Особенности построения современных систем ПАЗ

С.Л. Рогов (ООО «ТРЭИ ГМБХ»)

Сформулированы противоречия, имеющие место в отечественной нормативной базе в области построения систем ПАЗ. Представлены особенности новой архитектуры систем ПАЗ, основанной на функциональном принципе, показаны ее преимущества по сравнению с классическими архитектурными решениями.

Ключевые слова: подсистема противоаварийной защиты, АСУТП, опасные производственные объекты, функциональная архитектура, безопасность.

Среди многочисленных задач АСУТП одной из важнейших является обеспечение безопасного функционирования потенциально опасных производственных объектов (ОПО), которая обычно реализуется с помощью подсистем противоаварийной защиты (ПАЗ). Безопасность ОПО обеспечивается выполнением требований по защите от превышения давления, температуры, достижения предела опасной концентрации и т.д. Каждое из этих требований обеспечивается соответствующей функцией безопасности, согласно ГОСТ Р МЭК 61508-2007. Входными параметрами функции безопасности являются значения физических параметров (давления, температуры, уровня и др.), результатом выполнения функции безопасности является воздействие посредством исполнительного механизма и перевод ОПО в безопасное состояние.

Рассмотрим существующие на сегодняшний момент особенности построения систем ПАЗ.

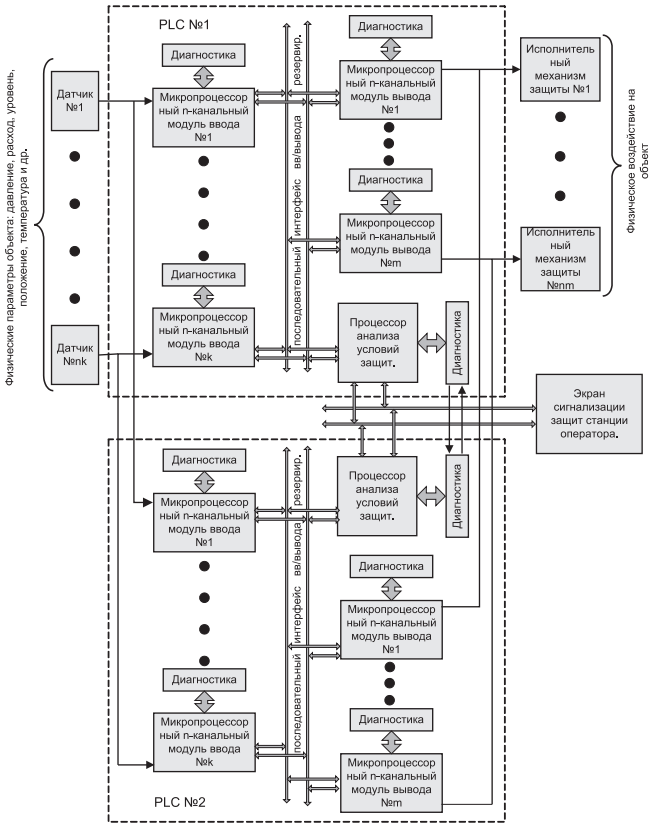

Рис. 1. Архитектура централизованной контроллерной, дублированной подсистемы ПАЗ, интегрированной в АСУТП

Противоречия в существующей нормативной базе

На практике проектантами, производителями и пользователями подсистем ПАЗ АСУТП используется около 10 основных нормативных документов. Самым последним по дате публикации является ГОСТ Р МЭК 61508-2007 «Функциональная безопасность электрических, электронных, программируемых электронных подсистем, связанных с безопасностью». Этот ГОСТ устанавливает общий подход к вопросам обеспечения безопасности для всего жизненного цикла подсистем, состоящих из электрических и/или электронных и/или программируемых электронных систем, которые используются для выполнения функций безопасности. Такой унифицированный подход был принят, чтобы разработать рациональную и последовательную техническую концепцию для всех электрических систем, связанных с безопасностью. Основной целью при этом является содействие разработке новых государственных и отраслевых стандартов. Остальные нормативные документы уже не соответствуют современным требованиям и часто

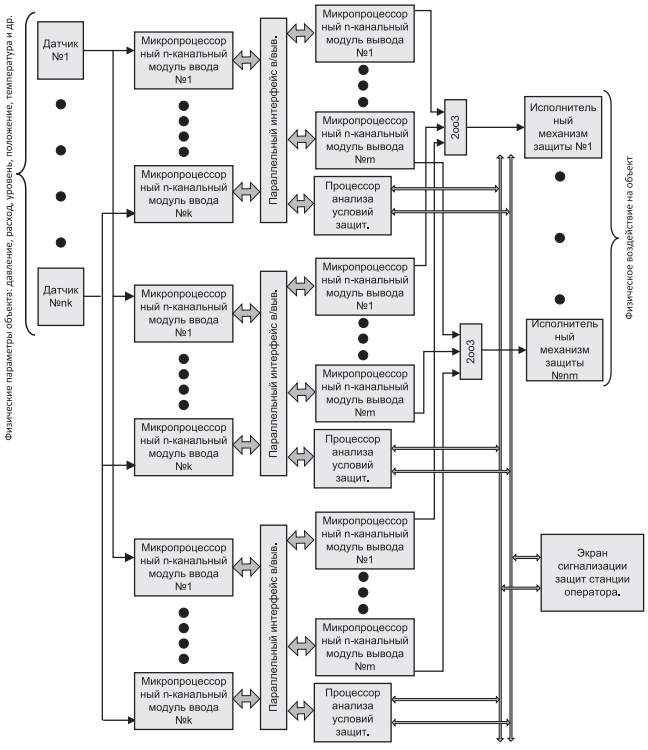

Рис. 2. Архитектура троированной контроллерной, централизованной подсистемы ПАЗ, интегрированной в АСУТП

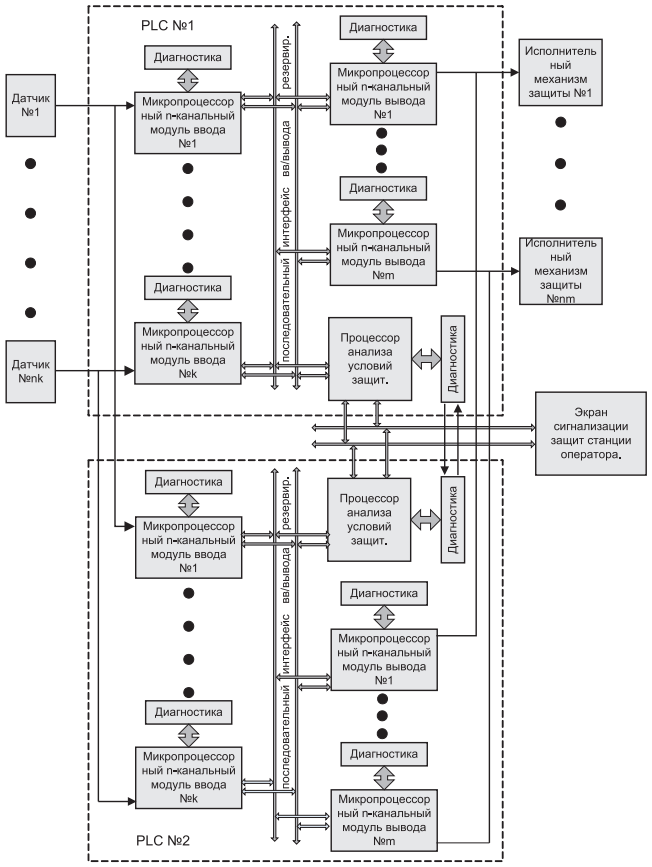

Рис. 3. Архитектура контроллерной, децентрализованной подсистемы ПАЗ, интегрированной в АСУТП

противоречат друг другу и ГОСТ Р МЭК 61508-2007. Приведение стандартов в соответствие его требованиям и разработка новых государственных стандартов и отраслевых нормативов практически не ведется.

Из российских стандартов, безусловно, одним из самых важных, является труд группы специалистов ОРГРЭС – РД 153-34.1-35.137-00. Этот документ и до сегодняшнего дня определяет требования к подсистемам ПАЗ и их функциональной безопасности в энергетике. Однако отсутствие в этом стандарте количественных критериев безотказности и нечеткость формулировок дает возможность проектировщикам и поставщикам оборудования вольно интерпретировать требования этого документа. Для нефтехимических предприятий промышленности основным нормативным документом являются ПБ 09-540-03 – «Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств». Но этот документ также не определил требования к функциональной безопасности подсистем ПАЗ, предоставив это право проектанту технологического оборудования. В пункте 6.1.3. требование сформулировано таким образом: «Оптимальные методы и средства противоаварийной автоматической защиты выбираются на основе анализа их опасностей технологических объектов, условий возникновения и развития возможных аварийных ситуаций, особенностей ТП и аппаратурного оформления. Рациональный выбор средств для систем ПАЗ осуществляется с учетом их надежности, быстродействия и т.п.». Концовка фразы рождает много неопределенности в понимании требований стандарта разными специалистами.

Необходимо вносить изменения в нормативные документы, кратко перечислим суть этих изменений:

• ввести в перечень защит РД 153-34.1-35.137-00 соответствие между видом защит и уровнем потенциальной опасности, согласно нормативам ГОСТ Р МЭК 61508-2007. Провести соответствие между конкретной функцией безопасности, видом защит и уровнем SIL оборудования обеспечения защит;

• дополнить терминологию ГОСТ 24.701-86 п. 1.6 «Группа функциональных подсистем» термином «функция безопасности» в соответствии с ГОСТ Р МЭК 61508-2007. Дополнить п. 1.6.1 требованием определения отдельных показателей надежности для каждой функции безопасности;

• дополнить ПБ 09-540-03 п. 6.2 «Перечень обязательных требований к АСУТП» требованием – реализация подсистемой ПАЗ АСУТП функций безопасности объекта;

• дополнить ПБ 09-540-03 п. 6.3.2 требованием – разработчиком подсистемы ПАЗ ИИУС ОПО должна быть выбрана математическая модель безотказности подсистемы, позволяющая производить контроль параметров безотказности на всех этапах жизненного цикла подсистемы ПАЗ.

Несоответствие стандартных архитектур современным требованиям

Из литературы[1] известны основные типы архитектур и способы резервирования:

1) классическая централизованная дублированная архитектура (рис. 1);

2) троированная (мажоритарная) централизованная архитектура ПАЗ (рис. 2);

3) резервированная децентрализованная архитектура (рис. 3).

Проведем оценку функциональной безопасности перечисленных архитектур (таблица).

Из таблицы видно, что общепринятые архитектуры не соответствуют актуальным требованиям построения систем ПАЗ. На основании этого анализа, специалистами фирмы TREI была разработана и запатентована новая архитектура систем ПАЗ, основанная на функциональном принципе и названная функциональной архитектурой ПАЗ (рис. 4).

Обязательным и необходимым условием существования новой архитектуры подсистемы ПАЗ является удовлетворение всем техническим требованиям ГОСТ Р МЭК 61508-2007. Проверим, как удовлетворяет функциональная архитектура критериям, перечисленным в таблице. Выбираем только те критерии, которым ни одна из существующих архитектур не соответствовала:

[1] *Федоров Ю. Н.* Справочник инженера АСУТП: Проектирование и разработка. М.: Инфра-Инженерия. 2008.

Таблица. Оценка функциональной безопасности архитектур систем ПАЗ

№	Наименование критерия	Архитектура рис.1	Архитектура рис.2	Архитектура рис.3
1.	Возможность построения систем ПАЗ с уровнем безопасности SIL3	+	+	+
2.	Возможность построения систем ПАЗ с уровнем безопасности SIL1, SIL2	+	-	+
3.	Наличие 100% резерва аппаратных средств	+	+	+
4.	Устойчивость к любой однократной неисправности	+	+	+
5.	Возможность построения децентрализованных систем	-	-	+
6.	Функциональная законченность реализации локальной функции безопасности	-	-	-
7.	Возможность тестирования методом «черного ящика»	-	-	-
8.	Возможность индивидуального тестирования, верификации и модификации функции безопасности	-	-	-
9.	Отсутствие аппаратной избыточности при создании малых систем ПАЗ	-	-	-
10.	Диагностика ошибок и восстановление при передаче данных внутри ПЛК	-	-	+
11.	Диагностика ошибок и восстановление при передаче данных во внешнюю среду	+	+	+
12.	Возможность программной блокировки функций ИИУС ОПО, не относящихся к функциям безопасности (управление, регулирование)	+	+	+
13.	Возможность аппаратной блокировки функций ИИУС ОПО, не относящихся к функциям безопасности (управление, регулирование)	+	-	+
14.	Возможность программной сигнализации (средствами экрана сигнализации станции оператора ИИУС ОПО) о включении функции безопасности	+	+	+
15.	Возможность аппаратной сигнализации (средствами табло сигнализации ИИУС ОПО) о включении функции безопасности	+	-	+

№ 6. «Функциональная законченность реализации локальной функции безопасности». Соответствие этому критерию – одно из главных преимуществ функциональной архитектуры. Каждая функция безопасности реализуется программно и аппаратно независимо. Каждая функция безопасности имеет весь набор необходимых метрологических и функциональных инструментов для реализации своего предназначения.

№ 7. «Возможность тестирования методом «черного ящика»». *Метод «черного ящика»*, согласно требованиям ГОСТ Р МЭК 61508-2007, подразумевает подачу всех возможных тестовых комбинаций входных воздействий на подсистему ПАЗ с целью проверки отсутствия ложных срабатываний функции безопасности подсистемы ПАЗ. В функциональной архитектуре число входов ограничено принадлежностью только к одной функции безопасности, что позволяет выполнять тестирование на практике. Стандартные дискретные входы проверяются на практике в двух устойчивых состояниях. Дискретные входы с контролем обрыва линии проверяются в трех устойчивых состояниях. Аналоговые входы проверяются в следующих устойчивых состояниях: 1) параметр сигнала в норме, 2) параметр сигнала соответствует предупредительной сигнализации, 3) параметр сигнала соответствует аварии. Каждое устойчивое состояние по уровню входного сигнала должно находиться не менее чем в трех Δmax от соседнего устойчивого состояния (Δmax – предельно допустимое значение приведенной погрешности для данного канала ввода).

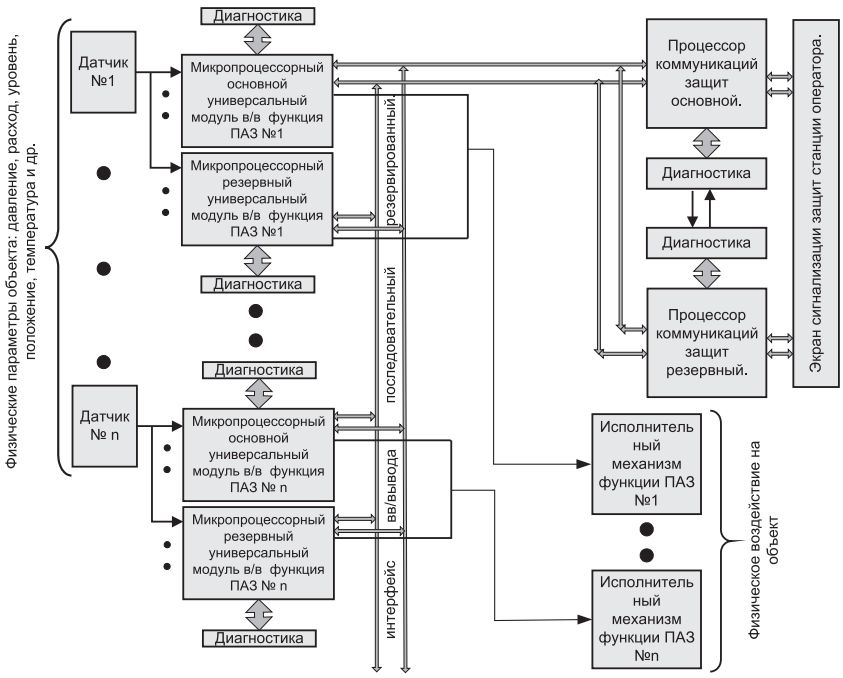

Рис. 4. Функциональная резервированная архитектура подсистемы ПАЗ интегрированной в АСУТП

№ 8. «Возможность индивидуального тестирования, верификации и модификации функции безопасности». Соответствие этому критерию является также одним из главных преимуществ функциональной архитектуры. Функциональная архитектура позволяет создавать аппаратно и программно независимые функции безопасности. Значит выполнение останова функции,

Какая разница между хорошим и прекрасным? Хорошее требует доказательств, а прекрасное не требует.
Вольтер

загрузки тестовых приложений, ремонт, верификация и модификация функции может выполняться индивидуально. На практике это значит, что можно проводить все необходимые манипуляции с подсистемой ПАЗ без остановки ТП. Так как по технологическим требованиям практически все ответственные исполнительные механизмы имеют дублирование функции безопасности или ручное дублирование, то проверяемую функцию можно вывести из режима дублирования или перевести временно на ручное управление и провести все необходимые манипуляции, а после завершения работ провести индивидуальное тестирование или верификацию. В существующих архитектурах такие действия невозможны и запрещены, так как в случае ошибки персонала возможна потеря контроля над всей подсистемой ПАЗ, а не над одной конкретной функцией. Временная потеря одной функции безопасности легко компенсируется организационными методами.

№ 9. «Отсутствие аппаратной избыточности при создании малых подсистем ПАЗ». Функциональная архитектура подсистем ПАЗ благодаря применению универсальных интеллектуальных модулей ввода/вывода позволяет создавать подсистемы без аппаратной избыточности. На модули устанавливаются только те каналы ввода/вывода, которые принимают участие в работе конкретной функции безопасности. В других архитектурах подсистем ПАЗ пользователь вынужден применять стандартные многоканальные модули ввода/вывода кратностью 8 или 16 каналов. Таким образом, например, используя в малой подсистеме ПАЗ только один канал ввода сигнала термопреобразователя, пользователь применяет 16-канальный модуль, а 15 неиспользуемых каналов увеличивают интенсивность отказов подсистемы и ухудшают экономические параметры подсистемы ПАЗ и ИИУС в целом.

Новые качественные характеристики подсистемы ПАЗ, полученные благодаря функциональной архитектуре

Возможность реализации внутри одной функции безопасности параметрических каналов разной метрологической точности. Использование в качестве конструктива универсального интеллектуального модуля ввода/вывода позволяет применять входные и выходные аналоговые и импульсные параметрические каналы ввода/вывода с разными точностными характеристиками, что было невозможно или экономически невыгодно в известных ранее архитектурах при применении многоканальных модулей ввода/вывода.

Возможность реализации внутри одной подсистемы ПАЗ функций безопасности с разными уровнями SIL. В настоящее время, если в подсистеме присутствуют несколько функций безопасности разного уровня SIL, то подсистему проектируют по требованиям максимального из существующих в подсистеме уровней. Например, если в подсистеме пять функций уровня SIL1, четыре функции уровня SIL2 и одна функция безопасности уровня SIL3, то выбирают все программно-аппаратное обеспечение, соответствующее уровню SIL3. При применении функциональной архитектуры имеется возможность выбирать программно-аппаратную реализацию функции безопасности в соответствии с индивидуальным уровнем SIL, то есть производить дублирование или резервирование функции индивидуально без зависимости от других функций подсистемы.

Возможность корректировки показателей безотказности подсистемы ПАЗ по диагностическим данным в процессе эксплуатации. Диагностические возможности элементов современных подсистем ПАЗ позволяют в процессе эксплуатации производить мониторинг основных эксплуатационных параметров элементов подсистемы. Изменение этих характеристик позволяет производить перерасчет безотказности всей подсистемы ПАЗ по каждой функции индивидуально.

Возможность плановой замены элементов подсистемы ПАЗ с прогнозируемым изменением безотказности. Благодаря свойствам функциональной архитектуры у пользователя появляется возможность использовать в подсистемах ПАЗ элементы с низкими показателями безотказности, но производить расчет общих показателей подсистемы с учетом плановой замены элементов. Используя при этом функциональную архитектуру, замену можно производить без останова всей подсистемы ПАЗ и ОПО, так как функциональная архитектура имеет в своем составе ограниченное число элементов. Замена одного из них на новый элемент существенно улучшает параметры безотказности конкретной функции безопасности.

Основные «вынужденные» нарушения при эксплуатации систем ПАЗ

Раскроем термин «вынужденные» – это означает, что эксплуатирующие организации идут на эти нарушения, руководствуясь экономическими соображениями, и оправдывают их несовершенством нормативных документов.

1. Продление времени эксплуатации ПАЗ без проведения периодической процедуры верификации. Как правило, это происходит по технологическим причинам, когда время между процедурами верификации меньше времени безостановочной эксплуатации объекта, или по технологическим причинам переносится срок профилактической остановки объекта (временное отсутствие дублирующих мощностей, смена режима эксплуатации или др.).

Устранить эти противоречия можно, если ввести в практику норматив остаточного эксплуатационного ресурса, который можно рассчитывать по фактическим эксплуатационным данным.

2. Продление времени эксплуатации ПАЗ свыше межповерочного интервала (МПИ) средств измерения (СИ), участвующих в работе ПАЗ (ПЛК, датчики, исполнительные механизмы и др.). Это происходит по причинам аналогичным п. 1. и приводит к формальному нарушению закона о средствах измерения и стандарта ГОСТ Р 8.596-2002. ГСИ. «Метрологическое обеспечение измерительных систем. Основные положения». Устранить это нарушение можно двумя способами: 1) применять СИ классом ниже, имеющие больший МПИ, если это не противоречит требованиям технологии; 2) производить поверку СИ высокого класса на большую погрешность, и требовать от производителя СИ внесения в сертификат и методику поверки градацию МПИ пропорционально увеличению погрешности.

3. Фактическая замена элементов ПАЗ в интервале между процедурами верификации без проведения верификации по факту замены. Формально такая процедура нарушает требования ГОСТ Р МЭК 61508-2007, особенно если это касается ПЛК или других элементов, связанных с функциональной безопасностью. Но реальный жизненный цикл систем ПАЗ допускает наличие, пусть незначительной, но реальной интенсивности отказов элементов ПАЗ. Сама по себе такая ситуация – предмет отдельного расследования того, что явилось причиной: неверный расчет показателей надежности системы ПАЗ, неверный выбор оборудования или брак производителя оборудования. В любом случае решение данной проблемы наиболее безопасно, если система построена по функциональной архитектуре, так как пользователь имеет возможность замены элемента только в одной функции безопасности, без останова остальных. Более того, в некоторых случаях технология позволяет без остановки процесса произвести верификацию этой функции.

Сертификат SIL для систем ПАЗ

Последнее время в тендерных документах стали появляться требования к оборудованию подсистем ПАЗ с указанием уровня SIL в соответствии с ГОСТ Р МЭК 61508-2007. Фирма TREI единственный на сегодняшний момент российский разработчик и производитель контроллерного оборудования для систем ПАЗ, прошедший сертификацию в немецком центре TÜV на соответствие уровню SIL3 (всего существует 4 уровня SIL). Поэтому на основании опыта сертификации и знания процедур, приведем некоторые рекомендации разработчикам систем ПАЗ и устроителям тендерных процедур.

a. *Наличие сертификата SIL у производителя оборудования не означает, что все его оборудование соответствует данному интегральному уровню безопасности.* Требуйте у поставщика копию протокола испытаний, в которой есть приложение с перечнем конкретных модулей, устройств и конкретного базового ПО (!), которые проходили испытания и получили сертификат. Так системные интеграторы известной мировой фирмы производителя ПЛК для систем ПАЗ предлагают в России состав оборудования, который в Германии им применять не разрешат, так как из списка разрешенных для уровня SIL3 там присутствуют только центральные процессорные модули.

b. *Наличие в тендерных документах требований по соответствию оборудования уровню SIL неправомочно без аттестации опасных объектов производства по уровню опасности, согласно ГОСТ Р МЭК 61508-2007.* То есть сначала необходимо определиться с уровнем опасности объекта, критериями и вероятностями рисков, потом определить соответствие уровня SIL этим критериям. Даже два одинаковых объекта (например, установка риформинга нефти), расположенные в городской черте и в степи, имеют разные уровни потенциальной опасности.

c. *Несоответствие величины интенсивности отказов в технической документации на оборудование величинам в протоколах испытаний.* Например, в технической документации одного из производителей датчиков для систем ПАЗ указано значение интенсивности не детектируемых опасных отказов λ_{DU}=11FIT (примечание: 1 FIT= 10^{-9}1/ч). В протоколе сертификации на уровень SIL на тот же прибор определены разные виды отказов, при этом значение интенсивности не детектируемых опасных отказов (Dangerous undetected failure) равно 37 FIT.

Пользователь должен знать, что если в его системе ПАЗ не анализируются диагностические сообщения с прибора, то общая интенсивность отказов приближается к 1000 FIT, но и сам параметр λ_{DU} в документации занижен более чем в 3 раза по сравнению с протоколом SIL. К чести производителя, протокол испытаний на соответствие уровню SIL3 выложен в открытом доступе и ссылка на него есть с информационной страницы прибора на сайте производителя. Поэтому дело потребителя, как воспользоваться этой информацией.

Выводы

Таким образом, основным действующим документом в России стал переведенный на русский язык стандарт IEC 61508, который в виде национального стандарта называется ГОСТ Р МЭК 61508-2007. Одна из главных его целей – служить базовой основой для разработки отраслевых стандартов, отвечающих специфическим требованиям конкретных отраслей. К сожалению, практически не работают как создатели стандартов такие известные организации, как ОРГРЭС, ВТИ и др. Поэтому создание новых отраслевых нормативов по системам ПАЗ – удел энтузиастов или лоббистов техники и решений конкретных производителей.

Рогов Сергей Львович *– ген. директор ООО "ТРЭИ ГМБХ".*
Контактные телефоны: (8412) 55-58-90, 49-95-39.
E-mail: rogov@trei-gmbh.ru http://www.trei-gmbh.ru