УДК 65.014.12

ВЫБОР И ОБОСНОВАНИЕ КОМПОНЕНТОВ ПАЗ С УЧЕТОМ ТРЕБОВАНИЙ ПОЛНОТЫ БЕЗОПАСНОСТИ. ПОДТВЕРЖДЕНИЕ СООТВЕТСТВИЯ

Ю.Д. Индык, А.В. Струков, И.А. Можаева (ООО «СПИК СЗМА»)

Введение

При выборе оборудования для технологических процессов следует руководствоваться указаниями регулятора в области промышленной безопасности и надлежащей инженерной практикой, в том числе той, которая касается проектирования, эксплуатации или технического обслуживания систем противоаварийной автоматической защиты (ПАЗ).

Федеральные нормы и правила однозначно определяют, что «… Методы создания ПАЗ должны определяться в соответствии с требуемым уровнем полноты безопасности…» [1]. Таким образом определено, что компоненты систем ПАЗ должны соответствовать требованиям стандартов серии ГОСТ Р МЭК 61508.

Выбор любой части оборудования (компонентов, элементов, подсистем) для систем ПАЗ зависит от их функциональности, надежности, условий эксплуатации и технологических требований. В дополнение к этому, оборудование выбирается для обеспечения заданного уровня полноты безопасности (УПБ) для каждой инструментальной функции безопасности (ФБ) в соответствии со спецификацией требований безопасности (СТБ).

Практический подход к выбору элементов, используемых в ПАЗ, заключается в применении комбинации свидетельств соответствия с требованиями МЭК 61508-2 для аппаратной части (МЭК 61508-3 для программного обеспечения) и эксплуатационного опыта. При этом необходимо продемонстрировать, что компонент, элемент или подсистема ПАЗ достаточно надежны для обеспечения заданной полноты безопасности, которая может быть выражена в терминах средней вероятности отказа на запрос или средней частоты опасных отказов. Кроме того, необходимо рассмотреть архитектурные ограничения, которые связаны с определением доли безопасных отказов, значение которой определяется диагностическим покрытием. Одним из основных доказательств применимости компонентов в системах ПАЗ является подтверждение достаточно низкой вероятности систематических отказов, что является важной задачей оценивания предыдущего опыта их применения.

В данной статье рассматриваются вопросы подтверждения соответствия элементов, применяемых в ПАЗ, требованиям стандартов серии МЭК 61508.

В настоящее время сложилась известная международная практика применения сертификатов как способа документального оформления третьей стороной доказательств возможности использования компонентов (изделий, устройств, оборудования) в системах, связанных с безопасностью.

В стандартах ГОСТ Р МЭК 61508-2–2012 и ГОСТ Р МЭК 61508-3–2012 (далее МЭК 61508-2 и МЭК 61508-3) понятие «сертификат» не используется. Тем не менее, указывается, что для каждого применяемого изделия, для которого требуется соответствие стандартам серии МЭК 61508, должно быть разработано руководство по безопасности (РБ) в соответствии с приложением D. В примечании к п.7.4.9.7 МЭК 61508-2 отмечено, что требования, не обеспеченные достаточными доказательствами, не помогают установить корректность и полноту функции безопасности, в реализации которой участвует компонент.

По определению (МЭК 61508-4) «Руководство по безопасности для применяемых изделий (safety manual for compliant items): Документ, предоставляющий всю

информацию, связанную с функциональной безопасностью компонента, выполняющего указанные функции безопасности, гарантирующий, что система соответствует требованиям серии стандартов МЭК 61508». Требование соответствия стандартам серии МЭК 61508 означает в общем случае выполнение всех требований каждого раздела и подраздела.

Для систем ПАЗ, имеющих низкую сложность, и при наличии у специалистов достаточного практического опыта, дающего необходимую уверенность в достижении целевой полноты безопасности, допускается освобождение компонентов от необходимости соответствия некоторым требованиям стандарта, при условии, что это решение будет обосновано. Системы, имеющую низкую сложность, характеризуются тем, что отказы каждого отдельного компонента хорошо определены, а поведение самой системы в условиях сбоя полностью известно.

Цель руководства по безопасности состоит в документальном оформлении информации, которая необходима для обеспечения интеграции применяемого компонента в связанную с безопасностью систему.

Хорошая практика сертификации применяемых в ПАЗ изделий показывает, что достаточно подготовленные в области функциональной безопасности сертификационные центры разрабатывают такую схему сертификации, при которой компетентные специалисты центра оказывают реальную поддержку и помощь изготовителям компонентов в получении доказательств соответствия требованиям отдельных частей или пунктов стандарта МЭК 61508-2. Опыт сертификационной работы показывает, что изготовитель не всегда имеет полностью разработанное РБ к началу процессу сертификации, но в окончательном варианте сертификата обычно указывается, что в конкретном проекте обязательно использование данных из РБ.

В идеальном случае РБ применяемого в ПАЗ изделия должно содержать следующую информацию:

- классификацию типа А или В той части применяемого изделия, которая обеспечивает выполнение функции безопасности;
- виды случайных отказов аппаратных средств, приводящих к отказу функции безопасности, обнаруженных и не обнаруженных внутренней диагностикой;
- предполагаемую интенсивность отказов для каждого вида отказов;
- интервал диагностических проверок для каждого вида отказов, обнаруживаемых внутренней диагностикой (diagnostic test interval);
- требования к периодическим контрольным проверкам (proof test) и/или техническому обслуживанию;
- стойкость к систематическим отказам применяемого изделия (ССО);
- любые указания или ограничения, связанные с применением изделия, реализующего ФБ, которые могут предотвратить систематические отказы этого изделия.

В заявлениях (декларациях) производителя и сертификатах третьей стороны обычно говорится, что продукт пригоден для использования до указанного УПБ, если продукт эксплуатируется в соответствии с РБ. Здесь важны детали отчета о подтверждении пригодности оборудования к применению в ПАЗ.

В качестве примера исходных данных, необходимых для оценки уровня полноты безопасности и учета архитектурных ограничений, рассмотрим фрагменты РБ датчиков температуры (ДТ) и измерительных преобразователей в полевом исполнении (ИПП), изготавливаемых в ООО «ПК ТЕСЕЙ», и датчиков-газоанализаторов ДГС ЭРИС-210, ДГС ЭРИС-230, изготавливаемых в группе компаний «ЭРИС».

В табл.1 приведены показатели надежности ДТ и ИПП, в табл.2 – датчиков-газоанализаторов.

Таблица 1 – Показатели надежности ДТ и ИИП (фрагмент РБ)

Исполнение ДТ	Тип компонента	*λdu*	*λdd*	*λsu*	*λsd*	ДБО
КТxxEx01	A	30	100	20	0	80%
Исполнение ДТ и ИПП с преобразователем PR 53335, PR 6337						
В комплекте с термопарой	A	425	4973	0	142	92.3%

Таблица 2 – Показатели надежности датчиков-газоанализаторов (фрагмент РБ)

Название газоанализатора	ДГС ЭРИС 210
Тип анализатора	Тип B (сложное устройство)
λdu (интенсивность опасных необнаруженных отказов)	85
λdd (интенсивность опасных обнаруженных отказов	149
λsu (интенсивность безопасных необнаруженных отказов)	1862
λsd (интенсивность безопасных обнаруженных отказов)	982
Доля безопасных отказов, %	97.3

В таблицах 1 и 2 используются следующие обозначения:

- *λdu* – интенсивность опасных необнаруженных отказов;
- *λdd* – интенсивность опасных обнаруженных отказов;
- *λsu* – интенсивность безопасных необнаруженных отказов;
- *λsd* – интенсивность безопасных обнаруженных отказов.

В таблицах 1 и 2 значения интенсивностей отказов приведены в FIT (10^{-9} 1/час).

Доля безопасных отказов (ДБО) рассчитывается как отношение суммы интенсивности безопасных отказов и опасных обнаруженных отказов к сумме интенсивностей безопасных и опасных отказов, то есть по формуле

$$ДБО = (\lambda sd + \lambda su + \lambda dd) / (\lambda sd + \lambda su + \lambda dd + \lambda du). \quad (1)$$

Для определения архитектурных ограничений на применение изделий в системах ПАЗ используются данные таблиц 2 и 3 стандарта МЭК 61508-2. Требования к отказоустойчивости аппаратных средств указанных таблиц применяются для определения максимального значения УПБ, который может быть предъявлен к системе, в которой используется данный компонент. Отказоустойчивость аппаратных средств (ОАС) выражается в структурной избыточности элемента или подсистемы. При ОАС=0 резервирование не требуется, при ОАС=1 применяется архитектура, в которой отказ одного элемента не приводит к отказу ФБ, например 1oo2, 2oo3. При ОАС=2 необходима архитектура, в которой отказ двух элементов не приводит к отказу ФБ, например, 1oo3, 2oo4. В табл. 3 приводятся объединенные данные таблиц 2 и 3 стандарта МЭК 61508-2.

Таблица 3 – Максимальный УПБ для ФБ, реализуемой элементом или подсистемой

ДБО / ОАС	Отказоустойчивость аппаратных средств					
	Элемент типа А			Элемент типа В		
	0	1	2	0	1	2
менее 60%	УПБ 1	УПБ 2	УПБ 3	–	УПБ 1	УПБ 2
от 60% до 90%	УПБ 2	УПБ 3	УПБ 4	УПБ 1	УПБ 2	УПБ 3
от 90% до 99%	УПБ 3	УПБ 4	УПБ 4	УПБ 2	УПБ 3	УПБ 4
более 99%	УПБ 3	УПБ 4	УПБ 4	УПБ 3	УПБ 4	УПБ 4

К элементам типа А относятся такие элементы, для которых виды отказов всех составляющих компонентов определены, поведение элемента в условиях отказа также полностью определено, а данные рекламационной работы достаточно надежны.

Если хотя бы одно из условий не выполняется, то элемент относится к типу В.

К элементам типа В относятся, в частности, те элементы, для которых в технической документации указан только такой показатель надежности, как средняя наработка до отказа *T*ср (MTTF) или интенсивность отказов *λ*.

Следует отметить, что показатель ДБО тесно связан с показателем охвата диагностикой опасных отказов (DC). Показатель DC – это часть опасных отказов, выявляемая автоматическими диагностическими тестами в неавтономном режиме.

В Приложении С стандарта МЭК 61508-2 охват диагностикой опасных отказов определяется следующим выражением

$$DC = \frac{\lambda dd}{\lambda dd + \lambda du}. \qquad (2)$$

Для определения оценок интенсивностей отказов и, следовательно, показателей DC и ДБО, необходимо проведение процедуры анализа видов и последствий отказов (АВПО) компонентов или группы компонентов с использованием данных по отказам из признанного промышленного источника. Для проведения такого анализа необходимы подробные схемные решения, описывающие каждый компонент и его влияние на выполнение ФБ, виды и интенсивности отказов и связанные соотношения безопасных и опасных отказов к полной интенсивности отказов в процентах.

В табл.4 приведен фрагмент примера расчета показателей DC и ДБО, приведенного в Приложении С стандарта МЭК 61508-6.

Таблица 4 – Расчет охвата диагностикой и доли безопасных отказов

Ком-понент	Тип	Распределение на безопасные и опасные отказы для каждого вида отказов						Распределение на безопасные и опасные отказы для охвата диагностикой и рассчитанных интенсивностей отказов (x10^{-9} ч$^{-1}$)					
		обрыв		КЗ		изменение значения		$DC_{комп}$		1	2	3	4
		S	D	S	D	S	D	S	D	λ_S	λ_D	λdu	$\lambda_S + \lambda_D$
C1	100 нФ	1	0	1	0	1	0	1	0	3.2	0	0	3.2
C2	10 мкФ	0	0	1	0	0	0	1	0	0.8	0	0	0.8
R4	1 М	0.5	0.5	0.5	0.5			1	1	1.7	1.7	0	3.4
OSC1	OSC24МГц	0.5	0.5	0.5	0.5	0.5	0.5	1	1	16.0	16.0	0	32.0
U8	74HCT85	0.5	0.5	0.5	0.5	0.5	0.5	0.99	0.99	22.8	22.8	0.228	45.6
U16	MC68000	0	1	0	1	0.5	0.5	0.90	0.90	260.4	483.6	48.36	744.0
									Всего	304.9	524.1	48.588	829

В табл.4 использованы следующие обозначения:
S – безопасный отказ; D – опасный отказ; КЗ – короткое замыкание;
$DC_{комп}$ – охват диагностикой для компонента.

Использование табл. 5 дает следующие результаты:

- охват диагностикой для опасных отказов

$$DC = \frac{\lambda dd}{\lambda dd + \lambda du} = \frac{\lambda_D - \lambda du}{\lambda_D} = \frac{524.1 - 48.588}{524.1} = 90.7\%,$$

$$ДБО = \frac{\lambda dd + \lambda_S}{\lambda_D + \lambda_S} = \frac{\lambda_D - \lambda du + \lambda_S}{\lambda_D + \lambda_S} = \frac{524.1 - 48.588 + 304.9}{524.1 + 304.9} = 94.1\%.$$

В предположении, что опасные отказы составляют 50% от общего числа отказов, то есть $\lambda_D = \frac{\lambda}{2}$ (табл.В1 стандарта МЭК 61508-6, где λ – общая интенсивность отказа компонента), доля безопасных отказов рассчитывается по формуле

$$ДБО = \frac{1 + DC/100}{2}. \qquad (3)$$

В табл.5 приведены примеры соответствия показателей охвата диагностирования DC и доли безопасных отказов ДБО.

Таблица 5 – Соответствия показателей DC и ДБО для случая $\lambda_D = \frac{\lambda}{2}$

DC, уровень	–	низкий	средний	высокий
DC, %	0	60	90	99
ДБО, %	50	80	95	99.5

Как видно из табл.5, если нет информации об охвате диагностикой изделия (DC=0), то есть известны только показатели надежности *T*ср или λ, тогда следует принять значение ДБО = 50 %. В этом случае для комбинации элементов типа В с отказоустойчивостью, равной 1, согласно табл.3 максимально допустимым УПБ для функции безопасности, выполняемой этой комбинацией, является УПБ1.

В табл.5 оценки уровней DC (низкий, средний, высокий) указаны в соответствии с таблицей А1 Приложения А «Управление отказами в процессе эксплуатации» стандарта МЭК 61508-2. Таблица А1 «Ошибки и отказы, которые …учитываются при определении доли безопасных отказов» поддерживается таблицами А.2–А14 для отдельных компонентов или группы компонентов – электромеханические устройства, устройства ввода-вывода, шины, процессоры, датчики, исполнительные механизмы.

Некоторые примеры уровней и диапазонов охвата диагностикой различных подсистем (компонентов) приведены в табл.С2 стандарта МЭК 61508-6. В частности, для датчиков и исполнительных механизмов низкий охват диагностикой соответствует диапазону 50% – 70%, средний охват – диапазону 70% – 85%, высокий охват – диапазону выше 85%.

Несмотря на заявления производителей о соответствии отдельных компонентов определенным УПБ, следует принимать во внимание, что понятие УПБ относится к контуру ПАЗ, к функции безопасности, а не к свойству отдельного компонента.

Датчик УПБ1, подключенный к логическому вычислителю УПБ1 с выходом на конечный элемент с УПБ1, не всегда могут обеспечить УПБ 1 для функции безопасности. Более того, ошибочно полагать, что для обеспечения функции безопасности, например, УПБ2, достаточно, чтобы все компоненты соответствовали УПБ2 [2]. Окончательное решение принимается только после расчета сформированного контура ПАЗ.

Полнота безопасности для контура ПАЗ рассчитывается как сумма вероятностей отказов последовательно соединенных подсистем. В большинстве случаев необходимо выбирать устройства, которые могут обеспечить более высокий УПБ, чем это необходимо, чтобы весь контур достиг желаемого УПБ. Для решения данной задачи необходимо с помощью исходных данных, приведенных в РБ на компоненты контура ПАЗ, выразить надежность этих компонентов в терминах средней вероятности отказа на запрос или средней частоты опасных отказов и оценить достигнутую меру отказов функции безопасности с учетом архитектуры каждой подсистемы контура ПАЗ. Для этой цели доступны многие методы моделирования, такие как анализ деревьев неисправностей, структурные схемы надежности [3], сети Петри. Упрощенный подход, который может быть использован для оценки достигнутого УПБ, описан в приложении В МЭК 61508-6.

Средняя вероятность отказа на запрос (*PFDavg*) функции безопасности для режима с низкой интенсивностью запросов (не чаще одного раза в год) определяется как сумма средней вероятности отказа подсистемы датчиков $PFDavg_S$, средней вероятности отказа логической подсистемы $PFDavg_L$ и средней вероятности отказа подсистемы исполнительных элементов $PFDavg_{FE}$, то есть

$$PFDavg = PFDavg_S + PFDavg_L + PFDavg_{FE}. \quad (4)$$

Для режима с высокой интенсивностью запросов формула (4) для средней частоты опасных отказов контура ПАЗ имеет вид:

$$PFH = PFH_S + PFH_L + PFH_{FE}. \quad (5)$$

Компонентами подсистемы датчиков могут быть, например, датчики, искробезопасные барьеры, согласующие цепи, компонентами логической подсистемы – процессоры, сканеры, интерфейсные модули, а компонентами подсистемы исполнительных элементов – искробезопасные барьеры, привода и исполнительные механизмы.

Каждая подсистема представляет собой как одну или более голосующих групп 1oo1, 1oo2, 1oo2D, 2oo3 или 1oo3. Для каждой голосующей группы опубликованы таблицы, в которых заданы следующие исходные данные:

- межпроверочный интервал (Proof Test Interval) *TI* (6 месяцев, 1 год, 2 года, 10 лет);
- интенсивность опасных отказов (λ_D=0.5E-07, 2.5E-7, …, 2.5E-05);
- диагностическое покрытие DC (0%, 60%, 90%, 99%);
- коэффициент модели отказов по общей причине β (2%, 10%, 20%).

Для нерезервированной структуры 1oo1 средняя вероятность отказа на запрос рассчитывается по формуле, приведенной в подразделе B.3.2.2.1 стандарта МЭК 61508-6

$$PFDavg = \lambda du \frac{TI}{2} + \lambda dd \cdot MTTR , \qquad (6)$$

где *MTTR* – среднее время восстановления элемента.

Для голосующих групп 1oo2, 1oo2D, 2oo3 и 1oo3 в приложении B стандарта МЭК 61508-6 приведены приближенные расчетные формулы. Необходимость использования приближенных формул объясняется сложностью применения в инженерной практике точных формул, полученных на основе Марковских моделей. Отсюда и расхождения результатов расчетов по формулам с данными соответствующих таблиц при значениях интенсивности опасных отказов более 2.5E-06 для десятилетнего интервала между контрольными проверками (proof test). Кроме того, в п.B.3.1 МЭК 61508-6 представлены предположения, на которых основываются расчеты по приведенным формулам, и которые не всегда выполняются на практике. Для структуры 1oo2D есть дополнительное ограничение – интенсивность безопасных отказов принимается равной интенсивности опасных отказов. На практике это не всегда выполнятся. Кроме того, рекомендуется без объяснений физической сути использовать коэффициент K=0.98, который показывает «…эффективность межканального сравнения/механизма переключения…». Структура 1oo2D является более надежной, чем структура 1oo2, при высоком охвате диагностикой. Следует отметить, что буква D означает не просто диагностирование (оно присутствует во всех избыточных структурах), а динамическое диагностирование, потому что при нормальной работе реализуется логика 2oo2 для снижения вероятности ложного срабатывания. При отказе одного из каналов структура 1oo2D деградирует в структуру 1oo1. Из-за сложности реализации диагностирования двух каналов с высоким показателем DC структуры 1oo2D чаще используются в контроллерной части ПАЗ.

Если в реальной системе ПАЗ используются иные структуры, то необходимо учитывать тот факт, что при моделировании надежности с использованием программной реализации метода анализа деревьев неисправностей возможно занижение оценок средней вероятности отказа на запрос и средней частоты опасных отказов. Указанное занижение может достигать 15–20% при расчете контуров ПАЗ с УПБ1 [2]. В более надежных контурах это занижение незначительно.

Для ориентировочного расчета контура ПАЗ при неполной информации о надежности некоторых компонентов возможно использование интервальных оценок интенсивности опасных необнаруженных отказов, которые получены на основе анализа достаточно большого числа сертификатов компанией *exida*.

Таблица 6 – Обобщенные интервальные оценки интенсивности опасных необнаруженных отказов

Тип элемента	λdu н.гр	λdu в.гр	Tср (г)
Сигнализатор давления механический	50	1000	57.1
Датчик давления	20	150	380.5
Сигнализатор температуры механический	50	1000	57.1
Датчик температуры	25	90	634.2
Термопара	5	100	570.8
Сигнализатор уровня	50	1000	57.1
Датчик уровня радарный	70	750	76.1
Датчик уровня емкостной	50	150	380.5
Датчик уровня вибрационный	15	150	380.5
Датчик уровня ультразвуковой	40	150	380.5
Расходомер магнитный	100	400	142.7
Расходомер ультразвуковой	200	700	81.6
Расходомер вихревой	100	400	142.7
Процессор (ЦПУ)	3	300	190.3
Источник питания 24В	3	50	1141.6
Модуль аналогового ввода	50	150	380.5
Модуль дискретного ввода	50	150	380.5
Модуль дискретного вывода	10	30	1902.6
Привод пневматический поршневой	120	700	81.6
Привод гидравлический поршневой	130	1300	43.9
Привод гидравлический мембранный	110	910	62.7
Реечный пневмопривод	300	900	63.4
Клапан-бабочка с тройным смещением	450	800	71.4

В табл.6 использованы следующие обозначения:

- λdu н.гр, λdu в.гр – нижняя и верхняя границы интервальной оценки интенсивности опасных необнаруженных отказов соответственно (10^{-9} 1/ч);
- Tср (г) – минимальная средняя наработка до отказа в годах, рассчитанная по формуле $Tcp = \frac{1}{2 \cdot \lambda du \text{ в.гр}}$ в предположении, что интенсивность безопасных отказов равна интенсивности опасных отказов, при этом охват диагностикой опасных отказов DC = 0.

Имея информацию о значении интенсивности опасных необнаруженных отказов λdu, полученную из руководства по безопасности конкретного компонента, или используя ее интервальную оценку, можно по упрощенной формуле (6), которая широко используется в инженерной практике, определить уровни полноты безопасности в соответствии со стандартами МЭК 61508 (табл.7).

Таблица 7 – УПБ и показатели функциональной безопасности [2]

УПБ	PFDavg (низкая интенсивность запросов)	RRF (коэффициент снижения риска)	PFH (1/ч) (высокая интенсивность запросов)
4	$\geq 10^{-5}$ и $< 10^{-6}$	От 100000 до 10000	$\geq 10^{-9}$ и $< 10^{-8}$
3	$\geq 10^{-4}$ и $< 10^{-3}$	От 10000 до 1000	$\geq 10^{-8}$ и $< 10^{-7}$
2	$\geq 10^{-3}$ и $< 10^{-2}$	От 1000 до 100	$\geq 10^{-7}$ и $< 10^{-6}$
1	$\geq 10^{-2}$ и $< 10^{-1}$	От 100 до 10	$\geq 10^{-6}$ и $< 10^{-5}$

В табл.7 коэффициент снижения риска *RRF* рассчитывается как величина, обратная средней вероятности отказа на запрос *PFDavg*.

Заключение

Естественным и необходимым шагом для выполнения указаний Ростехнадзора [1] является разработка изготовителями компонентов, применяемых в системах ПАЗ,

руководств по безопасности в соответствии с приложением D стандарта МЭК 61508-2, в котором подробно изложены требования к содержанию этого документа. Тем не менее, существует сложный вопрос классификации безопасных и опасных отказов. Классификация отказов изделия иногда определяется ограничениями его применения. Отсюда возникают трудности оценки отказоустойчивости и доли безопасных отказов. Как правило, изготовитель или поставщик применяемого в ПАЗ изделия не имеет прямого представления о параметрах процесса и условий окружающей среды, средств и ресурсов для контрольных проверок и тестирования. Точно так же системный интегратор обычно не имеет достаточной информации о конструкции элемента и поэтому полагается на информацию, представляемую поставщиком.

Опираясь на многолетний международный опыт сертификации в области функциональной безопасности, формируются отечественные сертификационные центры, на сайтах которых можно получить информацию о процедуре сертификации, которая содержит следующие основные этапы: анализ и оценка комплекта документации, оценка системы менеджмента качества, подготовка отчета об оценке соответствия стандартам серии МЭК 61508 45].

Описанный в статье способ выбора компонентов для системы ПАЗ, в общем, соответствует способу 1_H, приведенному в стандарте МЭК 61508-2. Современная практика работ в области функциональной безопасности показывает, что также необходимо применение способа 2_H, основанного на получении данных о надежности компонентов от конечных пользователей.

Литература

1 Федеральные нормы и правила в области промышленной безопасности «Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств». Утверждены приказом РТН №533 от 15 декабря 2020 г.

2 Ландрини Г. Критерии выбора компонентов с уровнем SIL3 для РСУ и систем ПАЗ в соответствии со стандартами МЭК. Часть 2 // Стандартизация и сертификация. 2009, №4, С.80–88.

3 Можаева И.А., Струков А.В. Особенности оценки показателей функциональной безопасности систем противоаварийной автоматической защиты с использованием деревьев неисправностей // Надежность. 2022, №4, С.45–54.

4 Реестр сертификатов соответствия в системе Endurance (https://sil3.ru/reestr/).