Безопасность по расчету. Важные параметры при выборе оборудования для систем с требованием SIL

А.А. Ершов (ООО «Феникс Контакт РУС»)

Рассматриваются параметры, применяемые для описания оборудования и систем, удовлетворяющих требованиям функциональной безопасности. Компания Phoenix Contact предлагает широкий ассортимент устройств и оборудования, сертифицированного в соответствии с требованиями МЭК 61508.

Ключевые слова: уровень функциональной безопасности, аппаратная отказоустойчивость, вероятность отказа выполнения требуемой функции, доля безопасных отказов оборудования, интервал функциональной проверки.

На всех стадиях существования ответственных производств и установок: от проектирования до их эксплуатации вопросы, связанные с обеспечением необходимого уровня функциональной безопасности (SIL) занимают одно из главных мест. Причина этого понятна: любой отказ машин, механизмов или ПО в системах, функционирующих в потенциально взрывоопасной среде, может привести к самым серьезным последствиям. Соответствие требованиям стандартов является важнейшим критерием выбора устройств и компонентов, предназначенных для систем безопасности ТП. Например, стандарт МЭК 61511 «Функциональная безопасность. Приборные системы безопасности для ТП в промышленности» рекомендует в приложениях, предназначенных для обеспечения безопасности, всегда использовать искробезопасное оборудование, соответствующее SIL, если это возможно.

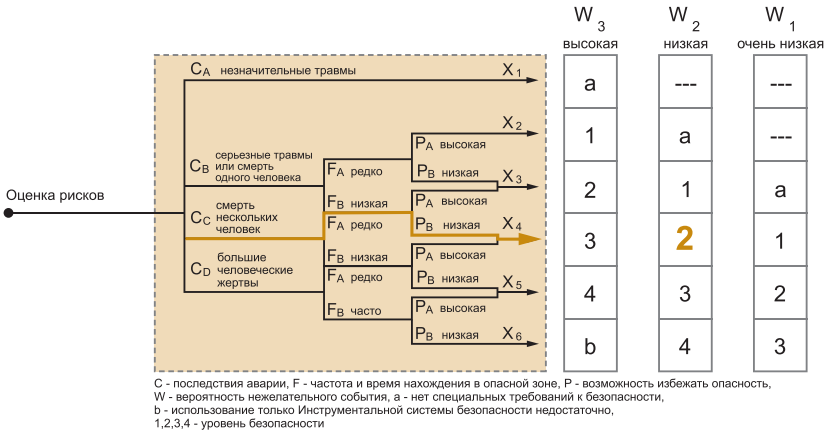

Рис. 1. Диаграмма рисков с результатами выбора уровня SIL

Стандарт МЭК 61508 является руководящим документом для производителей оборудования, а МЭК 61511 предназначен для тех, кто проектирует и эксплуатирует системы безопасности в нефтяной, газовой, химической промышленности. Технологи, специалисты по безопасности производства и инженеры, выполняя оценку опасных факторов и рисков, прогнозируют, насколько производство или система представляет опасность для персонала и окружающей среды. Задача будущей системы безопасности – снизить риски до приемлемого уровня, так как исключить их полностью невозможно.

Снижение риска в системах безопасности производственным процессом

При анализе рисков определяются эффекты, которые могут возникнуть в случае аварийной ситуации в соответствии с определенным уровнем SIL. Кроме того, принимаются во внимание частота и вероятность возникновения аварийной ситуации, так как риск пропорционален вероятности наступления рискового события и возможным потерям от него. Таким образом, событие с тяжелыми последствиями, но очень маловероятное, может иметь меньший уровень риска, чем событие гораздо менее тяжелое, но более вероятное. В МЭК 61511-3 приводятся различные методы анализа рисков, но наиболее часто используется диаграмма рисков (рис. 1).

При создании системы безопасности производства или установки используется инструментальная система безопасности (SIS – Safety Instrumented System), которая в свою очередь состоит из функций безопасности (SIF – Safety Instrumented Function). Для каждой SIF, состоящей в общем случае из входной цепи, логической цепи и выходной цепи, определяется «безопасное состояние». Необходимо определить действия, которые должны произойти, например, в случае отключения

Таблица 1. Аппаратная отказоустойчивость для устройств типа A/B

Доля безопасных отказов (SFF)	HFT		
	0	1	2
< 60%	SIL 1/ не допускается	SIL 2/ SIL 1	SIL 3/ SIL 2
60...90%	SIL 2/ SIL 1	SIL 3/ SIL 2	SIL 4/ SIL 3
90...99%	SIL 3/ SIL 2	SIL 4/ SIL 3	SIL 4/ SIL 4
>99%	SIL 3/ SIL 3	SIL 4/ SIL 4	SIL 4/ SIL 4

Таблица 2. Соответствие уровней SIL и PFD_{avg}

SIL (по МЭК 61508)	PFD (вероятность отказа требуемой функции)	RRF (фактор снижения риска)
SIL 4	$< 10^{-4}$	> 10000
SIL 3	$10^{-4}...10^{-3}$	1000...10000
SIL 2	$10^{-3}...10^{-2}$	100...1000
SIL 1	$10^{-2}...10^{-1}$	10...100

питания. Кроме того, пользователь должен определить уровень SIL как меру снижения уровня риска для каждой функции. По сути, SIL показывает вероятность, с которой SIS выполнит SIF в течение определенного периода времени. Каждый элемент SIF должен соответствовать этому уровню. Кроме датчиков и исполнительных элементов во входные/выходные цепи могут входить также искробезопасные барьеры или преобразователи аналоговых сигналов с гальванической развязкой. Однако недостаточно просто взять элементы с соответствующим SIL и соединить их между собой, необходимо провести расчеты и убедиться, что требуемый SIL всей функции при этом сохраняется.

Уровень SIL конкретного устройства означает всего лишь возможность его использования в цепях систем безопасности и выполнение требований стандартов на всех стадиях его жизненного цикла, включая разработку. Соответствующий уровень SIL обычно указывается в сертификате, прилагаемом к изделию.

Рис. 2. Оборудование Phoenix Contact для систем безопасности

Важные термины и величины из области безопасности

При проектировании SIF необходимо определить, сколько дополнительных устройств нужно установить для ее реализации. Так называемая архитектура Voting MooN или «голосование» M устройств из N ед. показывает, какое число этих дополнительных устройств потребуется. В итоге получаем важный параметр HFT (Hardware Fault Tolerance или аппаратная отказоустойчивость). Например, если установлены два датчика, каждый из которых способен вызвать срабатывание SIF, считается, что система имеет архитектуру 1oo2, которая допускает отказ одного из датчиков. В этом случае HFT = 1. При HFT = 0 (архитектуры 1oo1, 2oo2 и т.д.) даже один отказ ведет к потере безопасности. Решение о выборе HFT и архитектуры принимается на основе требований к безопасности объекта, его эксплуатационной готовности и эффективности затрат.

Все устройства в рамках стандарта МЭК 61508 делятся на две категории: к типу А относятся простые устройства, поведение которых и виды отказов хорошо известны (а значит, прогнозируемы и детектируемы); устройства типа В могут содержать комплексные компоненты с потенциально неизвестными видами отказов, например, микропроцессоры. В этом случае используется понятие функциональной безопасности (Safe Failure Fraction, SFF) – доля безопасных отказов оборудования, которые потенциально не приведут к опасному состоянию системы или потере функции безопасности.

В зависимости от типа устройства по МЭК 61850 (А или В) значение SFF в комбинации с выбранным значением HFT определят максимальный уровень SIL функции безопасности схемы, в которую может быть установлен данный прибор (табл. 1). Если при этом не достигается необходимое значение фактора снижения риска, то должна быть выбрана другая архитектура (определяющая HFT) или другое устройство с более высокой долей безопасных отказов.

Кроме HFT и SFF также учитывается средняя вероятность отказа выполнения требуемой функции PFDavg (Probability of Failure on Demand). Этот параметр предсказывается только на ограниченный период времени –интервал функциональной проверки Tproof. По истечении этого периода необходимо проверять работоспособность SIF, так как PFDavg растет со временем, а значит, увеличивается вероятность того, что SIF не выполнит свою задачу в нужный момент. Интервал Tproof выбирается эксплуатантом системы, исходя из необходимости поддержания требуемого SIL системы безопасности.

Когда для данной SIF выбраны все составляющие ее компоненты, и известны все основные параметры этих компонентов (SFF, HFT, PFDavg), необходимо убедиться, что PFDavg всей функции соответствует требуемому SIL (табл. 2). Вероятность отказа всей функции вычисляется суммированием значений PFD всех ее компонентов. При этом может оказаться, что хотя все компоненты удовлетворяют заданному уровню SIL, функция в целом не соответствует этому уровню снижения риска. Поэтому к выбору оборудования для систем безопасности необходимо подходить особенно тщательно, обращая внимание на все перечисленные параметры.

Широкая продуктовая гамма оборудования для систем безопасности

Требования к оборудованию при проектировании систем безопасности SIS постоянно возрастает, поэтому Phoenix Contact предлагает широкий ассортимент устройств и оборудования, сертифицированного в соответствии с требованиями МЭК 61508. Примером может служить силовая электроника: пускатели семейства Contactron (управление двигателем), промежуточные реле безопасности PSR-FSP со встроенным предохранителем в выходной цепи, а также аналоговые преобразователи серии MACX MCR, доступные как в стандартном, так и в искробезопасном исполнении (MACX MCR-EX), соответствующие уровням SIL2 или SIL3 (рис. 2). Для всех этих устройств Phoenix Contact предоставляет необходимые данные для расчета систем безопасности на их основе, а также сертификаты подтверждения уровня SIL.

Ершов Алексей Анатольевич *– инженер технической поддержки ООО "Феникс Контакт РУС".*
Контактный телефон (495) 933-85-48, факс 931-97-22.
E-mail: info@phoenixcontact.ru Http://www.phoenixcontact.ru