

Новая Квадро Архитектура: Описание и Оценка

Dr. Lawrence V. Beckman

HIMA-Americas, Inc

Резюме

Новая Квадро архитектура (QMR) предложенная фирмой HIMA, доступная в настоящее время в приложениях для систем безопасности и контроля критических ситуаций, является значительным прорывом в области систем безопасности. В данной архитектуре предусмотрены 4 процессора, благодаря чему решаются проблемы, возникающие при двухпроцессорной архитектуре, когда могут происходить опасные неопределяемые отказы одного или двух процессоров.

Это существенное технологическое усовершенствование позволяет системе безопасности работать на 3-м уровне SIL (RC6) на одном или двух каналах в течение неограниченного периода времени, без необходимости каких-либо внешних устройств. Это позволяет добиться значительного увеличения как технологической безопасности, так и технологической надежности, превосходящих в три раза предусматриваемые троированной архитектурой (TMR). Кроме того, QMR архитектура гораздо менее восприимчива к отказам, вызванным обычными причинами, так как резервные каналы полностью разделены, изолированы и функционируют независимо друг от друга.

Отдавая должное повышению уровня безопасности и надежности, самым привлекательным преимуществом новой архитектуры является более низкая стоимость полного эксплуатационного цикла, благодаря чему появляется возможность использования системы как в крупных, так и в небольших проектах в приложения безопасности.

Исходные данные

Новая квадро архитектура, доступная в настоящее время для построения систем безопасности и контроля критических ситуаций – безусловный шаг вперед в развитии инструментальных средств безопасности (SIS). Это развитие шло от двойной архитектуры к тройной, и на данный момент представляет собой архитектуру с четырехкратным резервированием.

Типичная дублированная система может быть реализована либо в конфигурации безопасности (2-0), либо в конфигурации надежности (2-1-0). В конфигурации безопасности система нетолерантна к ошибкам и отказ в одном из действующих каналов приводит к ложному срабатыванию. По сути, это сверхбезопасно, но при этом имеет место низкая технологическая надежность. Такая система в три раза безопаснее, но значительно менее надежна.

Конфигурация 2-1-0 обеспечивает высокую надежность, но имеет очень низкие характеристики безопасности. Действительно, надежность системы в три раза выше, чем в тройной (TMR) архитектуре, но при этом она в два раза менее безопасна, чем в симплексной конфигурации (один канал). Это происходит потому, что должны отказать оба канала, чтобы в системе произошло ложное срабатывание, и оба канала должны функционировать, чтобы достичь безопасного состояния, и именно в этом заключается проблема.

Для того, чтобы обеспечить и безопасность, и надежность, сегодня дублированная архитектура реализуется в конфигурации 1oo2D. Эта архитектура является толерантной к ошибкам, в случае, если она работает в режиме 2-1-0; в случае появления ошибки, которая не может быть устранена, этот режим меняется на 2-0. Таким образом, характеристики безопасности находятся в сильной зависимости от эффективности внешней диагностики системы, а функциональная надежность – от способности системы устранять ошибки и отключать отказавший канал, при этом система продолжает благополучно функционировать на оставшемся действующем канале.

Не все реализации 1oo2D одинаковы, у некоторых из них серьезные проблемы с надежностью, возникающие в результате внедрения требуемых сравнительных диагностик. Так или иначе, все сталкиваются с общей проблемой – строгим ограничением времени работы в режиме единичного канала. Некоторые поставщики пытаются обойти это ограничение, используя математическую модель для **предсказания скорости требуемой для процесса**. Такой подход однозначно не рекомендуется для поддержания безопасности, так как данные, используемые в подобной модели, в лучшем случае приблизительные, и полученные результаты не могут быть использованы для принятия ответственных решений, связанных с безопасностью.

Троированные системы хорошо известны и продолжают оставаться выбором, характерным для недостаточно информированных пользователей (for the under informed). Они используются во многих ситуациях, хотя зачастую это неоправданно ни технически, ни экономически. Будучи и безопасной и надежной, эта архитектура должна работать в режиме 3-2-0 для приложений безопасности. TMR система осуществляет диагностику при помощи голосования, либо сравнения (после потери одного канала.) Фактически, функционирование на одном канале не допускается, так как не осуществляется полноценная полная внутренняя диагностика, и такое функционирование не может считаться безопасным. Фактически, ограничения по времени накладываются на двухканальную работу, и необходимо предпринять определенные шаги, чтобы подтвердить, что система будет закрыта после потери второго канала. Другая проблема, которая влияет на TMR архитектуру, заключается более высокой (в 3 раза) восприимчивости к ошибкам, вызванным обычными причинами благодаря третьему уровню резервирования, и тому факту, что множественные каналы имеют общую аппаратную платформу, то есть обычный I/O модуль или модуль процессора. Кроме того, и начальная стоимость, и стоимость цикла эксплуатации (включая обслуживание) довольно высоки.

Функционирование в условиях ошибки

В приложениях для систем безопасности, системы с единичным каналом (1-0) чувствительны к ошибкам, и в случае ошибки должны безопасно прерывать работу. Двойственная архитектура может либо выполнить безопасное прерывание работы (2-0), либо перейти в режим работы на одном канале(2-1-0) в особых условиях ошибки и строгих ограничений по времени, указанных в сертификационном отчете о мерах безопасности. Рекомендуется иметь в наличии копию такого отчета для каждой Программируемой Электронной Системы (PES).

И TMR (3-2-0), и QMR (4-2-0) архитектуры переходят в двухканальный режим работы после первой ошибки. Однако квадратура сохраняет полную внутреннюю диагностику, не имеет ограничений по времени в течение работы в данном режиме, а также обеспечивает безопасность в соответствии с уровнем SIL3 (RC6). См. рис. 1 для сравнения рабочих сценариев после появления Первой Ошибки.

Safe Operation After First Fault

Simplex:	1 - 0	→	Fall-Safe (RC4 only)
Dual:	1oo2D	→	1oo1D (Severe Time Restriction)
TMR:	2oo3	→	1oo2 (Time Restriction)
QMR:	2oo4	→	1oo2D (No Time Restriction)

Рис. 1.

Переход на операционный уровень SIL3 (RC6) требует от PES вспомогательных средств, обеспечивающих отключение питания выводов. Эти средства могут быть либо внешними, либо являться частью модулей вывода, но в любом случае должны обязательно присутствовать, чтобы соответствовать требованиям безопасности. Ограничения также относятся к работе PES после появления второй ошибки. Для TMR архитектуры вторая ошибка может быть связана либо с процессором, либо с блоком ввода-вывода IO. Появление любой из них потребует остановки

системы. В QMR архитектуре только ошибки процессора на втором канале вызывают остановку системы, так как ошибки ввода-вывода управляются независимым образом, благодаря полной внутренней диагностике. По сути, QMR архитектура обеспечивает дополнительную нечувствительность к ошибкам и более высокий уровень операционной надежности.

Характеристики безопасности.

Архитектуры PES обязаны предусматривать и безопасность, и надежность. Частые ложные прерывания процесса опасны и нежелательны с экономической точки зрения. Поскольку двойственная архитектура традиционно более доступна, чем тройственная, перед разработчиками стоит задача сделать двойственную архитектуру равной, или лучше по характеристикам безопасности, чем TMR.

Прежде, суть проблемы состояла в опасном неопределяемом отказе одного или двух (дублированных) процессоров. Единичный процессор не может провести самодиагностику достаточно полно, чтобы считаться абсолютно безопасным, существует возможность, что такой сбой может повлечь остановку обоих каналов в опасном состоянии, и сделает для PES невозможным выполнение надлежащей функции безопасности. Именно в этом заключается причина строгих ограничений по времени, которые налагаются на уровень SIL 3 (RC 6) для дублированных архитектур в условиях ошибки.

Квадро архитектура обеспечивает пару двойственных процессоров, функционирующих в режиме безопасности (2-0) для каждого канала. Последующее существенное улучшение диагностируемости работы этих процессоров полностью решило вопросы безопасности, связанные с опасными неопределимыми отказами процессоров, что в свою очередь сняло все ограничения по времени для работы системы в одноканальном режиме.

Для наглядности, можно провести сравнение характеристик безопасности (средняя вероятность отказа в выполнении заданной функции безопасности – PFD) различных архитектур систем ПАЗ. Обратившись к ISA TR84.02, Часть 2, 1998, можно быстро определить, что QMR архитектура (2004) сравнима с ультра-безопасной архитектурой 1003, так как и та и другая используют члены третьей степени в своих уравнениях для расчета средней вероятности отказа (PFD). Таким же образом, архитектура TMR (2003) сравнима архитектурой 1002D, так как обе имеют квадратные члены в своих уравнениях. Это сравнение приводит к выводу, что QMR (2004) архитектура обеспечивает на порядок лучшие характеристики безопасности, чем архитектуры TMR (2003) или 1002D, и является значительным технологическим достижением в характеристиках систем безопасности.

Другой важный момент в характеристиках систем ПАЗ – это способность PES определять внутреннюю ошибку и быстро исправлять ее. Другими словами, PES должна быть способна реагировать в промежуток времени безопасности указанный для процесса, контролируемого данной системой ПАЗ.

Время Безопасности Процесса конкретного технологического процесса – это время его нечувствительности к ошибке, предшествующее наступлению опасной ситуации. Таким образом, если опасная ситуация продолжает свое существование дольше Времени Безопасности Процесса, то она переходит в опасное состояние. Чтобы удовлетворять данному требованию, PES должна поддерживать безопасное состояние, определяя опасные внутренние ошибки и исправляя их в течение времени безопасности процесса, иначе она считается неподходящей для систем ПАЗ для данного технологического процесса.

Типичным примером может служить Система Управления Печами (Burner Management System – BMS), в которой TUV (DIN VDE 0116) определяет время безопасности процесса равным одной (1) секунде. Так как для того, чтобы определить и исправить внутреннюю ошибку, требуется два (2) цикла сканирования PES, время определения и исправления ошибки PES не может превышать

пятисот (500) миллисекунд. Если безопасность PES не удовлетворяет этому условию, по стандарту, она не может использоваться в системах BMS.

Рассмотрение стоимости эксплуатационного цикла системы.

Стандарты безопасности ближайшего будущего и существующие сегодня требуют выполнения SIS для уменьшения риска связанного с работой процессов с возможными опасными последствиями. Игнорировать эти требования недопустимо, поэтому возникает необходимость выполнять их, но с как можно меньшими затратами. Таким образом, должны учитываться как цена самого SIS, так и стоимость эксплуатационного цикла.

Известно, что некоторые архитектуры по причине присущей им сложности довольно дороги как сами по себе, так и в обслуживании. Особенно это касается небольших проектов, или проектов требующих защиты уровня SIL1 или SIL2. Для таких проектов, использование тройственной архитектуры может оказаться чрезмерно дорогим, учитывая стоимость покупки и стоимость эксплуатационного цикла.

Кроме того, если процесс может быть классифицирован как требующий SIL1 или SIL2, вместо SIL3, можно добиться существенной экономии в других областях, таких как датчики или концевые элементы, так как пропадает необходимость в двойных или тройных элементах с резервированием, требуемых для SIL3.

Новая QMR архитектура обладает высокой гибкостью и может быть сконфигурирована для любого из трех уровней SIL. Она может действовать в одноканальном режиме или как система с резервированием; с единичными, дублированными или троированными устройствами, в соответствии с требованиями для каждого уровня безопасности. В каждой конфигурации – симплексной, с выборочным резервированием или полным резервированием, она обеспечивает характеристики безопасности SIL3. При добавлении резервирования, надежность значительно возрастает, и одновременно сохраняются характеристики безопасности.

Добавление резервирования не требует чрезмерных затрат, так как стоимость модулей процессора и ввода-вывода значительно меньше, чем переход на новую архитектуру. Кроме того, поскольку эти модули менее сложные, чем сравниваемые модули TMR, среднее время работы между отказами так же значительно больше, и расходы на поддержание системы значительно ниже.

Рассматриваемая архитектура значительно более выгодная с точки зрения затрат, а ее дополнительным преимуществом является то, что PES стали относить к тому блоку, который она защищает. Этот единственный пункт согласно концепции PES был введен в ряд стандартов безопасности, появившихся в последнее время. Таким образом, больше нет необходимости объединять множественные технологические блоки в одну PES с целью достичь большей эффективности затрат. В результате внедрение системы безопасности, ее тестирование и дальнейшая эксплуатация упрощается, и соответственно меньше вероятность ошибок, связанных с человеческим фактором.

Кроме повышения безопасности, специализированная PES значительно проще в эксплуатации и модификации. Возможность ложного останова технологического процесса полностью исключена, и осуществление процедур тестирования упрощается. В целом преимущества такого индивидуального подхода действительно значительные и должны быть подробно изучены.

Заключение

Новая quadro архитектура (QMR) является значительным технологическим улучшением в характеристиках систем безопасности. Она обеспечивает более высокий уровень безопасности и работоспособности, чем TMR (2oo3) или 1oo2D. По сравнению с TMR, она гораздо менее восприимчива к ошибкам, вызванным обычными причинами, благодаря полному разделению, изоляции и работе резервированных каналов.

Так как каждый канал имеет пару дублированных процессоров, работающих в режиме безопасности (2-0), опасные неопределяемые отказы процессоров исключены, а система предусматривает неограниченную по времени работу SIL3 в симплексной, выборочно резервированной, либо полностью резервированной конфигурации.

Эта новая архитектура предусматривает перенастраиваемую конфигурацию и может использоваться для приложений SIL1, SIL2, и SIL3. Тем не менее, самой привлекательной стороной новой архитектуры остается низкая стоимость ее эксплуатационного цикла, что позволяет использовать ее как в небольших, так и в крупных системах ПАЗ. Соответственно, больше нет необходимости объединять множественные технологические блоки в одну PES, для большей эффективности затрат.

Глоссарий

2-0 Режим работы, при котором дублированная система останавливает работу, после того, как диагностируется первая ошибка.

2-1-0 Режим работы, при котором дублированная система останавливает работу после того, как диагностируется вторая ошибка.

3-2-0 Режим работы, при котором троированная система останавливает работу после того, как диагностируется вторая ошибка.

4-2-0 Режим работы, при котором quadro система останавливает работу после того, как диагностируется вторая ошибка

QMR Четырехкратное модульное резервирование (2oo4)

PES Программируемая Электронная Система (не ПЛК –программируемый логический контроллер).

RC6 класс требований 6 для DIN 19250.

SIL уровень совокупной безопасности (1, 2 or 3).

TI Промежуток между контрольными испытаниями

λ_{DU} Уровень опасных неопределимых отказов.