



SIL – ЭТО НЕСЛОЖНО

Michael A. Mitchell

От редакции. Аббревиатур в англоязычной технической литературе больше даже, чем в свое время в советском государственном устройстве. Едва некое словосочетание становится общепупотребимым, его записывают с заглавных букв, а затем до них и сокращают.

Но далее, по мере практического применения, смысл аббревиатур может оказаться шире первоначального. Они становятся «устойчивыми», практически самостоятельными словами. В таких случаях, особенно если эти новые слова являются четкими терминами в рамках специфической концепции, их перевод (замена кириллической аббревиатурой) часто бывает не вполне адекватен и неудобен для понимания. Лучше оставлять в употреблении латинские буквы.

Вышесказанное в полной мере относится к англоязычной терминологии, принятой в сфере безопасности. Предлагаемая вашему вниманию статья, опубликованная в летнем номере журнала Valve Magazine 2011 г., посвящена разъяснению данной терминологии американским арматуристом. Но, думается, и для российских специалистов было бы нелишним приобщиться к пониманию своих зарубежных коллег. Пусть в РФ система безопасности устроена пока несколько иначе, получить представление о том, как она устроена в мире, полезно как для общей эрудиции, так и в практической плоскости – ведь если вам придется поставлять арматуру для объектов, регламентируемых стандартами IEC, вы напрямую столкнетесь со всем тем, о чем рассказано в статье.

Три основных термина, которым посвящена статья, таковы:

SIS – Safety Instrumented System. Мы предлагаем такой перевод данного термина: «Аппаратная Система Безопасности». SIS – это система управления производственными процессами, направленная на предотвращение опасных сбоев, вот именно в «железном» исполнении. То есть, это некоторый комплекс устройств, автоматически реагирующий на отклонения критических параметров процесса (таких параметров, изменение которых за пределы определенных рамок представляют угрозу безопасности) и приводящий их к норме.

Конечно, система безопасности предприятия в целом включает в себя не только аппаратную часть, но и организационную. То есть, проблемы халатности и лени персонала, а также вопросы открытия задвижек с помощью лома и кувалды к понятию SIS отношения не имеют.

SIF (Safety Instrumented Function) – Аппаратная Функция Безопасности, часть SIS, отвечающая за отдельно взятый критический параметр процесса. Представляет собой реализованный аппаратно контрольно-информационный цикл (систему с обратной связью). SIS может состоять из одной или нескольких SIF, ведь параметров, которые требуется удерживать в установленных пределах, у одного процесса может быть сразу несколько.

SIL (Safety Integrity Level) – Системный Уровень Надежности. Статья как раз и посвящена тому, что это такое.

А. Горелов

Не все понимают, что такое SIL и как он задается. Между тем, каждый, кто имеет дело с оборудованием, используемым в системах безопасности, обязан знать, откуда взялась эта аббревиатура и что она означает.

Многие пользователи арматуры, инженеры трубопроводных систем и арматуростроители имеют дело с оборудованием, используемым в системах безопасности. Но нередко «люди от арматуры», будучи знатоками механических устройств, не особо сведущи в КИП. А ведь сегодня каждый специалист, имеющий дело с арматурой, может оказаться ответственным за оборудование, предназначенное (причем иногда ошибочно) к применению там, где имеется системный уровень надежности (SIL). Вопрос присвоения SIL тому или иному устройству может смущать и напрягать того, кто не совсем понимает, что означает этот термин.

Данная статья написана, чтобы помочь людям, далеким от КИП, получить общее представление о SIL и о том, как его учитывать, используя и покупая арматуру и приводы – в частности, когда они используются в испытаниях неполного хода (PST¹). Из статьи вы сможете в общих чертах уяснить основные концепции, связанные с SIL, осознавая при этом, что всегда найдутся исключения из правил.

Мы надеемся, что эта статья сорвет покровы тайны с понятия SIL и поможет вам преодолеть смущение и недоверие, заменив эти глупые переживания на чувство чего-то понятного и привычного, и позволит арматурщикам делать свое дело увереннее и лучше.

Что такое SIL?

Чтобы разобраться, что такое SIL, давайте для начала выясним, откуда взялось это понятие и что оно в себе включает.

В результате промышленных аварий 80-х годов, таких как катастрофа на заводе ядохимикатов в Бхопале² или взрыв на платформе Piper Alpha в Северном море³, в мире резко возросло внимание к вопросам промышленной безопасности. По нынешним временам нам с вами никуда не деться от тех рисков, которые связаны с опасными производствами, ведь такие вещества как очищенное топливо, гидрокарбонаты, продукты нефтехимии – столь необходимы для современного образа жизни.

И мы постоянно ищем возможности продлить работу подобных производств на максимально длительный срок – на столько месяцев и лет, на сколько это возможно – ведь их остановка чревата падением прибылей. Необходимость постоянной работы промышленных систем, вкуче с появлением современных процедур без-

¹ Partial Stroke Testing.

² Бхопальская катастрофа – крупнейшая в мире техногенная катастрофа. Авария произошла на заводе Union Carbide 3 декабря 1984 года. Аварийный выброс паров метилизоцианата (сырья для производства инсектицида «Севил») повлек смерть по меньшей мере 18 тысяч человек, число пострадавших оценивается в 150–600 тыс. человек (прим. ред.).

³ 6 июля 1988 г. на нефтяной платформе Piper Alpha случилась крупнейшая катастрофа в истории данной отрасли, когда в результате взрыва газа погибло 167 человек. Застрахованный ущерб составил 3,4 млрд долл. (прим. ред.).

Об авторе

Michael A. Mitchell, менеджер Cameron Flow Control, DYNATORQUE, имеет более чем 34-летний опыт продаж приводной арматуры.

Пишите ему по адресу: mike.mitchell@c-a-m.com.

Данная статья является адаптированным вариантом доклада, сделанного автором на конференции Valve World Conference 2010.

опасности, развитием инжиниринга и многими другими обстоятельствами приводит к резкому увеличению времени между остановами на ТО (для обслуживания оборудования и проверки систем безопасности). Что, в свою очередь, ведет к повышенному вниманию к вопросам снижения рисков.

Растущее число промышленных аварий и усилившееся в результате давление со стороны страховых компаний и правительственных структур побудило создать стандарты для классификации промышленных систем безопасности. Надзорные органы поставили перед заводами-производителями такой вопрос:

«Если завод намерен продолжать безостановочную работу длительное время, как мы можем удостовериться, что системы безопасности завода работают правильно, когда в том возникнет нужда?»

Промышленность ответила на этот вопрос приемом ряда стандартов (по сути, «полугосударственных» нормативных актов), таких как ISA-S84.01 и IEC 61508/61511, измеряющих требуемый уровень эффективности функционирования этих систем. Строгое соблюдение стандартов ныне фактически стало «передовой практикой», которой стараются придерживаться все ведущие производители. Заметим, что стандарты – это не предписания и инструкции, они ориентированы на результат. Они гласят лишь о том, какой уровень должен быть достигнут, но не регламентируют, каким образом это сделать, побуждая конечных пользователей самих решать, как данного уровня достичь.

Аппаратные системы безопасности разработаны, чтобы предотвратить или снизить последствия опасных инцидентов (событий) путем приведения процессов в безопасное состояние, когда нарушаются регламентированные условия работы. Аппаратная система безопасности SIS – это обычно Система аварийного останова, Система защитной блокировки или Система безопасного останова. Каждая система SIS включает в себя одну или несколько аппаратных функций безопасности SIF. Эти функции могут быть, например, таковы:

- если давление в емкости стало слишком высоким – открывается предохранительный клапан;
- если раствор в емкости стал слишком горячим – впускной паровой клапан закрывается.

Конечно, любая аппаратная реализация функции безопасности – это комбинация целого ряда устройств: логических контроллеров, сенсоров, электромагнитных катушек и исполнительных устройств типа приводного клапана. Каждая из аппаратных функций, образующих систему безопасности, обладает некоторым системным

уровнем надежности (SIL). Эти уровни у разных аппаратных функций могут быть одинаковыми или же отличаться, в зависимости от особенностей регулируемых процессов. Типичное заблуждение состоит в том, будто вся система должна иметь один и тот же уровень надежности для всех функций SIF.

Уровень SIL, по сути, отражает надежность системы с точки зрения Вероятности Отказа при Запросе⁴. Поскольку наша цель – «снизить риск», сначала мы должны понять, что такое «риск». Простейшее выражение для риска таково:

$$\text{Риск} = \text{Вероятность} * \text{Последствия}.$$

«Вероятность» можно понимать как «частоту опасных ситуаций» (то есть, насколько часто процесс выходит за рамки нормативных условий, из-за чего должен быть приведен в безопасное состояние), а «Последствия» – как последствия опасной ситуации (что случится с производством, людьми и внешней средой в случае, если процесс не будет приведен в безопасное состояние).

Откуда берется значение SIL, кем и как оно определяется? Для этого существует несложный порядок действий:

- Принимается решение, что на заводе должен выполняться международный стандарт по системам безопасности, обычно IEC 61511;
- На заводе формируется рабочая группа по оценке возможных опасностей и работоспособности оборудования HAZOP.⁵ По существу, процедура такой оценки являет собой полное описание всех процессов, включая систематический анализ каждой их составляющей на предмет того, какие отклонения от заданного режима работы могут в принципе иметь место. После выявления возможных отклонений выясняется, способны ли эти отклонения или их последствия негативно повлиять на безопасную и эффективную работу производства. При необходимости принимаются меры для исправления ситуации. По большому счету, при анализе широко используется закон Мерфи: «Всё, что способно пойти не так – обязательно пойдет не так». Рабочая группа как раз и должна конкретно разобраться, что именно может пойти не так. Группа должна состоять из инженеров, проектировавших технологический процесс, операторов процесса, ремонтников, специалистов по КИП и т.п.
- В ходе оценки опасности и работоспособности все аппаратные средства защиты (которые и представляют собой SIS) идентифицируются и проверяются на предмет своей способности предотвратить собой или смягчить

его последствия. Присвоение уровня SIL каждой системе SIS – это следующий шаг после того, как процедура оценки подтвердит способность SIS обеспечить необходимое снижение риска.

- По существу, рабочая группа выявляет, какой максимальный риск несет в себе производственная система без учета всех SIF, и определяет влияние возникающей опасной ситуации, т.е. ее последствия.
- Последствия отказа могут быть самыми разными. Их нужно конкретно оценить. То есть, группа должна сформулировать нечто вроде: «В случае отказа системы...»
 - Завод потеряет \$15000 в день;
 - Завод потеряет \$1 млн в день;
 - Завод встанет на три недели;
 - Существует высокая вероятность нанесения ущерба жизни и здоровью персонала и окружающей среде;
 - Существует высокая вероятность взрыва и нанесения ущерба жизни и здоровью людей за пределами территории завода.

В конечном счете, владельцам завода и его оперативному руководству следует самим определиться, какой уровень риска приемлем согласно их собственным критериям (передовой опыт, философия компании, условия страхования, финансовые возможности, и т.д.). Границы риска субъективны и зависят от многих факторов (например, от местоположения завода).

Когда границы риска установлены, могут быть установлены и уровни SIL отдельно для каждой из функций SIF, составляющих систему безопасности SIS.

Роль вероятности

Прежде чем выяснять, как присваивается численное значение SIL, нам нужно лучше понять, что такое Вероятность Отказа при Запросе (PFD).

Проще выразить вероятность с точки зрения отказов, нежели с точки зрения работоспособности. Как указано в упомянутых выше стандартах, есть четыре уровня SIL, от 1 до 4; чем выше SIL, тем выше уровень безопасности и тем ниже вероятность, что система вдруг не сработает должным образом (*см. таблицу 1*).

Разные уровни SIL хорошо бы еще сопоставить с упомянутыми выше последствиями отказа. (Чем страшней последствия – тем, вообще говоря, выше должен быть SIL.)

Для целей данной статьи уместно думать о SIL как о «степени уверенности в том, что наша система будет работать, когда мы от нее этого хотим». (Как правило, SIL 4 за пределами тех возможностей, которые мы наблюдаем в промышленности.) А «аппаратную функцию» можно представить себе как систему аварийного останова, обычно включающую в себя сенсор определенного типа (давление, уровень жидкости, температура) и логический

⁴ Probability of Failure on Demand – PFD.

⁵ Hazard and Operability.

Таблица 1. Системные уровни надежности

Системный уровень надежности	Степень снижения риска	Вероятность Отказа при Запросе
SIL 4	от 100,000 до 10,000	от 10 ⁻⁵ до 10 ⁻⁴
SIL 3	от 10,000 до 1,000	от 10 ⁻⁴ до 10 ⁻³
SIL 2	от 1,000 до 100	от 10 ⁻³ до 10 ⁻²
SIL 1	от 100 до 10	от 10 ⁻² до 10 ⁻¹

контроллер, который посылает сигнал на арматурный исполнительный узел. Который, в свою очередь, может состоять из привода (пневматического, электрического, гидравлического и т.п.), электромагнитного клапана, клапана-разрядника и исполнительного элемента – предохранительного клапана как такового. «Система» может состоять из нескольких аппаратных функций, допустим, она могла бы включать пять клапанов аварийного останова, защищающих сосуд под давлением, используемый в производственном процессе. А может быть и так, что единственная функция составляет всю аппаратную систему безопасности SIS.

Итак, рабочая группа должна определить уровень SIL, основываясь на оценке вероятности отказа PFD. Майкл Янг из Джeneral Мониторс⁶ хорошо рассказал об этом в своей статье «Сколько безопасности мне нужно?»:

Простой пример поможет проиллюстрировать принципы SIS, SIF и SIL. Представим себе емкость, в которой под давлением находится легко воспламеняющаяся жидкость. Она обслуживается под проектным рабочим давлением с помощью обычной системы управления. В случае сбоя системы управления давление в емкости может стать слишком высоким, что приведет к ее повреждению, утечке содержимого, его воспламенению и даже взрыву. Если владелец оборудования считает, что риск такого сценария слишком высок, должна быть внедрена аппаратная система безопасности (SIS), чтобы в дальнейшем снизить риск до приемлемого уровня.

Аппаратная система безопасности независима от основной системы управления и действует для того, чтобы предотвратить или ослабить опасное состояние системы, связанное с ростом давления. SIS включает в себя SIF, объединяющую датчик, реагирующий на завышенный уровень давления, логический контроллер и электромагнитный клапан, который может сбросить среду из предохраняемой емкости (в факельную трубу, во внешнюю среду, в резервный бак), нормализовав давление в ней.

Если согласно оценке опасности и работоспособности (HAZOP) требуется снизить риск более чем в 100 раз, для функции SIF будет установлен системный уровень надежности SIL = 2. Потребуется рассчитать компоненты аппаратной функции, дабы убедиться, что вероятность отказа при запросе меньше 10^{-2} , что и будет означать, что SIL = 2 и риск снижен в 100 раз. Данная аппаратная функция может быть единственной в системе безопасности, или же система может быть композицией нескольких функций, предназначенных для предотвращения других недопустимых состояний оборудования.

Из **таблицы 1** и из приведенного выше примера видно, что численное значение SIL равно десятичному логарифму минимального значения снижения риска, SIL 1 = 10, SIL 2 = 100. Теперь нам несложно понять, что значит SIL.

SIL и арматуростроение

Поскольку данная статья в первую очередь для тех, кто не силен в вопросах КИП, им полезно будет узнать,

⁶ GENERAL MONITORS – американская компания, производящая продукцию для предприятий нефтегазового комплекса: инфракрасные детекторы, датчики углеводорода, газовые детекторы.

как SIL применяется в производстве арматуры и приводов.

Рабочая группа HAZOP внимательнейшим образом изучает автоматизированные системы безопасности, всегда включающие в себя арматуру, которая должна сработать, чтобы привести технологический процесс в безопасное состояние, если какие-то его рабочие параметры будут выше нормы. Для простоты мы будем говорить об устройстве аварийного останова (ESD), соответственно, будем иметь в виду аварийный клапан⁷.

Рабочая группа хочет знать, какова вероятность того, что клапан сработает, когда это будет нужно. Она проводит анализ рисков и присваивает некоторый уровень SIL системе аварийного останова. SIL касается всей этой системы: и сенсора, и клапана как такового, и всего, что между ними. Важно понимать, что SIL присваивается системе в целом, охватывая все ее отдельные элементы. Поэтому не может быть, например, привода с уровнем надежности SIL 3, цифрового контроллера уровня 3 или электромагнитного клапана SIL 3. Все это – просто элементы, достаточно надежные для того, чтобы быть приемлемыми в условиях SIL 3.

То есть, когда речь идет об оборудовании для управления потоками рабочих сред, неуместно говорить: «Это – SIL 2». Правильная формулировка такова: «Это подходит для SIL 2». Точно так же некорректен вопрос консультанта или конечного пользователя поставщику: «Какой у вашего оборудования SIL?» Правильнее спрашивать о характерных рисках отказов.

В вопросе о том, может ли данное оборудование использоваться в системах с определенным уровнем SIL, определяющим фактором являются показатели, отражающие степень его надежности, такие как Вероятность Отказа при Запросе (PFD).

Для производителей и потребителей арматуры актуальна Средняя Вероятность Отказа при Запросе (PFD_{AVG}) Как показано на **рис. 1** и **2**, вероятность отказа резко растет вскоре после каждого испытания полного цикла. Видно, что испытания неполного хода арматуры существенно снижают среднюю вероятность отказа. Другими словами, неполный ход повышает уверенность в том, что система и арматура сработают, когда это будет нужно (**рис. 2**).

В связи с необходимостью наращивать надежность и с желанием конечных пользователей соответствовать современным стандартам безопасности, возникла целая индустрия испытаний неполного хода. На рынке, как грибы после дождя, появляются новые и новые, все более изощренные продукты, обещающие сделать ваши SIS надежнее. В итоге голова идет кругом не только у поставщиков, но и у консультантов, да и у конечных пользователей тоже.

Чтобы разобраться в ситуации, представим себе систему безопасности, которая включает в себя 10 аппаратных элементов и должна иметь SIL 2. Проиллюстрируем выбор устройств (приборов и оборудования), необходимых для комплектации системы, таким образным примером:

⁷ Клапан аварийного останова, или клапан аварийной отсечки (**прим. ред.**).

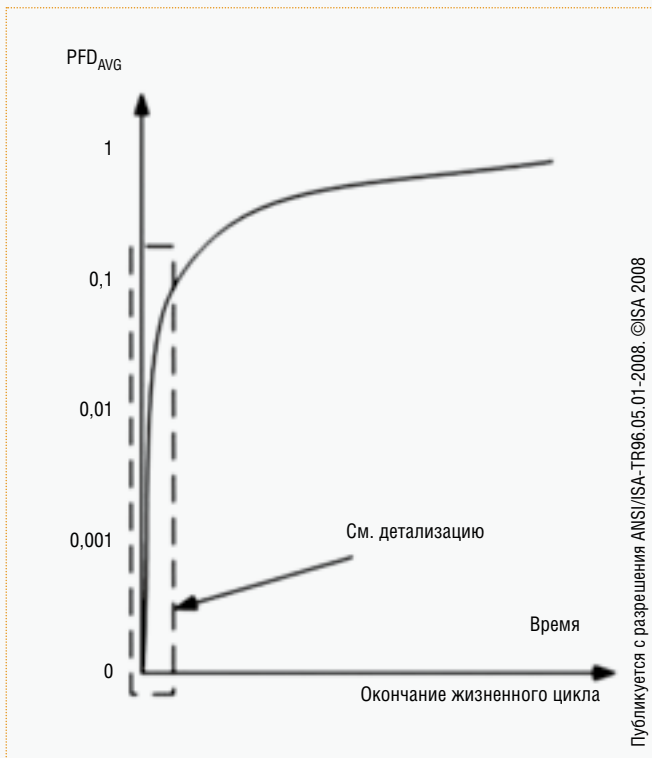


Рис. 1. Средняя Вероятность Отказа при Запросе (PFD_{AVG}) и график жизненного цикла арматуры

Пусть у нас есть бутылка емкостью 1 литр. Литр — тот максимальный объем жидкости, который в нее можно налить — это как бы то максимальное количество отказов, которые вправе случиться в системе безопасности. Ну, то есть, у нас в «бюджете» имеется лишь 1000 мл отказов. Если мы превысим этот «бюджет», то наша система — это не система SIL 2.

А вокруг бутылки расставлены 25 чашек по 200 мл каждая, и в каждой разное количество жидкости. Многие заполнены более чем наполовину, иные почти полны. Если мы объединим воду из всех чашек, общий ее объем явно превысит 1 литр.

Эти 25 чашек иллюстрируют разнообразные компоненты, которые могут быть выбраны для нашей 10-компонентной системы безопасности — различные контроллеры, соленоиды, арматура, и т.п. Уровень жидкости в некоей чашке отражает средний уровень вероятности отказа PSD_{AVG} соответствующего устройства.

Если рассматривать чашки по отдельности, то жидкость из каждой, конечно же, никогда не заполнит нашу литровую бутылку. Но уровень SIL 2 мы получим только в том случае, если общий объем жидкости в выбранных нами десяти чашках поместится в бутылку, то есть будет меньше 1 литра.

И выходит вот что: каждое из 25 предлагаемых к установке устройств может иметь характеристики, допускающие его использование в системе SIL 2. Одна-

ко, если суммарный риск⁸ всех 10 выбранных элементов превысит требуемый для системы SIL 2 уровень, присвоить этой системе SIL 2 мы не сможем. Мы должны правильно скомплектовать систему, чтобы уложиться в ее «бюджет риска».

Главное, что мы хотели показать приведенным примером: тот факт, что отдельные элементы оборудования «имеют» SIL 2 (если все же выразаться таким не вполне корректным образом) еще не означает, что система безопасности тоже «автоматически» будет SIL 2. Конечный пользователь или его консультант по безопасности должен произвести расчеты, основываясь на вероятности отказов и других данных, рассчитав влияние каждого компонента на уровень надежности системы.

Порой встречаются заявления типа: «По нашим оценкам, данное оборудование может быть использовано в системах безопасности вплоть до SIL 3 как единственный компонент». Подобное утверждение может быть обоснованным, но все-таки оно вводит в заблуждение, имея весьма и весьма условный смысл. Нет, ну вправду: многие ли системы безопасности состоят из единственного компонента? На самом деле, чтобы выяснить, может ли конкретное устройство ис-

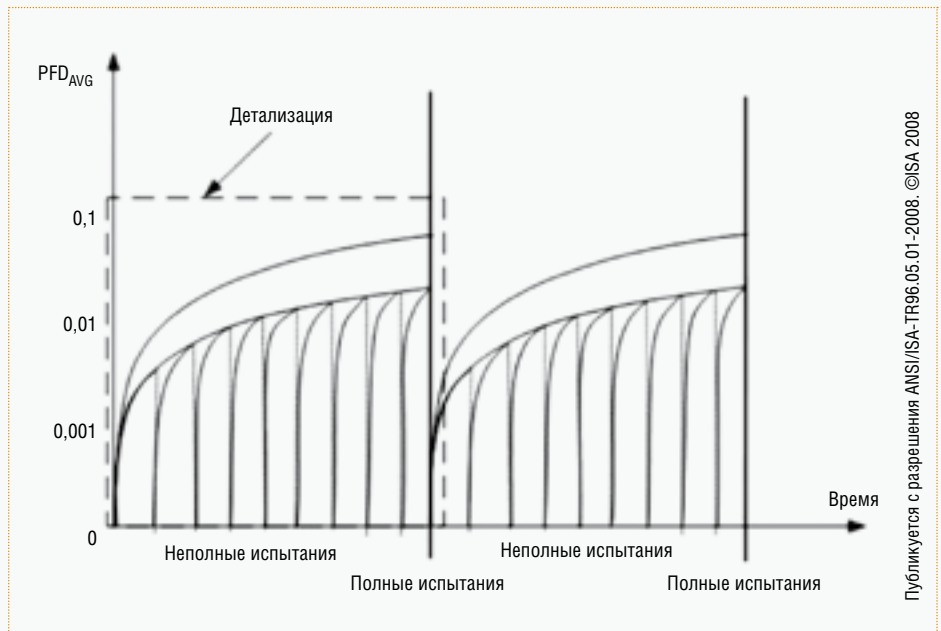


Рис. 2. Средняя Вероятность Отказа при Запросе (PFD_{AVG}) снижается благодаря испытанием неполного хода (PST) вкпе с испытаниями полного цикла

пользоваться в конкретной системе безопасности с определенным уровнем SIL, нам нужно знать его статистику отказов и иные характеристики. Конечный потребитель не может определить его пригодность сразу же при покупке. И продавец арматуры или привода не способен при продаже своего продукта утверждать, будто он подходит для любых систем безопасности с определенным SIL. (Исключение — перепускной предохранительный клапан, и вправду в одиночку

⁸ Строго говоря, риски суммируются не арифметически, а по правилам сложения вероятностей. Однако, для малых величин рисков, порядка 1/1000, результаты получаются почти идентичными (прим. ред.).

представляющий собой аппаратную систему безопасности. Он самостоятельно, без каких-либо датчиков, реагирует на превышение заданного уровня давления и предотвращает его дальнейший рост. Но наши рассуждения касались более сложных автоматизированных систем безопасности с приводной арматурой.)

Осмысливая в целом

Порой уместно, проявив мудрость, выбросить из головы постылый технический жаргон, всякие там числа с расчетами, и просто немного подумать о том, что конечная цель всех этих усилий и ухищрений – это наша с вами безопасность и сохранность той среды, в которой мы живем.

В рассуждениях об оборудовании и о его использовании в системах SIL важно, чтобы детали не увели в сторону от сути, важно помнить, что мы живем в мире людей, что в любой системе присутствует человеческий фактор, и как её ни контролируй, законы Мэрфи не отменить, и полностью избежать всех рисков невозможно.

Поэтому поставщикам и потребителям не стоило бы чересчур увлекаться оценками своего продукта в терминах SIL, его сертификацией и т.п., им нельзя забывать о том, что, будучи установленным, их оборудование станет элементом промышленной системы, частью всемирной техносферы, последствия сбоев которой отражаются на всей нашей жизни, на будущем человечества.

В заключение давайте еще раз вспомним основные понятия, о которых рассказано в данной статье. Итак:

- SIL – это показатель надежности системы;
- конечные пользователи (обычно с помощью рабочей группы HAZOP) определяют желаемый уровень SIL для своих аппаратных систем безопасности;
- основываясь на надежности отдельных компонент (по сути, на средней вероятности их отказов), эти компоненты могут использоваться в системах с определенным SIL;
- тот факт, что некое устройство маркировано, допустим, SIL 3 – еще не значит, что оно подходит для использования в конкретной системе SIL 3.

Надеемся, что с пониманием этих простых вещей последние покровы тайны спадут, и арматурщики и пользователи арматуры убедятся: SIL – это несложно.

Перевод и литературная обработка А. Горелова

СПИСОК ЛИТЕРАТУРЫ

1. *General Monitors Corporate Website: Frequently Asked Questions about Safety Integrity Levels; www.gmigasandflame.com/sil_faqs.html#SIS.*
2. *Michael Young, General Monitors; SIL 101: How Safe Do I Need to Be?; www.gmigasandflame.com/sil_info_101.html.*
3. *Lihou Technical & Software Services; Hazard & Operability Studies (Hazops); www.lihoutech.com/hazop1.htm.*
4. *Technip Benelux Services, a division of Technip Benelux B.V.; Hazard & Operability Studies (HAZOP) & Safety Integrity Level Classification (SIL).*
5. *International Society of Automation; ANSI/ISA-TR9605.01-2008, page 21; Figure 2 – Effect of partial testing on PFD_{AVG}.*