конденсаторами. Среднее время наработки на отказ для Kontron KISS 2U KTQ45/Flex Low Profile составляет 50 тыс. ч, а уровень издаваемого им шума не превышает 35 дБ. Изделие имеет класс защиты IP20, выдерживает удары силой 30g и рассчитано на работу при температурах 0...50°C.

Надежность за разумную цену

В профессиональных сферах должны использоваться высококачественные профессиональные решения, способные обеспечивать высокую надежность, тем более, что сегодня такие решения вполне доступны отечественному потребителю. Надежность – это интегральная многофакторная характеристика. На результирующую надежность конечной системы оказывают влияние как базовые аппаратные средства (процессоры и чипсеты из линейки Intel Embedded Roadmap, долгоживущие танталовые конденсаторы и т. п.), так и различные вспомогательные технологии, особенности организации контроля качества на стороне поставщика и обслуживания уже развернутых систем на стороне клиента. Для серверного сегмента с его высоким уровнем ответственности, жесткими условиями эксплуатации и требованиями доступности сервисов в режиме 24 часа в день/7 дней в неделю главное конкурентное преимущество профессиональных решений состоит в: возможности избегать частых отказов оборудования, суммарные потери от которых могут многократно превзойти начальную экономию на комплектующих, качестве дизайна, качестве сборки и тестировании.

Очень важно, что весь цикл разработки серверов Kontron CRMS и Kontron KISS с трехмерным моделированием задней стенки и воздушных потоков, созданием опытных образцов и их всесторонними испытаниями осуществляется на территории США и Германии американскими и немецкими инженерами. При этом наличие в РФ авторизованного производственного центра Kontron – компании РТСофт подрывает стереотипное мнение относительно дороговизны профессиональных западных компьютерных продуктов. Возможность кастомизации на отечественных производственных мощностях позволяет пользователям решений Kontron гибко управлять своими расходами в зависимости от конкретных проектных требований.

Ковалев Александр Николаевич *– директор направления ЗАО "РТСофт".*
Контактный телефон (495) 967-15-05.
Http://www.rtsoft.ru E-mail: pr@rtsoft.ru

Готовность, надежность, интегральный уровень безопасности. В чем разница?

ЗАО "ВСП Лтд"

Рассматриваются параметры, характеризующие готовность, надежность и интегральный уровень безопасности производственного оборудования и систем. Приводятся примеры расчетов интенсивности отказов компонентов системы автоматизации.

Ключевые слова: интегральный уровень безопасности, интенсивность отказов, средняя наработка на отказ, время неисправного состояния, вероятность опасного отказа, риски взрыва, взрывозащита, искробезопасность.

Готовность, надежность, интегральный уровень безопасности – эти и некоторые другие термины часто встречаются, когда речь идет об оборудовании и системах. Все они в определенной степени говорят о том, насколько хорошо оборудование или система будет выполнять определенную задачу; однако важно использовать правильный термин для конкретной задачи, иначе получить правильный ответ возможно ..., но на другой вопрос[1].

Надежность

Надежность – это «вероятность того, что объект будет выполнять необходимую функцию при указанных условиях в течение указанного периода времени». Существуют различные способы выражения надежности, одним из общепринятых является средняя наработка на отказ (MTBF) – это средняя наработка какого-либо оборудования или системы между отказами. Как показано на рис. 1 – это среднее значение t относительно эксплуатационной наработки оборудования. Показатель средней наработки на отказ часто используется для описания общей надежности единицы оборудования или системы.

Средняя наработка на отказ (MTBF) – применяется к оборудованию, подлежащему восстановлению, или для обозначения общей надежности оборудования. Если объект не подлежит восстановлению, более правильно использовать термин «наработка объекта от начала эксплуатации до возникновения первого отказа» (MTTF). Однако практически их значение

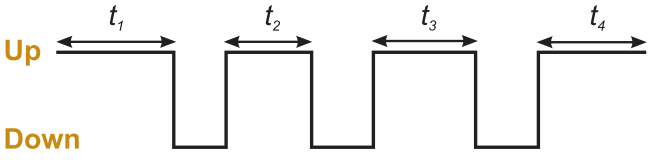

Рис. 1, где Up time – период доступности, Down time – период неисправного состояния

[1] При написании статьи использованы материалы работы Chris Towle, работающего в области искробезопасности с середины 1950 гг., одного из основателей MTL Instruments

одинаково. Часто термин «средняя наработка на отказ» также используется и для оборудования, не подлежащему восстановлению.

Неправильно предполагать, что MTBF означает средний срок службы или ожидаемый срок службы. На самом деле по истечении периода времени, равному MTBF, только 37% единиц оборудования еще будут функционировать.

Интенсивность отказов (λ) часто используется для описания надежности простых объектов или компонентов оборудования, а также для описания надежности определенных функций, например, опасная интенсивность отказов системы безопасности. Также обычно используется для описания надежности определенной функции, например, функции безопасности. Интенсивность отказов измеряется в единицах времени$^{-1}$.

Готовность можно определить как отрезок времени, в течение которого оборудование будет способно выполнять свою функцию. Понятие готовности отличается от надежности тем, что в него входит время на ремонт. Единичное устройство может быть не очень надежным, но если его можно быстро отремонтировать в случае отказа, тогда степень его готовности будет высокой.

Вернемся еще раз к рис. 1, из которого следует, что Up Time (период доступности) – это время, характеризующее готовность оборудования; Down Time (период неисправного состояния) – это время, в течение которого оборудование было неисправно и таким образом недоступно.

Усредненные величины следующие:

– среднее значение Up Time (время доступности), которое известно как средняя наработка на отказ (MTBF);

– среднее значение Down Time (время неисправного состояния) или MDT.

Иногда вместо MDT (время неисправного состояния) используют MTTR (среднее время восстановления после отказа). Но MTTR может иметь иное значение, нежели MDT, так как:

• неисправность может быть отмечена лишь по истечении некоторого времени;

• может быть принято решение отложить ремонт на некоторое время;

• после ремонта оборудование может быть введено в эксплуатацию не сразу.

Независимо от используемых понятий MDT/MTTR важно, отобразить общее время, в течение которого оборудование было не доступно для эксплуатации, иначе расчет готовности будет некорректным.

Иногда бывает полезным термин «неготовность» = 1- «готовность».

Вероятность опасного отказа выполнения требуемой функции – PFD

Системы безопасности часто разработаны с учетом их функционирования на втором плане для мониторинга процесса. При этом они не должны инициировать каких-либо действий до тех пор, пока не превышен порог безопасности, который требует от системы определенных действий для поддержания безопасности. Такие системы безопасности известны под названием системы противоаварийной защиты (ПАЗ).

Термин PFD означает неготовность функции защиты. Если возникает необходимость выполнения функции защиты, какова вероятность, что функция защиты уже находится в состоянии неготовности?

Запишем выражение для PFD (вероятности опасного отказа выполнения требуемой функции):

$PFDavg \approx \lambda_{DU} MDT$,

где *PFDavg* – усредненная по времени вероятность неготовности системы защиты (корректный термин, поскольку вероятность действительно изменяется во времени. Вероятность того, что система не выполнит свою функцию, будет зависеть от того, как давно систему тестировали); λ_{DU} – интенсивности опасных необнаруженных отказов (не учитываются «безопасные» отказы, поскольку они вызывают остановку процесса, а учитываются только те отказы, которые остаются скрытыми, но отклонят действие защитной функции, когда в ней возникнет необходимость).

Это важный момент, поскольку неправильно было бы предполагать, что устройство, связанное с системой обеспечения защиты в принципе более надежно, чем устройство общего назначения. Устройство, связанное с системой обеспечения защиты, разработано с учетом крайне низкой интенсивности отказов системы защиты, но суммарная интенсивность отказов (иными словами MTBF – средняя наработка на отказ) может быть менее впечатляющей величиной.

Таким образом, как соотнести MDT (время неисправного состояния) относительно функции защиты? По определению опасный необнаруженный отказ не будет проявляться до возникновения требования функции защиты или будет выявлен во время тестирования.

Допустим мы проверяем функцию защиты каждые T_1 часов. Одинаково вероятно, что функция защиты может отказать в любое время между одним диагностическим тестом и следующим, то есть в среднем $T_1/2$ часа.

Простейший расчет вероятности опасного отказа выполнения требуемой функции:

$PFDavg \approx ½\lambda_{DU} T_1$.

Что значит SIL?

Интегральный уровень безопасности SIL (Safety Integrity Level) является одним из наиболее неправильно используемых терминов в области надежности. Используя термин SIL, часто предполагают, что устройство обладает более высоким качеством, надежностью или другими привлекательными характеристиками. Это не соответствует действительности.

Интегральный уровень безопасности представляет собой дискретную величину в диапазоне 1...4, предна-

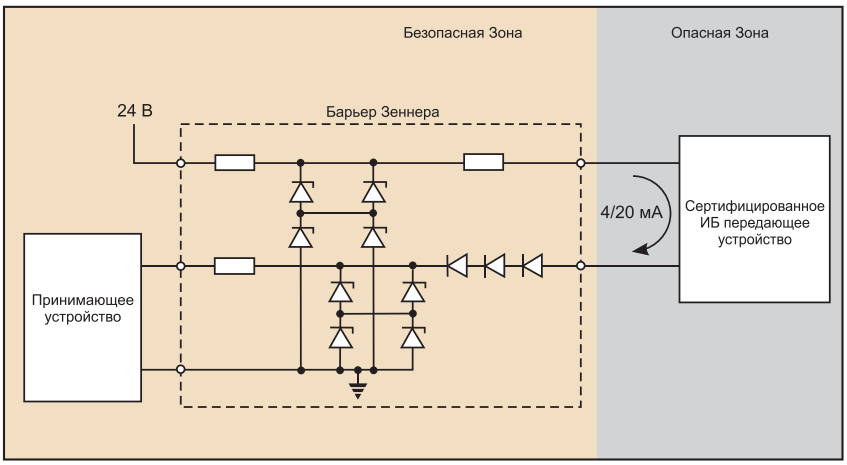

Рис. 2. Типичная ИБ цепь 4…20 мА

значенную для определения уровня требований к безопасности, который необходим для определенного процесса или системы безопасности с целью достижения необходимого уровня защиты. Характеристика SIL1 – это нижний уровень системы безопасности, SIL4 – высшая степень безопасности самой системы.

Ко многим устройствам применяют характеристику «категория по SIL», подразумевая, что эти устройства пригодны для использования в системах защиты. Так ли это в действительности, зависит от многих факторов, что не является предметом данной статьи. Однако полезно запомнить, что даже если устройство действительно соответствует требованиям SIL, это всего лишь говорит о том, что оно сможет выполнить определенную функцию в системе защиты. Уровень надежности по фактору безопасности может быть достаточно высоким, но общая надежность может быть на более низком уровне.

Применение статистических методов ко всем видам анализа надежности вызывает в последнее время все больший интерес. Рассмотрим далее три аспекта надежности простого диода Зеннера, установленного в цепи датчика 4...20 мА, и предположим, что такой подход может обозначить иной путь оценки рисков.

Таблица 1. Интенсивность отказов компонентов в FIT (1 FIT=10^{-9} отказов в час)

Компонент	Интенсивность отказов	Отказ по короткому замыканию	Отказ по разомкнутой цепи	Уход характеристик
Диод Зеннера	10	7	2	1
Диод Шоттки	7,5	6	1,5	0
Резистор и предохранитель	10	0	10	0

Таблица 2. Анализ интенсивности эксплуатационных отказов

Компонент	Механизм отказа	Интенсивность отказа (FIT)
Предохранители – x2	Разомкнутая цепь	20
Сопротивления – x1	Разомкнутая цепь	10
Диоды – x3	Разомкнутая цепь	4,5
Диоды Зенера – x8	Короткое замыкание + дрейф	64
	Всего	98,5

При рассмотрении надежности охватывают следующие три характеристики: отказы, вызывающие эксплуатационные отказы; очевидные отказы, например, те, которые используются в подходе к оценке надежности с точки зрения SIL (интегрального уровня безопасности); и отказы, которые могут привести к возникновению взрывоопасной ситуации.

В данном анализе ситуация рассматривается на примере шунт-диодного барьера 28 В (рис. 2), который обычно используется с датчиками 4...20 мА. Важно помнить о том, что любой анализ, касающийся рейтинга SIL, относится к отдельной системе, и каждая система должна рассматриваться индивидуально. Данные об отказах по какому-либо устройству всегда важны, но понятие интегрального уровня безопасности является системной концепцией.

Интенсивность отказов компонентов

Существенную трудность при любой оценке надежности представляет определение достоверной интенсивности отказов компонентов. В данном анализе использованы цифры из двух источников: PD IEC TR 62380:2004 и BT Handbook of reliability data; сделаны определенные предположения и реализован консервативный подход к некоторым показателям, таким как окружающие условия. Полученные результаты целесообразно трактовать как показатель порядка вещей, а не точный анализ, ведущий к неоспоримым выводам. Данные по интенсивности отказов, которые были использованы в расчетах, указаны в табл. 1.

Нулевая интенсивность отказов резисторов по короткому замыканию соответствует концепции «надежного компонента», используемой в искробезопасности, и вследствие ухудшения параметров компонентов безопасности, очевидно, оправдана. Диоды Зеннера, используемые в барьерах, проходят индивидуальное импульсное тестирование, и их номинальные характеристики снижаются с коэффициентом 1,5. Таким образом, более низкое значение интенсивности отказов может быть оправдано. Однако в данном анализе используется нормальная интенсивность отказов.

Интенсивность эксплуатационных отказов

Разомкнутая цепь последовательных компонентов и короткое замыкание шунтирующих компонентов приводят к эксплуатационному отказу (табл. 2).

Предположим, что, если компания MTL поставила несколько миллионов барьеров за последние 30 лет, интенсивность отказов может быть установлена достаточно точно. На практике

не все вышедшие из строя барьеры возвращаются на завод или об этих отказах сообщается. Причиной большинства отказов является приложение избыточного напряжения на разъемы в безопасной зоне. В этих обстоятельствах барьер как раз и выполняет свою функцию, и эти случаи не должны рассматриваться как отказы в контексте данного анализа. Возможно, что рассчитанная интенсивность отказов порядка 0,1%/г кажется пессимистической величиной, однако установить такой низкий уровень отказов с какой-либо степенью достоверности, основываясь на информации по отказам в полевых условиях, чрезвычайно трудно.

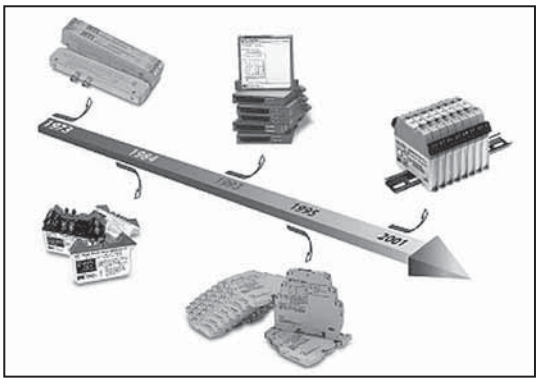

Рис. 3. Эволюция барьера Зеннера

В действительности, с течением времени барьеры были конструктивно улучшены (рис. 3), технологии производства и тестирования усовершенствованы, а надежность компонентной базы повышена. Следовательно, текущие характеристики надежности возможно лучше, чем первоначальные.

Интенсивность обнаруженных и необнаруженных отказов

В цепи датчика 4...20 мА при требовании высокой интегральной целостности общей практикой является обеспечение мониторинга и генерирование тревоги при выходе сигнала за пределы диапазона 4...20 мА. При соблюдении вышеуказанного единственным условием возможного необнаруженного эксплуатационного отказа является отказ диода Зеннера и наличие небольшого тока утечки. Это может привести к погрешности в измерениях.

Погрешность может возникнуть только из-за утечки в диодах в обратном контуре барьера. Можно возразить, что не всякое ухудшение характеристики может привести к небольшому току утечки. Но для упрощенного рассуждения принимаем, что для четырех соответствующих диодов общая интенсивность отказов при данном режиме будет равна 4 FIT (1 FIT=10^{-9} отказов в час). Значения (которые связаны с расчетами SIL для системы, включающей обнаружение выхода значения за пределы диапазона) составляют величину 4 для уровня системы безопасности и общую интенсивность отказов, равную 98,5.

Ежегодно тестируемая система с характеристикой SIL3, показывает приемлемую интенсивность отказов выполнения требуемой функции равной 10^{-4}...10^{-3}/год. Характеристика 4FIT соответствует 4 x 10^{-5}/год. Таким образом, можно предположить, что использование этого барьера необходимо принять во внимание в системах уровня SIL3. Однако один контур аналогового датчика, как правило, не сможет обеспечить интегральный уровень безопасности SIL3, и для систем с более низким уровнем интенсивность отказов барьера предположительно не будет иметь большого значения. Низкий коэффициент отношения отказов выполнения требуемой функции к общей интенсивности отказов, который составляет 4%, означает, что использование показателей по этому барьеру, обычно улучшает для большинства систем долю показателя по безопасным отказам.

Отказы, создающие риски взрыва

Отказы, вследствие которых барьер будет неэффективным с точки зрения взрывоопасности, это отказ по разомкнутой цепи двух диодов Зеннера на одной и той же ветке цепи шунтирующего диода или, наоборот, отказ по короткому замыканию трех последовательных диодов на обратном канале. Интенсивность отказов по разомкнутой цепи двух параллельных диодов Зеннера носит нелинейный характер с нарастанием по времени. Аппроксимация интенсивности отказов часто используемого сочетания представляет собой выражение:п 2 х (интенсивность отказов компонента)^2 х время^2. При консервативном подходе, предполагая, что интенсивность отказов после 10 лет эксплуатации находится на должном уровне, интенсивность отказов можно вычислить, как показано в табл. 3.

Аналогичным образом, аппроксимацию интенсивности отказов по короткому замыканию всех трех последовательных диодов можно представить следующим образом: 3 х (интенсивность отказов компонента)^2 х время^2. В точке времени 10 лет интенсивность отказов последовательных диодов составляет 3 х (6 х 6 10^{-9})^2 х (10^5)^2 = 6,5 х 10^{-15} ч$^{-1}$. Следовательно имеет значение только интенсивность отказов шунта диода Зеннера, равная 1,6 х 10^{-12}.

Чтобы образовался достаточный уровень энергии, способный вызвать взрыв, источник питания датчика или оборудование, контролирующее обратный сигнал, должно генерировать отказ. Кроме того, чтобы произошел взрыв, необходимо присутствие воспламеняющейся смеси газов и одновременно наличие искры или горячей поверхности. Эти дополнительные факторы еще больше снижают риск возникновения взрыва, но, с другой стороны, их сложнее

Таблица 3.

Интенсивность отказов/час двух параллельных диодов Зеннера после 10 лет – разомкнутая цепь	= 2x [2x 10^{-9}]^2 x 10^5	= 4 x 10^{-13}
Интенсивность отказов одной из двух последовательных веток	= 2 x 4 x 10^{-13}	= 8 x 10^{-13}
Интенсивность отказов одного из двух каналов	= 2 x 8 x 10^{-13}	= 1,6 x 10^{-12}

определить количественно. В этом типе анализа не принимаются во внимание обычные отказы, которые при такой предполагаемой низкой интенсивности отказов должны учитываться. Однако поскольку их число практически невозможно определить, вероятность отказов обычного типа, как правило, не принимается во внимание. Причиной таких отказов могут послужить ошибки при производстве или сборке комплектующих.

Такой расчет показывает, что при статистическом подходе возможно снижение требований к разработке искробезопасного оборудования. Например, вероятно, потребуется рассмотреть возможность исключения требования коэффициента безопасности 1,5 при оценке компонентов безопасности.

Обслуживание и инспекция

Возможно, больше всего этот тип анализа скажется на отношении к инспекции и рутинной процедуре тестирования. При условии возможности установить, что сигнал 4...20 мА находится вне пределов диапазона, нет особого смысла в проверке эксплуатационной целостности барьера, поскольку практически все отказы являются самообнаруживающимися. В тех случаях, когда точность измерения критична, при калибровочной поверке полевого прибора также выявляется вероятность утечки диода (4FIT).

Необходимость проверки барьера на интегральную искробезопасность отсутствует, поскольку вероятность отказа по фактору риска взрыва незначительна ($<1{,}6x10^{-12}$). Эффективную проверку можно выполнить, только удалив барьер, но вероятность ошибки при выполнении этой операции намного превышает риск отказа барьера. Периодическая проверка, чтобы убедиться, что не было произведено неправильной замены барьера и что заземление в порядке, может быть оправдана, но даже это не будет представлять собой вероятного риска.

Выводы

Расчетная интенсивность эксплуатационных отказов (при использовании вышеуказанных данных) шунта диодного барьера составляет 0,1%/год (98,5 FIT). Возможно, это пессимистическая оценка, но данный анализ позволяет эффективно сравнивать интенсивность отказов в различных режимах. Возможно, в результате аналогичных расчетов всей цепи мы получим значение >1%/год, и соответственно установка барьера лишь минимально повлияет на эксплуатационную надежность.

Всегда сложно определить отказы по фактору опасности использования определенного устройства в системе SIL, поскольку это неизбежно определяется каждой конкретной системой. В данном случае при условии, что рассматривается стандартная система, анализ достаточно очевидный. В результате получаемая интенсивность отказов, равная 4 FIT, соответствует $4x10^{-5}$/год. Это означает некоторое отрицательное влияние на рейтинг системы SIL3, но более вероятно, что для системы SIL2 и SIL1 установка барьера не будет иметь существенного значения.

Значения, полученные по риску взрыва, показывают, что явным риском можно пренебречь. Можно возразить, что по принятым стандартам других способов взрывозащиты, барьер характеризуется избыточными конструктивными характеристиками. Возможно, в будущем будут внесены изменения в статистические методы, или существующий подход создания устройств с реализацией принципа «безопасно насколько возможно» будет продолжен – это вопрос для специального комитета по вопросам искробезопасности. Существующей вопрос к разработке диктуется необходимостью соответствия требованиям международного стандарта IEC по искробезопасности.

Можно возразить относительного того, что такого рода анализу нужно подвергать все искробезопасные интерфейсы. Конкретный барьер Зеннера, который был проанализирован в данной электрической цепи, был намеренно выбран в качестве простого примера. Почти во всех других приложениях присутствуют ситуации, которые сложнее подвергнуть количественному анализу, и такой анализ является менее определяющим. В общем, такой анализ более спекулятивен и обычно является дидактическим по своему характеру.

Официальный дистрибьютор MTL Instruments – компания ЗАО "ВСП Лтд".

Http://www.vsp-co.org

Новая система MicroTCA.0 (4 U)

Компания Schroff пополнила ассортимент изделий системой MicroTCA.0 (4 U), чтобы сократить потребность в пространстве для установки систем MicroTCA, не отказываясь при этом от надежного охлаждения и резервирования. Компания предлагает теперь полный ряд систем для телекоммуникационных приложений высотой 1, 3, 4, 6 и 8 U для горизонтальной или вертикальной установки печатных плат.

Базой для разработки системы 4 U послужила существующая система 6 U с вертикальным монтажом печатных плат, в которой пространство 1 U вверху и внизу используется для вентиляции. Поскольку для MicroTCA.0 не предусмотрено пространство Rear IO, высота системы была уменьшена за счет переноса обеих вставных вентиляторных кассет в зону позади объединительной платы. За счет этого глубина системы увеличилась на 300 мм. Использование двух вентиляторных кассет, каждая из которых оснащена двумя вентиляторами, также обеспечивает резервирование. Обе вентиляторные кассеты контролируются и управляются с помощью устройства управления охлаждением.

Новая система MicroTCA.0 (4 U) имеет 12 слотов AdvancedMC для модулей Single Mid-size, 2 слота MCH и 2 слота для модулей электропитания MicroTCA шириной до 12 HP. Объединительная плата выполнена с топологией Dual Star, что позволяет создать полностью резервированную систему.

Http://www.schroff.ru