ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ИЗГОТОВИТЕЛЬ»

Адрес:

ОГРН: 1234567890

Телефон:

Электронная почта:

Отчет об оценке функциональной безопасности

№ 27.12.40-001-ОКПО-2024 ФБ от 00.00.2024

УТВЕРЖДАЮ:

Генеральный директор

ООО «ИЗГОТОВИТЕЛЬ»

_____ ФИО

«_____» _____2024 г.

Оборудование: Низковольтное комплектное устройство НКУ

Область применения: предназначенное для распределения и управления

Изготовитель: ООО «ИЗГОТОВИТЕЛЬ»; ОГРН: 1234567890

г. Москва

2024 г.

Оглавление

1. Заявитель на сертификацию
ООО «ИЗГОТОВИТЕЛЬ»; ОГРН: 1234567890; адрес: XXXX

2. Изготовитель продукции
ООО «ИЗГОТОВИТЕЛЬ»; ОГРН: 1234567890; адрес: XXXX

3. Наименование продукции
Низковольтное комплектное устройство НКУ

4. Перечень стандартов на соответствие которым проведена оценка функциональной безопасности

Обозначение стандарта	**Наименование стандарта**
ГОСТ Р МЭК 61508-1-2012	Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования
ГОСТ Р МЭК 61508-2-2012	Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам
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	
ГОСТ Р МЭК 61508-4-2012	Функциональная безопасность систем электрических, электронных, программируемых электронных связанных с безопасностью. Часть 4. Термины и определения
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
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
ГОСТ Р МЭК 61508-7-2012	Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства

5. Перечень рассмотренной документации

ТУ 27.12.40-002-ОКПО-2023	Технические условия
27.12.40-002-ОКПО-2023 РЭ	Руководство по эксплуатации
27.12.40-002-ОКПО-2023 ПС	Паспорт 5 шт.

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.

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.

Adu - интенсивность необнаруженных опасных отказов.

Add - 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 электронной 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 электронной системы, связанной с безопасностью, выполняющей указанную функцию безопасности в течение заданного периода времени.

p - 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.

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

7.1 НКУ должен обеспечивать в автоматическом режиме в различных условиях эксплуатации (в том числе в условиях ограниченной видимости и (или) повышенного шума, в сложных погодных условиях, в ночное время суток):

- …..;

- …..;

- ……

7.2 Требования к устройствам, входящим в состав НКУ.

7.2.1 ……..

7.2.2 ……..

7.2.3 ……..

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 МЭК61508 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 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 УПБ2 (SIL2).

8.3 Описание требований к жизненному циклу системы безопасности

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 к проектированию;
- Планирование подтверждения соответствия безопасности;
- Проектирование и разработка;
- 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.

8.4 Описание требований к аппаратной части устройства

8.4.1 Структурные требования

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

ДБО для компонентов типа А.

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

ДБО для компонентов типа В

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	УПБЗ
от 90% до менее 99%	УПБ 2	УПБЗ	УПБ 4
более и равно 99%	УПБ 2	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).

Величина ДБО (SFF) 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:

$$SFF = \frac{\sum \lambda_{DD}}{\sum \lambda_{DD} + \sum \lambda_{DU}}$$

где:
λ_{DD} - интенсивность опасных детектируемых отказов;
λ_{DU} - интенсивность опасных не детектируемых отказов;

Величина отказоустойчивости аппаратных средств определяется в зависимости от канальной архитектуры подсистемы

Определение РАС (HFT)

УПБ	Режим запросов выполнения работы контура – контур безопасности	Минимально допустимое число отказов аппаратных средств
1	Любой – модуль в составе системы	0
2	Редкие запросы	0
2	Частые (непрерывные) запросы – наличие взрывоопасной среды и/ или непрерывного требования соблюдения режима безопасной работы изделия модуль НКУ ОПБ-23	1
3	Любой - барьер искрозащиты	1
4	Любой – датчики / система диагностики	2

8.4.2 Вероятные требования

Интегральный уровень безопасности SIL	Допустимая вероятность отказа PFDavg
SIL 4	10^{-5} -- 10^{-4}
SIL 3	10^{-4} -- 10^{-3}
SIL 2	10^{-3} -- 10^{-2}
SIL 1	10^{-2} -- 10^{-1}

8.4.3 Расчет и методика расчета PFDavg представлен в руководстве РФБ 26.20.12-НКУ пункт 4.2.

8.5 Требования к программному обеспечению устройства.

Разработка, испытание, верификация, и подтверждение соответствия прикладных программ должна проводится в соответствии с ГОСТ Р МЭК 61508-3-2018.

Перечень методов и средств, используемых для достижения Уровня Полноты Безопасности (SIL) программным обеспечением, приведен в приложениях А и В ГОСТР МЭК 61508-3 и в ГОСТР МЭК 61508- 7. Для каждого из них приведены рекомендации по уровню полноты безопасности, изменяющемуся от 1 до 4. 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.

9. Результаты оценки функциональной безопасности

9.1 Процессы жизненного цикла изделия и меры предотвращения систематических отказов

В ходе оценки жизненного цикла НКУ проверялось соответствие стандарта ГОСТ Р МЭК 61508 в части процессов, процедур и методов, используемых при проектировании и разработке заявленного изделия на соответствие уровню полноты безопасности УПБ2.

В компании ООО «ИЗГОТОВИТЕЛЬ» внедрен процесс управления жизненным циклом изделия, что описано в руководстве по эксплуатации 27.12.40-002-ОКПО-2023 РЭ.

Спецификация требования к оборудованию описана в технических условиях, а также в отдельных спецификациях. Проведение испытаний изделия описаны также в технических условиях, а также в отдельных методиках испытаний на соответствующие показатели. Также разработан документ по качеству.

Установленный процесс внесения изменений описан в документах по качеству.

Конструкция изделия включает в себя программное обеспечение, которое также имеет необходимый жизненный цикл методами соответствующими 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 в основном описано в технических условиях на продукцию. Процесс внесения изменений описан в документах по качеству. Данный процесс и входящие в него процедуры отвечают требованиям ГОСТ Р МЭК 61508.

Управление версиями

Внесение изменений в техническую документацию происходит в соответствии документами по качеству.

Обучение, компетентность сотрудников

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

9.1.2 Описание требований безопасности и проектирование конструкции

Общие требования к конструкции изделия описаны в технических условиях. 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 УПБ2.

Применение полуформальных методов не требуется.

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 УПБ2.

9.1.4 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 УПБ2.

Испытания методами черного ящика, полевые испытания, статическое и динамическое тестирование не требуется.

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 УПБ2.

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 УПБ2.

9.1.7 Эксплуатационная документация

В состав эксплуатационной документации входят:

- Руководства 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.

В руководстве по функциональной безопасности упоминается FMEDA анализ устройства, который 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 УПБ2.

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

9.2 Результаты оценки аппаратной части устройства

9.2.1 Методика оценки

В соответствии с ГОСТ Р МЭК 61508 должны быть определены архитектурные ограничения устройства. Это можно осуществить, используя метод 1н в соответствии с П7.4.4.2 ГОСТ Р МЭК 61508-2-2012 или методом 2н в соответствии с п.7.4.4.3 ГОСТ Р МЭК 61508-2-2012.

Для оценки аппаратной части НКУ был выбран метод 1н. Специалистами ООО «ИЗГОТОВИТЕЛЬ» 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.

Эти результаты следует рассматривать в комбинации со значениями средней вероятности отказа по запросу PFDavg или PFH других устройств, принимающих участие в работе автоматизированной системы безопасности (SIS), чтобы установить соответствие всей системы необходимому уровню полноты безопасности УПБ (SIL). Также для всех условий использования элементов необходимо проанализировать требования к архитектурным ограничениям ГОСТ Р 61508-2-2012, Таблицы 2 и 3. Конечный потребитель должен проверить и подтвердить это для всех условий использования и включить все компоненты системы в расчет.

9.2.2 Исходные предпосылки расчёта показателей функциональной безопасности

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;
- 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 МЭК60654-1, классе

9.2.3 Сводные значения и результаты оценки аппаратной части.

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

Модуль	Тип выходного сигнала	Режим	λ_{DD}	λ_{DU}	PFDavg
Коллективное устройство взаимодействия КУОБЗ	Радиосигнал L1 (1,6 ГГц) L2 (1,25 ГГц) GMSK BT — 0,3 BNC-RCA	Средняя частота	$9{,}69 \cdot 10^{-6}$	$5{,}27 \cdot 10^{-6}$	-
Сигнализационное индивидуальное устройство ИУ	GMSK BT — 0,3 BNC-RCA	Средняя частота	$4{,}45 \cdot 10^{-6}$	$2{,}36 \cdot 10^{-6}$	-
Индивидуальное устройство руководителя ИУР с ПО	Радиосигнал L1 (1,6 ГГц) L2 (1,25 ГГц) GMSK BT — 0,3 TMDS 165 МГц MHL	Средняя частота	$13{,}73 \cdot 10^{-6}$	$7{,}23 \cdot 10^{-6}$	-
Локомотивное устройство УИППС	Радиосигнал L1 (1,6 ГГц) L2 (1,25 ГГц) GMSK BT — 0,3 TMDS 165 МГц MHL	Средняя частота	$13{,}73 \cdot 10^{-6}$	$7{,}23 \cdot 10^{-6}$	-
Коммуникационный сервер	1 x 1 GbE Шина PCI/ISA AES3 (AES / EBU) CLK по линиям RST#, INTA#-INTD#, PME# и CLKRUN#	Средняя частота	$8{,}57 \cdot 10^{-6}$	$3{,}99 \cdot 10^{-6}$	-
Низковольтное комплектное устройство НКУ					
Все перечисленные модули	Все перечисленные каналы	Средняя частота	$50{,}17 \cdot 10^{-6}$	$26{,}08 \cdot 10^{-6}$	$0{,}13 \cdot 10^{-3}$

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).

9.2.4 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 УПБ2 (SIL 3) при отказоустойчивости аппаратных средств ОАО (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)

9.3 Результаты оценки программного обеспечения

Разработка, испытание, верификация, и подтверждение соответствия прикладных программ проводится в соответствии с ГОСТ Р МЭК 61508-3-2018.

Программное обеспечение изделия построено на языке программирования «С» с подмножеством и стандартом кодирования MISRA C, в качестве среды программирования используется IAR Embedded Workbench IDE со встроенными компиляторами и средствами тестирования, что соответствует необходимому уровню полноты безопасности УПБ2 (SIL 3).

9.3.1 Проектирование и разработка программного обеспечения: проектирование архитектуры программного обеспечения

Методы и средства проектирование архитектуры Программного обеспечения системы безопасности должны были быть выбраны в соответствии с уровнем полноты безопасности в соответствии с таблицей А.2 ГОСТ IEC 61508-3-2018

Проектирование и разработка 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	Выполняются проверки в области значений (выход за допустимый диапазон)	УПБ2
2 Коды обнаружения ошибок	R	Применяется. Для проверки целостности данных применяется циклический избыточный код CRC8, CRC16, а также контроль чётности.	УПБ2
4а Механизмы повторных попыток парирования сбоя	R	Не применяется. 4Ь	УПБ2

4Ь Постепенное отключение функций	R	Применяется. Нарушение работоспособности второстепенных функций (например, функции архивирования) из- за аппаратного отказа не приводит к отключению или прекращению работы функции измерения, отвечающей за безопасность.	УПБ2
7 Модульный подход	HR	Применяется, см таблицу ниже.	УПБ2
8 Использование доверительных/ проверенных элементов программного обеспечения (при наличии)	HR	Применяется. Используются программные модули, которые имеют положительный опыт эксплуатации в составе других изделий (например, модуль интерфейса, отвечающий за связь с внешними устройствами)	УПБ2
9 Прямая прослеживаемость между спецификацией требований к программному обеспечению системы безопасности и архитектурой ПО	R	Не применяется	УПБ 2
10 Обратная прослеживаемость между спецификацией требований к программному обеспечению системы безопасности и архитектурой ПО	R	Не применяется	УПБ 2
11a Методы структурный диаграмм	HR	Применяется. Построение диаграмм потоков данных	УПБ2
11b Полуформальные методы	R	Не применяется	УПБ2
12 Автоматизированные средства разработки спецификаций и проектирования	R	Не применяется	УПБ2
13a Циклическое поведение с гарантированным максимальным временем цикла	HR	Не применяется. Требования к синхронизации системы безопасности не предъявляются	УПБ2
13b Архитектура с временным распределением	HR	Не применяется. Требования к синхронизации системы безопасности не предъявляются	УПБ2
13c Управление событиями с гарантированным максимальным временем реакции	HR	Не применяется. Требования к синхронизации системы безопасности не предъявляются	УПБ2
14 Статическое выделение ресурсов	R	Применяется. Динамические переменные используются в ограниченном количестве, динамические объекты не используются	УПБ2
Итоговый достигнутый уровень УПБ – SIL 2			

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

Языки программирования и их компиляторы для системы безопасности должны были быть выбраны в соответствии с уровнем полноты безопасности в соответствии с таблицей А.3 ГОСТ IEC 61508-3-2018.

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. В качестве языка программирования выбран язык Си и подмножество языка Си - MISRA C, которое предназначено для разработки программного обеспечения с высокими требованиями к безопасности. MISRA C отвечает требованиям ГОСТ Р МЭК 61508-7	УПБ2
2 Строго типизированные языки программирования	HR	Применяется. MISRA C является подмножеством языка Си.	УПБ2
3 Подмножество языка	HR	Применяется. MISRA C содержит набор правил (относительно базового языка Си), снижающих вероятность внесения ошибок в программный код и повышающих вероятность обнаружения оставшихся ошибок	УПБ2
4а Сертифицированные средства и сертифицированные трансляторы	R	Не применяется	УПБ2
4Ь Инструментальные средства, заслуживающие доверия на основании опыта использования	HR	Применяется. Среда разработки IAR Embedded Workbench IDE имеет положительный опыт эксплуатации, применяется в качестве среды разработки программного обеспечения для многих серийно-выпускаемых изделий. Недостатки и ошибки в IAR Embedded Workbench IDE не выявлены	УПБ2
Итоговый достигнутый уровень УПБ – SIL 3			

9.3.3 Оценка функциональной безопасности

Оценка функциональной безопасности программного обеспечения должна производиться методами в соответствии с уровнем полноты безопасности в соответствии с таблицей А. 10 ГОСТ IEC 61508-3-2018.

Оценка функциональной безопасности

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	УПБ2
2 Таблицы решений (таблицы истинности)	R	Не применяется	УПБ2
3 Анализ отказов	R	Не применяется	УПБ2
4 Анализ отказов по общей причине различного программного обеспечения (если используется различное программное обеспечение)	R	Не применяется	УПБ2
5 Структурные схемы надежности	R	Не применяется	УПБ2
6 Прямая прослеживаемость между требованиями раздела 8 и планом оценки функциональной безопасности программного обеспечения	R	Не применяется	УПБ2
Итоговый достигнутый уровень УПБ – SIL 2			

9.3.4 Выводы по оценке программного обеспечения устройства

Программное обеспечение, используемое в НКУ соответствует требованиям к программному обеспечению, предъявляемым стандартом по функциональной

безопасности ГОСТ Р МЭК 61508-3 для уровня полноты безопасности УПБ2 (SIL 3).

10. Заключение по результатам оценки

По результатам оценки НКУ можно сделать следующие краткие выводы: о Процессы жизненного цикла изделия и меры предотвращения отказов соответствуют требуемому уровню полноты безопасности УПБ2 (SIL 2).

■ Аппаратная часть, частоты отказов, доля безопасных отказов, значения PFD и PFH соответствуют требованиям, предъявляемым к уровню полноты безопасности УПБ2 (SIL 3) с учетом применяемых архитектур и условий избыточности аппаратных средств.

Уровень полноты безопасности УПБ (SIL) всей инструментальной функции безопасности (SIF), в которой применяется датчик 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 УПБ2 (SIL 3)

Низковольтное комплектное устройство НКУ соответствуют требованиям, предъявляемым стандартами по функциональной безопасности для:

- уровня полноты безопасности УПБ2 (SIL 2) при отказоустойчивости аппаратных средств ОАС (HFT) = 0.

Отметка ОТК
(клеймо ответственного
за приёмку)

_____ (Ф.И.О)
дата

Особые отметки: