Критерии выбора компонентов с уровнем SIL 3 для РСУ и систем ПАЗ в соответствии со стандартами МЭК

Часть 2

Глизенте Ландрини

В настоящей статье описаны критерии выбора компонентов для использования в распределённых системах управления (РСУ) и различных системах обеспечения безопасности с уровнями SIL 2 и SIL 3, рекомендованные в стандартах МЭК 61508 и 61511, а также даны практические примеры применения этих критериев.

Средняя вероятность отказа на запрос выполнения функции безопасности (PFDavg) и интегральные уровни безопасности (SIL)

Как уже было рассказано в [1], определение уровня SIL для конкретной инструментальной функции безопасности SIF (Safety Instrumented Function) производится на основе результатов анализа опасностей и рисков, присущих контролируемому технологическому процессу. Анализ оценивает величину снижения риска, необходимую для того, чтобы достичь приемлемого уровня безопасности. Конструктивные требования к системе безопасности SIS (Safety Instrumented System) должны проверяться на соответствие выбранному уровню SIL.

Таблица 4, взятая из стандартов МЭК 61508 и 61511 [2, 3], используется для расчёта уровней SIL функций безопасности SIF отдельных компонентов, а затем — уровня SIL функции безопасности всей системы в целом. Из этой таблицы видно, что соответствующие граничные значения PFDavg для соседних уровней SIL отличаются в 10 раз (на порядок). Однако в пределах одного уровня SIL минимальное и максимальное значения PFDavg тоже отличаются в 10 раз (на порядок). Таким образом, при сравнении компонентов (систем) некорректно учитывать один лишь уровень SIL; для правильного сравнения необходимо опираться на значение PFDavg.

Так, устройство с уровнем SIL 3 (такое, например, как модуль D1014 повторителя источника питания производства компании GM International), вклад которого в общую PFDavg функции безопасности SIF составляет только 10%, имеет PFDavg для 1 года, эквивалентную уровню SIL 4. Это означает, что подобное устройство может использоваться в системах с уровнем SIL 3 при условии годового межтестового интервала Tproof или в системах с уровнем SIL 2 при условии 10-летнего межтестового интервала, что позволяет обеспечить значительное сокращение времени и стоимости обслуживания системы.

Таблица 4

Уровни интегральной безопасности и вероятности отказа на запрос в соответствии со стандартами МЭК 61508 и МЭК 61511

SIL интегральный уровень безопасности	PFDavg средняя вероятность отказа на запрос в год (низкая интенсивность запросов)	RRF фактор снижения риска	PFDavg средняя вероятность отказа на запрос в час (высокая интенсивность запросов)
SIL 4	$\geq 10^{-5}$ и $< 10^{-4}$	От 100000 до 10000	$\geq 10^{-9}$ и $< 10^{-8}$
SIL 3	$\geq 10^{-4}$ и $< 10^{-3}$	От 10000 до 1000	$\geq 10^{-8}$ и $< 10^{-7}$
SIL 2	$\geq 10^{-3}$ и $< 10^{-2}$	От 1000 до 100	$\geq 10^{-7}$ и $< 10^{-6}$
SIL 1	$\geq 10^{-2}$ и $< 10^{-1}$	От 100 до 10	$\geq 10^{-6}$ и $< 10^{-5}$

Многие инженеры думают, что для систем безопасности с уровнем SIL 3 необходимы компоненты тоже только с уровнем SIL 3 и, соответственно, для систем с уровнем SIL 2 все компоненты должны быть с уровнем SIL 2. Это ошибочное мнение, свойственное людям, не знакомым с расчётом уровня SIL для функций безопасности SIF [1].

Руководство по функциональной безопасности

Исходные данные для расчёта PFDavg и определения уровней SIL компонентов имеются в руководстве по функциональной безопасности, которое обязан предоставить производитель данных компонентов. Такие руководства производители должны предоставлять для каждого из устройств (датчика, контроллера или исполнительного элемента), которые используются в системах обеспечения безопасности и для которых требуется подтвердить соответствие стандартам МЭК 61508 и МЭК 61511.

Руководство по безопасности — это документ для пользователей продукции (компонента, устройства), в котором оговорена их ответственность за монтаж и эксплуатацию данного компонента или устройства в плане обеспечения проектного уровня безопасности.

Указанные стандарты обязывают производителя предоставить пользователям такое руководство.

Многие пользователи рассматривают руководство как предпродажный документ, поскольку ещё до покупки изделия они хотят знать, будут ли у них какие-либо серьёзные ограничения в его использовании.

Далее описаны основные требования к руководству по функциональной безопасности и сведения о содержащейся в нём информации.

Требования к руководству по функциональной безопасности

Стандарт **МЭК 61508** предъявляет производителям целый ряд требований.

- Рекомендовать процедуры для выполнения диагностических тестов, необходимых для выявления известных опасных отказов, идентифицированных в результате анализа FMEDA [1]. Процедуры должны включать указание, что результаты этих тестов обязательно должны быть документированы. Должны быть указаны все инструменты и средства, необходимые для выполнения тестов. Также должен быть оговорён уровень квалификации специалистов, проводящих тесты. Для проводимых тестов должен быть указан фактор диагностического покрытия (эффективность тестов с точки зрения выявления опасных отказов, например 90%, 95%, 99%).
- Рекомендовать процедуры по ремонту или замене изделия. Они должны включать указание, что обо всех отказах необходимо информировать производителя. Нужно перечислить все необходимые инструменты и средства. Также должен быть указан необходимый уровень квалификации персонала, выполняющего эти работы.
- Рекомендовать тестовые процедуры при монтаже на объекте и при проведении приёмосдаточных испытаний, необходимые для обеспечения безопасности.
- Если в изделии возможно обновление встроенного программного обеспечения (ПО), должны быть описаны процедуры, используемые для этого, с указанием всех необходимых средств. Также должен быть указан необходимый уровень квалификации персонала, выполняющего эти работы.
- Руководство по безопасности должно содержать оценки интенсивности отказов (или ссылку на отчёт FMEDA) и оценку β-фактора в случае использования в системе безопасности резервированных устройств.
- Если пределы срока службы изделия неизвестны, это должно быть указано. В противном случае должно быть отмечено, что присутствуют неизвестные механизмы износа.

  Примечание. Хотя это не требуется, можно сделать некоторые замечания о сроках службы изделий, даже если механизмы износа неизвестны.
- Все значения параметров, необходимые для обеспечения безопасности, должны быть указаны.
- Должны быть отмечены все ограничения по применению и по условиям окружающей среды (или даны соответствующие ссылки на другой документ).
- Для заявленного диагностического покрытия должен быть указан максимально допустимый временной интервал между диагностическими тестами.

В разделе 7.4.7.3 стандарта **МЭК 61508-2** приведена информация, которая должна быть указана для каждой подсистемы, связанной с обеспечением безопасности:

- спецификация функций и интерфейсов подсистемы, которые могут быть использованы для обеспечения безопасности;
- оценки интенсивности отказов (связанных со случайными отказами оборудования) всех видов, которые могут стать причиной опасных отказов электрической/электронной/программируемой электронной (E/E/PE) системы безопасности, выявляемых с помощью диагностических тестов;
- любые ограничения на условия окружающей среды для подсистемы, которые должны контролироваться с целью обеспечения достоверности оценок интенсивности отказов, обусловленных случайными отказами оборудования;
- любые ограничения на срок службы подсистемы, которые не должны превышаться, с тем чтобы обеспечить достоверность оценок интенсивности отказов, обусловленных случайными отказами оборудования;
- любые необходимые периодические диагностические проверочные тесты или процедуры обслуживания;
- диагностическое покрытие;
- интервал между диагностическими проверочными тестами;
- любая дополнительная информация (например, время ремонта), необходимая для определения среднего времени восстановления (MTTR) после обнаружения диагностикой отказа;
- вся информация, необходимая для расчёта доли безопасных отказов (SFF) подсистемы, используемой в составе E/E/PE системы безопасности;
- устойчивость подсистемы к отказам оборудования (аппаратным отказам);
- любые ограничения на использование подсистемы, которые должны соблюдаться, чтобы исключить систематические отказы;
- наивысший интегральный уровень безопасности (SIL), который может быть заявлен для функции безопасности, использующей эти подсистемы, на основе:
  - методов, применяемых для предотвращения систематических отказов, заложенных на этапе проектирования, изготовления оборудования, создания ПО подсистемы,
  - конструктивных особенностей, которые делают подсистему устойчивой к систематическим отказам. **Примечание.** Это не требуется для подсистем, характеристики которых подтверждены на практике;
- любая информация, необходимая для идентификации конфигурации оборудования и ПО подсистемы (управление конфигурацией оборудования и ПО вторичной системы обеспечивает возможность управления E/E/PE системой безопасности в соответствии с разделом 6.2.1 стандарта МЭК 61508-1);
- документальное свидетельство о валидации подсистемы.

В разделе 1.2.4.4.7 стандарта **МЭК 61511-1** изложены требования, которые должны быть отражены в руководстве по безопасности:

- использование диагностики для обеспечения функций безопасности;
- перечень сертифицированных/верифицированных библиотек безопасности;
- обязательный тест и логика процедуры аварийного останова системы;

Таблица 5

Вопросы контрольного листа для компонентов SIF

Позиция	Вопрос
1	Данные для идентификации компонента (тип, производитель и т.п.) полные?
2	Соответствуют функциональные и рабочие характеристики SIF-требованиям?
3	Предоставил производитель руководство по безопасности?
4	Подсистема сертифицирована или одобрена независимой экспертной организацией в соответствии с требованиями стандартов МЭК 61508 и МЭК 61511?
5	Относится компонент к типам A или B, указанным в таблицах 2 и 3 стандарта МЭК 61508-2?
6	Определено значение PFDavg? Если да, то каково значение PFDavg для интервала в один год?
7	Соответствует это значение PFDavg фактору снижения риска, требуемому для SIF?
8	Для какого значения интервала *TI* рассчитана PFDavg: 1, 3, 5 или 10 лет? a. Укажите значение PFDavg для *TI* = 1 год b. Укажите значение PFDavg для *TI* = 5 лет c. Укажите значение PFDavg для *TI* = 10 лет d. *TI* — другой
9	Адекватен ли полученный уровень устойчивости к отказам? a. Какова устойчивость к отказам компонента (0, 1, 2 или неизвестна)?
10	Соответствует рассчитанное значение PFDavg значению, заложенному при проектировании?
11	Известно значение SFF (%)? Если да, то каково оно?
12	Известно значение MTBF? Если да, то каково оно?
13	Известна суммарная интенсивность безопасных детектируемых отказов (λ_{sd})? Если да, то какова она (в год)?
14	Известна суммарная интенсивность безопасных недетектируемых отказов (λ_{su})? Если да, то какова она (в год)?
15	Известна суммарная интенсивность опасных детектируемых отказов (λ_{dd})? Если да, то какова она (в год)?
16	Известна суммарная интенсивность опасных недетектируемых отказов (λ_{du})? Если да, то какова она (в год)?
17	Определён уровень SIL для компонента и адекватен ли он требованиям?
18	Каков уровень устойчивости к отказам на запрос (PFDavg), полученный для уровня SIL, установленного для компонента?
19	Если необходимо резервирование, каково значение β-фактора?
20	Установлен статус безопасного отказа для SIF? Если да, то каков он?
21	Представлены в руководстве по безопасности процедуры и тесты, выполняемые для SIF при проведении периодических проверочных тестов с интервалом *TI?* Если да, то какова эффективность периодических тестов, определённая для каждого теста (см. [1])? a. Тест 1 b. Тест 2 c. Тест 3 d. Тест 4 e. Тест 5 f. Тест 6 g. Тест 7 h. Тест 8
22	Каково новое значение PFDavg, скорректированное с учётом эффективности периодических тестов, указанных в п. 21?
23	Соответствует это новое скорректированное значение PFDavg уровню SIL, назначенному после периодического теста?
24	Имеются ли компоненты с архитектурой, отличной от 1oo1? Если есть, то какие?
25	Рассчитано для этой новой архитектуры значение PFDavg в соответствии с интервалом *TI*, выбранным для SIF? Если да, то какое?
26	Определены и согласованы требования к монтажу?
27	Возможно проведение каких-либо изменений в оборудовании и/или ПО? a. Если да, то имеются ли процедуры, где требуется анализ последствий с соответствующим утверждением до ввода в действие? b. Одобрен анализ последствий компетентным экспертом или организацией?
28	Существуют ли какая-либо процедура обеспечения безопасности или меры предосторожности при выводе из эксплуатации?

- использование устройств сигнализации о неисправностях;
- требования и ограничения на средства и языки программирования;
- интегральный уровень безопасности, которому соответствует устройство или система.

Пример

В качестве примера можно привести руководство по функциональной безопасности, подготовленное компанией GM International для барьеров искробезопасности серии D1000, которые допускается использовать в системах безопасности с уровнями SIL 2 и SIL 3 [4].

Представленная в нём информация необходима для проектировщиков и инженеров по обслуживанию, системных интеграторов, а также для конечных пользователей, чтобы обеспечить правильное использование этих барьеров. Руководство по функциональной безопасности не заменяет руководства по монтажу и обслуживанию, а является дополнением к ним по части процедур верификации, которые выполняются при проведении диагностических проверочных тестов. Оно также полезно на этапе проектирования для выбора, например, барьера искробезопасности, пригодного для использования в системе с заданным уровнем SIL.

Контрольный лист для компонентов SIF

При выборе компонентов для системы безопасности рекомендуется ответить на все вопросы контрольных листов для каждого компонента. Данные для заполнения опросного листа берутся из руководства по функциональной безопасности.

В качестве примера в табл. 5 приведены вопросы контрольного листа. Эта таблица отличается от полноформатного контрольного листа только отсутствием полей для ответов на перечисляемые вопросы: «Да», «Нет», «Нет данных», «Комментарии/значения».

Контрольный лист предназначен для проверки наличия всех данных, необходимых для расчёта уровня SIL функции SIF. Данные из контрольных листов для простых подсистем будут группироваться в таблицу, из которой затем можно получать окончательные значения для функции безопасности всей системы в целом. ●

Литература

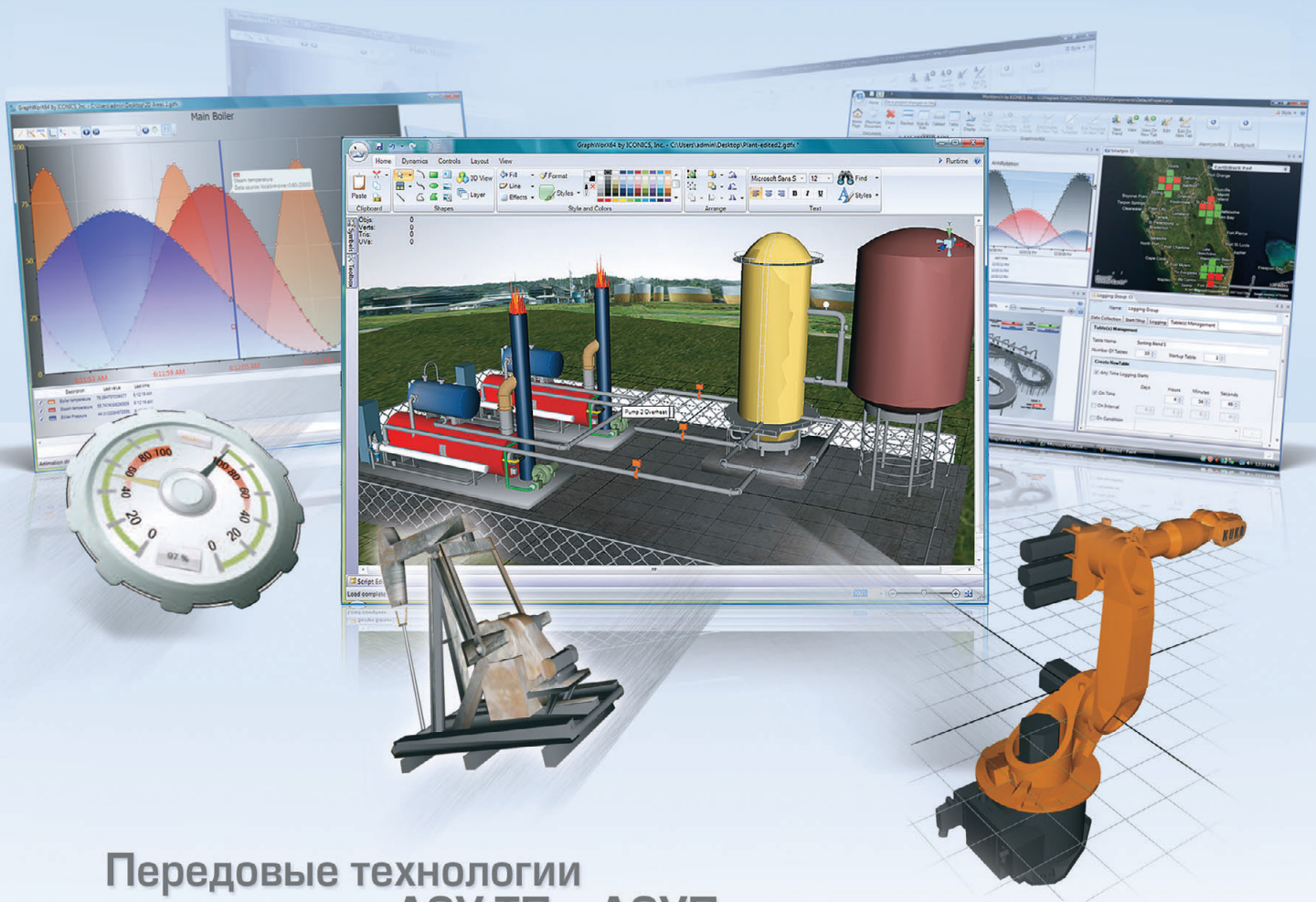
3. Стандарт МЭК 61511. Системы обеспечения безопасности для перерабатывающих отраслей промышленности.
4. Functional Safety Manual for Safety Related Systems and SIL 2, SIL 3 Applications according IEC 61508 & IEC 61511 Standards. GM International D1000 Series Intrinsically Safe Interface Modules and Switching Power Supply PSD1206, PSD1210 // Document ISM0071-9. — GM Internatio-nal, 2009. — 54 p.

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

GENESIS64™

Новое поколение программного обеспечения ICONICS для автоматизации

ICONICS



Передовые технологии для создания АСУ ТП и АСУП любого уровня

64

CERTIFIED FOR Windows Vista™

CERTIFIED FOR Windows Server® 2008

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР ПРОДУКЦИИ ICONICS В РОССИИ, СТРАНАХ СНГ И БАЛТИИ **#252**

ProSoft®

МОСКВА	Тел.: (495) 234-0636 • Факс: (495) 234-0640 • E-mail: info@prosoft.ru • Web: www.prosoft.ru
С.-ПЕТЕРБУРГ	Тел.: (812) 448-0444 • Факс: (812) 448-0339 • E-mail: info@spb.prosoft.ru • Web: www.prosoft.ru
ЕКАТЕРИНБУРГ	Тел.: (343) 376-2820 • Факс: (343) 376-2830 • E-mail: info@prosoftsystems.ru • Web: www.prosoftsystems.ru
САМАРА	Тел.: (846) 277-9166 • Факс: (846) 277-9165 • E-mail: info@samara.prosoft.ru • Web: www.prosoft.ru
НОВОСИБИРСК	Тел.: (383) 202-0960; 335-7001/7002 • E-mail: info@nsk.prosoft.ru • Web: www.prosoft.ru
КИЕВ	Тел.: (+380-44) 206-2343/2478/2496 • Факс: (+380-44) 206-2343 • E-mail: info@prosoft-ua.com • Web: www.prosoft.ru
УФА	Тел.: (347) 2925-216; 2925-217 • Факс: (347) 2925-218 • E-mail: info@ufa.prosoft.ru • Web: www.prosoft.ru
КАЗАНЬ	Тел.: (843) 291-7555 • E-mail: kazan@prosoft.ru • Web: www.prosoft.ru
ОМСК	Тел.: (3812) 286-521 • E-mail: omsk@prosoft.ru • Web: www.prosoft.ru
ЧЕЛЯБИНСК	Тел.: (351) 239-9360 • E-mail: chelyabinsk@prosoft.ru • Web: www.prosoft.ru
КРАСНОДАР	Тел.: (861) 224-9513 • Факс: (861) 224-9513 • E-mail: krasnodar@prosoft.ru • Web: www.prosoft.ru