTIFICATION

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Отчет об оценке по функциональной безопасности № ФБ01.0078/ФБ от 02.02.2024

Оборудование: Преобразователи уровня радиоволновые волноводные ТЭКФЛЕКС.

Изготовитель: Общество с ограниченной ответственностью «ИНВАРД».

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Оглавление

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

1. Заявитель на сертификацию

Общество с ограниченной ответственностью «ИНВАРД».

Место нахождения (адрес юридического лица) и адрес места осуществления деятельности: 390000, Россия, Рязанская область, город Рязань, улица Маяковского, дом 1А, помещение 51.

2. Изготовитель продукции

Общество с ограниченной ответственностью «ИНВАРД».

Место нахождения (адрес юридического лица) и адрес места осуществления деятельности: 390000, Россия, Рязанская область, город Рязань, улица Маяковского, дом 1А, помещение 51.

3. Наименование продукции

Преобразователи уровня радиоволновые волноводные ТЭКФЛЕКС

4. Перечень стандартов на соответствие которым проведена оценка функциональной безопасности

№	Обозначение стандарта	Наименование стандарта
1	ГОСТ Р МЭК 61508-1-2012	Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования
2	ГОСТ Р МЭК 61508-2-2012	Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам
3	ГОСТ IEC 61508-3-2018	Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению
При составлении отчета учтены положения связанных стандартов		
5	ГОСТ Р МЭК 61508-4-2012	Функциональная безопасность систем электрических, электронных, программируемых электронных связанных с безопасностью. Часть 4. Термины и определения
6	ГОСТ Р МЭК 61508-5-2012	Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности
7	ГОСТ Р МЭК 61508-6-2012	Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р МЭК 61508-3
8	ГОСТ Р МЭК 61508-7-2012	Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

5. Перечень рассмотренной документации

№	Обозначение документа	Наименование документа
1.	ГРВТ.407629.001 ТУ	Технические условия
2.	ГРВТ.407629.001 РЭ	Руководство по эксплуатации
3.	ГРВТ.407629.001 ПС	Паспорт
4.	ГРВТ.407629.001 СБ	Чертёж
5.	ГРВТ.687243.008 Э3	Схема электрическая
6.	ГРВТ.687243.008 ПЭ3	Перечень элементов
7.	ГРВТ.687243.008 СБ	Чертёж
8.	ГРВТ.758720.104	Печатная плата
9.	ГРВТ.687243.068 Э3	Схема электрическая
10	ГРВТ.687243.068 ПЭ3	Перечень элементов
11	ГРВТ.687243.068 СБ	Чертёж
12	ГРВТ.758720.100	Печатная плата
13	ГРВТ.407629.001 ФБ	Руководство по функциональной безопасности
14	РОСС RU.13СМ43.К01326	Сертификат соответствия системы менеджмента качества изготовителя требованиям ГОСТ Р ИСО 9001-2015 (ISO 9001:2015)
15	№ 230507	Протокол испытаний на электромагнитную совместимость
16	№ 230508	Протокол испытаний на электромагнитную совместимость
17	№ 230509	Протокол испытаний на электромагнитную совместимость
18	ЕЭАС N RU Д-RU.PA02.B.57391/23	Декларация о соответствии требованиям ТР ТС 020/2011
19	ЕЭАС RU C-RU.АЖ58.В.03638/23	Сертификат соответствия требованиям ТР ТС 012/2011
20	РИ ГРВТ.03-2023	Управление технической документацией
21	РК СМК 01-2022	Руководство по качеству
22	ДП СМК 02-2022	Управление документированной информацией
23	ДП СМК 05-2022	Управление планами качества
24	ДП СМК 06-2022	Управление персоналом
25	ДП СМК 16-2022	Входной контроль
26	ДП СМК 17-2022	Технический контроль продукции
27	ДП СМК 20-2021	Метрологической обеспечение
28	ДП СМК 23-2022	Управление проектированием и разработкой продукции
29	ДП СМК 28-2022	Порядок проведения испытаний опытных образцов изделий и серийной продукции
30	МИ ГРВТ 04-2023	Управление конструкторской и технологической документацией
31	-	Fmeda анализ устройства
32	-	Описание программного обеспечения
33	-	Протокол приёмо-сдаточных испытаний, технологический паспорт
34	ГРВТ.407629.001 СТБ	Спецификация требований безопасности
35	ГРВТ.407629.001 ППС	План верификации и подтверждения соответствия

6. Термины, определения и сокращения используемые в отчёте

Функциональная безопасность (Functional Safety) – часть общей системы безопасности, обусловленная применением управляемого оборудования и системы управления и зависящая от правильности функционирования электрических/электронных/программируемых электронных систем, связанных с безопасностью, и других средств по снижению риска.

Отказобезопасность – свойства изделия, ориентированные на сохранение безопасности в случае отказа.

Электрическая/электронная/программируемая электронная система; Э/Э/ПЭ-система - система управления, защиты или мониторинга, основанная на использовании одного или нескольких Э/Э/ПЭ устройств, включая все элементы системы, такие как источники питания, датчики и другие устройства ввода, магистрали данных и другие коммуникационные магистрали, исполнительные устройства и другие устройства вывода.

Отказ (failure) - прекращение способности функционального блока выполнять необходимую функцию либо функционирование этого блока любым способом, отличным от требуемого.

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

ДБО (SFF – safety fail fraction) **–** Доля Безопасных Отказов. Свойство элемента, связанного с безопасностью, определяемое отношением суммы средних частот безопасных отказов и опасных обнаруженных отказов к сумме средних частот безопасных и опасных отказов.

λsu – интенсивность необнаруженных безопасных отказов

λsd – интенсивность обнаруженных безопасных отказов

λdu – интенсивность необнаруженных опасных отказов.

λdd – интенсивность обнаруженных опасных отказов.

ОАС (HFT – hardware fault tolerance) **–** Отказоустойчивость Аппаратных Средств.

ОАС = X означает, что X+1 является минимальным числом отказов, которые могут привести к потере функции безопасности.

Средняя вероятность опасного отказа по запросу (probability of dangerous failure on demand, **PFDavg**) **–** средняя неготовность Э/Э/ПЭ системы, связанной с безопасностью, обеспечить безопасность, т.е. выполнить указанную функцию безопасности, когда происходит запрос.

Средняя частота опасного отказа в час (average frequency of a dangerous failure per hour, **PFH**) **–** средняя частота опасного отказа Э/Э/ПЭ системы, связанной с безопасностью, выполняющей указанную функцию безопасности в течение заданного периода времени.

β – эффективность теста по выявлению опасных отказов.

Полнота безопасности (safety integrity) – вероятность того, что система, связанная с безопасностью, будет удовлетворительно выполнять требуемые функции безопасности при всех оговоренных условиях в течение заданного периода времени.

Полнота безопасности программного обеспечения - составляющая полноты безопасности системы, связанной с безопасностью, касающаяся систематических отказов, проявляющихся в опасном режиме и относящихся к программному обеспечению.

Полнота безопасности, касающаяся систематических отказов - составляющая полноты безопасности системы, связанной с безопасностью, касающаяся систематических отказов, проявляющихся в опасном режиме.

Полнота безопасности аппаратных средств - составляющая полноты безопасности системы, связанной с безопасностью, касающаяся случайных отказов аппаратуры, проявляющихся в опасном режиме.

УПБ (SIL – safety integrity level) – Уровень полноты безопасности: дискретный уровень (принимающий одно из четырёх значений), определяющий требования к полноте безопасности для функции безопасности, который ставится в соответствии с Э/Э/ПЭС системам, связанным с безопасностью.

7. Описание оборудования

Преобразователи используют технологию рефлектометрии временного интервала.

Принцип действия преобразователя основан на распространении электромагнитного зондирующего импульса длительностью от 50 до 100 пс по волноводам различной конструкции (стержневой, тросовый или коаксиальный чувствительные элементы). При достижении импульсом границы раздела сред, часть энергии импульса отражается. Амплитуда отраженного импульса определяется разницей диэлектрических проницаемостей граничащих сред. Измеренное значение уровня измеряемой среды пропорционально времени распространения электромагнитного зондирующего импульса до раздела сред и обратно.

В общем случае преобразователи состоят из чувствительного элемента и блока электронного. Структурная схема преобразователей и подробное описание принципа работы и конструкции приведено в руководстве по эксплуатации ГРВТ.407629.001 РЭ.

Функция безопасности преобразователей уровня ТЭКФЛЕКС связана с выдачей токового сигнала 4-20 мА изменяющимся пропорционально измеренному значению уровня. Погрешность безопасности составляет 2%.

HART – сигнал преобразователей уровня не относится к функции безопасности и не должен использоваться как сигнал безопасности в приборных системах безопасности.

В нормальном состоянии выходной сигнал преобразователя находится в состоянии, соответствующим состоянию чувствительного элемента в соответствии с запросом со стороны процесса.

В безопасном состоянии (безопасный отказ) выходной сигнал преобразователя находится в пределах 4-20 мА и превышает заданный пользователем порог срабатывания (для контроля верхнего уровня – увеличение сигнала на 2%, для контроля нижнего уровня – уменьшение сигнала на 2%), что

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

потенциально приводит к ложному срабатыванию системы защиты.

В опасном состоянии (опасный отказ) выходной сигнал преобразователя находится в пределах 4-20 мА и не может достичь заданный пользователем порог срабатывания (для контроля верхнего уровня – уменьшение сигнала на 2%, для контроля нижнего уровня – увеличение сигнала на 2%), что потенциально приводит к несрабатыванию системы защиты.

Рис.1 – Внешний вид преобразователя уровня радиоволнового волноводного ТЭКФЛЕКС

8. Методика оценки функциональной безопасности и краткие требования

8.1 Методика оценки

Оценка функциональной безопасности предполагает оценку всех мер предотвращения отказов на этапе разработки устройства.

Оценка учитывает все требования серии стандартов ГОСТ Р МЭК 61508, за исключением требований, которые были признаны неприменимыми к данному оборудованию.

Оценка укрупнённо заключается в оценке аппаратной части устройства и программного обеспечения, используемого в оборудовании.

Оценка также включает в себя анализ существующих производственных процедур обеспечения качества, чтобы удостовериться в соблюдении требований системы качества и жизненного цикла согласно ГОСТ Р МЭК 61508.

В рамках оценки функциональной безопасности по стандартам ГОСТ Р МЭК 61508 были проверены следующие аспекты:

- Управление функциональной безопасностью, включая обучение и учет компетенции персонала, планирование управления функциональной безопасностью и управление модификациями;
- Процесс определения требований, методик и документирования спецификаций;
- Процесс проектирования, включая разрабатываемую документацию и используемые инструменты;
- Подтверждение соответствия, включая процедуры проверки разработки, планы и протоколы испытаний, процедуры производственных испытаний и документирование информации;
- Проверка соответствия заданным требованиям;
- Процесс изменения и модификации;
- Требования к монтажу, эксплуатации и техническому обслуживанию;
- Система качества производства;
- Конструкция изделия и соответствие аппаратной части заданным требованиям;
- Архитектура устройства и режимы отказов, описанные в отчете по результатам анализа отказов, их последствий и диагностики (FMEDA);
- Оценка программного обеспечения устройства, включая его разработку, тестирование и

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

используемые инструменты.

8.2 Уровень оценки

Оценка оборудования производилась в соответствии со стандартами ГОСТ Р МЭК 61508 до уровня полноты безопасности УПБ 2 (SIL 2).

Все методы и средства используемые в процессе разработки, а также необходимость их применения оценивалась как соответствующие УПБ 2 (SIL 2).

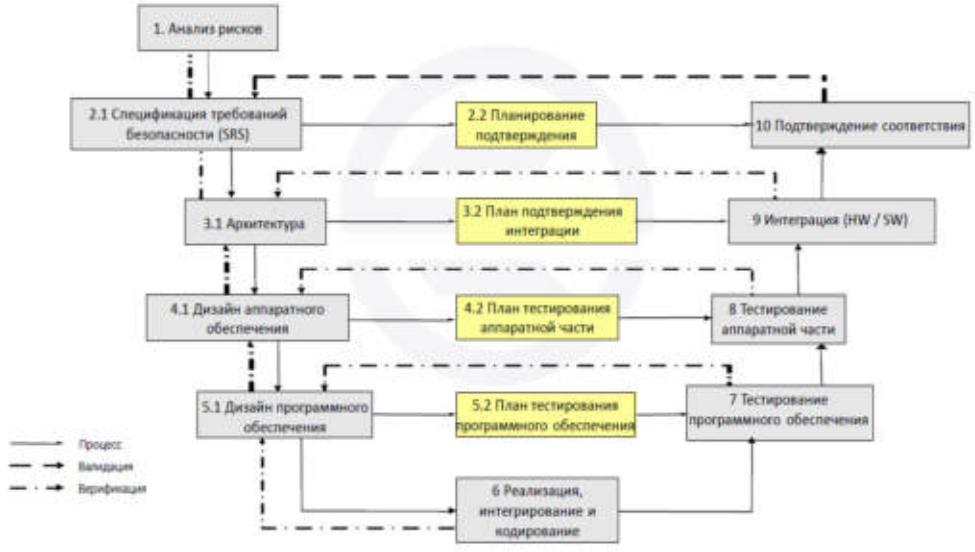
8.3 Описание требований к жизненному циклу.

Жизненный цикл системы безопасности должен соответствовать требованиям раздела 7 ГОСТ Р МЭК 61508-2-2012 с учетом обязательных приложений А и В. Методы и средства, применяемые при разработке жизненного цикла, должны соответствовать заявленному уровню полноты безопасности.

Жизненный цикл состоит из следующих этапов:

- Спецификация требований безопасности;
- Планирование подтверждения соответствия безопасности;
- Проектирование и разработка аппаратного обеспечения;
- Проектирование и разработка программного обеспечения;
- Тестирование аппаратного обеспечения;
- Тестирование программного обеспечения;
- Интеграция;
- Процедуры эксплуатации и технического обслуживания;
- Подтверждение соответствия безопасности;
- Модификация;
- Верификация.

Информация на всех этапах жизненного цикла должна быть документирована, должны быть указаны входы и выходы данного этапа, описаны цели и задачи.



Жизненный цикл безопасности (аппаратная часть и программное обеспечение)

Перечень методов и средств, применяемых на отдельных этапах жизненного цикла, для предотвращения систематических отказов, приведен в приложениях А (таблицы А.15-А.17) и В (таблицы В.1-В.5) ГОСТ Р МЭК 61508-2 и в ГОСТ Р МЭК 61508-7. Для каждого из них приведены рекомендации по необходимости применения для достижения Уровня Полноты Безопасности (SIL). Эти рекомендации обозначаются следующим образом:

М - данные методы или средства требуются обязательно (О) для данного уровня полноты безопасности;

HR - методы или средства крайне рекомендованы (КР) для данного уровня полноты безопасности. Если эти методы или средства не используются, то должно быть приведено подробное обоснование их

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

неиспользования;

R - методы или средства рекомендованы (P) для данного уровня полноты безопасности;

- - методы или средства, не имеющие рекомендаций за и против применения;

NR - методы или средства явно (положительно) не рекомендованы для данного уровня полноты безопасности. В случае применения этих методов или средств должно быть приведено подробное обоснование такого использования.

Требуемую эффективность методов и средств обозначают:

- "низкая (Low)" - данные методы, меры или средства должны использоваться в степени, необходимой для достижения по крайней мере уровня низкой эффективности противодействия систематическим отказам;

- "средняя (Medium)" - данные методы, меры или средства должны использоваться в степени, необходимой для достижения по крайней мере уровня средней эффективности противодействия систематическим отказам;

- "высокая (High)" - данные методы, меры или средства должны использоваться в степени, необходимой для достижения по крайней мере уровня высокой эффективности противодействия систематическим отказам.

8.4 Описание требований к аппаратной части устройства.

Для соответствия аппаратной части необходимому уровню УПБ (SIL) должны выполняться требования к архитектурным ограничениям и вероятностным показателям отказов.

Наиболее высокий уровень полноты безопасности аппаратных средств, который может потребоваться для функции безопасности, ограничен предельными значениями полноты безопасности аппаратных средств, которые достигаются одним из двух возможных способов (реализуемых на уровне системы или подсистемы):

- способ $1_н$ основан на концепции отказоустойчивости аппаратных средств и концепции, составляющей безопасных отказов;

- способ $2_н$ основан на полученных данных о безотказности компонентов, об их использовании конечными пользователями, повышающих уровни доверия и отказоустойчивость аппаратных средств для указанных уровней полноты безопасности.

Величина ДБО (SFF) для способа $1_н$ определяется по результатам Failure modes, effects, and diagnostic analysis (FMEDA). Методика и порядок оценки данным методом описан в Приложении С ГОСТ Р МЭК 61508-6-2012 и рассчитывается по формуле:

$$SFF = \frac{\lambda^{SD} + \lambda^{SU} + \lambda^{DD}}{\lambda^{SD} + \lambda^{SU} + \lambda^{DD} + \lambda^{DU}}$$

Где,

λdd – интенсивность опасных детектируемых отказов;

λsd – интенсивность безопасных детектируемых отказов;

λsu – интенсивность безопасных недетектируемых отказов;

λdu – интенсивность опасных недетектируемых отказов.

Архитектурные требования к устройствам, связанным с безопасностью, изложены в ГОСТ Р МЭК 61508-2-2012 и приведены ниже.

Доля безопасных отказов (ДБО) для компонентов типа А.

Доля безопасных отказов	**Отказоустойчивость аппаратных средств**		
	N = 0	**N = 1**	**N = 2**
Менее 60%	УПБ 1	УПБ 2	УПБ 3
от 60% до менее 90%	УПБ 2	УПБ 3	УПБ 4
от 90% до менее 90%	УПБ 3	УПБ 4	УПБ 4
более и равно 99%	УПБ 3	УПБ 4	УПБ 4

Доля безопасных отказов (ДБО) для компонентов типа В.

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Доля безопасных отказов	Отказоустойчивость аппаратных средств		
	N = 0	N = 1	N = 2
Менее 60%	не оговаривается	УПБ 1	УПБ 2
от 60% до менее 90%	УПБ 1	УПБ 2	УПБ 3
от 90% до менее 99%	УПБ 2	УПБ 3	УПБ 4
более и равно 99%	УПБ 3	УПБ 4	УПБ 4

Данная таблица в зависимости от значений ДБО (четыре диапазона значений) и отказоустойчивость аппаратных средств ОАС, устанавливает максимально обеспечиваемый данным устройством уровень УПБ (SIL) при применении метода 1_H.

Величина отказоустойчивости аппаратных средств определяется в зависимости от канальной архитектуры подсистемы

Определение ОАС (HFT)

Канальная архитектура	**Отказоустойчивость аппаратных средств**
1oo1	0
1oo2	1
1oo3	2
2oo2	0
2oo3	1

Вероятностные требования к функции безопасности, изложены в ГОСТ Р МЭК 61508-1-2012, и приведены ниже.

Вероятностные требования

Уровень полноты безопасности	PFDavg	PFH
УПБ 4	$>10^{-5}$ - $<10^{-4}$	$>10^{-9}$ - $<10^{-8}$
УПБ 3	$>10^{-4}$ - $<10^{-3}$	$>10^{-8}$ - $<10^{-7}$
УПБ 2	$>10^{-3}$ - $<10^{-2}$	$>10^{-7}$ - $<10^{-6}$
УПБ 1	$>10^{-2}$ - $<10^{-1}$	$>10^{-6}$ - $<10^{-5}$

Для систем с архитектурой 1oo1 формула расчёта PFDavg имеет вид:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$PFD_G = (\lambda_{DU} + \lambda_{DD})t_{CE}$$

Где MRT – среднее время ремонта в часах (обычно 8 часов);
MTTR – среднее время восстановления в часах (обычно 8 часов);
Ti – интервал времени между функциональными проверочными тестами (1–5–10 лет), обозначаемый также Tproof;
λdd – интенсивность опасных детектируемых отказов;
λdu – интенсивность опасных недетектируемых отказов

Для систем с архитектурой 1oo2 формула расчёта PFDavg имеет вид:

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

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

$$PFD_G = 2\,((1-\beta_D)\lambda_{DD} + (1-\beta)\,\lambda_{DU})^2\, t_{GE}\, t_{CE} + \beta_D\,\lambda_{DD} MTTR + \beta\,\lambda_{DU}\left(\frac{T_I}{2} + MRT\right)$$

Где MRT – среднее время ремонта в часах (обычно 8 часов);
MTTR – среднее время восстановления в часах (обычно 8 часов);
TI – интервал времени между функциональными проверочными тестами (1–5–10 лет), обозначаемый также Tproof;
λdd – интенсивность опасных детектируемых отказов;
λdu – интенсивность опасных недетектируемых отказов
β – доля необнаруженных отказов, имеющих общую причину (выражается в виде доли в уравнениях и в процентах в других местах) (предполагается, что $\beta = 2 \times \beta_D$)
β_D – доля обнаруженных отказов, которые имеют общую причину
Коэффициент β определяется согласно приложению D ГОСТ Р МЭК 61508-6-2012
Охват диагностикой опасных отказов определяют с помощью следующего выражения

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{total}}$$

Для расчета PFH при архитектуре 1oo1 используют аналогичные значение частот отказов, а также значение t_{CE}

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

Для систем с архитектурой 1oo1:

$$PFH_{1oo1} = \lambda_{DU}$$

Для систем с архитектурой 1oo2:

$$PFH_{1oo2} = 2 \cdot ((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})(1-\beta)\lambda_{DU} t_{CE} + \beta\lambda_{DU}$$

8.5 Описание требований к программному обеспечению устройства.

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

Согласно разделу 1 ГОСТ IEC 61508-3-2018 требования стандарта применяются к любому программному обеспечению, являющемуся частью системы, связанной с безопасностью, либо используемому для разработки системы, связанной с безопасностью. Такое программное обеспечение называется программным обеспечением, связанным с безопасностью.

Программное обеспечение, связанное с безопасностью, включает в себя операционные системы, системное программное обеспечение, программы, используемые в коммуникационных сетях, интерфейсы пользователей и обслуживающего персонала, встроенные программно-аппаратные средства, а также прикладные программы.

Согласно разделу 7 ГОСТ IEC 61508-3-2018 установлены требования к жизненному циклу разработки программного обеспечения.

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Жизненный цикл разработки программного обеспечения выглядит следующим образом:

Жизненный цикл разработки ПО ГОСТ IEC 61508-3-2018 (отдельно от общего жизненного цикла)

Перечень методов и средств, применяемых на отдельных этапах жизненного цикла программного обеспечения, приведен в приложениях А и В ГОСТ IEC 61508-3 и в ГОСТ Р МЭК 61508-7. Для каждого из них приведены рекомендации по необходимости применения для достижения Уровня Полноты Безопасности (SIL) программного обеспечения. Эти рекомендации обозначаются следующим образом:

Рекомендации по методам

HR	Настоятельно рекомендуется применять этот метод или средство для данного уровня полноты безопасности. Если этот метод или средство не используется, то на этапе планирования системы безопасности этому должно быть дано подробное объяснение со ссылкой на приложение С, и это объяснение должно быть согласованно 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 или средство не рекомендуется для этого уровня полноты безопасности. Если данный метод или средство применяют, то на стадии планирования системы безопасности этому должно быть дано подробное объяснение со ссылкой на приложение С, и это объяснение должно быть согласованно с экспертом.

Дополнительно ГОСТ IEC 61508-3-2018 разделяет программные средства, работающие в автономном режиме и неавтономном режиме. К средствам, работающим в неавтономном режиме (режиме реального времени), относятся операционная система реального времени, прикладные программы, коммуникационный софт. К такому программному обеспечению применяются все требования ГОСТ IEC 61508-3-2018. К средствам, работающим в автономном режиме, относятся средства поддержки проектирования (редактор кода, компилятор, среда программирования, средства тестирования, анализатор кода).

Средства поддержки программного обеспечения, работающие в автономном режиме можно разделить на следующие классы:

класс Т1 - не генерирует программ, которые явно или неявно включаются в рабочую программу

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

(включая данные) системы, связанной с безопасностью.

Примечание -Примерами класса Т1 являются: текстовый редактор или средства поддержки проектирования, написанные не на автокоде;

класс Т2 - включает в себя средства тестирования или верификации проекта либо рабочей программы, причем такие, ошибки в которых могут привести к сбою при обнаружении ошибок в рабочей программе, но эти средства не могут создавать ошибки в самой рабочей программе.

Примечание -Примерами класса Т2 являются: генератор тестовых программ, средства измерения тестового охвата, средства статического анализа;

класс Т3 - генерирует программы, которые явно или неявно включаются в рабочую программу системы, связанной с безопасностью. Примерами класса Т3 являются: оптимизирующий компилятор, связь между исходным кодом программы и сгенерированным объектным кодом, которого не очевидна, компилятор, который включает исполнимый пакет программ в рабочую программу.

В зависимости от влияния средства поддержки программного обеспечения в автономном режиме на функцию безопасности, такое программное обеспечение относится к связанному с безопасностью.

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

9. Результаты оценки функциональной безопасности

9.1 Процессы жизненного цикла изделия и меры предотвращения систематических отказов

В ходе оценки жизненного цикла устройства к проверялось соответствие стандарту ГОСТ Р МЭК 61508 в части процессов, процедур и методов, используемых при проектировании и разработке заявленного изделия на соответствие уровню полноты безопасности УПБ 2.

В компании Общество с ограниченной ответственностью «Инвард» внедрен процесс управления жизненным циклом изделия, что описано в руководстве по качеству, а также документе ДП СМК 23-2022.

Спецификация требования к оборудованию описана в технических условиях, а также в отдельных спецификациях безопасности (ГРВТ.407629.001 СТБ). Проведение испытаний изделия описаны также в технических условиях, а также в отдельных методиках испытаний на соответствующие показатели.

Установленный процесс внесения изменений описан в документе по качеству МИ ГРВТ 04-2023.

Конструкция изделия включает в себя программное обеспечение, которое также имеет необходимый жизненный цикл с применением методов соответствующих уровню УПБ 2. Подробный отчёт соответствия программного обеспечения приведён в разделе 9.3 данного отчёта.

9.1.1 Управление функциональной безопасностью

Планирование управления функциональной безопасностью

В компании реализован процесс проектирования и разработки изделий. Установлены обязательные требования к проектированию наряду с требованиями к проверке и испытаниям изделия. Это описано в технических условиях на продукцию, а также отдельных документах по качеству. Процесс внесения изменений описан в документе по качеству МИ ГРВТ 04-2023. Данный процесс и входящие в него процедуры отвечают требованиям ГОСТ Р МЭК 61508.

Управление версиями

Внесение изменений в техническую документацию происходит в соответствии документом по качеству ДП СМК 02-2022.

Обучение, компетентность сотрудников

Управление персоналом описано в документе по качеству РК СМК 01-2022. Все сотрудники проходят периодическую подготовку и обучение в соответствии с занимаемыми должностями и производственной необходимостью.

9.1.2 Описание требований безопасности и проектирования.

Общие требования к конструкции изделия описаны в технических условиях. При создании устройства создаётся техническое задание и спецификация требований безопасности. Также создаются спецификации, рабочие чертежи, схемы, процедуры изготовления отдельных элементов и требования к производственной среде при изготовлении.

В процессе задания спецификаций используются методы управления проектами, управление документацией, структурирование спецификаций. Согласно ГОСТ Р МЭК 61508-2-2012, Таблица В.1, данных методов достаточно для достижения требуемого уровня полноты безопасности УПБ 2.

Применение полуформальных методов не требуется.

Методы и средства по предотвращению ошибок во время формирования спецификации требований проектирования

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для заявляемого устройства.	Максимально достижимый уровень УПБ
1 Управление проектами	О (М) низкий	Применяется в соответствии с системой менеджмента качества	УПБ 3
2 Документация	О (М) низкий	Применяется	УПБ 3

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

3 Разделение Э/Э/ПЭ систем, связанных с безопасностью, и систем, не связанных с безопасностью	КР (HR) низкий	Не применяется.	УПБ 2
4 Структурирование спецификации	КР (HR) низкий	Применяется.	УПБ 3
5 Экспертиза спецификации	КР (HR) низкий	Применяется	УПБ 2
6 Полуформальные методы	Р (R) низкий	Не применяется	УПБ 2
7 Таблица контрольных проверок	Р (R) низкий	Не применяется	УПБ 3
8 Автоматизированные средства разработки спецификаций	Р (R) низкий	Не применяется	УПБ 3
9 Формальные методы	низкий	Не применяется	УПБ 3
Итоговый достигнутый уровень УПБ			УПБ 2

9.1.3 Изготовление и разработка устройства

В процессе проектирования и изготовления устройства применяются методы соблюдения руководящих материалов и стандартов, управление проектами, документация. Согласно ГОСТ Р МЭК 61508-2-2012, Таблица В.2, данных методов достаточно для достижения требуемого уровня полноты безопасности УПБ 2.

Методы и средства по предупреждению внесения ошибок во время проектирования и разработки

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для заявляемого устройства.	Максимально достижимый уровень УПБ
1 Соблюдение руководящих материалов и стандартов	О (М) высокий	Применяется в соответствии с системой менеджмента качества	УПБ 3
2 Управление проектами	О (М) низкий	Применяется в соответствии с системой менеджмента качества	УПБ 3
3 Документация	О (М) низкий	Применяется	УПБ 3
4 Структурное проектирование	КР (HR) низкий	Применяется	УПБ 2
5 Модульное Проектирование	КР (HR) низкий	Применяется, во время разработки части электроники прибора разбиваются на функциональные модули	УПБ 3

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

6 Использование достоверно испытанных компонентов	P (R) низкий	Не применяется	УПБ 2
7 Полуформальные методы	P (R) низкий	Не применяется	УПБ 2
8 Таблица контрольных проверок	P (R) низкий	Не применяется	УПБ 3
9 Средства автоматизированного проектирования	P (R) низкий	Не применяется	УПБ 2
10 Моделирование	P (R) низкий	Не применяется	УПБ 3
11 Сквозной анализ или поверка аппаратных средств	P (R) низкий	Не применяется	УПБ 3
12 Формальные методы	низкий	Не применяется	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 2**

9.1.4 Интеграция и подтверждение соответствия

Процесс подтверждения правильности описан в документах системы качества изготовителя таких как технические условия, программы-методики испытаний в процессе изготовления. Все устройства проходят приёмосдаточные испытания на заводе-изготовителе в объёме, установленном требованиями проекта.

В процессе испытаний проводится функциональное тестирование, управление проектом, документирование, испытания в условиях окружающей среды. Согласно ГОСТ Р МЭК 61508-2-2012, Таблица В.3, Таблица В.5 данных методов достаточно для достижения требуемого уровня полноты безопасности УПБ 2.

Методы и средства для предотвращения ошибок на стадии интеграции

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для заявляемого устройства.	Максимально достижимый уровень УПБ
1 Функциональное тестирование	O (M) высокий	Применяется. Каждый модуль тестируется как отдельно, так в сборе, для подтверждения соответствия заявленным характеристикам.	УПБ 3
2 Управление проектами	O (M) низкий	Применяется в соответствии с системой менеджмента качества	УПБ 3
3 Документация	O (M) низкий	Применяется.	УПБ 3
4 Тестирование методом "черного ящика"	P (R) низкий	Применяется.	УПБ 3

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

5 Полевые испытания	P (R) низкий	Применяется.	УПБ 3
6 Статистическое тестирование	- низкий	Не применяется	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 3**

Методы и средства по предотвращению ошибок при подтверждении соответствия безопасности

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для заявляемого устройства.	Максимально достижимый уровень УПБ
1 Функциональное тестирование	КР (HR) высокий	Применяется в соответствии со внутренними документами, регламентирующими процедуры проверки.	УПБ 3
2 Функциональные испытания в условиях окружающей среды	КР (HR) высокий	Применяется в соответствии со внутренними документами, регламентирующими процедуры проверки.	УПБ 3
3 Испытания на устойчивость к пиковым выбросам внешних воздействий	КР (HR) высокий	Применяется в соответствии со внутренними документами, регламентирующими процедуры проверки.	УПБ 3
4 Испытание с введением неисправностей (при требуемом охвате диагностикой >= 90%)	КР (HR) высокий	Применяется	УПБ 3
5 Управление проектами	О (M) низкий	Применяется	УПБ 3
6 Документация	О (M) низкий	Применяется	УПБ 3
7 Статический анализ, динамический анализ, анализ отказов	P (R) низкий	Не применяется	УПБ 2
8 Моделирование и анализ отказов	P (R) низкий	Не применяется	УПБ 3
9 Анализ наихудшего случая, динамический анализ и анализ отказов	средний	Не применяется	УПБ 3
10 Статический анализ и анализ отказов	P (R) низкий	Не применяется	УПБ 2
11 Расширенное функциональное тестирование	КР (HR) низкий	Применяется для условий эксплуатации, прописанных в эксплуатационной документации.	УПБ 3

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

12 Тестирование методом "черного ящика"	P (R) низкий	Не применяется	УПБ 2
13 Испытание с введением неисправностей (при требуемом охвате диагностикой >= 90%)	P (R) низкий	Не применяется.	УПБ 2
14 Статистическое тестирование	- низкий	Не применяется.	УПБ 3
15 Испытания в наихудших случаях	- низкий	Не применяется.	УПБ 3
16 Полевые испытания	P (R) низкий	Не применяется.	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 2**

9.1.5 Проверка соответствия заданным требованиям

Для каждого этапа проектирования и изготовления установлены задачи, необходимые исходные и итоговые документы, а также процедуры контроля и испытаний. Данные методы являются достаточными для достижения требуемого уровня полноты безопасности УПБ 2.

9.1.6 Внесение изменений

Перед утверждением все изменения рассматриваются и анализируются на предмет их влияния на проект и функции безопасности. Все изменения оформляются документально, и соответствующая информация вносится в необходимую техническую и проектную документацию. На предприятии имеются отдельно разработанные документы системы менеджмента качества по внесению изменений в конструкцию изделий и техническую документацию. Данные методы являются достаточными для достижения требуемого уровня полноты безопасности УПБ 2.

9.1.7 Эксплуатационная документация

В состав эксплуатационной документации входят:

- Руководство по эксплуатации;
- Паспорт;
- Руководство по функциональной безопасности.

Руководство по функциональной безопасности совместно с руководством по эксплуатации соответствуют требованиям ГОСТ Р МЭК 61508-2-2012, Приложение D и содержит необходимую информацию:

- функциональную спецификацию выполняемых функций;
- идентификацию конфигурации аппаратных средств и программного обеспечения;
- ограничения на использование применяемого изделия;
- виды отказов применяемого изделия;
- предполагаемую интенсивность отказов;
- диагностический испытательный интервал.

Руководство по функциональной безопасности содержит информацию о частоте отказов, режимах отказов и предлагаемых контрольных испытаниях.

Инструкции по эксплуатации учитывают удобство для пользователей, удобство для технического обслуживания, руководство проектом, документальное оформление, ограниченные возможности эксплуатации и допуск к эксплуатации только квалифицированного персонала. Данные методы соответствуют требованиям ГОСТ Р МЭК 61508-2-2012, Таблица В.4 и данных методов достаточно для достижения требуемого уровня полноты безопасности УПБ 2.

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Методы и средства по предотвращению ошибок и отказов в период эксплуатации и технического обслуживания

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для заявляемого устройства.	Максимально достижимый уровень УПБ
1 Инструкции по эксплуатации и техническому обслуживанию	КР (HR) высокий	Применяется	УПБ 3
2 Удобство общения с пользователем	КР (HR) высокий	Применяется	УПБ 3
3 Удобство общения с обслуживающим персоналом	КР (HR) высокий	Применяется	УПБ 3
4 Управление проектами	О (M) низкий	Применяется	УПБ 3
5 Документация	О (M) низкий	Применяется	УПБ 3
6 Сокращение работ на стадии эксплуатации	Р (R) низкий	Не применяется	УПБ 2
7 Защита от ошибок оператора	Р (R) низкий	Не применяется	УПБ 2
8 Эксплуатация только квалифицированным оператором	Р (R) низкий	Не применяется	УПБ 2
Итоговый достигнутый уровень УПБ			**УПБ 2**

9.1.8 Систематическая полнота безопасности. Управление отказами при проектировании, отказы, связанные с внешними нагрузками, отказы на стадии эксплуатации.

В процессе разработки устройства учтены обязательные требования по следующим аспектам систематических отказов:

- управления отказами, связанными с проектированием аппаратных средств;
- управления отказами, вызванными внешними нагрузками или влияниями;
- управления отказами на стадии эксплуатации.

Методы и средства управления систематическими отказами, источниками которых являются этапы разработки аппаратных средств

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для заявляемого устройства.	Максимально достижимый уровень УПБ

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

1 Мониторинг последовательности выполнения программ	КР (HR) низкий	Применяется, сторожевой таймер	УПБ 2
2 Обнаружение отказов путем мониторинга в режиме онлайн	Р (R) низкий	Применяется	УПБ 3
3 Тестирование избыточными аппаратными средствами	Р (R) низкий	Не применяется	УПБ 2
4 Стандартный тестовый порт доступа и архитектура граничного сканирования	Р (R) низкий	Не применяется	УПБ 3
5 Кодовая защита	Р (R) низкий	Не применяется	УПБ 3
6 Разнообразие аппаратных средств	низкий	Не применяется	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 2**

Методы и средства управления систематическими отказами, вызванными внешними нагрузками или влияниями

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для заявляемого устройства.	Максимально достижимый уровень УПБ
1 Меры против пропадания напряжения, изменений напряжения, перенапряжения, низкого напряжения и других явлений, таких как изменение частоты переменного тока электропитания, которое	О (М) средний	Применяется (фильтрация помех на уровне схемотехники)	УПБ 3
2 Разделение линий электрического питания и линий передачи информации	О (М)	Применяется (линии питания и передачи информации разделены)	УПБ 3
3 Повышение устойчивости к электромагнитным воздействиям	О (М) низкий	Применяется, фильтрация помех на уровне схемотехники.	УПБ 3

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

4 Средства против физического воздействия окружающей среды (например, температуры, влажности, воды, вибраций, пыли, разъедающих веществ)	O (M) высокий	Применяется, платы покрыты защитным составом, внешний корпус имеет защиту IP	УПБ 3
5 Мониторинг последовательности выполнения программ	КР (HR) низкий	Применяется	УПБ 3
6 Меры против повышения температуры	КР (HR) низкий	Применяется, измерение и защита от перегрева реализована на уровне схемотехники и встроенного ПО.	УПБ 3
7 Пространственное разделение групповых линий	КР (HR) низкий	Применяется.	УПБ 3
8 Принцип реактивного тока (нет необходимости в непрерывном контроле для достижения или поддержки безопасного состояния УО)	Р (R)	Применяется. Контактная группа реле неисправности размыкается при пропадании питания.	УПБ 3
9 Средства обнаружения обрывов и коротких замыканий в линиях передачи сигналов	Р (R)	Применяется на уровне схемотехники.	УПБ 3
10 Обнаружение отказов путем мониторинга в режиме онлайн	Р (R) низкий	Применяется, на уровне схемотехники и встроенного ПО.	УПБ 3
11 Тестирование избыточными аппаратными средствами	Р (R) низкий	Не применяется	УПБ 2
12 Кодовая защита	Р (R) низкий	Не применяется	УПБ 3
13 Передача неэквивалентных сигналов	Р (R) низкий	Не применяется	УПБ 3
14 Разнообразие аппаратных средств	низкий	Не применяется	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 2**

Методы и средства управления систематическими отказами при эксплуатации

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для заявляемого устройства.	Максимально достижимый уровень УПБ

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

1 Защита от модификаций	O (M) средний	Применяется.	УПБ 3
2 Обнаружение отказов путем мониторинга в режиме	P (R) низкий	Применяется.	УПБ 3
3 Подтверждение ввода	P (R) низкий	Не применяется	УПБ 2
4 Программирование с проверкой ошибок	P (R) низкий	Не применяется	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 2**

Вывод по оценке жизненного цикла устройства: Процессы жизненного цикла изделия и меры предотвращения систематических отказов соответствуют требуемому уровню полноты безопасности УПБ 2 (SIL 2).

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

9.2 Результаты оценки случайных отказов аппаратной части устройства

9.2.1 Методика оценки

В соответствии с приложением С ГОСТ Р МЭК 61508-2-2012 Охват диагностикой и доля безопасных отказов элемента рассчитываются следующим образом:

a) проводят анализ видов отказов и их влияния для определения влияния каждого вида отказов каждого компонента или группы компонентов в элементе на поведение Э/Э/ПЭ систем, связанных с безопасностью, в отсутствие диагностических проверок.

b) все виды отказов делят на категории по признаку, является ли он (в отсутствие диагностических испытаний):
- безопасным отказом или
- опасным отказом;

c) отказы компонентов, не принадлежащих Э/Э/ПЭ системе, связанной с безопасностью, а также отказы, не влияющие на поведение Э/Э/ПЭ системы, связанной с безопасностью, не должны учитываться при вычислении охвата диагностикой (ОД) или доли безопасных отказов (ДБО);

d) оценив частоты отказов каждого компонента или группы компонентов и с учетом видов отказов и результатов анализа последствий каждого вида отказа каждого компонента или группы компонентов, вычисляют частоту безопасных отказов и частоту опасных отказов . Если одна из этих интенсивностей отказов не будет иметь постоянного значения, то необходимо оценить ее среднее число за конкретный период времени и использовать для вычислений ОД и ДБО;

e) оценивают для каждого компонента или группы компонентов доли опасных отказов, которые могут быть обнаружены диагностическими тестами и, следовательно, частоты опасных отказов, обнаруженных диагностическими тестами;

f) вычисляют полные частоты опасных отказов, полные частоты опасных отказов, обнаруженных диагностическими тестами, и полные частоты безопасных отказов;

g) вычисляют охват диагностикой элемента;

h) вычисляют долю безопасных отказов элемента.

При вычислении охвата диагностикой для элемента (см. приложение С.1 ГОСТ Р МЭК 61508-2-2012) для каждого компонента или группы компонентов необходимо оценить долю опасных отказов, обнаруживаемых диагностическими тестами. Диагностические тесты, которые могут внести вклад в охват диагностикой, включают в себя (но не ограничиваются) такие меры, как:

- сравнительные проверки, например контроль и сравнение избыточных (резервных) сигналов;
- дополнительные встроенные тестовые программы, например вычисление контрольных сумм в устройстве памяти;
- контроль с помощью внешних воздействий, например пропусканием импульсного сигнала через контролируемые тракты;
- непрерывный контроль аналогового сигнала, например для обнаружения выхода из диапазона уровней показаний при отказе сенсора.

Рекомендуемые методы и средства диагностического тестирования (испытания) и рекомендуемые максимальные диагностические охваты, которые могут потребоваться, приведены в таблицах А.2-А.14 ГОСТ Р МЭК 61508-2-2012. Эти тесты проводят непрерывно или периодически (в зависимости от интервала диагностического тестирования).

Для определения интенсивностей отказов и доли безопасных отказов специалистами ООО СЦ "Эндьюренс" совместно с Общество с ограниченной ответственностью «Инвард» был выполнен **FMEDA** анализ устройства и проанализированы его результаты.

Анализ режимов отказов и их последствий (FMEA) — 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.

Анализ режимов отказов, их последствий и диагностики (FMEDA) — это расширенная версия FMEA. Данный метод объединяет стандартные методы FMEA с дополнительными методами, чтобы определить способы диагностики и режимы отказов, относящиеся к выполнению функции безопасности устройства.

Следующие **исходные предпосылки** были сделаны при анализе видов, эффектов и диагностики отказов:

- Интенсивность отказов является постоянной величиной;
- Отказы, возникающие в процессе задания параметров не рассматриваются;
- Устройство относится к компоненту типа В по ГОСТ Р МЭК 61508-1-2012;

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

- Отказом оборудования и модулей, входящих в состав, считается невозможность выполнения заявленных функций безопасности;

Данные по интенсивности отказов взяты из Siemens Standard SN 29500 являющимся надежным источником;

Приведенные интенсивности отказов соответствуют типичным условиям эксплуатации на промышленных предприятиях, описанным в стандарте МЭК 60654-1, класс С.

9.2.2 Сводные значения и результаты оценки случайных отказов аппаратной части.

Сводные значения результатов расчета показателей уровня полноты безопасности приведены в таблице.

Исполнение по выходному сигналу	λsd, FIT	λsu, FIT	λdd, FIT	λdu, FIT	ДБО (SFF), %	PFD_{avg}	PFH, 1/час
АЦ, А2Ц	0	89	872	87	91,7	$3{,}79 \cdot 10^{-4}$	$8{,}66 \cdot 10^{-8}$

1) FIT = 1отказ/10^{9} часов - единица измерения интенсивности отказов.
2) PFD_{avg} рассчитано для Troof = 1 год

PFH/PFDavg всей системы с учетом избыточных архитектур, интервала контрольных испытаний, эффективности контрольных проверок, любой автоматической диагностики, среднего времени ремонта и конкретной частоты отказов всех элементов системы, включенных в SIF. Каждый элемент должен быть проверен на соответствие минимальным требованиям отказоустойчивости оборудования (HFT).

9.2.3 Выводы по оценке аппаратной части

В процессе FMEDA анализа проанализированы режимы отказов оборудования и их частоты отказов.

В результате FMEDA анализа выявлено соответствие устройства уровню полноты безопасности УПБ 2 (SIL 2) при отказоустойчивости аппаратных средств ОАС (HFT) = 0.

Уровень полноты безопасности УПБ (SIL) всей инструментальной функции безопасности (SIF), в которой применяется изделие должен быть проверен путем расчета PFH/PFDavg всей системы с учетом избыточных архитектур, интервала контрольных испытаний, эффективности контрольных проверок, любой автоматической диагностики, среднего времени ремонта и конкретной частоты отказов всех элементов системы, включенных в SIF. Каждый элемент должен быть проверен на соответствие минимальным требованиям отказоустойчивости оборудования (HFT).

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

9.3 Результаты оценки программного обеспечения.

9.3.1 Общие данные о программном обеспечении

Программное обеспечение преобразователей является прикладной программой которая выполняется микроконтроллером серии STM32.

ПО написано на расширенном языке программирования “C” при использовании интегрированной среды разработки CodeBlocks 12.11 STM32.

Управление версиями осуществляется программной контроля версий GIT.

9.3.2 Спецификация требований к программному обеспечению системы безопасности

В ходе разработки программного обеспечения задаются спецификации требований к ПО. Составляется спецификации требований безопасности программного обеспечения. Спецификация задаётся в свободном виде.

Методы спецификации требований к программному обеспечению системы безопасности

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства	Максимально достижимый уровень УПБ
1a Полуформальные методы	R	Не применяются	УПБ 2
1b Формальные методы	R	Не применяется	УПБ 2
2 Прямая прослеживаемость между требованиями к системе безопасности и требованиями к программному обеспечению системы безопасности	R	Не применяется	УПБ 2
3 Обратная прослеживаемость между требованиями к системе безопасности и предполагаемыми потребностями безопасности	R	Не применяется	УПБ 2
4 Компьютерные средства разработки спецификаций для поддержки перечисленных выше подходящих методов/средств	R	Не применяется	УПБ 2
Итоговый достигнутый уровень УПБ			**УПБ 2**

Полуформальные методы

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1 Логические/ функциональные блок-схемы	R	Не применяется	УПБ 2
2 Диаграммы последовательности действий	R	Не применяется	УПБ 2
3 Диаграммы потоков данных	R	Не применяется	УПБ 3

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
4a Конечные автоматы/диаграммы переходов	R	Не применяется	УПБ 2
4b Моделирование во времени сетями Петри	R	Не применяется	УПБ 2
5 Модели данных сущность-связь-атрибут	R	Не применяется	УПБ 2
6 Диаграммы последовательности сообщений	R	Не применяется	УПБ 3
7 Таблицы решений и таблицы истинности	R	Не применяется	УПБ 2
8 UML-диаграммы	R	Не применяется	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 2**

В процессе разработки программного обеспечения создаются спецификации требований программного обеспечения. Применяется спецификация путём описания. Данных методов достаточно для соответствия уровню УПБ 2.

9.3.3 Планирование подтверждения соответствия безопасности системы для аспектов программного обеспечения

В процессе разработки программного обеспечения создаётся план контроля качества программного обеспечения. Применяемых методов достаточно для соответствия уровню полноты безопасности УПБ2.

9.3.4 Проектирование и разработка программного обеспечения: проектирование архитектуры программного обеспечения

В ходе разработки программного обеспечения обеспечиваются обязательные требования к проектированию архитектуры ПО. Выполняется модульный подход, применяются полуформальные методы. Данных методов достаточно для соответствия уровню УПБ 2.

Методы при проектировании и разработке программного обеспечения: проектирование архитектуры программного обеспечения

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1 Обнаружение ошибок	R	Применяется	УПБ 3
2 Коды обнаружения ошибок	R	Применяется	УПБ 3
4b Постепенное отключение функций	R	Не применяется	УПБ 2
7 Модульный подход	HR	Применяется	УПБ 3

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
8 Использование доверительных/ проверенных элементов программного обеспечения (при наличии)	R	Не применяется	УПБ 2
9 Прямая прослеживаемость между спецификацией требований к программному обеспечению системы безопасности и архитектурой ПО	R	Не применяется	УПБ 3
10 Обратная прослеживаемость между спецификацией требований к программному обеспечению системы безопасности и архитектурой ПО	R	Не применяется	УПБ 2
11a Методы структурных диаграмм	HR	Применяются	УПБ 2
11b Полуформальные методы	R	Не применяется	УПБ 2
12 Автоматизированные средства разработки спецификаций и проектирования	R	Не применяется	УПБ 2
13a Циклическое поведение с гарантированным максимальным временем цикла	HR	Не применяется, нет требований к времени цикла	УПБ 3
13b Архитектура с временным распределением	HR	Не применяется, нет требований	УПБ 3
13c Управление событиями с гарантированным максимальным временем реакции	HR	Не применяется, имеется сторожевой таймер для защиты от зависания.	УПБ 3
14 Статическое выделение ресурсов	R	Не применяется	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 2**

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Модульный подход

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1 Ограничение размера программного модуля	HR	Применяется	УПБ 3
2 Управление сложностью программного обеспечения	R	Не применяется	УПБ 2
3 Ограничение доступа/инкапсуляции информации	HR	Применяется	УПБ 3
4 Ограниченное число параметров/фиксированное число параметров подпрограммы	R	Не применяется	УПБ 2
5 Одна точка входа и одна точка выхода в каждой подпрограмме и функции	HR	Применяется	УПБ 3
6 Полностью определённый интерфейс	HR	Применяется	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 2**

9.3.5. Проектирование и разработка программного обеспечения: инструментальные средства поддержки и языки программирования

При проектировании программного обеспечения выбираются инструментальные средства поддержки соответствующие заданному уровню полноты безопасности. Для языков программирования применяются стандарты кодирования, для сокращения ошибок на этапе компиляции.

Проектирование и разработка программного обеспечения: инструментальные средства поддержки и языки программирования.

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1 Выбор соответствующего языка программирования	HR	Применяется	УПБ 3
2 Строго типизированные языки программирования	HR	Применяется	УПБ 3
3 Подмножество языка	HR	Применяется, использование Си по стандартам кодирования	УПБ 3

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
4a Сертифицираванные средства и сертифицированные трансляторы	R	Не применяется	УПБ 2
4b Инструментальные средства, заслуживающие доверия на основании опыта использования	HR	Применяется, GCC	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 2**

9.3.6 Проектирование и разработка программного обеспечения: детальное проектирование (включает в себя проектирование системы программного обеспечения, проектирование модуля программного обеспечения и кодирование)

При проектировании программного обеспечения применяется модульный подход, применяются стандарты кодирования. Данных методов достаточно для соответствия уровню УПБ 2.

Методы проектирования и разработки программного обеспечения: детальное проектирование.

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1a Методы структурных диаграмм	HR	Применяется	УПБ 3
1b Полуформальные методы	R	Не применяются	УПБ 2
1c Формальные методы проектирования и усовершенствования	R	Не применяется	УПБ 3
2 Средства автоматизированного проектирования	R	Не применяется	УПБ 2
3 Программирование с защитой	R	Не применяется	УПБ 2
4 Модульный подход	HR	Применяется, код разрабатывается модулями	УПБ 3
5 Стандарты для проектирования и кодирования	HR	Применяется	УПБ 3
6 Структурное программирование	HR	Применяется	УПБ 3

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
7 Использование доверительных/ проверенных программных модулей и компонентов (по возможности)	HR	Применяется	УПБ 3
8 Прямая прослеживаемость между спецификацией требований к программному обеспечению системы безопасности и проектом программного обеспечения	R	Не применяется	УПБ 2
Итоговый достигнутый уровень УПБ			**УПБ 2**

Стандарты для проектирования и кодирования

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1 Использование стандартов кодирования для сокращения вероятности ошибок	HR	Применяется	УПБ 3
2 Не использовать динамические объекты	HR	Применяется	УПБ 3
3a Не использовать динамические переменные	R	Применяется	УПБ 3
3b Проверка создания динамических переменных в неавтономном режиме	R	Не применяется	УПБ 3
4 Ограниченное использование прерываний	R	Не применяются	УПБ 2
5 Ограниченное использование указателей	R	Не применяются	УПБ 2
6 Ограниченное использование рекурсий	R	Не применяются	УПБ 2

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

7 Не использовать неструктурированное управление в программах, написанных на языках высокого уровня	HR	Применяются	УПБ 3
8 Не использовать автоматическое преобразование типов	HR	Применяется	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 2**

9.3.7. Проектирование и разработка программного обеспечения: тестирование и интеграция программных модулей

Методы тестирования и интеграции программных модулей включают динамический анализ и тестирование, функциональное тестирование методом чёрного ящика. Данных методов достаточно для соответствия уровню УПБ 2.

Методы тестирования и интеграции программных модулей.

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1Вероятностное тестирование	R	Не применяются	УПБ 3
2 Динамический анализ и тестирование	HR	Применяется	УПБ 3
3 Регистрация и анализ данных	HR	Применяется	УПБ 3
4 Функциональное тестирование и тестирование методом черного ящика	HR	Применяется	УПБ 3
5 Тестирование рабочих характеристик	R	Не применяются	УПБ 2
6 Тестирование, основанное на модели	R	Не применяются	УПБ 2
7 Тестирование интерфейса	R	Не применяются	УПБ 2
8 Управление тестированием и средства автоматизации	HR	Применяется	УПБ 3
9 Прямая прослеживаемость между спецификацией проекта программного обеспечения и спецификациями тестирования модуля и интеграции	R	Не применяются	УПБ 2

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
10 Формальная верификация	-	Не применяется	-
Итоговый достигнутый уровень УПБ			**УПБ 2**

Динамический анализ и тестирование

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1 Выполнение тестового примера, связанного с анализом граничных значений	HR	Применяется	УПБ 3
4 Выполнение тестового примера, сгенерированного на основе модели	R	Не применяется	УПБ 2
7a Структурный тест со 100-% охватом (точки входа)	HR	Применяется	УПБ 3
7a Структурный тест со 100-% охватом (операторы)	HR	Применяется	УПБ 3
7c Структурный тест со 100-% охватом (условные переходы)	R	Не применяется	УПБ 2
Итоговый достигнутый уровень УПБ			**УПБ 2**

Функциональное тестирование и проверка методом черного ящика

Метод/средство	Уровень необходимости применения метода для заявленного	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
2 Выполнение тестового примера, сгенерированного на основе модели	R	Не применяется	УПБ 2
4 Разделение входных данных на классы эквивалентности, включая анализ граничных значений	HR	Применяется	УПБ 3

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Метод/средство	Уровень необходимости применения метода для заявленного	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
Итоговый достигнутый уровень УПБ			**УПБ 2**

Тестирование рабочих характеристик

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1 Проверка на критические нагрузки и стресс-тестирование	R	Не применяется	УПБ 2
2 Ограничение на время ответа и объём памяти	HR	Применяется	УПБ 3
3 Требования к реализации	HR	Применяется	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 2**

9.3.8. Подтверждение соответствия безопасности системы аспектов программного обеспечения

Подтверждения соответствия аспектов программного обеспечения проводится с помощью функционального тестирования. Данных методов достаточно для соответствия уровню УПБ 2.

Подтверждение соответствия ПО

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1 Вероятностное тестирование	R	Не применяются	УПБ 2
2 Моделирование процесса	R	Не применяются	УПБ 2
3 Моделирование	R	Не применяются	УПБ 2
4 Функциональное тестирование и тестирование методом черного ящика	HR	Применяется, интегрированная система	УПБ 3

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
5 Прямая прослеживаемость между спецификацией требования к программному обеспечению и планом подтверждения соответствия программного обеспечения системы безопасности	R	Не применяются	УПБ 2
6 Обратная прослеживаемость между планом подтверждения соответствия программного обеспечения системы безопасности и спецификацией требования к программному обеспечению системы безопасности	R	Не применяются	УПБ 2
Итоговый достигнутый уровень УПБ			**УПБ 2**

9.3.9. Модификация программного обеспечения.

При модификации программных модулей проводится анализ влияния, осуществляется повторная верификация программных модулей. Данных методов достаточно для соответствия уровню УПБ 2.

Модификация программного обеспечения

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1 Анализ влияния	HR	Применяется	УПБ 3
2 Повторная верификация измененных программных модулей	HR	Применяется	УПБ 3
3 Повторная верификация программных модулей на которые оказывают влияние изменения в других модулях	R	Не применяется	УПБ 2
4a Повторное подтверждение соответствия системы в целом	R	Не применяется	УПБ 2
4b Регрессионное подтверждение соответствия	HR	Применяется	УПБ 3
5 Управление конфигурацией программного обеспечения	R	Не применяется	УПБ 2

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
6 Регистрация и анализ данных	HR	Применяется	УПБ 3
7 Прямая прослеживаемость между спецификацией требования к программному обеспечению и планом модификации программного обеспечения системы безопасности	R	Применяется	УПБ 3
6 Обратная прослеживаемость между планом модификации программного обеспечения системы безопасности и спецификацией требования к программному обеспечению системы безопасности	R	Не применяется	УПБ 2
Итоговый достигнутый уровень УПБ			**УПБ 2**

9.3.10. Верификация программного обеспечения

Верификация программного обеспечения (на отдельных этапах жизненного цикла) включает в себя методы статического анализа, динамическое тестирование. Данных методов достаточно для соответствия уровню УПБ 2.

Методы верификации программного обеспечения на различных этапах создания ПО.

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1 Формальное доказательство	R	Не применяется	УПБ 2
2 Анимация спецификации и тестирования	R	Не применяется	УПБ 2
3 Статический анализ	HR	Применяется	УПБ 2
4 Динамический анализ и тестирование	HR	Применяется	УПБ 3
5 Прямая прослеживаемость между спецификацией проекта программного обеспечения и планом верификации программного обеспечения	R	Не применяется	УПБ 2
6 Обратная прослеживаемость между планом верификации и программного обеспечения и спецификацией проекта	R	Не применяется	УПБ 2

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
7 Численный анализ в автономном режиме	R	Не применяется	УПБ 2
Итоговый достигнутый уровень УПБ			**УПБ 2**

9.3.10. Оценка функциональной безопасности.

Оценка функциональной безопасности программного обеспечения проводится с помощью

Оценка функциональной безопасности ПО

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1 Таблица контрольных проверок	R	Не применяется	УПБ 2
2 Таблицы решений (таблицы истинности)	R	Не применяется	УПБ 2
3 Анализ отказов	R	Не применяется	УПБ 2
4 Анализ отказов по общей причине различного программного обеспечения (если используется различное программное обеспечение)	R	Не применяется	УПБ 2
5 Структурные схемы надежности	R	Не применяется	УПБ 2
6 Прямая прослеживаемость между требованиями раздела 8 и планом оценки функциональной безопасности программного обеспечения	R	Не применяется	УПБ 2
Итоговый достигнутый уровень УПБ			**УПБ 2**

9.3.11 Выводы по оценке программного обеспечения устройства

Программное обеспечение, используемое в преобразователях уровня радиоволновых волноводных ТЭКФЛЕКС соответствует требованиям к программному обеспечению, предъявляемым стандартом по функциональной безопасности ГОСТ Р МЭК 61508-3 для уровня полноты безопасности УПБ (SIL) = 2.

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

10. Заключение по результатам оценки

По результатам оценки преобразователей уровня радиоволновых волноводных ТЭКФЛЕКС можно сделать следующие краткие выводы:

- Процессы жизненного цикла изделия и меры предотвращения систематических отказов соответствуют требуемому уровню полноты безопасности УПБ 2 (SIL 2).
- Аппаратная часть, частоты отказов, доля безопасных отказов, значения PFD и PFH соответствуют требованиям, предъявляемым к уровню полноты безопасности УПБ 2 (SIL 2) с учетом применяемых архитектур и условий избыточности аппаратных средств.

Уровень полноты безопасности УПБ (SIL) всей инструментальной функции безопасности (SIF), в которой применяется устройство должен быть проверен путем расчета PFH/PFDavg всей системы с учетом избыточных архитектур, интервала контрольных испытаний, эффективности контрольных проверок, любой автоматической диагностики, среднего времени ремонта и конкретной частоты отказов всех элементов системы, включенных в SIF. Каждый элемент должен быть проверен на соответствие минимальным требованиям отказоустойчивости оборудования (HFT).

- Программное обеспечение соответствует требования предъявляемым к уровню полноты безопасности УПБ 2 (SIL 2)

Преобразователи уровня радиоволновые волноводные ТЭКФЛЕКС соответствуют требованиям, предъявляемым стандартами по функциональной безопасности для:

- уровня полноты безопасности УПБ 2 (SIL 2) при отказоустойчивости аппаратных средств ОАС (HFT) = 0.

Отчёт составил:
Эксперт, Зубрев Е.О. подпись «02» февраля 2023 г.