(19) Евразийское патентное ведомство

(11) 034974 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2020.04.13

(21) Номер заявки
201700479

(22) Дата подачи заявки
2017.10.24

(51) Int. Cl. *G06F 11/14* (2006.01)

(54) СПОСОБ ОБЕСПЕЧЕНИЯ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ МОДУЛЯ ЦЕНТРАЛЬНОГО ПРОЦЕССОРА ПРОМЫШЛЕННОГО КОНТРОЛЛЕРА И МИКРОПРОЦЕССОРНАЯ СИСТЕМА ДЛЯ ОСУЩЕСТВЛЕНИЯ ДАННОГО СПОСОБА (ВАРИАНТЫ)

(43) **2019.04.30**
(96) **2017000106 (RU) 2017.10.24**

(71)(73) Заявитель и патентовладелец:
АКЦИОНЕРНОЕ ОБЩЕСТВО "ТЕКОНГРУП" (RU)

(56) RU-C1-2110834
US-A1-20050060605
US-A1-20160216704

(57) Изобретение относится к архитектуре модуля центрального процессора (далее модуль ЦП) промышленного программируемого логического контроллера и способу, ориентированному на безопасную работу модуля ЦП. Способ заключается в том, что в модуле ЦП (2) используют микропроцессорную систему, состоящую из центрального микропроцессора (8) (далее ЦМ), дополнительного микропроцессора (9) (далее ДМ) и микроконтроллера безопасности (10) (далее МБ). ЦМ и ДМ выполняют одинаковые задачи с одинаковыми входными данными от датчиков и передают результаты обработки этих входных данных в МБ, который сравнивает эти результаты. МБ принимает решение о разрешении передачи выходных данных из модуля ЦП в исполнительные механизмы в зависимости от результата сравнения результатов обработки из ЦМ и из ДМ, или от результата, осуществляемого МБ контроля времени выполнения задачи в ЦМ и ДМ, или от результата программной или аппаратной самодиагностики МБ. Аппаратная самодиагностика МБ осуществляется с помощью реализованных на его кристалле аппаратных механизмов.

034974 B1

034974 B1

Изобретение относится к архитектуре модуля центрального процессора (модуль ЦП) промышленного контроллера с программируемой логикой и способу, ориентированному на безопасную работу модуля ЦП. Промышленный контроллер (далее контроллер) является вычислительной и управляющей единицей в автоматизированных системах управления технологическими процессами (АСУ ТП).

Быстрый рост систем управления, используемых в областях (промышленность, медицина, автомобильный и железнодорожный транспорт), где их выход из строя может привести к опасным ситуациям, которые приводят к травмированию или смерти людей, причинению вреда окружающей среде, порче оборудования или нарушению производственного процесса, привёл к развитию серии стандартов ГОСТ Р МЭК 61508 "Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью".

С появлением микропроцессорных систем они стали применяться для осуществления функций обеспечения функциональной безопасности. Идея этих микропроцессорных систем обеспечения безопасности основывается на аппаратной избыточности, заключающейся в использовании параллельно нескольких вычислительных средств (например, процессоров) и в осуществлении сравнения их результатов обработки данных (вычислений) с помощью аппаратных элементов или программного обеспечения.

Так, известен модуль центрального процессора программируемого логического контроллера с расширенными функциями безопасности серии Quantum (Руководство на ПЛК безопасности Quantum №33003879 от 06/2007, стр.33-38 раздел "Модуль ЦП безопасности", компания Schneider Electric, http://schneider.nt-rt.ru/images/manuals/33003879RU.pdf), в состав которого входят два различных процессора - модель Intel Pentium и прикладной процессор. Каждый из этих процессоров независимо друг от друга выполняет расчёты, и по завершению каждого цикла каждый из процессоров сравнивает свой результат с результатом другого процессора. При обнаружении ошибки или при несоответствии результатов любой из процессоров может "отключить систему, т.е. перевести её в безопасное состояние". Работа такой микропроцессорной системы, состоящей из двух разных процессоров, для которых независимо друг от друга разрабатывается два исполняемых кода, позволяет выявить систематические отказы из-за ошибок в исходных текстах программ и случайные отказы, возникающие при работе модуля ЦП.

Аналогичные решения наличия избыточного процессора, взаимодействующего с основным процессором с целью взаимного контроля, известны из следующих патентных источников:

US 9,244,454 B2 под названием "Система управления для контроля критически безопасных и критически небезопасных процессов", компания ABB AG;

US 7,715,932 B2 под названием "Способ и устройство для управления критичным для безопасности процессом", компания Pilz GmbH&Co;

US 6,832,343 B2 под названием "Устройство для контроля критично важного процесса", компания Pilz GmbH&Co;

WO 2015/113994 A1 под названием "Способ и устройство для безопасного отключения электрической нагрузки", компания Pilz GmbH&Co. KG;

US 9,098,074 B2 под названием "Система управления, связанная с безопасностью, и способ для управления автоматизированной системой", компания Pilz GmbH&Co. KG, Moosmann Peter.

Известны решения микропроцессорных систем для осуществления функций обеспечения безопасности, содержащие центральный процессор, избыточный процессор и третий процессор, предназначенный для сравнения и выявления несоответствия в результатах первых двух процессоров.

Так, известна "Микропроцессорная система обеспечения безопасности, применимая, в частности, в области железнодорожного транспорта" (заявка на изобретение RU 94013455 A1), принятая в качестве ближайшего аналога для заявляемых микропроцессорных систем. Известная микропроцессорная система содержит по меньшей мере два работающих параллельно микропроцессора, выполняющих одну и ту же прикладную программу. Одни и те же входные данные от датчиков подают на входы этих микропроцессоров. Каждый из них ведёт обработку входных данных по прикладной программе с некоторым временным смещением по отношению к другому для предотвращения отказов из-за синфазных помех. Результаты обработки каждый из процессоров направляет в третий процессор сравнения. Процессор сравнения сравнивает результаты. Если это сравнение корректно, процессор сравнения формирует сигнатуру, которую подаёт на динамический контроллер. При получении сигнатуры, являющейся признаком нормальной работы процессора сравнения, динамический контроллер санкционирует общую передачу выходных данных микропроцессорами. Реально используются только выходные данные одного из микропроцессоров. Кроме этого каждый из микропроцессоров выполняет самодиагностику, результаты которой направляет в процессор сравнения. Возможны разные варианты исполнения микропроцессорной системы, например, от использования одинаковых программных средств, размещённых на двух одинаковых аппаратных средствах, до использования двух разных программных средств, размещённых на двух разных аппаратных средствах.

Решения аппаратной избыточности, описанные выше, используются для обеспечения безопасности так же в процессорных технологиях, поскольку современные процессоры или микроконтроллеры могут включать в себя множество ядер на одном кристалле (двухъядерные, четырёхъядерные, многоядерные варианты исполнения). Такие решения описаны в EP 1,973,017 A2 под названием "Программируемый

логический контроллер, ориентированный на безопасность", компания ABB AG; EP 2,237,118 A1 "Система безопасности для обеспечения безошибочного управления электрическими устройствами и предохранительным устройством", группа компаний Robert Bosch GMBH.

В последнее время появились микроконтроллеры, предназначенные для использования в системах с требованиями к обеспечению безопасности. Например, микроконтроллеры Hercules™, (Карл Глеб, Дев Прадхан, Микроконтроллеры Hercules™: микроконтроллеры реального времени для техники с особыми требованиями к обеспечению безопасности // Бюллетень научно-технической информации "Компоненты. Полный спектр применений", выпуск 3(35) 2012. - С.1-8, https://www.ti.com/graphics/reserved/eugraphics/35_ALL.pdf).

Кардинальное отличие такого микроконтроллера от ранее известных микроконтроллеров заключается в том, что для диагностирования отказов помимо программной самодиагностики в нём реализованы ещё и аппаратные механизмы самодиагностики, реализованные на кристалле микроконтроллера.

В микроконтроллерах Hercules™, разработанных корпорацией Texas Instrument, используется концепция архитектуры безопасности, которая называется "островок безопасности". Она заключается в том, что для ряда ключевых элементов выделяются непрерывно работающие аппаратно реализованные механизмы обеспечения безопасности. Этот набор ключевых элементов включает в себя устройство питания / тактирования / сброса, ЦПУ, flash-память, ОЗУ и соответствующие цепи взаимосвязи. Реализация аппаратного тестирования этих элементов даёт уверенность в том, что эти элементы работают правильно. В этом случае можно использовать программное обеспечение, исполняемое на этих элементах, для обеспечения программно-реализованной диагностики других элементов, таких как периферийные устройства.

Для диагностирования отказов по общей причине в микроконтроллерах Hercules™ применены следующие аппаратные реализованные механизмы:

для контроля питания использовано реализованное на кристалле устройство контроля напряжения;

для контроля тактирования использован реализованный на кристалле маломощный генератор;

обнаружение ошибок в формируемых и распространяемых тактовых сигналах диагностируются с помощью оконного сторожевого таймера;

для контроля ядер микроконтроллера применена система параллельных ядер, которая подразумевает наличие функционального ядра и контрольного ядра. При этом одни и те же входные данные подаются как на функциональное ядро, так и на контрольное ядро. Модуль сравнения контролирует выходы двух ядер, выполненных с одной и той же логикой, и сигнализирует о любых ошибках в системе. Реализовано разнесение двух ядер по времени, так что ядра работают не в фазе, а с отличием в 1,5 или 2 такта, для того чтобы уменьшить вероятность отказа по общей причине, связанной с тактированием. Кристалл контрольного ядра физически расположен зеркально и развёрнут относительно функционального ядра. Реализована встроенная самопроверка логики, которая обеспечивает охват диагностикой ядер на уровне транзисторов при включении питания или в ходе периодических интервалов проверки во время штатной работы.

ECC-контроллер для flash-памяти и статического ОЗУ расположен внутри ядра для гарантированного обнаружения повреждения данных в памяти и возможности исправления одиночных битовых ошибок.

Микроконтроллеры Hercules™ не ограничиваются логикой "островка безопасности", которая обеспечивает для ключевых элементов аппаратно реализованные механизмы обеспечения безопасности. Имеются аппаратно реализованные механизмы обеспечения безопасности для периферийных устройств, служащие для контроля случайных ошибок, которые нелегко выявить с помощью программного обеспечения.

Перечисленные выше средства аппаратной диагностики в микроконтроллерах Hercules™ позволили сократить объём программного обеспечения, связанного с диагностикой на 30%.

Производители такого микроконтроллера гарантируют, что он работает "безопасно" и отвечает требованиям, установленным ГОСТ Р МЭК 61508 к функциональной безопасности.

Использование такого микроконтроллера для целей обеспечения безопасности позволяет уйти от аппаратной избыточности.

Однако такие микроконтроллеры "безопасности", т.е. микроконтроллеры, в которых помимо программной диагностики использованы средства аппаратного тестирования, на сегодняшний день имеют низкую производительность, что не позволяет использовать их в промышленных контроллерах, предназначенных для управления большим количеством оборудования.

Так, разрабатываемый нами МФК5000 (Многофункциональный Контроллер 5000) должен обеспечивать управление объектом, где количеством сигналов может достигать пяти тысяч. При этом необходимо обеспечить быстродействие и требования функциональной безопасности.

Конкретно в данной заявке рассмотрен модуль центрального процессора CPU850, в котором должны обеспечиваться перечисленные требования.

Решению проблемы безопасности в системе управления промышленной автоматизации посвящен патент US 9,696,692 B2, компания ROCKWELL AUTOMATION TECHNOLOGIES, INC. В этом же патенте описан способ работы системы управления, который принят в качестве наиболее близкого аналога

для заявляемых способов. Система управления в программируемом логическом контроллере управляет промышленным оборудованием. Промышленное оборудование может представлять опасность для людей в случае возникновения отказа в системе управления. Поэтому необходимо обеспечить быстрое обнаружения ошибки в системе управления и исправление данной ошибки. Система управления включает в себя "первичный процесс управления", "вторичный процесс управления" и "процесс вывода". Способ заключается в том, что "первичный процесс управления" и "вторичный процесс управления" сконфигурированы для обработки одних и тех же входных данных в одной или нескольких программах управления. Программы в "первичном процессе управления" и "вторичном процессе управления" запускаются одновременно. Во время нормальной работы "процесс вывода" сконфигурирован для управления промышленным оборудованием посредством использования сигналов управления и данных, принятых из "первичного процесса управления", которые затем передаются в сеть и далее к промышленному оборудованию. "Вторичный процесс управления" периодически генерирует вторичное значение контроля данных, в то время как "первичный процесс управления" периодически генерирует первичное значение контроля данных. Это могут быть значения циклического избыточного кода (CRC). Главное, чтобы эти значения проверки данных были компактны (с точки зрения количества бит и байтов), которые можно быстро сравнить, чтобы определить состояние процессов управления. "Процесс вывода" сравнивает эти два значения для обнаружения отказа в "первичном процессе управления". Если значения CRC не совпадают, вероятно, произошёл отказ в "первичном процессе управления", и "процесс вывода" может переключить управление промышленным оборудованием на "вторичный процесс управления" или предпринять меры, направленные на аварийное выключение промышленного оборудования. Сведения о диагностике при описании работы системы управления по патенту US 9,696,692 B2 не использованы. Известно, что значительное преимущество в достижении функциональной безопасности электрической / электронной / программируемой электронной системы (Э/Э/ПЭ системы), связанной с безопасностью, может обеспечить диагностическое тестирование. Охват диагностикой каждого элемента в Э/Э/ПЭ системе, связанной с безопасностью, должен учитываться при оценке достигаемой меры отказов для функций безопасности (ГОСТ Р МЭК 61508-2-2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам. Приложение С (обязательное). Охват диагностикой и доля безопасных отказов).

Задача изобретений - обеспечение функциональной безопасности модуля центрального процессора промышленного контроллера.

Технический результат в предлагаемых изобретениях достигается тем, что при осуществлении необходимых мероприятий, от которых зависит безопасная работа модуля ЦП, применена избыточная микропроцессорная система, в которой контрольными проверками (проверка целостности передаваемых и обрабатываемых данных, времени выполнения прикладной программы или её частей) и высоким уровнем охвата диагностикой, происходит обнаружение отказа любого из устройств системы, и предпринимаются меры по прекращению выдачи выходных данных из модуля ЦП.

Для этого способ обеспечения функциональной безопасности модуля центрального процессора промышленного контроллера заключается в том, что используют микропроцессорную систему, расположенную в модуле центрального процессора и состоящую из центрального микропроцессора, дополнительного микропроцессора, с архитектурой ядра, отличной от архитектуры ядра центрального микропроцессора, и микроконтроллера безопасности, при этом центральный микропроцессор и дополнительный микропроцессор выполняют одинаковые задачи с одними и теми же входными данными от датчиков и затем передают результаты обработки входных данных в микроконтроллер безопасности, который сравнивает эти результаты, при этом микроконтроллер безопасности принимает решение о разрешении передачи выходных данных из модуля центрального процессора в исполнительные механизмы в зависимости от результата сравнения результатов из центрального и дополнительного микропроцессоров или в зависимости от результатов осуществляемого микроконтроллером безопасности контроля времени выполнения задачи центральным и дополнительным микропроцессорами или в зависимости от результатов программной или аппаратной самодиагностики, при этом аппаратная самодиагностика микроконтроллера безопасности осуществляется с помощью реализованных на его кристалле аппаратных механизмов.

При сравнении результатов, полученных в центральном и в дополнительном микропроцессорах, микроконтроллер безопасности может сравнивать значения выходных данных или значения проверки выходных данных, например циклические избыточные коды. В центральном микропроцессоре и в дополнительном микропроцессоре для решения одинаковых задач могут быть использованы разные исходные тексты прикладной программы.

Для осуществления способа предложена микропроцессорная система, содержащая центральный микропроцессор, дополнительный микропроцессор, выполненный с архитектурой ядра, отличной от архитектуры ядра центрального микропроцессора, и предназначенный для выполнения такой же задачи с теми же входными данными от датчиков, что и центральный микропроцессор, и микроконтроллер безопасности, имеющий на кристалле аппаратные механизмы для самодиагностики, предназначенный для сравнения результатов выполненной центральным и дополнительным микропроцессорами задачи и предназначенный для принятия решения о разрешении передачи выходных данных, полученных в цен-

тральном микропроцессоре, в исполнительные механизмы в зависимости от результата сравнения результатов выполненной центральным и дополнительным микропроцессорами задачи или в зависимости от результатов выполняемой им функции контроля времени выполнения задачи в центральном и дополнительном микропроцессорах или в зависимости от результатов его аппаратной или программной самодиагностики. Микроконтроллер безопасности может содержать два ядра, одно из которых является функциональным, а другое контрольным и модуль сравнения, который выполнен с возможностью контроля выходов двух ядер и имеет возможностью сигнализировать о любых ошибках.

Вместо "микроконтроллера безопасности" для осуществления способа и для изготовления микропроцессорной системы может быть использован микропроцессор.

Для последующего описания возможности осуществления заявленного устройства и способа приведены следующие чертежи:

фиг. 1 - структурная схема контроллера, датчика, контактора и двигателя;

фиг. 2 - первый вариант структурной схемы микропроцессорной системы модуля ЦП;

фиг. 3 - второй вариант структурной схемы микропроцессорной системы модуля ЦП.

Прилагаемые чертежи, показывающие предпочтительные варианты осуществления настоящих изобретений, приведены в качестве иллюстрации, а не ограничения раскрытия информации, и могут быть изменены в объёме прилагаемой формулы изобретения вместе с её полным объёмом эквивалентов. Например, фраза "выходные данные переданы из центрального микропроцессора в исполнительные механизмы" не ограничивается прямой связью, но включает в себя связь через другие конструктивные элементы (контроллер шины, шину, модуль вывода и т.п.), что понятно специалистам в области радиоэлектроники.

При описании работы микропроцессорной системы модуля ЦП следует оговорить следующие понятия и условия, используемые в данной заявке.

Под функциональной безопасностью устройства (модуля ЦП) в данной заявке понимается безопасность, которая зависит от правильности функционирования устройства, основанного на электрической и/или электронной, и/или программируемой электронной технологии.

В АСУ ТП под "безопасным состоянием" понимается такое состояние выходов контроллера, при котором подключенные к ним исполнительные механизмы находятся в состоянии, наиболее безопасном для объекта управления, а именно состоянии, не приводящем к поломке объекта управления.

В данной заявке описана работа нерезервированного модуля ЦП, неисправность в работе которого приведёт к исчезновению (отключению) управляющего сигнала на выходе контроллера. Это приведёт к тому, что контакты контактора будут приведены в "безопасное состояние", т.е. контакты будут разомкнуты, при этом регулирующие и отсечные клапаны займут безопасное для технологического процесса положение в соответствии с требованиями технологического регламента, а двигатели будут остановлены. Для пояснения приведена фиг. 1, где контроллер 1 (на чертеже PLC) содержит нерезервированный модуль ЦП 2 (на чертеже CPU). Модули 3 ввода-вывода (на чертеже I/O) осуществляют общение с модулем ЦП 2 по последовательной шине 4. Датчик 5 подключён к модулю ввода. Управление двигателем 6 осуществляется через контактор 7. При возникновении неисправности в работе модуля ЦП 2 выходы модуля вывода примут состояние, как при отключенном питании. Это приведёт к размыканию контактов контактора 7, прекращению подачи питания на двигатель 6 и его остановке.

В заявке рассматриваются нерезервированные модули ввода/вывода.

Контроллер предназначен для сбора и обработки больших массивов данных, получаемых от контрольно-измерительных приборов (датчиков), включая прием информации от других подсистем автоматизированного управления, а также выработке управляющих воздействий согласно запрограммированным алгоритмам управления и передаче этих воздействий на исполнительные механизмы. Блоки алгоритмов прикладного программного обеспечения контроллера включают в себя блоки обработки аналоговых, дискретных и цифровых сигналов, блоки управления арматурой и механизмами, блоки автоматического регулирования, блоки технологической защиты и сигнализации, блоки логического управления. Поэтому прикладная программа реализована в виде множества независимых задач. Работа микропроцессорной системы в данной заявке описана в рамках решения одной из множества независимых задач, в которой обрабатываются данные, относящиеся к технологической защите. Микропроцессорная система модуля ЦП (фиг. 2 и фиг. 3) состоит из центрального микропроцессора 8 (на чертеже MPU1), дополнительного микропроцессора 9 (на чертеже MPU2) и микроконтроллера 10 безопасности (на чертеже MCU). Связь между центральным микропроцессором 8, дополнительным микропроцессором 9 и микроконтроллером 10 безопасности может происходить посредством FPGA 11, внутри которой организованы области двухпортовой памяти DPRAM. В этой же FPGA 11 может быть организован контроллер 12, поддерживающий обмен данными между модулем ЦП 2 и модулями ввода-вывода 3 (далее контроллер шины). Контроллер 12 шины может быть встроен и в микроконтроллер 10 безопасности. На границе модуля ЦП 2 и шины 4 показан физический (аппаратный) уровень интерфейса 13. Микроконтроллер 10 безопасности содержит оконный сторожевой таймер 14. Сторожевой таймер 14 требует, чтобы реакция ядра микроконтроллера была в пределах заданного временного интервала, что указывает на то, что микроконтроллер остаётся в работоспособном состоянии и работает с правильными значениями временных пара-

метров.

Центральный микропроцессор 8 предназначен для выполнения прикладной (технологической) программы контроллера. Для описания работы заявляемой микропроцессорной системы работа центрального микропроцессора определена в рамках решения им одной независимой задачи. В рамках этой задачи обрабатываются входные данные от датчика (датчиков), а результатом обработки являются выходные данные для управления исполнительным механизмом (механизмами).

Дополнительный микропроцессор 9 предназначен для выполнения прикладной (технологической) программы контроллера с целью проверки правильности работы центрального микропроцессора 8. Дополнительный микропроцессор 9 выполнен с архитектурой ядра (ядер), отличной от архитектуры ядра (ядер) центрального микропроцессора 8.

Для описания работы заявляемой микропроцессорной системы работа дополнительного микропроцессора определена как решение им точно такой же задачи, какую решает и центральный микропроцессор с такими же входными данными.

В центральном микропроцессоре и дополнительном микропроцессоре для решения одинаковых задач могут быть использованы разные исходные тексты прикладной программы (разные машинные коды).

Прикладная программа в центральном микропроцессоре и прикладная программа в дополнительном микропроцессоре могут работать под управлением одинаковых или разных операционных систем, или вообще без операционных систем.

Использование в микропроцессорной системе двух разных микропроцессоров, работающих с разными текстами прикладной программы в разных операционных системах или без операционных систем, применено для снижения количества общих систематических отказов.

Микроконтроллер 10 безопасности предназначен для контроля работы центрального микропроцессора 8 и дополнительного микропроцессора 9. Вместо микроконтроллера безопасности может быть использован микропроцессор, конструктивные и программные возможности которого позволяют ему выполнить перечисленные далее функции. Далее по тексту описания будет использован термин "микроконтроллер безопасности". Микроконтроллер 10 безопасности имеет реализованные на кристалле аппаратные механизмы самодиагностики. Так, например, в микроконтроллере 10 безопасности применена система параллельных ядер, которая подразумевает наличие функционального ядра и контрольного ядра. При этом одни и те же входные данные подаются как на функциональное ядро, так и на контрольное ядро. Модуль сравнения контролирует выходы двух ядер, выполненных с одной и той же логикой, и сигнализирует о любых ошибках в системе.

Микроконтроллер безопасности осуществляет следующие мероприятия:

микроконтроллер безопасности сравнивает результаты, полученные в результате решения задач в центральном микропроцессоре и в дополнительном микропроцессоре и в зависимости от результата этого сравнения принимает решение о разрешении передачи выходных данных из модуля ЦП в исполнительные механизмы, в предпочтительном варианте микроконтроллер безопасности сравнивает значения проверки выходных данных (например, CRC);

микроконтроллер безопасности контролирует время выполнения задачи центральным и дополнительным микропроцессорами и в результате этого контроля принимает решение о разрешении передачи выходных данных из модуля ЦП в исполнительные механизмы;

микроконтроллер безопасности принимает результаты периодически исполняемых программных диагностик из центрального микропроцессора и дополнительного микропроцессора и в зависимости от полученных результатов принимает решение о разрешении передачи выходных данных из модуля ЦП в исполнительные механизмы;

микроконтроллер безопасности проводит периодически исполняемую программную и аппаратную самодиагностику.

Микроконтроллер безопасности принимает решение о прекращении передачи выходных данных из модуля ЦП в исполнительные механизмы при выявлении отказа в любом из перечисленных выше мероприятий (при выявлении отказа в любой из контрольных проверок и при выявлении отказа любой из диагностик).

Более подробно перечисленные мероприятия будут раскрыты далее.

Работа микропроцессорной системы осуществляется следующим образом.

Последовательность осуществления действий показана на фиг. 2 буквенными обозначениями от "a" до "n":

Входные данные с шины 4 передают в контроллер 12 шины (действие a). Далее входные данные из контроллера 12 шины передают в центральный микропроцессор 8 (действие b). В центральном микропроцессоре 8 входные данные фиксируются. Затем этот зафиксированный массив входных данных передаётся из центрального микропроцессора 8 в дополнительный микропроцессор 9 (действие c). После поступления массива входных данных в дополнительный микропроцессор 9 в обоих микропроцессорах 8 и 9 начинается выполнение одной из множества независимых задач прикладной программы. В рамках этой задачи происходит обработка входных данных. Результаты обработки (это могут быть, как и выходные данные, так и только значения проверки выходных данных, например циклические избыточные коды

CRC) из центрального микропроцессора 8 и из дополнительного микропроцессора 9 передаются в микроконтроллер 10 безопасности (действие d и действие e). Микроконтроллер 10 безопасности программно сравнивает эти результаты, и, в зависимости от результата этого сравнения, разрешает или запрещает передачу выходных данных центральным микропроцессором 8 в шину 4. Предпочтительно, если микроконтроллер 10 безопасности будет сравнивать циклические избыточные коды CRC. Главное, чтобы эти значения, предназначенные для проверки выходных данных, были компактны (с точки зрения количества бит и байтов), которые можно сравнить быстро. Если циклические избыточные коды результатов центрального и дополнительного микропроцессоров равны, то микроконтроллер 10 безопасности санкционирует (разрешает) (действие F) передачу выходных данных центральным микропроцессором 8 в контроллер 12 шины (действие h) и далее в шину 4 (действие k). Если значения циклических избыточных кодов (CRC) не равны, значит, произошёл отказ в одном из микропроцессоров (центральном или дополнительном). В этом случае микроконтроллер 10 безопасности инициирует прекращение передачи выходных данных из модуля ЦП 2. Для этого микроконтроллер 10 безопасности формирует сигнал RESET, который направляет (действие G) в центральный микропроцессор 8, который прекращает выполнение инструкций, и/или направляет в контроллер 12 шины (действие т), который прекращает обмен данными по шине 4, и/или формирует запрещающий сигнал на физический уровень интерфейса 13 (действие п), где размыкается канал передачи выходных данных в шину 4.

Дополнительно микроконтроллер 10 безопасности принимает результаты периодически исполняемых программных диагностик (диагностика работоспособности сервисов, сетевых интерфейсов и т.п.) из центрального микропроцессора 8 и дополнительного микропроцессора 9. При отказе любого из микропроцессоров действия микроконтроллера 10 безопасности будут направлены на прекращение передачи выходных данных из модуля ЦП 2 в шину 4, а именно действие G и/или действие m и/или действие n.

Дополнительно микроконтроллер 10 безопасности программно контролирует время выполнения задачи каждым из микропроцессоров 8 и 9. Время выполнения задачи должно находиться в заданном интервале (временном окне), определяемой для каждой задачи исходя из объёма обрабатываемых/пересылаемых данных. Если время выполнения задачи одним из микропроцессоров находится вне такого интервала, это воспринимается как отказ. В этом случае действия микроконтроллера 10 безопасности будут направлены на прекращение передачи выходных данных из модуля ЦП 2 в шину 4, а именно действие G и/или действие m и/или действие n.

Микроконтроллер безопасности 10 проводит периодически исполняемую программную и аппаратную самодиагностику. При опасном отказе сторожевой таймер 14 не получит вовремя сигнал перезапуска таймера 14. В этом случае таймер 14 выдаст сигнал RESET микроконтроллеру безопасности. По этому сигналу все выводы микроконтроллера 10 безопасности автоматически переводятся в состояние сброса. Такое состояние выводов микроконтроллера 10 безопасности является активным состоянием сигнала сброса для центрального микропроцессора 8, а также такое состояние выводов микроконтроллера 10 безопасности является запрещающим для передачи данных контроллером 12 шины и аппаратными средствами интерфейса 13.

Использование в микропроцессорной системе третьего устройства (микроконтроллера), который с помощью программного обеспечения контролирует первое и второе устройства (микропроцессоры), в отличие от использования для контрольных проверок простых логических элементов, позволяет предусмотреть различные варианты поведения микропроцессорной системы. Так, действия микроконтроллера 10 безопасности, направленные на прекращение передачи выходных данных из модуля ЦП 2, не всегда должны приводить к остановке работы микропроцессорной системы. Можно предусмотреть любые другие дальнейшие действия, например, перезагрузку микропроцессоров и микроконтроллера, их дальнейшую диагностику, выдачу данных диагностики на монитор оператора, и принятие решения оператором о прекращении работы микропроцессорной системы.

Для реализации описанной микропроцессорной системы могут быть использованы следующие устройства.

В качестве центрального микропроцессора может быть использован четырёхъядерный процессор T1040 серии QorIQ®, производимый NXP SEMICONDUCTORS, с архитектурой ядра Power Architecture e5500, с тактовой частотой 1200 МГц и DMIPS 3600 на одно ядро.

В качестве дополнительного микропроцессора может быть использован двухъядерный процессор LS1020 серии QorIQ®, производимый NXP SEMICONDUCTORS, с архитектурой ядра ARM Cortex™-A7, с тактовой частотой 1000 МГц и DMIPS 2500 на одно ядро.

В качестве микроконтроллера безопасности может быть использован микроконтроллер Hercules™, TMS570 с архитектурой ядра ARM® Cortex-R5F™, разработанный для транспорта (автомобильного, железнодорожного и аэрокосмического). К такому микроконтроллеру не предъявляются требования высокой производительности, которые необходимы для работы контроллера в больших АСУ ТП, но зато такой микроконтроллер обладает высоким уровнем диагностики, что делает его высоконадёжным устройством. Так, микроконтроллер Hercules™, TMS570 ARM® Cortex-R5F™, имеет тактовую частоту до 300 МГц и DMIPS 500. К тому же в микроконтроллер Hercules™, TMS570 ARM® Cortex-R5F™ встроен контроллер протокола FlexRay™, который может быть использован для обмена данными по шине между мо-

дулем ЦП и модулями ввода-вывода.

Следует отметить, что описанная выше последовательность действий в микропроцессорной системе может быть осуществлена иначе. Так, например, входные данные от датчиков могут поступать в центральный микропроцессор через микроконтроллер безопасности. И выходные данные из центрального микропроцессора могут передаваться на исполнительные механизмы через микроконтроллер безопасности. Такая последовательность действий описана в ближайшем аналоге (US 9,696,692 B2). Для более подробного описания такого варианта исполнения микропроцессорной системы представлена фиг. 3. Входные данные с шины 4 передаются в контроллер 12 шины (действие a), который в данном варианте показан встроенным в микроконтроллер 10 безопасности. Затем, входные данные из микроконтроллера 10 безопасности передаются в центральный микропроцессор 8 (действие p). В центральном микропроцессоре 8 входные данные фиксируются. Затем этот зафиксированный массив входных данных передаётся из центрального микропроцессора 8 в дополнительный микропроцессор 9 (действие c). После поступления массива входных данных в дополнительный микропроцессор 9 в обоих микропроцессорах 8 и 9 начинается выполнение одной из множества независимых задач прикладной программы. В рамках этой задачи происходит обработка входных данных. Результаты обработки из центрального микропроцессора 8 и из дополнительного микропроцессора 9 передаются в микроконтроллер 10 безопасности (действие x и действие y). Предпочтительно, чтобы из центрального микропроцессора в микроконтроллер 10 безопасности передавались выходные данные с циклическими избыточными кодами (CRC), а из дополнительного микропроцессора в микроконтроллер 10 безопасности передавались только циклические избыточные коды (CRC). Затем микроконтроллер 10 безопасности программно сравнивает CRC выходных данных из центрального 8 микропроцессора с CRC выходных данных из дополнительного микропроцессора 9. Если циклические избыточные коды равны, то микроконтроллер 10 безопасности разрешает передачу выходных данных, поступивших в микроконтроллер 10 безопасности из центрального микропроцессора 8, в шину 4 (действие k). Если значения циклических избыточных кодов (CRC) не равны, значит, произошёл отказ в одном из микропроцессоров (центральном или дополнительном). В этом случае микроконтроллер 10 безопасности прекращает передачу выходных данных из модуля ЦП 2. Для этого микроконтроллер 10 безопасности прекращает работу контроллера 12 шины и/или формирует запрещающий сигнал (действие n) на физический уровень интерфейса 13, где размыкается канал передачи выходных данных в шину 4. В таком варианте исполнения микропроцессорной системы в случае отказа микроконтроллера 10 безопасности выходные данные гарантированно не передаются в шину 4.

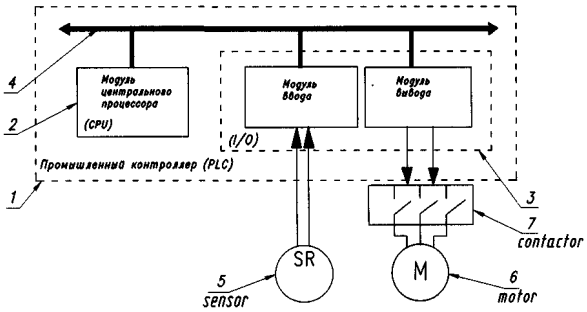
ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ обеспечения функциональной безопасности модуля центрального процессора промышленного контроллера, заключающийся в том, что в модуле центрального процессора используют микропроцессорную систему, предназначенную для обработки входных данных от датчиков и для принятия решения о разрешении передачи выходных данных, предназначенных для управления исполнительными механизмами, из модуля центрального процессора или о прекращении передачи выходных данных из модуля центрального процессора, отличающийся тем, что для этого используют микропроцессорную систему, состоящую из центрального микропроцессора, дополнительного микропроцессора с архитектурой ядра, отличной от архитектуры ядра центрального микропроцессора, и микроконтроллера безопасности, выполненного с возможностью аппаратной самодиагностики, для чего он содержит два параллельных ядра, выполненных с одной и той же логикой, на которые подаются одни и те же входные данные, и модуль сравнения, предназначенный для контроля выходов двух ядер и для сигнализации об ошибках в их работе, при этом одни и те же вхрдные данные от датчиков подают в центральный микропроцессор и в дополнительный микропроцессор, в которых выполняют одинаковые задачи для обработки входных данных, результаты которых передают в микроконтроллер безопасности, в котором сравнивают результаты из центрального микропроцессора и из дополнительного микропроцессора и производят контроль времени выполнения задачи в каждом из микропроцессоров, которое должно находится в заданном интервале времени, который определяют исходя из объёма обрабатываемых данных, после чего в микроконтроллере безопасности принимается решение о разрешении передачи выходных данных из модуля центрального процессора в случае, если отсутствуют ошибки в работе ядер микроконтроллера безопасности, и соблюдено равенство результатов из центрального и из дополнительного микропроцессоров, и время выполнения задачи в каждом из микропроцессоров находилось в заданном интервале времени.

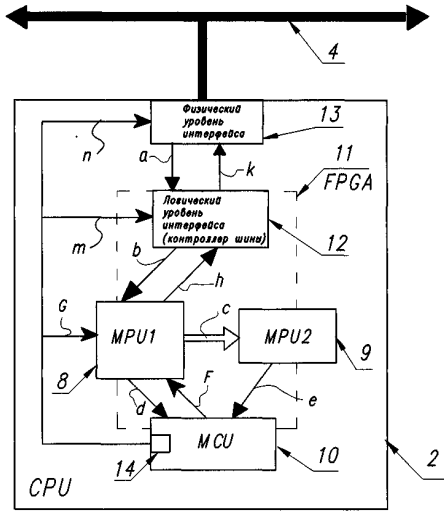
2. Способ по п.1, отличающийся тем, что в микроконтроллере безопасности сравнивают результаты обработки входных данных из центрального и из дополнительного микропроцессоров, в качестве которых могут быть использованы как значения выходных данных, так и значения проверки выходных данных, например значения циклического избыточного кода.

3. Способ, по п.1, отличающийся тем, что, в центральном микропроцессоре и в дополнительном микропроцессоре для решения одинаковых задач используют разные исходные тексты прикладной программы.

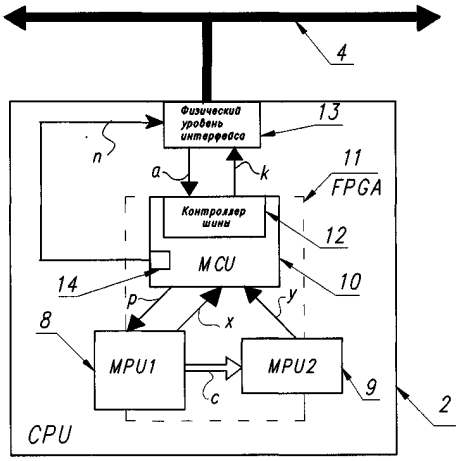
4. Микропроцессорная система модуля центрального процессора промышленного контроллера для осуществления способа по п.1, содержащая центральный микропроцессор, предназначенный для выполнения задачи, в результате которой обрабатываются входные данные от датчиков, дополнительный микропроцессор, выполненный с архитектурой ядра, отличной от архитектуры ядра центрального микропроцессора, и предназначенный для выполнения такой же задачи с теми же входными данными от датчиков, что и центральный микропроцессор, и микроконтроллер безопасности, имеющий для аппаратной самодиагностики два параллельных ядра, выполненных с одной и той же логикой, на которые подаются одни и те же входные данные, и модуль сравнения, предназначенный для контроля выходов двух ядер и для сигнализации об ошибках в их работе, и предназначенный для сравнения результатов обработки из центрального микропроцессора и из дополнительного микропроцессора и для контроля времени выполнения задач в каждом из микропроцессоров, которое должно находится в заданном интервале времени, который определяют исходя из объёма обрабатываемых данных, и имеющий возможность разрешать передачу выходных данных, предназначенных для управления исполнительными механизмами, из центрального микропроцессора в случае, если отсутствуют ошибки в работе ядер микроконтроллера безопасности, и соблюдено равенство результатов обработки в центральном и в дополнительном микропроцессорах, и время выполнения задачи в каждом из микропроцессоров находится в заданном интервале времени.



Фиг. 1



Фиг. 2


4
Физический уровень интерфейса
13
n
a
k
11
FPGA
Контроллер шины
12
MCU
14
10
p
x
y
8
MPU1
MPU2
9
c
2
CPU

Фиг. 3