SIL и функциональная безопасность

Доктор В.Йессель, Draeger Safety AG & Co. KGaA, Германия

Совершенных систем не бывает. Любые системы могут давать сбои. В том числе и системы, обеспечивающие безопасность – безопасность жизнедеятельности людей, промышленных объектов, окружающей среды. Концепция надежности таких систем основана на ключевом вопросе: "Насколько вероятно, что защитная система даст сбой в тот момент, когда она должна выполнять свои функции обеспечения безопасности?" Эта актуальная тема рассмотрена на примере построения газоизмерительных систем Draeger Safety.

При хранении, заполнении, переработке или транспортировке горючих газов и паров никогда не следует исключать, что при возникновении сбоя такие вещества смогут воспламениться и нанести значительный ущерб людям и имуществу. Необнаруженные выбросы сжатых или сжиженных криогенных газов, утечки в системах трубопроводов или испарение горючих жидкостей, при повреждении вентилей или недостаточно герметичных уплотнителях могут приводить к взрывам с серьезными последствиями или крупным, трудно контролируемым пожарам. Системами раннего предупреждения, позволяющими обнаруживать такие потенциально взрывоопасные ситуации и заблаговременно инициировать меры противодействия, чтобы избежать повреждения оборудования или, по крайне мере, свести его к минимуму, являются газоизмерительные системы.

Средняя вероятность отказа при выполнении заданной функции безопасности в течение заданного интервала тестирования и количественное соотношение необнаруживаемых опасных отказов - это ключевые параметры защитных систем. Чтобы создавать газоизмерительные системы, которые можно квалифицировать как, например, SIL 2, их проектировщикам приходится делать особый анализ при выборе используемых подсистем, чтобы определить количественные предельные уровни, которые применяются к этим параметрам надежности, в то же время, согласуясь с требованиями к метрологическим характеристикам.

Метрологические стандарты

Такие газоизмерительные системы не только удовлетворяют Директиве 94/9/EC (ATEX 95), потому что они, естественно, должны иметь взрывобезопасное исполнение, а, прежде всего потому, что они способны обнаруживать потенциально взрывоопасные атмосферы на ранней стадии и, позволяя принять меры противодействия, могут даже предотвратить их появление. Кроме того, газоизмерительные системы составляют неотъемлемую часть цепи безопасности и должны дополнительно проверяться уполномоченными организациями на пригодность для использования в приложениях по обеспечению безопасности (Директива 94/9/EC, Приложение II, 1.5.5 "Функция измерения для обеспечения взрывобезопасности"). Стандарты, на которых основана проверка, EN 50054 ff, были гармонизированы с Директивой 94/9/EC, но сейчас заменены серией стандартов EN 61779.

На основании EN 1127_1, другого гармонизированного стандарта, про-

веренные таким образом газоизмерительные системы рассматриваются как активные системы для ограничения концентрации (Раздел 6.2.2.2) - основной меры защиты от взрыва, которая имеет более высокий приоритет, чем введенный несколько десятилетий назад, но все еще широко используемый термин "первичная взрывозащита". Менее известен тот факт, что использование метрологически аттестованных газоизмерительных систем может в действительности значительно уменьшить размер потенциально взрывоопасных зон ("Ex зон") и, таким образом, не только упростить процесс эксплуатации, но и, в конечном итоге, снизить издержки.

Газоизмерительные системы для измерения содержания кислорода также подходят под область действия Директивы, если они контролируют ограничение содержания кислорода в процессах инертизации. В этом контексте для проверки метрологических характеристик используется гармонизированный стандарт EN 50104.

Метрологические стандарты дополнены EN 50271, поскольку инструменты для обнаружения газов содержат цифровую электронику. При про-

верке согласно этому стандарту оценивается, в частности, структура программного обеспечения и стабильность, всевозможные специальные состояния, внутренние возможности диагностики и, конечно, аппаратные средства, взаимодействие между отдельными электронными компонентами и надежность функциональной концепции.

При пересмотре EN 50271 главной целью являлась функциональная безопасность, и не удивительно, что некоторые требования "стандарта SIL", EN 61508, уже были включены в этот стандарт.

Класс безопасности эксплуатации оборудования

Рассмотрим некоторые аспекты EN 61508, которые позволяют разработчикам систем, при соблюдении определенных условий, гарантировать надежность систем, предназначенных для обеспечения безопасности, посредством числовой оценки. Согласно EN 61508, устройство защиты, используемое для предотвращения нанесения вреда людям, среде и имуществу, должно удовлетворять определенным требованиям к надежности в зависимости от возможного объема ущерба, который определяется на основе так называемого класса безопасности эксплуатации оборудования (SIL). Концепция надежности основана на утверждении вероятности: "Насколько вероятно, что защитная систем даст сбой в тот момент, когда она должна выполнять свои функции обеспечения безопасности?"

Опасные отказы

Ориентированные на обеспечение безопасности системы должны разрабатываться таким образом, чтобы любые отказы, которые могут иметь негативное влияние на безопасность функционирования, были распознаны, проанализированы и о них сообщено соответствующей функцией самодиагностики и процедурой проверки, и вся система была приведена в безопасное состояние. Таким образом, обнаруженные опасные отказы должны быть немедленно устранены. Это и в интересах оператора, поскольку система в безопасных условиях, даже будучи безопасной, не всегда может быть готова к работе. Однако, и системы диагностики имеют свои ограничения. В некоторой мере, всегда будут иметь место необнаруженные опасные отказы, например, неисправности, которые остаются невыявленными и приводят к сбоям функций обеспечения безопасности или функций полноты безопасности (SIF). Единственный шанс выявления таких неисправностей - регламентные проверки системы. По этой причине время между двумя подобными проверками, интервал тестирования T_P, играет важную роль в анализе безопасности.

Количество безопасных отказов (например, отказов, которые, несмотря на снижение ими функций безопасности, обнаруживаются, или сбоев в работе, которые не оказывают влияния на функции безопасности) по отношению к полному количеству отказов называется долей безопасных отказов (SFF). Для систем SIL 2, SFF должен быть выше 90% или доля необнаруженных опасных отказов не должна превышать 10%. Однако, это не единственное требование. Если такие необнаруженные опасные отказы существуют, то вероятность их появления в течение интервала тестирования также должна быть определенной, например, определяется вероятность того, что такая защитная система даст сбой именно в тот момент, когда требуются функции обеспечения безопасности.

Вероятность отказов при выполнении заданной функции безопасности

Статистический параметр, который описывает необнаруженные опасные отказы и интервал тестирования, известен как средняя вероятность отказов при выполнении заданной функции безопасности PFD_{AVG} и, в зависимости от требуемого SIL, не должен превышать некоторые пределы. Так для систем, соответствующим SIL 2, необходимо предпринять шаги, чтобы гарантировать, что PFD_{AVG} не превышает 0,01, т. е., система защиты может давать сбои только 1 раз из 100, когда от нее требуется выполнение функции обеспечения безопасности.

Однако, функциональная безопасность и, следовательно, средняя вероятность отказа при выполнении заданной функции безопасности PFD_{AVG}, относится к системе в целом, которую можно разделить на следующие подсистемы:

- сенсор (SE, вероятность отказа при выполнении заданной функции безопасности PFD_{SE}),
- логическое решающее устройство (LS, вероятность отказа при выполнении заданной функции безопасности PFD_{LS})

■ конечные элементы (FE, вероятность отказа при выполнении заданной функции безопасности PFD_{FE}).

Для системы в целом, вероятность отказов при выполнении заданной функции безопасности рассчитывается путем суммирования этих трех параметров:

$$PFD_{AVG} = PFD_{SE} + PFD_{LS} + PFD_{FE}$$

Чтобы вычислить PFD_{SE} сенсора, необходимо провести очень детальную оценку каждого мыслимого типа отказа и его последствия на каждом уровне, вплоть до уровня компонентов (FMEDA, режимы отказа, последствия и диагностический анализ), что фактически невозможно без помощи экспертов, специализирующихся в таких анализах. Результат FMEDA - это список различных типов отказов и рассчитанная частота отказов λ(в $час^{-1}$), на основе которой, в частности, можно рассчитать интенсивность λ_{DU} необнаруженный опасных отказов (DU относится к опасным необнаруженным). Такой отказ мог бы возникнуть, например, если из-за внутреннего сбоя в газоизмерительной головке информационный сигнал имеет значение 4 мА, т.е. нет газа, несмотря на наличие опасновысоких концентраций газов. Если возник этот тип редкого условия отказа, то он останется невыявленным до проведения следующей регламентной проверки (интервал тестирования), при которой, конечно, отказ будет немедленно обнаружен и устранен за очень короткое время (MTTR, среднее время на восстановление). Говоря статистическим языком, этот сбой остается невыявленным в течение половины интервала тестирования. В течение этого же периода, плюс время, необходимое на ремонт, система также не способна выполнять свои функции обеспечения безопасности. Соответственно, в этом случае среднюю вероятность отказа при выполнении заданной функции безопасности можно рассчитать следующим образом:

$$PFD_{AVG} = 1/2*\lambda_{DU}*(T_P+MTTR)$$
$$PFD_{AVG} \approx 1/2*\lambda_{DU}*T_P$$

Аппроксимация допустима начиная с ремонтов, обычно занимающих только несколько часов, в то время как интервал тестирования составляет несколько месяцев.

Опасные отказы, выявленные средствами диагностики (интенсивность отказов λ_{DD}, DD относится к опасным обнаруженным), также влияет на PFD, пусть даже и в меньшей степени, поскольку функции обеспечения безопасности не доступны в течение продолжительности MTTR. MTTR обычно рассчитывается как 8 часов, хотя при этом подразумевается достаточный запас запасных частей и услуг по ремонту, которые предоставляются незамедлительно, без задержки. За это отвечает инженер по технике безопасности, как и за соблюдение заданного интервала тестирования T_P. Если части системы - это конструкции с резервированием или предусматривают "голосование" (например, решение два из трех), применяемые правила отличаются от приведенной выше формулы. Так, при двукратном резервировании вероятность отказа при выполнении функции равна:

$$PFD_{AVG} = 1/3*(\lambda_{DU}*T_P)^2.$$

Результирующие значение будет очень малым и, тем не менее, необходимо реально проанализировать отказы, которые воздействуют на обе подсистемы одновременно, по сути, устраняя резервирование. Это так называемые общие возникающие отказы. Их доля определяется коэффициентом β, который обычно предполагается равным 0,05 или 0,1.

$$PFD_{AVG} = 1/3*(\lambda_{DU}*T_P)^2 + \beta*\lambda_{DU}*T_P$$

На практике вторая составляющая обычно больше, даже в случае малого коэффициента β.

Пример: интенсивность необнаруженных опасных отказов $\lambda_{DU} = 10^{-6}$ $ч^{-1}$ (т. е. один отказ за 10^6 часов или 114 лет).
Если система тестируется раз в год (каждые 8 760 часов), то:
$$PFD_{AVG} = 1/2 * \lambda_{DU} * T_P = 1/2 * 10^{-6} * 8760 = 4.38 * 10^{-3}$$

Конструкция системы

PFD_{AVG} системы в целом определяется:

■ интенсивностью необнаруженных опасных отказов λ_{DU}

■ выбором интервала тестирования T_P

■ архитектурой (линейная, с резервированием, режим "голосования").

Для подсистемы интенсивность отказов λ_{DU} определяется проведением FMEDA и обычно сертифицируется независимой тестирующей организацией и гарантируется мероприятиями по гарантии качества. Поэтому проектировщик системы способен определить интервал между проверочными испытаниями и архитектуру системы в целом. Имеются, однако, практические ограничения: компании не слишком заинтересованы в очень коротких интервалах между проверками, поскольку это может привести к более частым простоям, а дублирование и "голосование" связано с дополнительными затратами. Поэтому задача проектировщиков систем - использовать подсистемы, которые, проверяясь только один раз в год и используясь без резервирования, будут отказывать как можно реже по сравнению с максимально допустимым PFD.

Например, для систем, классифицированных как SIL 2, проектировщик достигнет вышеупомянутой цели, используя сенсор с PFD_{SE} = 0,002 и логическую схему с PFD_{LS} = 0,001 (оба на основе ежегодного тестирования).

Таблица 1

устойчивость к аппаратным отказам (HFT)	< 60%	60...<90%	90..<99%
1	-	SIL 1 (PFDAVG<0.1)	SIL 2 (PFDAVG<0.01)
2	SIL 1 (PFDAVG<0.1)	SIL 2 (PFDAVG<0.01)	SIL 3 (PFDAVG<0.001)
3	SIL 2 (PFDAVG<0.01)	SIL 3 (PFDAVG<0.001)	SIL 4 (PFDAVG<0.00001)

Таблица 2

измерительная головка	принцип измерения	λ_{DU}	SFF	PFD (Tp=1 год *
Polytron 2 IR	инфракрасный, горючие газы и пары	2.92 o 10^{-8} $ч^{-1}$	96.5%	1.28 o 10^{-4}
Polytron Pulsar	трассовый, инфракрасный, горючие газы и пары	1.09 o 10^{-7} $ч^{-1}$	91.9%	4.75 o 10^{-4}
Polytron 7000	электрохимический, токсичные газы и пары	2.92 o 10^{-7} $ч^{-1}$	90.8%	1.56 o 10^{-4}

* - для систем SIL 2, PFD_{SE} для сенсора не должен превышать 3.5 o 10^{-3}

Для того, чтобы обеспечить PFD_{AVG} < 0,01, необходимое для SIL 2, используемые конечные элементы должны иметь PFD_{FE} менее 0,007, если они также будут тестироваться раз в год.

HFT и резервирование

Устойчивость к аппаратным отказам HFT описывает поведение всей системы или подсистемы в условиях сбоя. При линейной архитектуре, т.е. для систем без резервирования, функция обеспечения безопасности не гарантируется при возникновении лишь одного сбоя (HFT=0), в то время как архитектура с резервированием останется работоспособной при возникновении сбоя (HFT = 1 или выше, таблица 1).

Как можно видеть из приведенной таблицы (см. EN 61508, разрез 7.4.3.1.4), для линейной архитектуры (HFT=0) классификации SIL 2 можно добиться, только если SFF больше 90%, т. е. доля необнаруженных опасных отказов должна быть ниже 10%. С другой стороны, если SFF только 80%, SIL 2 можно достичь путем резервирования (HFT=1).

Поэтому функциональная безопасность подсистемы может быть полностью указана, если определены PFD с соответствующим интервалом тестирования TP, SFF и HFT. Например, представленные в таблице 2 характеристики газоизмерительных сенсоров Dreger Safety, оцененные независимым институтом, свидетельствуют о том, датчики Polytron идеально подходят для создания газоизмерительных систем, классифицированных как SIL 2.

Для ясности и простоты изложения в статье был опущен тот факт, что EN 61508 требует принимать во внимание полный срок службы системы защиты, особенно аспекты работы и обслуживания. Вместо этого, внимание было сосредоточено на ознакомлении с соответствующими терминами и определениями, приведенными в данном стандарте, касающихся систем защиты.

КОНТАКТЫ:
e-mail: wolfgang.jessel@draeger.com
e-mail: PolytronCIS@draeger.com