Интегральные уровни безопасности в соответствии со стандартами МЭК 61508 и 61511 и анализ их связи с техническим обслуживанием

Глизенте Ландрини

В статье рассмотрены основные показатели функциональной безопасности систем, связанных с обеспечением безопасности производственных технологических процессов на предприятиях перерабатывающих отраслей промышленности, приведены примеры их оценки в соответствии с рекомендациями стандартов МЭК 61508 и 61511, а также проанализирована их зависимость от организации технического обслуживания и диагностики этих систем.

На текущий момент в России нет единой нормативной базы, регламентирующей требования по выбору технических средств для построения систем безопасности промышленных объектов. Существуют лишь далеко не всегда увязанные между собой нормативные документы контрольно-надзорных и сертификационных органов, отраслевые документы и корпоративные стандарты крупных компаний.

Все перечисленные нормативные документы, как правило, ориентированы на обеспечение конкретных задач, в них отсутствуют единая терминология и комплексный подход к задаче обеспечения безопасности промышленных объектов. Поэтому в последнее время разработчики корпоративных документов, регламентирующих проектные работы, вносят в требования по выбору оборудования обязательное соответствие средств автоматизации, используемых в системах, связанных с обеспечением безопасности производственных процессов, европейским стандартам МЭК 61508 и 61511 [1, 2].

Эти стандарты в настоящее время широко используются в странах Европейского Союза и в ряде в других стран для регламентации требований к оценке уровня потенциальной опасности объектов и оценке соответствия электрического, электронного, программируемого электронного оборудования систем обеспечения безопасности уровню опасности объекта.

Зона действия этих стандартов подошла уже к границам России. Вступление республик Балтии в Евросоюз, начавшийся процесс гармонизации национальных стандартов Украины, Казахстана и других стран СНГ обуславливает интерес к данным стандартам у российских системных интеграторов и собственников опасных промышленных объектов.

В этой связи настоящая статья, подготовленная автором на основе опыта компании GM International в разработке и производстве оборудования для АСУ ТП и систем противоаварийной защиты взрывоопасных производств нефтяной и нефтехимической отраслей, может быть полезной для специалистов, занимающихся системами обеспечения безопасности объектов в перерабатывающих отраслях промышленности.

Безопасность и допустимый риск

Безопасность определяется как «свобода от неприемлемых рисков». При этом под риском понимается комбинация вероятности возникновения ущерба и тяжести этого ущерба. Опасность – это потенциальный источник ущерба. Допустимым считается риск, приемлемый в данных обстоятельствах, с учётом существующих в настоящее время социальных ценностей (рис. 1).

Все эти понятия подробно описаны в части 4 стандарта МЭК 61508.

Средняя вероятность отказа на запрос выполнения функции безопасности

Первым параметром, определяющим интегральный уровень безопасности SIL (*Safety Integrity Level*), является средняя вероятность отказа на запрос выполнения функции безопасности PFDavg (*Probability of Failure on Demand*).

Фактор снижения риска RRF (*Risk Reduction Factor*), представляющий собой отношение частоты инцидентов без принятия мер защиты и допустимой частоты инцидентов, является величиной, обратной PFDavg:

$$RRF = \frac{\text{Частота инцидентов без принятия мер защиты}}{\text{Допустимая частота инцидентов}} = \frac{1}{PFDavg}.$$

Это означает, что если, например, количество инцидентов в год без принятия

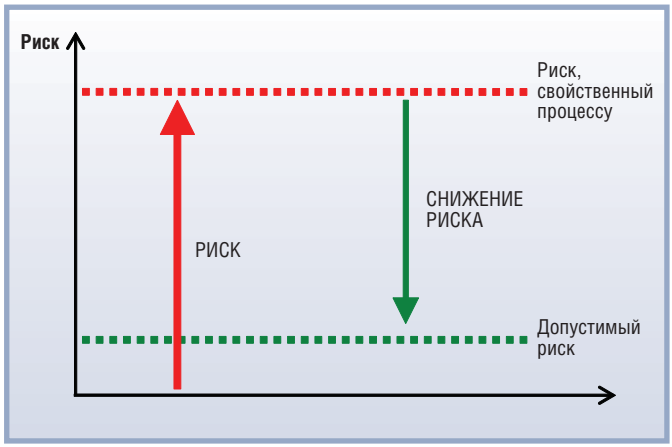

Рис. 1. Основной принцип снижения риска

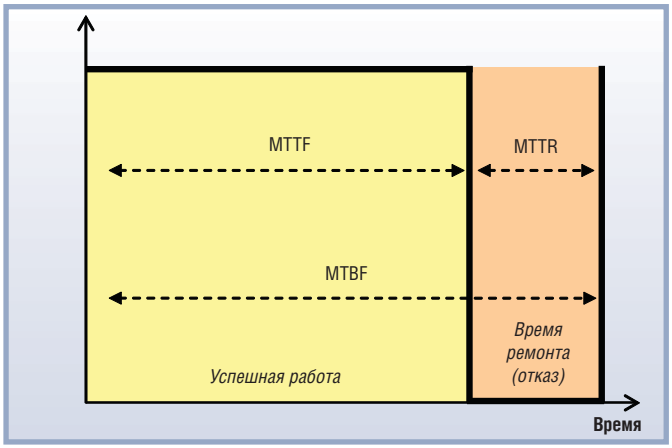

Рис. 2. Схематическое представление MTTF, MTTR, MTBF

мер защиты равно 10, а допустимое количество инцидентов равно 1 в 100 лет, то RRF должен быть равен 1000 и, соответственно, PFDavg равна 0,001 в год. Это значение согласно стандарту МЭК 61508 соответствует уровню SIL 2. С учётом того, что в году приблизительно 10 000 часов (8760), это означает, что неготовность инструментальной функции безопасности SIF (*Safety Instru-mented Function*) равна примерно 10 часам в год, то есть в течение в среднем 10 часов в год невозможно будет обеспечивать перевод контролируемого технологического процесса в безопасное состояние при возникновении такой необходимости. Если это время слишком велико и неготовность SIF должна быть снижена, например, до 1 часа в год, её интегральный уровень безопасности должен быть более высоким, например SIL 3.

Среднее время наработки на отказ и интенсивность отказов

MTTF (*Mean Time To Failure*) – среднее время наработки на отказ – является показателем среднего времени успешной работы устройства (системы) до наступления отказа любого вида. Этот показатель может интерпретироваться и как срок службы устройства, если оно не подлежит восстановлению или ремонту.

Характеристикой ремонтопригодных устройств является среднее время их восстановления MTTR (*Mean Time To Repair*).

Среднее время между двумя последовательными отказами MTBF (*Mean Time Between Failures*) обычно выражается в годах.

Между данными показателями существуют следующие соотношения (рис. 2):

- MTBF = MTTF + MTTR;
- MTTF = MTBF – MTTR.

Почему так важен показатель MTBF? Потому что обратная ему величина $\lambda = 1/\text{MTBF}$ – это интенсивность отказов компонента или устройства:

$$\text{MTBF} = \frac{1}{\lambda};$$

$$\text{Интенсивность отказов} = \lambda = \frac{\text{Количество отказов в единицу времени}}{\text{Количество компонентов, подверженных отказу}}.$$

Интенсивности отказов различных категорий

Общая интенсивность отказов λ_{tot} делится на две основные категории: интенсивность безопасных отказов λ_s и интенсивность опасных отказов λ_d.

$$\lambda_{tot} = \lambda_s + \lambda_d.$$

Опасными являются отказы, которые приводят к потере функциональной безопасности системы и/или к потере её безопасного состояния. Применительно к системам, в нормальном режиме находящимся во включённом состоянии (например, системам противоаварийной защиты), безопасными считаются отказы, которые приводят к ошибочному отключению выхода и останову контролируемого технологического процесса (ложное срабатывание). Опасными отказами, наоборот, является отказы, препятствующие отключению выхода и останову процесса при возникновении аварийной ситуации.

В каждой из указанных категорий отказы, в свою очередь, подразделяются на детектируемые (λ_{sd}, λ_{dd}) и недетектируемые (λ_{su}, λ_{du}) онлайновой диагностикой:

$$\lambda_s = \lambda_{sd} + \lambda_{su};$$
$$\lambda_d = \lambda_{dd} + \lambda_{du};$$
$$\lambda_{tot} = \lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}.$$

Величина, обратная λ_s, – это MTBFs, или среднее время (в годах) между возможными ложными остановами. В свою очередь, величина, обратная λ_d, – это MTBFd, среднее время (в годах) между возможными опасными отказами.

Рассмотрим, **как определяются интенсивности отказов различных категорий**.

Эта работа обычно выполняется на этапе проектирования конкретных устройств.

Для этой цели проводится анализ видов отказов и диагностики (*Failure Mode Effect and Diagnostic Analysis* – FMEDA). Для пояснения принципов FMEDA обратимся к диаграмме, представленной на рис. 3.

Датчик-преобразователь давления с токовым выходом 4...20 мА тестируется для определения значений λ_{sd}, λ_{su}, λ_{dd}, λ_{du}. Предположим, приемлемый диапазон допуска

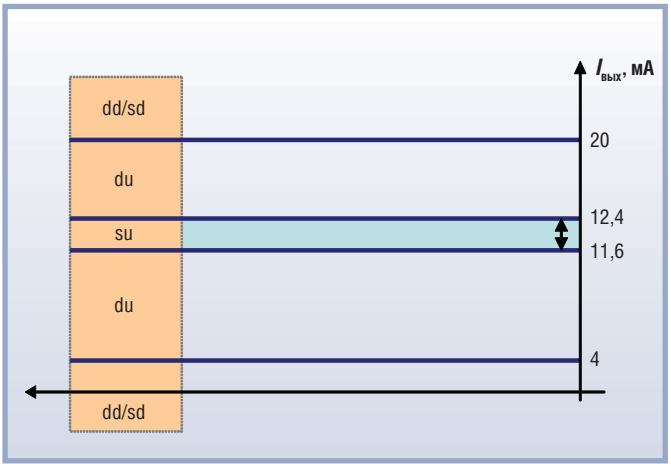

Рис. 3. Пример для выходного сигнала 4...20 мА

определён равным 0,8 мА (5% от рабочего диапазона).

На датчик подаётся питание и устанавливается выходной сигнал 12 мА. Один за другим по очереди моделируются отказы различных видов (короткое замыкание, обрыв, девиация и т.д.) для каждого электронного и механического компонента датчика. Например, если это резистор 1 кОм, сопротивление его устанавливается равным 0, 500, 2000 Ом, а затем он размыкается. Происходящие при этом изменения выходного тока фиксируются. Если диапазон изменений менее 0,8 мА, отказ классифицируется как безопасный недетектируемый (su). Если сигнал выходит за пределы допуска, но находится в диапазоне 4...20 мА, отказ классифицируется как опасный недетектируемый (du). Если же сигнал ниже 4 мА или выше 20 мА, отказ может быть безопасным или опасным в зависимости от условий применения данного датчика, но в любом случае он будет классифицироваться как детектируемый.

Такое тестирование и анализ выполняются для каждого компонента, затем полученные результаты суммируются для получения общих значений интенсивностей отказов λ_{sd}, λ_{su}, λ_{dd}, λ_{du}.

Необходимо отметить, что для определения неготовности системы безопасности (PFDavg) в основном имеет значение интенсивность опасных недетектируемых отказов (du). Это означает, что чем она ниже, тем более высокий интегральный уровень безопасности SIL может быть достигнут для данного устройства.

Доля безопасных отказов (SFF)

Вторым параметром, определяющим интегральный уровень безопасности, является доля безопасных отказов SFF (*Safety Failure Fraction*).

Таблица 1

SFF для компонентов типа A

SFF	Устойчивость к аппаратным отказам 0	Устойчивость к аппаратным отказам 1	Устойчивость к аппаратным отказам 2
< 60%	SIL 1	SIL 2	SIL 3
60–90%	SIL 2	SIL 3	SIL 4
90–99%	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

Примечание. Устойчивость к аппаратным отказам N означает, что (N+1)-й отказ может привести к нарушению функции безопасности устройства.

Таблица 2

SFF для компонентов типа B

SFF	Устойчивость к аппаратным отказам 0	Устойчивость к аппаратным отказам 1	Устойчивость к аппаратным отказам 2
< 60%	Не допускается	SIL 1	SIL2
60–90%	SIL 1	SIL 2	SIL 3
90–99%	SIL 2	SIL 3	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

Примечание. Устойчивость к аппаратным отказам N означает, что (N+1)-й отказ может привести к нарушению функции безопасности устройства.

Таблица 3

Фактор снижения риска как функция уровня SIL и готовности (из стандартов МЭК 61508 и МЭК 61511)

SIL интегральный уровень безопасности	PFDavg средняя вероятность отказа на запрос в год (низкая интенсивность запросов)	(1–PFDavg) готовность безопасности	RRF фактор снижения риска	PFDavg средняя вероятность отказа на запрос в час (высокая интенсивность запросов)
SIL 4	$\geq 10^{-5}$ и $<10^{-4}$	От 99,99 до 99,999%	От 100 000 до 10 000	$\geq 10^{-9}$ и $<10^{-8}$
SIL 3	$\geq 10^{-4}$ и $<10^{-3}$	От 99,9 до 99,99%	От 10 000 до 1 000	$\geq 10^{-8}$ и $<10^{-7}$
SIL 2	$\geq 10^{-3}$ и $<10^{-2}$	От 99 до 99,9%	От 1000 до 100	$\geq 10^{-7}$ и $<10^{-6}$
SIL 1	$\geq 10^{-2}$ и $<10^{-1}$	От 90 до 99%	От 100 до 10	$\geq 10^{-6}$ и $<10^{-5}$

В соответствии со стандартом МЭК 61508 компоненты или подсистемы относятся к типу A или B (см. табл. 1 и табл. 2):

- **компоненты типа A** – это простые устройства, поведение и виды отказов которых хорошо известны;
- **компоненты типа B** – это комплексные компоненты с потенциально неизвестными видами отказов, например микропроцессоры, специализированные процессоры и т.п.

Фактически в табл. 1 и 2 представлены ограничения на использование простых и резервированных архитектур в системах с различными уровнями SIL.

Значение SFF определяется по формуле:

$$SFF = \frac{\sum \lambda_{dd} + \sum \lambda_{sd} + \sum \lambda_{su}}{\sum \lambda_{dd} + \sum \lambda_{du} + \sum \lambda_{sd} + \sum \lambda_{su}} =$$

$$= 1 - \frac{\sum \lambda_{du}}{\sum \lambda_{dd} + \sum \lambda_{du} + \sum \lambda_{sd} + \sum \lambda_{su}}.$$

Чтобы увеличить значение SFF, суммарное значение $\sum \lambda_{du}$ должно быть как можно меньше.

Расчёт PFDavg

Для систем с архитектурой 1oo1 формула расчёта PFDavg имеет вид:

$$PFDavg(TI) = \lambda_{dd} \times RT + \lambda_{du} \times TI/2,$$

где

RT – время восстановления в часах (обычно 8 часов);

TI – интервал времени между функциональными проверочными тестами (1–5–10 лет), обозначаемый также Tproof;

λ_{dd} – интенсивность опасных детектируемых отказов;

λ_{du} – интенсивность опасных недетектируемых отказов.

Для TI = 1 год = 8760 ч и RT = 8 ч:

$$PFDavg = \lambda_{dd} \times 8 + \lambda_{du} \times 8760/2.$$

Поскольку слагаемое $(\lambda_{dd} \times 8)$ существенно меньше, чем $(\lambda_{du} \times 4380)$, формулу можно упростить:

$$PFDavg = \lambda_{du} \times TI/2 = \lambda_{du} \times 8760/2.$$

Интегральные уровни безопасности

В табл. 3 приведены значения PFDavg для двух режимов: низкой и высокой интенсивности запросов.

Режим низкой интенсивности запросов – режим, когда частота запросов на

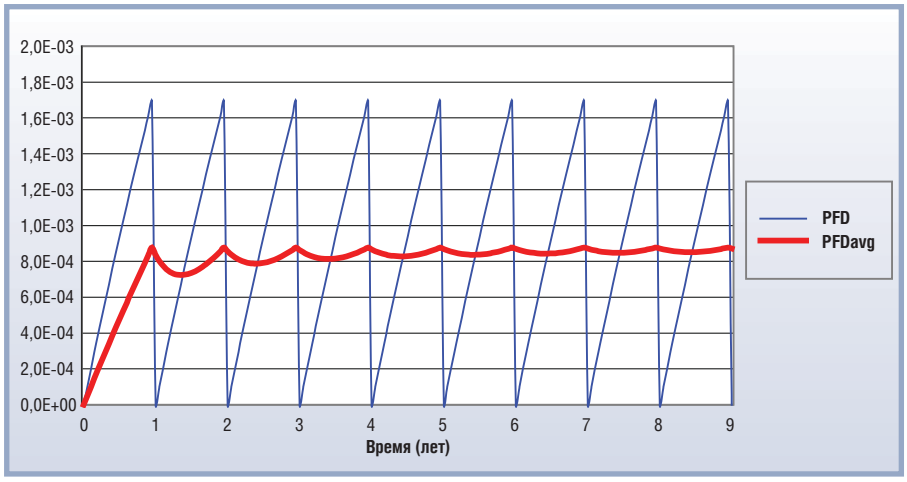

Рис. 4. PFD и PFDavg для системы с архитектурой 1oo1 и Tproof, равным 1 году

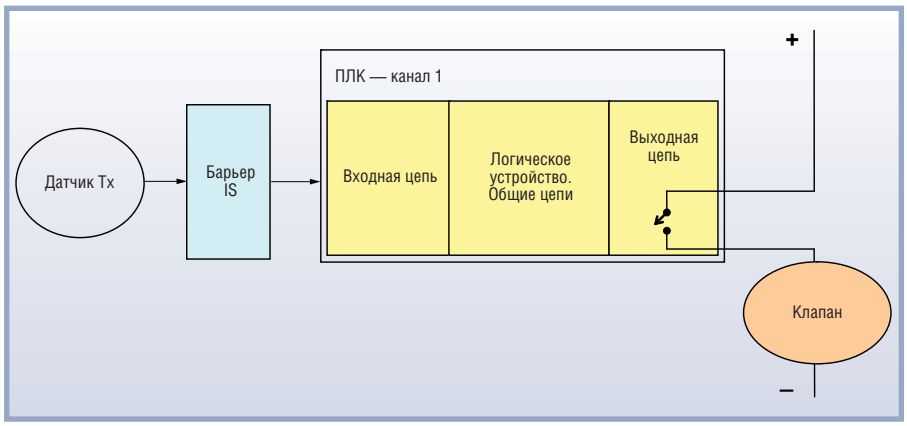

Рис. 5. Рассматриваемая в качестве примера система с архитектурой 1oo1

выполнение функции безопасности не превышает одного запроса в год и не более чем в два раза превышает частоту проведения проверочных тестов.

Режим высокой интенсивности запросов – режим, когда частота запросов на выполнение функции безопасности больше одного запроса в год и больше чем в два раза частоты проведения проверочных тестов.

Частота проведения проверочных тестов показывает, как часто производится функциональное тестирование системы безопасности, чтобы гарантировать её полную работоспособность.

Хотя непрерывный режим кажется более жёстким, следует помнить, что значения вероятностей для него приведены исходя из количества отказов в час. Для режима низкой интенсивности запросов приведённые значения соответствуют временному интервалу, равному примерно одному году. Учитывая, что в году примерно 10 000 часов (точно 8760), значения PFDavg для этих двух режимов примерно одинаковые.

Необходимо также отметить, что поскольку фактор снижения риска RRF является величиной, обратной PFDavg, для оценки уровней SIL вместо PFDavg проще использовать RRF, так как целые положительные значения более наглядны для понимания.

Замечания по поводу уровней SIL

1. Приведённые в табл. 3 значения относятся к функции безопасности SIF в целом, а не к отдельным её компонентам.
2. Разница между соседними уровнями SIL равна одному порядку (10).
3. Такая же разница в один порядок (10) существует между минимальными и максимальными значениями для каждого уровня SIL. Например, RRF = 120 соответствует SIL 2 и RRF = 980 тоже соответствует SIL 2, но между ними существует большая разница, поэтому данные значения несопоставимы, несмотря на то что они оба относятся к уровню SIL 2.
4. Зачастую думают, что уровень SIL (1–2–3–4), определённый для инструментальной функции безопасности SIF, будет таким всегда. Это заблуждение, поскольку интегральный уровень безопасности SIL зависит от значения вероятности PFD, которое увеличивается со временем. Уровень SIL остаётся неизменным только в течение определённого периода времени Tproof – это временной интервал между проведением проверочных диагностических тестов системы безопасности, обычно он составляет 1, 3, 5, 10, 15 лет (для удобства представления параметр Tproof обозначен в формулах как *TI*).
5. На рис. 4 показаны PFD и PFDavg для системы с архитектурой 1oo1 и Tproof, равным 1 году. PFD – вероятность отказа на запрос выполнения функции безопасности без учёта проведения диагностических тестов с целью выявления недетектируемых отказов, а PFDavg – усреднённая вероятность отказа на запрос выполнения функции безопасности с учётом выполнения диагностических тестов. Существуют специальные процедуры проведения проверочных тестов с целью определения для каждого устройства интенсивности опасных недетектируемых отказов $\Sigma\lambda_{du}$, которые не выявляются обычными онлайновыми диагностическими тестами. Если не выполнять такие периодические тесты, значение PFD функции безопасности SIF перейдёт из заданного уровня SIL в более низкий уровень, например из SIL 3 в SIL 2, SIL 1, SIL 0.
6. Уровень SIL, который соответствует межтестовому интервалу 1 год, существенно отличается от уровня, соответствующего интервалу 10 лет, хотя оба уровня относятся к одной и той же функции безопасности.
7. Для повышения уровня SIL конкретной SIF существуют два способа: снижение межтестового интервала Tproof и использование резервирования компонентов, кроме того, возможно комбинирование обоих этих способов.

Пример расчёта характеристик SIF

В данном примере показан порядок расчёта PFDavg и уровня SIL как для отдельных компонентов SIF, так и для SIF в целом.

Рассчитаем значения MTBF, MTBFs для ложных срабатываний, PFDavg, RRF и возможный уровень SIL для функции безопасности SIF системы, представленной на рис. 5. Эта система состоит из датчика-преобразователя Tx, барьера искробезопасности, программируемого логического контроллера

Таблица 4

Исходные и расчётные данные для примера, показанного на рис. 5, — система с архитектурой 1oo1 и *TI*, равным 1 году

Подсистемы	MTBF (лет)	λ/год = 1/MTBF	MTBFs = $1/\lambda_s$ (лет)	λ_s/год	λ_{dd} /год	λ_{du}/год	PFDavg 1oo1 = λ_{du}/2	% от общей PFDavg	RRF = 1/PFDavg	SFF	Допустимый SIL
Датчик Tx	102	0,00980	125	0,00800	0,0010	0,00080	0,000400	3,40%	2500	91,8%	SIL 2
Барьер D1014S	314	0,00318	629	0,00159	0,0014	0,00019	0,000095	0,81%	10 526	94,0%	SIL 3
ПЛК	685	0,00146	741	0,00135	0,0001	0,00001	0,000005	0,04%	200 000	99,3%	SIL 3
Клапан	12	0,08333	24	0,04150	0,0200	0,02183	0,010915	92,87%	92	73,8%	SIL 1
Источник питания	167	0,00600	189	0,00530	0,0000	0,00070	0,000350	2,97%	2 857	88,3%	SIL 3
Общая (SIF)	10	0,10377	17	0,05774	0,0225	0,02353	0,011765	100%	85	—	SIL 1

Таблица 5

Исходные и расчётные данные для примера, показанного на рис. 5, — система с архитектурой 1oo1 и *TI*, равным 1 году для всех компонентов, кроме клапана, *TI* которого сокращён до 4 месяцев

Подсистемы	MTBF (лет)	λ/год = 1/MTBF	MTBFs = $1/\lambda_s$ (лет)	λ_s/год	λ_{dd} /год	λ_{du}/год	PFDavg 1oo1 = λ_{du}/2	% от общей PFDavg	RRF = 1/PFDavg	SFF	Допустимый SIL
Датчик Tx	102	0,00980	125	0,00800	0,0010	0,00080	0,000400	8,98%	2500	91,8%	SIL 2
Барьер D1014S	314	0,00318	629	0,00159	0,0014	0,00019	0,000095	2,13%	10 526	94,0%	SIL 3
ПЛК	685	0,00146	741	0,00135	0,0001	0,00001	0,000005	0,11%	200 000	99,3%	SIL 3
Клапан	36	0,02750	73	0,01370 /4 месяца	0,0066 /4 месяца	0,00720 /4 месяца	0,003602 /4 месяца	80,91% /4 месяца	278	73,8%	SIL 2
Источник питания	167	0,00600	189	0,00530	0,0000	0,00070	0,000350	7,86%	2 857	88,3%	SIL 3
Общая (SIF)	21	0,04794	33	0,02994	0,00910	0,00890	0,004452	100%	225	—	SIL 2

(ПЛК) и электромагнитного клапана, который является оконечным исполнительным элементом.

В качестве исходных данных при расчёте использованы значения параметров компонентов системы (MTBF, λ_{du}, λ_{dd}, λ_s), которые можно найти в руководствах по безопасности, предоставляемых их производителями.

Исходные и расчётные данные сведены в табл. 4 и табл. 5. Из таблиц видно, что основным критерием определения уровня SIL является PFDavg или фактор снижения риска RRF.

В данном примере заведомо низкие характеристики оконечного исполнительного элемента (клапана) были выбраны для лучшей иллюстрации условий реальных применений, соответствующих промышленному производству.

По поводу расчёта характеристик SIF необходимо сделать ряд замечаний.

1. Различие между табл. 4 (SIL 1 для клапана) и табл. 5 (SIL 2 для клапана) состоит в величине межтестового интервала *TI* для клапана. В первом случае он равен 1 году, а во втором – 4 месяцам.
2. Выбранный клапан не сертифицирован на соответствие SIL. Стандарт МЭК 61508 допускает его использование и позволяет принять $\lambda_s = \lambda_d = \lambda_{tot}/2$. Но поскольку в этом случае он не соответствует даже уровню SIL 1, необходимо проводить онлайновое тестирование клапана с неполным ходом (*Partial Stroking Test – PST*) при диагностическом покрытии не менее 52% (λ_{du} /λ_s ×100%), чтобы перевести часть опасных недетектируемых отказов $\sum \lambda_{du}$ в детектируемые $\sum \lambda_{dd}$ и таким образом обеспечить для клапана, как минимум, уровень SIL 1.
3. В случаях, когда значение PFDavg оконечного элемента такое высокое, как в рассматриваемом примере, другие компоненты системы должны иметь уровни безопасности не ниже SIL 3. Таким образом, компоненты с уровнем SIL 3 используются не только тогда, когда необходимо обеспечить уровень SIL 3 для всей системы, но и в тех случаях, когда для системы требуется уровень SIL 1, а один из её компонентов, имея

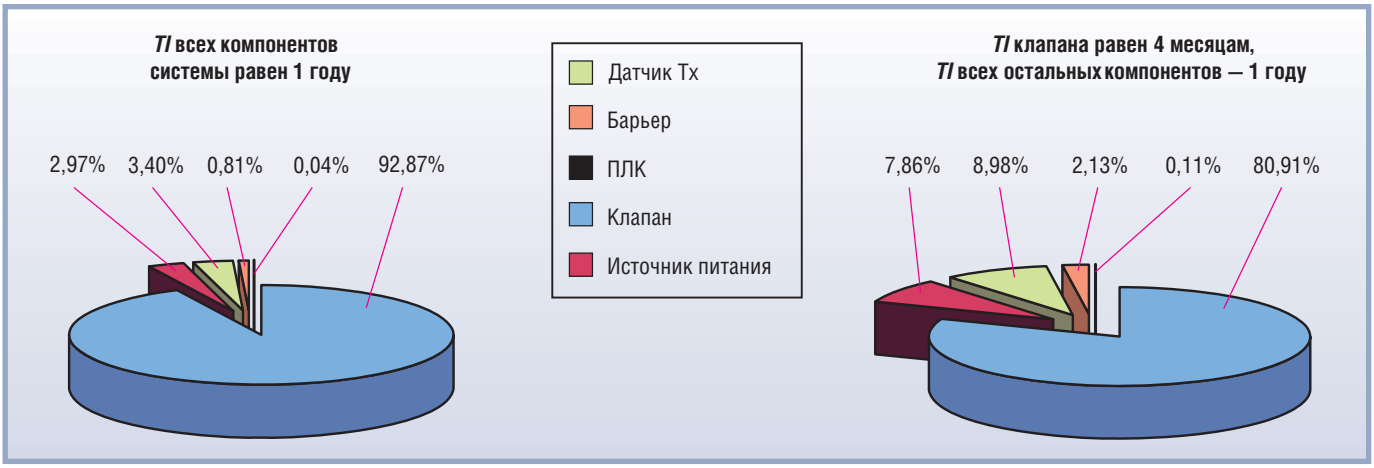

Рис. 6. Распределение PFDavg в рамках SIF (иллюстрация к примеру системы, показанной на рис. 5)

высокую интенсивность отказов, вносит большой вклад в общую PFDavg. Вклад каждого из компонентов в общую PFDavg системы показан на рис. 6.

4. Датчик, который имеет высокий RRF (2500), тем не менее, пригоден только для использования в системах с уровнем не выше SIL 2 (компонент типа B с устойчивостью к аппаратным отказам 0 – табл. 2), поскольку его SFF не соответствует применениям с уровнем SIL 3.
5. Что нужно сделать, если необходимый уровень SIL 2 для SIF должен обеспечивать фактор снижения риска RRF примерно равным 900? Возможным решением является использование для клапана архитектуры с резервированием 1oo2. При проведении периодических тестов клапаны по очереди могут включаться в обход и проверяться без остановки процесса. В этом случае межтестовый интервал для клапана может быть сокращён, например, до 4 месяцев. Принимая фактор отказов по общей причине равным 5% и межтестовый интервал TI = 4 месяца, получим RRF системы с уровнем SIL 2, равный 970.

Таблица 6

Межтестовые интервалы для компонентов системы, показанной на рис. 5

Компонент, подсистема	Межтестовый интервал (Tproof)
Датчик	1 год
Барьер	10 лет
ПЛК системы безопасности	20 лет
Клапан	4 месяца
Источник питания	10 лет

Таким образом, минимальный межтестовый интервал в рассмотренной системе имеет клапан, для других компонентов системы межтестовые интервалы при данном RRF существенно выше (табл. 6).

Влияние эффективности проверочных тестов на PFDavg

Стандарт МЭК 61508 требует, чтобы в результате периодических проверочных тестов устройство восстанавливало характеристики до состояния «нового». Другими словами, эти тесты должны выявлять все опасные недетектируемые отказы, существующие в устройстве. Поскольку на практике это невозможно, эффективность таких тестов варьируется от 99 до 50%.

Для каждого компонента SIF, когда эффективность периодических тестов по выявлению опасных отказов равна 100%, формула для расчёта PFDavg упрощается:

$$\text{PFDavg} = \lambda_{du} \times \frac{TI}{2}.$$

Если эффективность не равна 100%, формула имеет вид:

$$\text{PFDavg} = Et \times \lambda_{du} \times \frac{TI}{2} + (1 - Et) \times \lambda_{du} \times \frac{SL}{2},$$

где

Et – эффективность теста по выявлению опасных отказов (например, 90%);

SL – интервал между периодическими проверочными тестами с эффективностью 99–100% или между двумя полными заменами устройства, либо срок жизни системы или устройства, если они никогда полностью не тестируются и не заменяются.

Для TI = 1 году и SL = 12 годам формула для PFDavg имеет вид:

$$\text{PFDavg}\big|_{TI=1,\, SL=12} = .$$

$$= Et \times \frac{\lambda_{du}}{2} + (1 - Et) \times \lambda_{du} \times \frac{12}{2}.$$

Пример 1

λ_{du} = 0,01/год;
TI = 1 год;
Et = 90% = 0,9;
SL = 12 лет.
Для новой системы:
PFDavg = 0,01/2 = 0,005;
RRF = 1/PFDavg = 1/0,005 = 200 (SIL 2).
После 1 года:
PFDavg = (0,9×0,01/2) + (0,1×0,01×6) = = 0,0105;
RRF = 1/PFDavg = 1/0,0105 = 95 (SIL 1).
Вывод: после года работы (или после каждого межтестового интервала) уровень меняется с SIL 2 на SIL 1.

Пример 2

λ_{du} = 0,01/год;
TI = 1 год;
Et = 99% = 0,99;
SL = 12 лет.
После 1 года:
PFDavg = (0,99×0,01/2) + (0,01×0,01×6) = = 0,0056;
RRF = 1/PFDavg = 1/0,0056 = 178 (SIL 2).
Вывод: после одного года (или после каждого межтестового интервала) уровень SIL 2 остаётся практически неизменным (исходные значения PFDavg и RRF такие же, как в первом примере).

Влияние длительности проверочного теста на PFDavg

Для тестирования системы безопасности в онлайновом режиме (то есть без остановки технологического процесса) часть системы ставится в режим обхода, чтобы исключить какие-либо ложные срабатывания и отключения. Длительность тестирования может оказывать существенное влияние на общие характеристики системы безопасности, так как во время тестирования система не способна перевести процесс в безопасное состояние при возникновении такой необходимости. Длительность тестирования может дополнительно увеличиться, если по результатам теста устройство подлежит замене, и ещё более возрасти, если при этом компоненты, необходимые для замены, отсутствуют и их необходимо заказывать.

На время тестирования симплексная система 1oo1 должна быть отключена от процесса. Её готовность во время тестирования равна нулю. Однако резервированная система при тестировании не должна полностью включаться в обход. В дублированной системе на время теста можно поставить в режим обхода только одну ветвь (или модуль) системы, в результате на это время система превратится из дублированной в простую симплексную. Соответственно, троированная система при таких условиях превратится в дублированную.

Таким образом, упрощённое выражение для расчёта PFDavg

$$\text{PFDavg} = \lambda_{du} \times \frac{TI}{2}.$$

должно быть модифицировано с учётом задержки на время тестирования *TD*:

$$\text{PFDavg} = \lambda_{du} \times \frac{TI}{2} + \frac{TD}{TI}.$$

Пример 3

λ_{du} = 0,002/год;
TI = 1 год;
TD = 8 ч (временной интервал).
PFDavg = 0,001 + 0,0009 = 0,0019;
RRF = 1/0,0019 = 526 (SIL 2).
Вывод: после одного года (или после каждого межтестового интервала) уровень SIL 2 остаётся неизменным.

Пример 4

λ_{du} = 0,002/год;
TI = 1 год;
TD = 96 часов.
PFDavg = 0,001 + 0,01 = 0,011;
RRF = 1/0,011 = 90 (SIL 1).
Вывод: после года работы (или после каждого межтестового интервала) уровень меняется с SIL 2 на SIL 1.

Конечное выражение

С учётом эффективности и длительности проверочного теста выражение для расчёта PFDavg системы с архитектурой 1oo1 в общем случае имеет следующий вид:

$$\text{PFDavg} = Et \times \lambda_{du} \frac{TI}{2} + \frac{TD}{TI}(1 - Et) \times \lambda_{du} \times \frac{SL}{2}.$$

Более подробную информацию по рассмотренным в статье вопросам можно найти в книге [3] и руководстве [4], которые написаны инженерами компании GM International. ●

Литература

1. Стандарт МЭК 61508. Функциональная безопасность электрических, электронных, программируемых электронных систем, связанных с безопасностью.
2. Стандарт МЭК 61511. Системы обеспечения безопасности для перерабатывающих отраслей промышленности.
3. Функциональная безопасность систем, связанных с обеспечением безопасности: руководство по проектированию и обслуживанию. — GM International S.r.l., 2008. — 425 стр.
4. Руководство по функциональной безопасности барьеров GM International серии D1000 в применениях с уровнями SIL 2 и SIL 3 согласно стандартам IEC 61508 и IEC 61511. — GM International S.r.l., 2008. — 72 стр.

Автор — генеральный директор компании GM International S.r.l. (Италия)

НОВОСТИ НОВОСТИ

Сетевая технология LONWORKS принята в качестве стандарта ISO/IEC

Международная некоммерческая ассоциация LONMARK International, призванная способствовать развитию и продвижению технологии LONWORKS, сообщила 3 декабря 2008 г. о том, что имеющие право голоса члены Объединённого технического комитета № 1 Международной организации по стандартизации (ISO) и Международной электротехнической комиссии (IEC) официально признали технологию LONWORKS в качестве стандарта ISO/IEC 14908, части 1, 2, 3 и 4.

Впервые технология LONWORKS появилась на рынке в 1990 году. С самого начала LONWORKS заслужила признание как технология коммуникационных сетей управления. Уже на протяжении нескольких лет она является национальным стандартом в странах Европы, в Америке и Китае. С признанием в качестве стандарта ISO/IEC технология LONWORKS достигла высшей ступени международных стандартов.

Признание технологии в качестве стандарта ISO/IEC будет способствовать интенсификации применения технологии LONWORKS на мировом рынке автоматизации. Прежде всего это касается области строительства и недвижимости. Технология LONWORKS активно используется также и в других областях, например, в области управления уличным освещением, транспорта, энергообеспечения, управления процессами и домашней автоматизации. Но наибольшая часть Lon-устройств, а это свыше 100 миллионов установленных приборов, используется в области автоматизации зданий.

Стандарт состоит из четырёх частей: протокол, витая пара в качестве среды передачи данных для кабельной проводки свободной топологии, линии электросети в качестве среды передачи данных и использование межсетевого протокола (IP) в качестве транспортной среды для туннелирования. ●