Функциональная безопасность

На опасных промышленных объектах неправильное функционирование системы автоматизации может привести к человеческим жертвам, экологическим катастрофам или большим финансовым потерям. Полностью исключить ситуации, приводящие к таким последствиям, невозможно. Речь может идти только о вероятности их возникновения и допустимом уровне риска.

Риском в области безопасности называют произведение вероятности возникновения опасной ситуации на тяжесть (стоимость) последствия. Допустимый уровень риска оценивается в каждом конкретном случае индивидуально. Из определения риска следуют пути его снижения: уменьшение вероятности появления опасной ситуации и ограничение тяжести ее последствий.

Под **безопасностью систем** понимается такое их функционирование, при котором отсутствуют опасные отказы и недопустимый ущерб.

Функциональной безопасностью называют безопасность, которая связана с непреднамеренно вызванными отказами в выполнении отдельных функций системы.

Причинами отказов могут быть дефекты программ, данных, аппаратуры, влияние внешней среды и непреднамеренно неправильные действия обслуживающего персонала.

Функциональную безопасность следует отличать от:

- информационной безопасности, которая связана в основном с умышленным воздействием на систему;
- электробезопасности, которая относится к защите человека от поражения электрическим током;
- взрывопожаробезопасности, которая изучает методы предотвращения воспламенения горючих газов, ЛВЖ, пыли и волокн.

Функциональная безопасность

Функциональная безопасность отличается от понятия надежности тем, что она учитывает не только частоту отказов системы, но и вероятность возникновения опасной ситуации во время отказа.

Пример

Надежность контроллера, стоящего в системе автоматического пожаротушения и контроллера в системе управления лифтом, может быть одинаковой, однако лифтом пользуются много раз в день, и практически каждый отказ может привести к нарушению безопасности, в то время как отказ системы пожаротушения может не проявиться никогда, даже если этот отказ произойдет. Из этого следует, что одного понятия надежности недостаточно для описания степени безопасности систем автоматизации.

Термин «функциональная» применительно к безопасности систем автоматизации означает безопасность, которая зависит от корректного функционирования системы, т.е. от правильного выполнения системой своих функций. В отличие от этого, надежность описывает частоту отказов независимо от назначения системы и тяжести последствий, вызванных отказами. Тем не менее, показатели надежности используются при количественном описании функциональной безопасности.

При анализе функциональной безопасности рассматриваются опасные отказовые ситуации, которые приводят к авариям, катастрофам и человеческим жертвам. Функциональной безопасности программируемых электронных систем посвящен международный стандарт МЭК 61508 и серия связанных с ним стандартов [МЭК - IEC].

Функциональная безопасность

Стандарт выделяет четыре "уровня полноты безопасности" (Safety Integrity Level, SIL), которые выбираются в зависимости от тяжести последствий, которые могут наступить при неправильном функционировании системы.

Уровень SIL4 является самым высоким, наиболее труднодостижимым. Для его обеспечения требуется чрезвычайно высокая квалификация и работа "на грани искусства". Поэтому следует избегать необходимости его применения.

Уровень SIL3 ниже, чем SIL4, но также требует высокой квалификации и высокого уровня организации процесса проектирования. Немногие исполнители способны обеспечить этот уровень безопасности.

Уровень SIL2 требует управления работами в соответствии со стандартом ИСО 9001 Системы менеджмента качеством.

Достижение этого уровня требует большего числа испытаний, чем SIL1, что приводит к увеличению стоимости проекта.

Уровень SIL1 является самым низким, для его выполнения достаточно наличия хорошего опыта разработок.

Функциональная безопасность

Уровни SIL определяют величину допустимого риска для системы.

Они являются мерой вероятности того, что система будет правильно выполнять свои функции, влияющие на безопасность. При оценке риска используется понятие "demand on the safety" - "запрос безопасности", которое означает возникновение ситуации, в которой может проявиться свойство безопасности.

Пример

Ситуация, при которой срабатывает система аварийной защиты (ПАЗ), является "запросом безопасности". Этот запрос может не реализоваться, если во время запроса система находится в состоянии отказа, или реализоваться в виде срабатывания системы.

Величина риска зависит от частоты запроса безопасности. Например, если покушение на ограбление банка ("запрос безопасности") случается 1 раз в год, то вероятность отказа системы охранной сигнализации в течение года должна быть равна 0,1, чтобы ограбление было возможно не чаще чем 1 раз в 10 лет.

Функциональная безопасность

В таблице приведены границы вероятности отказов при наличии запроса к системе при низкой частоте запросов (реже 1 раза в год), устанавливаемые стандартом МЭК 61508.

Вероятность отказов при частоте запросов менее одного раза в год

Уровень SIL	Вероятность отказа при наличии запроса	Предельно допустимое число отказов
SIL1	$\leq 10^{-2} < 10^{-1}$	Один опасный отказ за 10 лет
SIL2	$\leq 10^{-3} < 10^{-2}$	Один опасный отказ за 100 лет
SIL3	$\leq 10^{-4} < 10^{-3}$	Один опасный отказ за 100 лет
SIL4	$\leq 10^{-5} < 10^{-4}$	Один опасный отказ за 10000 лет

Функциональная безопасность

При высокой частоте запросов (например, если взрывоопасная пыль в шахте присутствует постоянно и вероятность взрыва существует всегда, т.е. запрос безопасности существует непрерывно), вероятность отказа в зависимости от уровня безопасности SIL выбирается из таблицы. В этой таблице использована величина вероятности отказа системы в течение часа, в то время как в предыдущей таблице - вероятность отказа в течение часа, умноженная на интервал между запросами.

Вероятность отказов при частоте запросов более одного раза в год

Уровень SIL	Вероятность отказа в течение часа	Предельно допустимое число отказов
SIL1	$\leq 10^{-6} < 10^{-5}$	Один опасный отказ за 100 тыс. час.
SIL2	$\leq 10^{-7} < 10^{-6}$	Один опасный отказ за 1 млн. час.
SIL3	$\leq 10^{-8} < 10^{-7}$	Один опасный отказ за 10 млн. час.
SIL4	$\leq 10^{-9} < 10^{-8}$	Один опасный отказ за 100 млн. час.

Функциональная безопасность

Стандарт МЭК 61508 устанавливает два способа расчета величины риска. Поскольку риск определяется как произведение вероятности возникновения опасной ситуации на тяжесть (стоимость) последствия, первой стадией в оценке риска является определение вероятность возникновения опасности. Количественный метод расчета вероятности основан на анализе частоты отказов системы.

При анализе функциональной безопасности различают случайные отказы и систематические.

Систематические отказы (типовой случай - отказы программного обеспечения) существуют постоянно, даже в момент пуска системы в эксплуатацию.

Случайные отказы появляются с течением времени. Основным средством уменьшения интенсивности случайных отказов является резервирование компонентов системы.

Количество систематических отказов может быть снижено преимущественно в процессе разработки, для чего стандарт устанавливает требования к процессу разработки, модернизации, а также к архитектуре аппаратного и программного обеспечения.

Функциональная безопасность

В системах промышленной автоматизации компонентами, влияющими на функциональную безопасность, являются:

- датчики;
- контроллер с программным обеспечением;
- исполнительные устройства;
- линии связи между ними.

Стандарт МЭК 61508 требует анализа соответствия такой системы одному из уровней безопасности. Отметим, что если отдельные компоненты системы удовлетворяют требованию, например, уровня SIL2, то это не означает, что система в целом соответствует SIL2, поскольку вероятность отказа системы всегда выше, чем отдельных ее компонентов.

В то же время, используя резервирование, можно построить систему более высокого уровня безопасности, чем уровень входящих в нее компонентов.

Требования функциональной безопасности необходимо выполнять на протяжении всего жизненного цикла системы автоматизации, который включает проектирование, производство, снабжение, контроль, проведение испытаний, упаковку и хранение, доставку, монтаж у заказчика, эксплуатацию, обучение персонала эксплуатирующей организации, техническую поддержку, утилизацию.

Функциональная безопасность

Многие результаты применения принципов обеспечения функциональной безопасности систем автоматизации изложены в отраслевых правилах промышленной безопасности, где сформулированы требования к допустимой частоте отказов, к видам защиты и способам их выполнения, требования к резервированию, к построению систем сигнализации, блокировок и аварийного останова, к алгоритмам работы систем автоматической противоаварийной защиты (ПАЗ) и др.

Функциональная безопасность

Заключение

Таким образом, алгоритм выбора и установки технических средств для опасных промышленных объектов можно представить в виде следующей последовательности шагов:

1. Определяют, является ли опасный производственный объект взрывоопасным. Если не является, то единственным требованием к техническим средствам является наличие разрешения Ростехнадзора на его применение.
2. Если является взрывоопасным, то:

- определяют класс взрывоопасной зоны, пользуясь проектной или эксплуатационной документацией. В зависимости от класса выбирают уровень взрывозащиты (первая цифра в маркировке);
- определяют категорию взрывоопасности технологического блока; в зависимости от категории взрывоопасности формулируются требования к техническим характеристикам по надежности (необходимости резервирования), быстродействию, допустимой погрешности и др; категория взрывоопасности влияет также на выбор вида взрывозащиты (d, m, ia и др);
- в зависимости от энергии воспламенения взрывоопасной среды или состава взрывоопасной смеси выбирают группу электрооборудования (в маркировке следует за видом взрывозащиты);
- в зависимости от температуры воспламенения взрывоопасной смеси выбирают температурный класс оборудования (в маркировке следует за группой электрооборудования).

Функциональная безопасность

Заключение

Если объект не является взрывоопасным, но является пожароопасным, то определяют степень защиты оболочки оборудования.

Проверяют наличие разрешения Ростехнадзора на применение технического средства, срок его действия и соответствие маркировки вида взрывозащиты необходимым требованиям.

Установка технического средства (системы автоматизации) на объект должна выполняться строго в соответствии с проектом строительства опасного производственного объекта. Если в проект вносятся изменения в связи с модернизацией (реконструкцией), то эти изменения должны пройти экспертизу промышленной безопасности в организации, имеющей лицензию на данный вид деятельности и соответствующую область аккредитации. Заключение экспертизы утверждаются в территориальном органе Ростехнадзора. По окончании установки производится приемка объекта в эксплуатацию.

Монтажная (проектная) организация должна иметь членство в СРО с разрешением на выполнение работ из перечня. Работники монтажной (проектной) организации должны пройти обучение, аттестацию и иметь удостоверения Ростехнадзора о проверке знаний в области промышленной безопасности.