РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 662 571** (13) **C2**

(51) МПК
G05B 9/02 (2006.01)
G05B 19/042 (2006.01)
G05B 19/418 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G05B 9/02 (2006.01); G05B 19/0428 (2006.01); G05B 19/418 (2006.01); G05B 2219/24031 (2006.01); G05B 2219/24117 (2006.01); G05B 2219/24211 (2006.01)

(21)(22) Заявка: **2016101149, 27.06.2014**

(24) Дата начала отсчета срока действия патента:
27.06.2014

Дата регистрации:
26.07.2018

Приоритет(ы):
(30) Конвенционный приоритет:
28.06.2013 US 13/931,239

(43) Дата публикации заявки: **02.08.2017** Бюл. № 22

(45) Опубликовано: **26.07.2018** Бюл. № 21

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **28.01.2016**

(86) Заявка PCT:
US 2014/044486 (27.06.2014)

(87) Публикация заявки PCT:
WO 2014/210410 (31.12.2014)

Адрес для переписки:
197101, Санкт-Петербург, а/я 128, "АРС-ПАТЕНТ", М.В. Хмара

(72) Автор(ы):
СЕБЕРГЕР Стивен Дж. (US),
СНОУБЭРДЖЕР Джимми Л. (US)

(73) Патентообладатель(и):
ФИШЕР КОНТРОЛЗ ИНТЕРНЕШНЕЛ ЛЛС (US)

(56) Список документов, цитированных в отчете о поиске: **US 2008/0163936 A1, 10.07.2008. US 4245310 A, 13.01.1981. US 2005/0109395 A1, 26.05.2005. RU 2406102 C2, 10.12.2010.**

(54) СИСТЕМА И СПОСОБ ОТКЛЮЧЕНИЯ ПОЛЕВОГО УСТРОЙСТВА

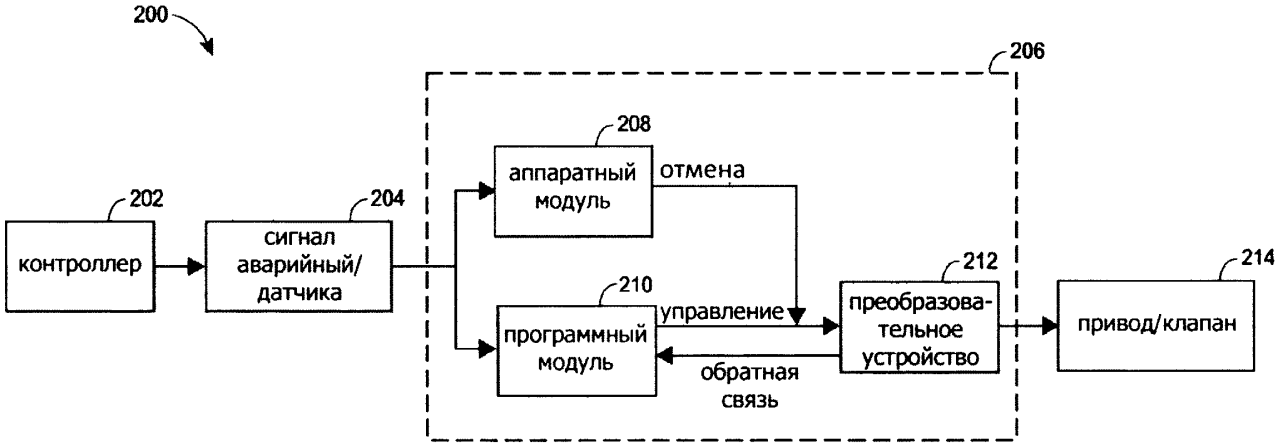
(57) Реферат:

Способ управления полевым устройством включает обнаружение аппаратным модулем возникновения аварийного происшествия, связанного с полевым устройством, отмену аппаратным модулем нормального управления полевым устройством для перевода полевого устройства в безопасное состояние в ответ на обнаруженное возникновение аварийного происшествия, причем отмена нормального управления полевым устройством включает то, что аппаратный модуль вырабатывает аппаратный сигнал управления; обнаружение программным модулем возникновения аварийного происшествия, связанного с полевым устройством; отслеживание программным модулем отмены нормального управления полевым устройством посредством отслеживания аппаратного сигнала управления, выработанного аппаратным модулем; проверка программным модулем отмены нормального управления полевым устройством посредством сравнения сигнала безопасного состояния с отслеженным аппаратным сигналом управления; и передача программным модулем программного сигнала

RU 2662571 C2

RU 2662571 C2

управления для перевода полевого устройства в безопасное состояние. Обеспечивается высокий уровень безопасности. 3 н. и 14 з.п. ф-лы, 3 ил.



Фиг. 2

RU 2662571 C2

RU 2662571 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 662 571** (13) **C2**

(51) Int. Cl.
G05B 9/02 (2006.01)
G05B 19/042 (2006.01)
G05B 19/418 (2006.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G05B 9/02 (2006.01); G05B 19/0428 (2006.01); G05B 19/418 (2006.01); G05B 2219/24031 (2006.01); G05B 2219/24117 (2006.01); G05B 2219/24211 (2006.01)

(21)(22) Application: **2016101149, 27.06.2014**

(24) Effective date for property rights:
27.06.2014

Registration date:
26.07.2018

Priority:
(30) Convention priority:
28.06.2013 US 13/931,239

(43) Application published: **02.08.2017** Bull. № **22**

(45) Date of publication: **26.07.2018** Bull. № **21**

(85) Commencement of national phase: **28.01.2016**

(86) PCT application:
US 2014/044486 (27.06.2014)

(87) PCT publication:
WO 2014/210410 (31.12.2014)

Mail address:
197101, Sankt-Peterburg, a/ya 128, "ARS-PATENT", M.V. Khmara

(72) Inventor(s):
SEBERGER Stiven Dzh. (US),
SNOUBERDZHER Dzhimmi L. (US)

(73) Proprietor(s):
FISHER CONTROLS INTERNATIONAL LLC (US)

RU 2662571 C2

RU 2662571 C2

(54) SYSTEM AND METHOD FOR SHUTTING DOWN FIELD DEVICE

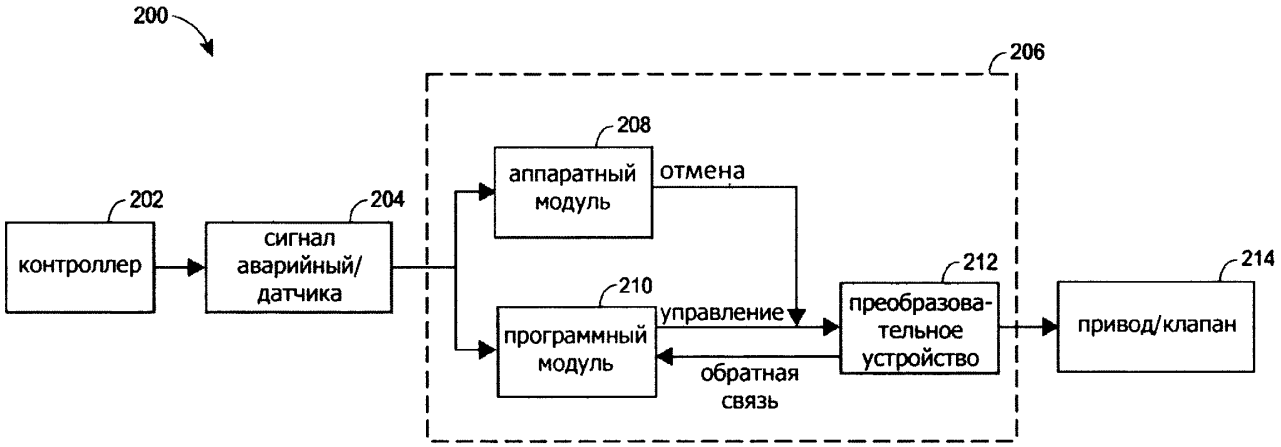
(57) Abstract:

FIELD: control; regulation.

SUBSTANCE: method of controlling a field device comprises detecting, by a hardware module, an occurrence of a safety event associated with a field device, overriding, by the hardware module, normal control of the field device to cause the field device to enter a safe state in response to the detected occurrence of the safety event, wherein overriding normal control of the field device includes the hardware module providing a hardware control signal; detecting, by a software module, the occurrence of the safety event associated with the field device; monitoring, by the software module, the overriding of normal control of the field device by monitoring the hardware control signal generated by the hardware module; verifying, by the software module, the overriding of normal control of the field device by comparing the safe state signal with the monitored hardware control signal; and transmitting, by the software module, a software control signal to cause the field device to enter the safe state.

EFFECT: providing a high level of security.

17 cl, 3 dwg



Фиг. 2

RU 2662571 C2

RU 2662571 C2

ОБЛАСТЬ ТЕХНИКИ

[0001] Это изобретение относится в основном к управлению полевым устройством в автоматической системе безопасности и, более конкретно, к системе и способу переведения полевого устройства в безопасное состояние.

УРОВЕНЬ ТЕХНИКИ

[0002] Системы управления технологическими процессами, подобные тем, что используются в химических, нефтеперерабатывающих и других технологических процессах, в типичном случае, включают один или более число технологических контроллеров, соединенных посредством связи по меньшей мере с одной главной рабочей станцией или пользовательской рабочей станцией и с одним или несколькими полевыми устройствами с помощью аналоговых, цифровых или комбинированных аналогово/цифровых шин(ы). Полевые устройства, которые могут включать, например, регулирующие клапаны, позиционеры клапанов, переключатели и передатчики (например, датчики температуры, давления и расхода) выполняют в технологическом процессе такие функции, как открывание или закрывание клапанов, и измерение параметров технологического процесса. Контроллер технологического процесса принимает сигналы, характерные для измерений процесса, выполняемых полевыми устройствами, и/или другую информацию, относящуюся к полевым устройствам, и использует эту информацию, для реализации управляющей программы, генерируя сигналы управления, передающиеся по шинам на полевые устройства с целью управления ходом технологического процесса. В случае отказа полевого устройства, рабочее состояние всей системы управления технологическим процессом может быть подвержено риску.

[0003] Для защиты системы управления технологическим процессом и предотвращения опасных последствий, таких как утечка токсических, пожароопасных или взрывоопасных химических веществ, может быть применена автоматическая система безопасности (SIS). SIS является отдельной, безотказной системой, используемой для дополнения системы управления технологическим процессом и предпринимающей действия для переведения системы управления технологическим процессом в безопасное состояние, когда это необходимо. SIS использует датчики, логические решающие устройства и приводы для реализации предохранительной функции КИПиА (SIF) для достижения или поддержания безопасного состояния. Уровень обеспечения безопасности (SIL) является статистическим отображением обеспечения SIS и может быть определен по условиям фактора снижения степени риска (RRF). Другими словами, SIL является одним из способов отображения уровня допустимого отказа отдельной функции безопасности. Противоположностью к RRF является вероятность отказа по требованию (PFD) и несколько отдельных уровней SIL, связанных с PFD, причем SIL уровня 1 отображает наивысший уровень допустимого риска, а SIL уровня 4 отображает наименьший уровень допустимого риска.

[0004] SIS обычно может содержать два типа устройств, оборудования, подсистем или модулей; называемых Тип А и Тип Б. В общем, узлы, классифицированные как Тип А, являются устройствами без сложного встроенного процессора и все возможные отказы каждого из компонентов, например, клапанов, реле, соленоидов, переключателей и т.д., могут быть определены. Узлы, классифицированные как тип Б, содержат по меньшей мере один компонент, подверженный отказу, который плохо определяется, например микропроцессоры, проблемно-ориентированные интегральные микросхемы (ASICs), "умные" передатчики. С точки зрения безопасности, отказы могут быть разделены на две категории: безопасные отказы и опасные отказы. Безопасными

отказами являются такие отказы, которые на уровне модулей и подсистем внутри устройства приводят к безопасному состоянию и которые могут или не могут быть обнаружены внутренней диагностикой. Опасным отказом является отказ, который не приводит к безопасному состоянию. Однако опасный отказ может быть обнаружен внутренней диагностикой, которая сигнализирует пользователю о неисправности и разрешает временный ремонт, таким образом, вероятность отказа по требованию (PFD) не нарушается, что было бы в случае, если отказ мог произойти без обнаружения. Параметр «доля безопасных отказов» (SFF) отображает долю общего уровня отказов устройства, которые приводят к безопасным отказам по сравнению ко всем отказам. SFF может быть определен как 1 - (опасные не обнаруженные отказы)/(общее количество отказов), причем общее количество отказов включает обнаруженные безопасные отказы, не обнаруженные безопасные отказы, обнаруженные опасные отказы и не обнаруженные опасные отказы. Не обнаруженные опасные отказы негативно влияют на PFD и/или SFF, связанные с устройством.

[0005] Описаны примерные системы и способы улучшения управляемости работы промышленной установки. В одном примере способ реализован на компьютерном устройстве, причем способ управления полевым устройством, реализованным в автоматической системе безопасности, включает обнаружение аппаратным модулем возникновения аварийного происшествия, связанного с полевым устройством, реализованным в автоматической системе безопасности, отмена аппаратным модулем нормального управления полевым устройством, побуждая полевое устройство перейти в безопасное состояние в ответ на обнаружение появления аварийного происшествия, обнаружение программным модулем появления аварийного происшествия, связанного с полевым устройством автоматической системы безопасности, отслеживание программным модулем отмены нормального управления полевым устройством, проверку программным модулем отмены нормального управления полевым устройством, и передачу программным модулем программного сигнала управления, побуждающего полевое устройство перейти в безопасный режим.

[0006] В другом примерном варианте реализации изобретения, система управления управляющим элементом, реализованным в автоматической системе безопасности, содержит полевое устройство, содержащее аппаратный модуль, функционально связанный с программным модулем. Аппаратный модуль функционально связан с управляющим входом преобразовательного устройства, и аппаратный модуль реагирует на появление аварийного происшествия, причем сразу после обнаружения появления аварийного происшествия аппаратный модуль блокирует программное управление полевым устройством и вырабатывает аппаратный сигнал управления для перевода преобразовательного устройства в безопасное состояние. Программный модуль содержит процессор, функционально связанный с запоминающим устройством и управляющим входом преобразовательного устройства. Программный модуль реагирует на появление аварийного происшествия, причем сразу после обнаружения появления аварийного происшествия, программный модуль проверяет отмену управления полевым устройством аппаратным модулем и затем передает программный сигнал управления для перевода преобразовательного устройства в безопасное состояние.

[0007] В дополнительном примере способа реализации изобретения, система управления устройством управления, реализованным в автоматической системе безопасности содержит устройство для обнаружения возникновения аварийного происшествия, связанного с полевым устройством реализованным в автоматической системе безопасности, устройство для отмены нормального управления полевым

устройством, для перевода полевого устройства в безопасное состояние в ответ на обнаружение появления аварийного происшествия, устройство для отслеживания отмены нормального управления полевым устройством, устройство для проверки отмены нормального управления полевым устройством, и устройство для передачи программного сигнала управления для перевода полевого устройства в безопасное состояние.

[0008] В еще одном примере реализации изобретения, физический постоянный машиночитаемый носитель содержит команды, хранящиеся на нем, причем при их выполнении одним или более процессорами, вызывает обнаружение одним или более процессоров в программном модуле возникновения аварийного происшествия, связанного с полевым устройством автоматической системы безопасности; отслеживание программным модулем отмены аппаратным модулем нормального управления полевым устройством; проверку программным модулем отмены аппаратным модулем нормального управления полевым устройством; и передачу программным модулем программного сигнала управления побуждающего полевое устройство перейти в безопасное состояние.

[0009] Далее, в соответствии с описанными аспектами изобретения, любой один или более из упомянутых выше вариантов реализации изобретения может дополнительно включать в себя любой один или более из следующих вариантов изобретения.

[0010] В другом варианте реализации изобретения, отслеживание отмены нормального управления полевым устройством включает отслеживание аппаратного сигнала управления функционально соединенного с входом полевого устройства.

[0011] В другом варианте реализации изобретения, проверка отмены нормального управления полевым устройством включает сравнение сигнала безопасного состояния с аппаратным сигналом управления.

[0012] В другом варианте реализации изобретения, способ включает запись проверки отмены нормального управления полевым устройством.

[0013] В другом варианте реализации изобретения, запись проверки отмены нормального управления полевым устройством включает регистрацию обнаруженного отказа, если отслеживаемый аппаратный сигнал управления не эквивалентен сигналу безопасного состояния.

[0014] В другом варианте реализации изобретения, система содержит преобразователь сигнала управления, функционально подсоединенный между аппаратным модулем и полевым устройством, причем преобразователь сигнала управления дополнительно функционально соединен между программным модулем и полевым устройством.

[0015] В другом варианте реализации изобретения, преобразователь сигнала управления является преобразователем ток-давление (I/P) или преобразователем напряжение-давление (E/P).

[0016] В другом варианте реализации изобретения, система содержит первый датчик функционально соединенный с аппаратным модулем для обнаружения возникновения аварийного происшествия, причем сразу после обнаружения возникновения аварийного происшествия, первый датчик инициирует передачу аппаратного сигнала управления от аппаратного модуля к преобразователю сигнала управления, и второй датчик, функционально связанный с программным модулем для обнаружения возникновения аварийного происшествия, причем сразу после обнаружения возникновения аварийного происшествия, второй датчик инициирует передачу программного сигнала управления от программного модуля к преобразователю сигнала управления. Альтернативно, первый и второй датчики не обязательно должны быть отдельными датчиками, но

могут быть одним датчиком. То есть, отдельный датчик для обнаружения возникновения аварийного происшествия может быть функционально соединен с аппаратным модулем и программным модулем, причем сразу после обнаружения возникновения аварийного происшествия, отдельный датчик инициирует передачу аппаратного сигнала управления от аппаратного модуля и программного сигнала управления от программного модуля.

[0017] В другом примерном варианте реализации изобретения, полевое устройство является контроллером пневматического клапана, содержащим аппаратный модуль, классифицированный как устройство Типа А, и программный модуль, классифицированный как устройство Типа Б.

КРАТКОЕ ОПИСАНИЕ ГРАФИЧЕСКИХ МАТЕРИАЛОВ

[0018] Фиг. 1 является схематическим изображением примерной промышленной установки, содержащей систему управления технологическим процессом и автоматическую систему безопасности.

[0019] Фиг. 2 является блок-схемой примерной конструкции части промышленной установки (построенной в соответствии с принципами настоящего изобретения) для переведения конечного управляющего элемента, такого как клапан, в безопасное состояние.

[0020] Фиг. 3 иллюстрирует примерный модуль или карту технологического процесса, который может использоваться на промышленной установке, изображенной на Фиг. 2 для переведения полевого устройства в безопасное состояние.

ПОДРОБНОЕ ОПИСАНИЕ

[0021] Представленное изобретение предназначено обеспечить систему управления и способ надежного переведения полевого устройства, реализованного в автоматической системе безопасности в безопасное состояние. Примерная промышленная установка 10. показанная на Фиг. 1, способна реализовать один или более вариантов воплощения настоящего изобретения, содержащих систему управления технологическим процессом 12 и систему безопасности 14 (изображена пунктирными линиями), которая в общем работает как автоматическая система безопасности (SIS). SIS 14 способна реализовать предохранительную функцию КИПиА (SIF) для достижения или поддержания безопасного состояния системы управления технологическим процессом 12. Если необходимо, SIS 14 может заблокировать управление системы управления технологическим процессом 12.

[0022] Промышленная установка 10 содержит одну или более главных рабочих станций 16 или вычислительных устройств, таких как персональный компьютер, например, содержащий пользовательский интерфейс, содержащий клавиатуру и экран монитора, доступные для производственного персонала. В показанном примере по Фиг. 1, две рабочие станции 16 проиллюстрированы как соединенные с узлом управления технологическим процессом/управления безопасностью 18 и с архивным хранилищем данных 20 посредством линии связи или шины 22. Архивным хранилищем данных 20 может быть любой требуемый тип устройства сбора данных, содержащий любой требуемый тип запоминающего устройства и любые требуемые или известные программные, аппаратные или программно-аппаратные средства для хранения данных. Хотя архивное хранилище данных 20 проиллюстрировано как отдельное устройство на Фиг. 1, оно взамен или дополнительно может быть частью одной из рабочих станций 16 или другого устройства, такого как сервер. Коммуникационная шина 22 может быть реализована при помощи любой желаемой аппаратуры на шинной или не шинной основе, при использовании любой желаемой проводной или беспроводной структуры связи, и используя любой желаемый или подходящий протокол связи, такой как протокол

Ethernet.

[0023] В общем, промышленная установка 10 содержит как устройства системы управления технологическим процессом, так и устройства системы безопасности, функционально соединенные вместе посредством шинной структуры, которая может быть реализована на материнской плате 26, на которой смонтированы различные контроллеры технологического процесса и входные/выходные устройства. Промышленная установка 10, показанная на Фиг. 1, содержит по меньшей мере один контроллер технологического процесса 24, а также одно или более входных/выходных (I/O) устройств системы управления технологическим процессом 28, 29, 30, 31, 32. Каждое из I/O устройств системы управления технологическим процессом 28, 29, 30, 31, 32 посредством связи соединено с рядом связанных с управлением технологическим процессом полевых устройств, проиллюстрированных на Фиг. 1, таких как полевые устройства 40, 41, 42, 48. Контроллер технологического процесса 24, I/O устройства 28, 29, 30, 31, 32, и полевые устройства контроллера 40, 41, 42, 48 в общем составляют систему управления технологическим процессом 12 по Фиг. 1.

[0024] Контроллер технологического процесса 24, который может быть, исключительно в качестве примера, DeltaV™ контроллером, проданным Emerson Process Management или контроллером технологического процесса любого желаемого типа, запрограммирован на обеспечение функционирования управления технологическим процессом при использовании устройств 28, 29, 30, 31, 32 и полевых устройств 40, 41, 42, 48. В частности, контроллер 24 реализует или управляет одни или более модулями управления технологическим процессом 46 или программами, сохраненными в присутствующем или каким-либо образом связанном запоминающем устройстве и связывается с полевыми устройствами 40, 41, 42, 48 и рабочей станцией 16 для управления промышленной установкой 10 или частью промышленной установки 10 любым желаемым способом.

[0025] Программы управления 46, которые могут быть модулями управления или любой частью процедуры управления, такой как подпрограммы, частями подпрограмм (такой как строки кода), и т.д., могут реализовываться в любом желаемом формате программ, например, используя многоступенчатую логику, последовательные графики функций, диаграммы программ управления, объектно-ориентированное программирование или любой другой язык программирования или конструкторский принцип. Так же, программы управления, описанные в данном документе, могут быть записаны в структуру, например, одной или более EPROMs, EEPROMs, проблемно-ориентированных интегральных микросхем (ASICs), PLCs или других аппаратных или программно-аппаратных элементов. Программы управления могут разрабатываться с использованием любых желаемых конструкторских инструментов, в том числе средств графического дизайна или программного/аппаратного/программно-аппаратных инструментов программирования или конструирования любого другого типа.

[0026] Контроллер 24 может быть выполнен с возможностью реализации программы управления или стратегии управления любым желаемым способом. Например, контроллер 24 может реализовывать стратегию управления при использовании того, что общеизвестно как функциональные блоки, в которых каждый функциональный блок является частью или объектом всей программы управления и работает совестно с другими функциональными блоками (посредством связи, называемой соединения) для реализации цепей управления технологическим процессом в системе управления технологическим процессом 12. Функциональные блоки обычно выполняют одно из следующего: функцию ввода подобную той, что связана с преобразователем, датчиком

или другим устройством, измеряющим параметры технологического процесса; функцию управления подобную той, что связана с программой управления, выполняющей PID, нечеткую логику, и подобное управление; или функцию вывода подобную той, что управляет работой нескольких устройств, таких как клапан для выполнения некоторых физических функций в системе управления технологическим процессом 12. Могут существовать гибриды, а также другие типы этих функциональных блоков.

[0027] Функциональные блоки и программы управления могут сохраняться и выполняться контроллером 24, как обычно и бывает, если эти функциональные блоки используются для или связаны со стандартными 420 мА устройствами и некоторыми типами умных полевых устройств, такими как устройства HART. Функциональные блоки и программы управления могут также сохраняться и реализовываться полевыми устройствами, что может быть в случае с устройствами Fieldbus.

[0028] В целях настоящего описания, термины «стратегия управления», «программа управления», «модуль управления», «функциональный блок управления», «модуль безопасности», «модуль логики безопасности», и «цепь управления» по существу обозначают программу управления, выполняемую для управления технологичесим процессом и эти термины могут использоваться здесь взаимозаменяемо. Однако, в целях последующего изложения, будет использоваться термин «модуль». Дополнительно следует отметить, что модуль, описанный в данном документе, может содержать части реализованные или выполняемые различными контроллерами или другими устройствами, если так необходимо. Дополнительно, описанные в данном документе модули, реализованные в системе управления технологическим процессом 12 и системе безопасности 14 могут принимать любую форму, в том числе программную, аппаратную, программно-аппаратную и любую их комбинацию.

[0029] Полевые устройства 40, 41, 42, 48 могут быть любого желаемого типа, такого как датчики, клапаны, преобразователи, позиционеры и т.д. и могут согласовываться с любыми желаемыми открытыми, приватными или другими проводными и/или беспроводными протоколами связи или программирования включая, например, HART или 4-20 мА протокол (как показано для полевых устройств 40), любой протокол шины, такой как протокол Foundation® Fieldbus (как показано для полевых устройств 41) или CAN, Profibus, и AS-Interface протоколы, не говоря уже о других. Подобным образом, каждое из I/O устройств 28, 29, 30, 31, 32 может быть I/O устройством управления технологического процесса любого известного типа, использующим любой подходящий протокол связи.

[0030] Дополнительно или вместо проводной связи, могут устанавливаться беспроводные связи между контроллером 24 и полевыми устройствами 40, 41, 42, 48, используя любое желаемое оборудование беспроводной связи, в том числе аппаратное, программное, программно-аппаратное или любую их комбинацию, известную сейчас или разработанную позже. В варианте реализации изобретения, проиллюстрированном на Фиг. 1, антенна 47 подключена и предназначена для осуществления беспроводной связи для передатчика 42, в то время как беспроводный маршрутизатор или другой модуль 43 содержащий антенну 45 подключен для поддержания посредством связи беспроводного соединения для передатчиков 42 подключенных к нему функционально. Аналогичным образом, антенна 37 соединена со сборкой управляющего клапана 48 с целью осуществления беспроводной связи для сборки регулирующего клапана. Полевые устройства или связанные аппаратные устройства 40, 41, 42, 48 могут реализовывать стековые операции протоколов, используемые соответствующими беспроводными протоколами связи для получения, декодирования, маршрутизации, кодирования и

отправления беспроводных сигналов посредством антенн 37, 45, 47 для реализации беспроводной связи между контроллером технологического процесса 24 и передатчиками 42 и сборкой управляющего клапана 48.

[0031] Если необходимо, передатчики 42 могут составлять отдельное соединение между различными датчиками технологического процесса (передатчиками) и контроллерами технологического процесса 24 и, таким образом, полагаться на отправление точных сигналов контроллеру 24 чтобы убедиться в том, что выполнение технологического процесса не нарушено. Передатчики, часто упоминаемые как передатчики переменных технологического процесса (PVTs), тем не менее могут играть значительную роль в управлении общим процессом управления. Кроме того, сборка управляющего клапана 48 может передавать измерения, выполненные датчиками в сборке управляющего клапана 48, или может передавать другие данные, генерируемые или вычисленные посредством сборки управляющего клапана 48, на контроллер 24, в качестве части выполняемой ею работы. Разумеется, как известно, сборка управляющего клапана 48 также может принимать сигналы управления от контроллера 24, чтобы воздействовать на физические параметры, например, на поток, внутри технологического процесса в целом.

[0032] Контроллер технологического процесса 24 соединен с одним или более I/O устройствами 31, 32, каждое из которых подключено к приемной антенне 33, 35, и эти I/O устройства и антенны работают как передатчики/приемники для осуществления беспроводной связи с беспроводными полевыми устройствами 42, 48 посредством одной или больше коммуникационных сетей. Беспроводная связь между полевыми устройствами может осуществляться с использованием одного или большего количества известных протоколов беспроводной связи, таких как протокол WirelessHART®, протокол Ember, протокол Wi-Fi, стандарт беспроводной связи IEEE и т.д. Более того, I/O устройства 31, 32 могут реализовывать операции стека протоколов, используемых этими протоколами связи для приема, декодирования, маршрутизации, кодирования и передачи беспроводных сигналов через антенны 33, 35, чтобы осуществлять беспроводную связь между контроллером 24 и передатчиками и узлом 48 управляющего клапана.

[0033] Технологическая установка 10 содержит одно или более решающих устройств системы безопасности 50, 51, 52, 53. Каждое из логических решающих устройств 51, 52, 53, 54 может быть контроллером безопасности (также постоянно упоминаемый как устройство I/O), содержащим процессор 54, который выполняет модули логики безопасности 58, сохраненные в запоминающем устройстве и посредством связи соединенные для передачи сигналов управления и/или получения сигналов от полевых устройств системы безопасности 60, 62, 65, 66. Контроллеры безопасности 50, 51, 52, 53 и полевые устройства системы безопасности 60, 62, 65, 66 в целом составляют систему безопасности 14 (SIS) по Фиг. 1.

[0034] Полевые устройства безопасности 60, 62, 65, 66 могут быть полевыми устройствами любого желаемого типа, соответствующие или использующие любой известный или желаемый проводной и/или беспроводный протокол связи, как те, что упоминались выше по отношению к системе управления технологическим процессом 12. В частности, полевые устройства 60, 62, 65, 66 могут быть полевыми устройствами, связанными с безопасностью такого типа, которые условно управляются отдельной, специальной связанной с безопасностью системой управления, такими как клапан аварийной остановки (ESD). В промышленной установке 10, показанной на Фиг. 1, полевые устройства безопасности 60 проиллюстрированы как использующие

специальные или протоколы связи точка-точка, такие как HART или 4-20 мА протокол, хотя полевые устройства безопасности 62 проиллюстрированы как использующие протоколы шины связи, такие как протокол Fieldbus. В общем, устройства безопасности (также контроллеры 50, 51, 52, 53 и полевые устройства системы безопасности 60, 62, 65, 66), используемые как часть системы безопасности 14, будут ранжированы как устройства безопасности, что обычно означает, что эти устройства должны пройти рейтинговую процедуру, чтобы быть ранжированными соответствующим звеном как устройство безопасности.

[0035] Подобно системе управления технологическим процессом 12, система безопасности 14 может также содержать множество беспроводных полевых устройств 65, 66, расположенных по промышленной установке для осуществления управления. Полевые устройства 65, 66 могут содержать передатчики 65, такие как датчики переменных технологического процесса, а также сборку управляющего клапана 66, например, содержащую управляющий клапан и привод. Беспроводная связь может быть установлена между контроллером безопасности 50, 51, 52, 53 и полевыми устройствами 60, 62, 65, 66 с использованием любого желаемого оборудования беспроводной связи, включая аппаратные, программные, программно-аппаратные средства или любое их сочетание, известное в настоящем или разработанное позднее. В варианте реализации изобретения, проиллюстрированном на Фиг. 1, антенна 67 подключена и предназначена для осуществления беспроводной связи для передатчика 65, в то время как беспроводный маршрутизатор или другой модуль 63, содержащий антенну 69, подключен для поддержания посредством связи беспроводного соединения для передатчиков 65, подключенных к нему функционально. Аналогичным образом, антенна 59 соединена со сборкой управляющего клапана 66 с целью осуществления беспроводной связи для сборки управляющего клапана. Периферийные устройства или соответствующие аппаратные устройства 60, 62, 65, 66 могут выполнять стековые операции, которые используются соответствующим протоколом беспроводной связи для того, чтобы принимать, декодировать, маршрутизировать, кодировать и передавать радиосигналы через антенны 59, 67, 69 для осуществления беспроводной связи между контроллером безопасности 50, 51, 52, 53 и передатчиками 65, а также сборкой управляющего клапана 66.

[0036] Каждый передатчик 65 может осуществлять одно из нескольких соединений между различными датчиками технологического процесса (передатчиками) и контроллером безопасности 50, 51, 52, 53 и, таким образом, на него полагаются в передаче точных сигналов контроллеру безопасности для проверки того, что выполнение технологического процесса не нарушено. Дополнительно, сборка управляющего клапана 66 может обеспечивать измерения, проводимые датчиками в сборке управляющего клапана, или может предоставлять другие данные, генерируемые или вычисляемые сборкой управляющего клапана контроллеру 50, 51, 52, 53 как часть своей работы. Разумеется, как известно, сборка управляющего клапана 66 также может принимать сигналы управления от контроллера 50, 51, 52, 53, чтобы воздействовать на физические параметры, например, на поток, внутри технологического процесса в целом.

[0037] Общая материнская плата 26 (обозначенная пунктирной линией в контроллере технологического процесса 24, I/O устройства 28, 29, 30, 31, 32 и контроллеры безопасности 50, 51, 52, 53) используется для связи контроллера технологического процесса 24 с I/O картами технологического процесса 28, 29, 30, 31, 32, также как с контроллерами безопасности 50, 51, 52, 53. Контроллер технологического процесса 24 также посредством связи соединен с шиной 22 и может работать как устройство

арбитража шины для предоставления возможности каждому из I/O устройств 28, 29, 30, 31 32 и контроллерам безопасности 50, 51, 52, 53 связаться с любой из рабочих станций 16 по шине 22. Материнская плата 26 дополнительно предоставляет возможность контроллерам безопасности 50, 51, 52, 53 связываться друг с другом и координировать функции безопасности, реализуемые этими устройствами, для передачи данных друг другу, или для выполнения других интегрированных функций.

[0038] Каждая из рабочих станций 16 содержит процессор рабочей станции 34 и запоминающее устройство 36, которое может хранить приложения или модули, адаптированные для выполнения любым из процессоров 24, 34, 50, 51, 52, 53 на промышленной установке 10. Дисплейное приложение 44 проиллюстрировано в частичном виде на Фиг. 1 как сохраненное в запоминающем устройстве 36 одной из рабочих станций 16. Однако, если необходимо, дисплейное приложение 44 может храниться и выполняться на другой рабочей станции 16 или в другом вычислительном устройстве, связанном с промышленной установкой 10. Дисплейное приложение 44 может быть интерфейсом любого типа, который, например, разрешает пользователю манипулировать значениями данных (например, выполнять считывание и запись), тем самым изменяя работу модулей управления 46 или модулей безопасности 58 по отдельности или в обоих системе управления 12 и системе безопасности 14. Таким образом, если выбрано произвести запись в модуль управления 46, связанный с системой управления 12, или в одно из полевых устройств 40, 41, 42, 48, например, дисплейное приложение 44 предоставляет возможность того, что запись будет иметь место. Дополнительно, если выбрано сделать запись в логический модуль безопасности 58, связанный с системой безопасности 14 или в полевые устройства 60, 62, 65, 66, например, дисплейное приложение 44 предоставляет возможность того, что запись будет иметь место.

[0039] Диагностическое приложение 38, которое может содержать один или более диагностических модулей, например, может также храниться в запоминающем устройстве рабочей станции 16 для более позднего использования производственным персоналом системе управления 12 или безопасности 14. В общем, при выполнении соответствующими процессорами 24, 34, 50, 51, 52, 53 в системе управления 12 или безопасности 14, диагностическое приложение 38 способно проверять или тестировать рабочее состояние используемых здесь полевых устройств 40, 41, 42, 48, 60, 62, 65, 66. Например, тюнер цепи управления (который может, например, использоваться как в цепи управления системы управления технологическим процессом 12 или цепи управления системы безопасности 14) может быть одним модулем в диагностическом приложении 38, модуле управления 46, или модуле логики безопасности 58, способном выполняться процессорами 24, 34, 50, 51, 52, 53. Пользователь может выбрать запустить этот отдельный модуль, в случае если данные диагностики о цепи управления показывают, что цепь управления плохо настроена или не работает в желаемых допусках.

[0040] Другой пример диагностического приложения 38 содержит резервный модуль проверки безопасности для проверки функциональной работоспособности полевого устройства, используемого в системе безопасности 14. Резервный модуль проверки безопасности может содержать аппаратный модуль и программный модуль, каждый из которых настраивается на переведение полевого устройства в безопасное состояние, например, отключение, в ответ на обнаружение появления аварийного происшествия, требующего, чтобы полевое устройство было переведено в безопасное состояние. Для того, чтобы разрешить классифицировать устройство как устройство Типа А,

аппаратный модуль выполнен так, чтобы переводить полевое устройство в безопасное состояние сразу после обнаружения аварийного происшествия вне зависимости от программного модуля. Программный модуль Типа Б также выполнен так, чтобы в ответ на аварийное происшествие перевести свой выход в безопасное состояние, что переведет полевое устройство в безопасное состояние даже, если аппаратный модуль не сможет заблокировать программный модуль. Таким образом, если аппаратный модуль не сможет перевести полевое устройство в безопасное состояние, программный модуль переведет полевое устройство в безопасное состояние. Дополнительно, программный модуль может отслеживать функцию безопасности аппаратного модуля и записывать состояния в случае, если аппаратный модуль успешно инициировал перевод клапана в безопасное состояние и/или не смог успешно инициировать переведение клапана в безопасное состояние.

[0041] Фиг. 2 иллюстрирует блок-схему примерной конфигурации 200 для нормального отключения устройства системой управления и системой безопасности. В этом варианте реализации изобретения, система безопасности содержит полевое устройство 206, ответственное за нормальный сигнал управления и появление аварийного происшествия, вызываемого изменением в сигнале управления. Полевое устройство 206 может быть контроллером для конечного элемента управления 214, таким как пневматически управляемый клапан и т.д., который требуется открывать или закрывать при появлении аварийного происшествия. Появление аварийного происшествия может обнаруживаться другим устройством в системе безопасности, таким как контроллер 202 или датчик или управляющим персоналом. Например, датчик и/или процессор в контроллере 202 может обнаружить появление аварийного происшествия и отправит сигнал безопасности/датчика полевому устройству 206, которое способствует движению с помощью преобразовательного устройства 212 привода и/или клапана 214. При получении сигнала безопасности/датчика от датчика 204, аппаратный модуль 208 вырабатывает аппаратный сигнал управления (например, сигнал отмены) преобразующему устройству 210, которое выдает соответствующий сигнал управления давлением на привод/клапан 214 для открывания или закрывания клапана. Преобразующее устройство 212 может быть устройством ток-давление или напряжение-давление. Если коротко, аппаратный модуль 206 эффективно отменяет нормальное управление полевым устройством 206, которое обычно выполняется программным модулем 210, который может содержать процессор и I/O устройства, такие как контроллер, изображенный на Фиг. 1. Программный модуль 210 может независимо обнаруживать появление аварийного происшествия с помощью сигнала безопасности/датчика 204, переданного программному модулю тем же или другим контроллером или датчиком системы безопасности или управляющим персоналом. Сразу после получения сигнала безопасности/датчика, программный модуль 210 будет отслеживать и/или проверять выработал ли аппаратный модуль 208 сигнал управления на преобразующее устройство 212. Программный модуль может отслеживать блокировку аппаратным модулем с помощью сигнала обратной связи, получаемого от преобразующего устройства (например, I/O сигнал проверки записи). Программный модуль может проверять инициировал ли аппаратный модуль блокировку нормального управления полевым устройством (или преобразователем), сравнивая аппаратный сигнал управления с сигналом безопасного состояния. Если программный модуль 210 определяет, что аппаратный модуль 208 не смог заблокировать управление полевым устройством 206, или инициировал блокирование полевого устройства 206 и выработал аппаратный сигнал управления преобразующему устройству 212, программный модуль

210 может записать и/или подать отчет об отказе. В не зависимости работает ли аппаратный модуль 208 как следует или нет, программный модуль 210 будет передавать программный сигнал управления (например, сигнал управления) преобразующему устройству 212. В любом случае, программный сигнал управления будет преобразован в управляющий сигнал давления в преобразующем устройстве 212 для отправки с целью открытия и/или закрытия привода/клапана 214. Если аппаратный модуль 208 удовлетворительно выполнил функцию отмены, программный сигнал управления не будет иметь эффекта. Однако, если аппаратный модуль 208 провалил выполнение своей функции отмены, программный сигнал управления переведет клапан 214 в безопасное состояние.

[0042] Обратимся теперь к Фиг. 3, блок-схема примерного способа 300 одного из вариантов реализации изобретения, пригодного к реализации в системе управления, проиллюстрированной на Фиг. 1 или 2. Более конкретно, появление аварийного происшествия обнаруживается аппаратным модулем (блок 302). Появление аварийного происшествия также обнаруживается программным модулем (блок 304). Аварийное происшествие может быть происшествием требующим, чтобы полевое устройство и/или управляющий элемент, управляемый полевым устройством, был переведен в безопасное состояние, такое как полностью открыть или полностью закрыть клапан аварийного отключения. В ответ на обнаружение появления аварийного происшествия, аппаратный модуль вызывает переведение клапана с помощью привода в безопасное состояние или состояние отключения (блок 306). То есть, аппаратный модуль способен независимо брать на себя управление клапаном, вырабатывая аппаратный сигнал управления преобразующему устройству, функционально связанному с приводом/клапаном. Программный модуль, который может в нормальном состоянии управлять работой привода/клапана с помощью преобразовательного устройства, отслеживает отмену, выполняемую аппаратным модулем (блок 308) и проверяет чтобы аппаратный модуль инициировал передачу аппаратного сигнала управления на преобразующее устройство для переведения привода/клапана в безопасное состояние, например, состояние выключения (блок 310). В одном из вариантов реализации изобретения, программный модуль может отслеживать аппаратный сигнал управления в форме электрического тока I/P преобразующему устройству для проверки отмены аппаратным модулем. Программный модуль может проверять, инициировал ли аппаратный модуль отмену, сравнивая аппаратный сигнал управления (например, сигнал отмены), передаваемый аппаратным модулем, с сигналом безопасного состояния. Если аппаратный сигнал управления эквивалентен сигналу безопасного состояния, отмена была инициирована аппаратным модулем. Если аппаратный сигнал управления не эквивалентен сигналу безопасного состояния, аппаратный модуль провалил инициацию отмены. Программный модуль записывает результаты проверки и может хранить любое содержимое, связанное с проверкой, в устройстве хранения (блок 312). Например, если аппаратное устройство удовлетворительно выполнило инициацию выключения клапана, программный модуль соответственно ее запишет. С другой стороны, если аппаратный модуль не удовлетворительно инициировал отключение клапана, программный модуль соответственно запишет эту информацию. Дополнительно, вне зависимости от того перевело ли аппаратное устройство привод/клапан в безопасное состояние, программный модуль передает программный сигнал управления на преобразующее устройство для перевода в безопасное состояние (блок 314). Программный сигнал управления преимущественно передается от программного модуля после проверки программным модулем того, что аппаратный модуль выполнил

или не выполнил отмену управления преобразующим устройством и/или привода/клапана, передав аппаратный сигнал управления.

[0043] Система и способ описанные выше реализуют две отдельные функции, каждая из которых будет вызывать отключение, если вторая откажет, таким образом обеспечивая резервность функции и более высокую надежность, чем при реализации по отдельности. Конкретнее, полевое устройство содержит аппаратный модуль, классифицированный как устройство Типа А, объединенный с программным модулем, классифицированным как устройство Типа Б, причем традиционные зависимые аспекты аппаратного модуля поддерживаются программным модулем для перевода полевого устройства и/или конечного элемента управления в безопасное состояние. Обнаружение программным модулем отказа аппаратного модуля при блокировке управления полевым устройством чтобы вызвать отключение позволяет эти отказы не учитывать при расчете параметра доли безопасных отказов (SFF) и/или значению вероятности отказа по требованию (PFD) связанных с полевым устройством. При увеличении количества обнаруженных отказов аппаратного модуля, SFF и/или PFD полевого устройства могут быть таким образом улучшены. Полевое устройство с улучшенными SFF и/или PFD может избежать необходимости в резервном оборудовании в автоматической системе безопасности и/или может позволять производить диагностическое тестирование для достижения требуемой средней PFD менее часто.

[0044] Хотя в данном документе были описаны определенные примерные способы, устройство и промышленные изделия, сфера охвата данного патента этим не ограничивается. Напротив, этот патент включает все способы, устройства и промышленные изделия, находящиеся в пределах прилагаемой формулы изобретения, буквально или в силу доктрины об эквивалентах.

(57) Формула изобретения

1. Способ управления полевым устройством, реализованным в автоматической системе безопасности, включающий:

обнаружение аппаратным модулем возникновения аварийного происшествия, связанного с полевым устройством, реализованным в автоматической системе безопасности;

отмена аппаратным модулем нормального управления полевым устройством для перевода полевого устройства в безопасное состояние в ответ на обнаруженное возникновение аварийного происшествия, причем отмена нормального управления полевым устройством включает то, что аппаратный модуль вырабатывает аппаратный сигнал управления;

обнаружение программным модулем возникновения аварийного происшествия, связанного с полевым устройством автоматической системы безопасности;

отслеживание программным модулем отмены нормального управления полевым устройством посредством отслеживания аппаратного сигнала управления, выработанного аппаратным модулем;

проверка программным модулем отмены нормального управления полевым устройством посредством сравнения сигнала безопасного состояния с отслеженным аппаратным сигналом управления; и

передача программным модулем программного сигнала управления для перевода полевого устройства в безопасное состояние.

2. Способ по п. 1, дополнительно включающий:

запись программным модулем проверки отмены нормального управления полевым

устройством.

3. Способ по любому из пп. 1 или 2, отличающийся тем, что запись проверки отмены нормального управления полевым устройством включает регистрацию обнаруженного отказа аппаратного модуля, если отслеженный аппаратный сигнал управления не эквивалентен сигналу безопасного состояния.

4. Способ по любому из пп. 1 или 2, отличающийся тем, что аппаратный модуль классифицируется как устройство типа А, содержащее управляющий выход, функционально соединенный с управляющим элементом.

5. Способ по любому из пп. 1 или 2, отличающийся тем, что программный модуль классифицируется как устройство типа Б, содержащее управляющий выход, функционально соединенный с управляющим элементом.

6. Система для управления полевым устройством, функционально соединенным с управляющим элементом, реализованным в автоматической системе безопасности, содержащая:

полевое устройство, функционально связанное с управляющим элементом и реализованное в автоматической системе безопасности, содержащее аппаратный модуль, функционально соединенный с программным модулем, причем

аппаратный модуль функционально связан с управляющим входом управляющего элемента, при этом аппаратный модуль реагирует на появление аварийного происшествия, причем сразу после обнаружения аппаратным модулем появления аварийного происшествия аппаратный модуль отменяет нормальное управление полевым устройством и вырабатывает аппаратный сигнал управления на управляющий элемент; и

указанный программный модуль, содержащий процессор, функционально соединенный с запоминающим устройством и управляющим входом управляющего элемента, причем данный программный модуль реагирует на появление аварийного происшествия, причем сразу после обнаружения программным модулем появления аварийного происшествия программный модуль проверяет отмену нормального управления полевым устройством посредством сравнения сигнала безопасного состояния с отслеженным аппаратным сигналом управления и передает программный сигнал управления на управляющий элемент.

7. Система по п. 6, отличающаяся тем, что управляющим элементом является клапан.

8. Система по любому из пп. 6 или 7, дополнительно содержащая:

преобразовательное устройство, функционально соединенное с аппаратным модулем, программным модулем и управляющим элементом.

9. Система по любому из пп. 6 или 7, в которой преобразующее устройство является преобразователем ток-давление (I/P) или напряжение-давление (E/P).

10. Система по любому из пп. 6 или 7, отличающаяся тем, что аппаратный сигнал управления передается преобразующему устройству.

11. Система по любому из пп. 6 или 7, отличающаяся тем, что программный сигнал управления передается преобразующему устройству.

12. Система по любому из пп. 6 или 7, дополнительно содержащая:

датчик, функционально соединенный с аппаратным модулем, для обнаружения возникновения аварийного происшествия, причем сразу после обнаружения возникновения аварийного происшествия, датчик инициирует передачу аппаратного сигнала управления на управляющий элемент, и датчик, функционально связанный с программным модулем для обнаружения возникновения аварийного происшествия, причем сразу после обнаружения возникновения аварийного происшествия, датчик

инициирует передачу программного сигнала управления на управляющий элемент.

13. Система по любому из пп. 6 или 7, отличающаяся тем, что проверка отмены нормального управления полевым устройством включает сравнение аппаратного сигнала управления с сигналом безопасного состояния.

14. Система по любому из пп. 6 или 7, отличающаяся тем, что программный модуль регистрирует обнаруженный отказ аппаратного модуля, если аппаратный сигнал управления не эквивалентен сигналу безопасного состояния.

15. Система по любому из пп. 6 или 7, отличающаяся тем, что аппаратный модуль классифицируется как устройство типа А, а программный модуль классифицируется как устройство типа Б.

16. Процессор, соединенный с материальным энергонезависимым машиночитаемым носителем информации и способный выполнять сохраняемые в указанном машиночитаемом носителе информации кодированные команды, причем команды побуждают процессор:

обнаруживать программным модулем возникновение аварийного происшествия, связанного с полевым устройством автоматической системы безопасности;

отслеживать программным модулем отмену аппаратным модулем нормального управления полевым устройством для перевода полевого устройства в безопасное состояние, причем отслеживание отмены включает то, что аппаратный модуль вырабатывает аппаратный сигнал управления;

проверять программным модулем отмену аппаратным модулем нормального управления полевым устройством, причем проверка отмены включает в себя сравнение сигнала безопасного состояния с аппаратным сигналом управления; и

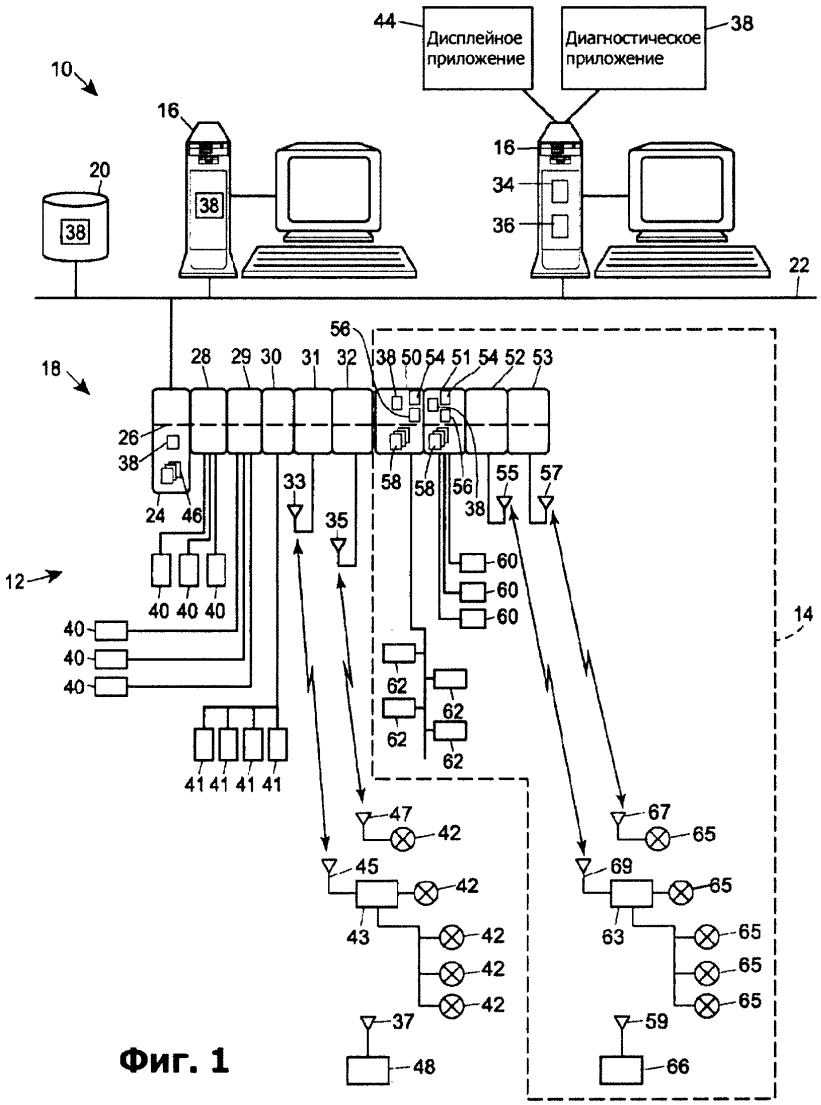
передавать программным модулем программный сигнал управления для перевода полевого устройства в безопасное состояние.

17. Процессор по п. 16, выполненный с возможностью исполнения дополнительной кодированной команды, сохраняемой в указанном машиночитаемом носителе информации, побуждающей процессор:

записывать программным модулем проверку отмены нормального управления полевым устройством.

1

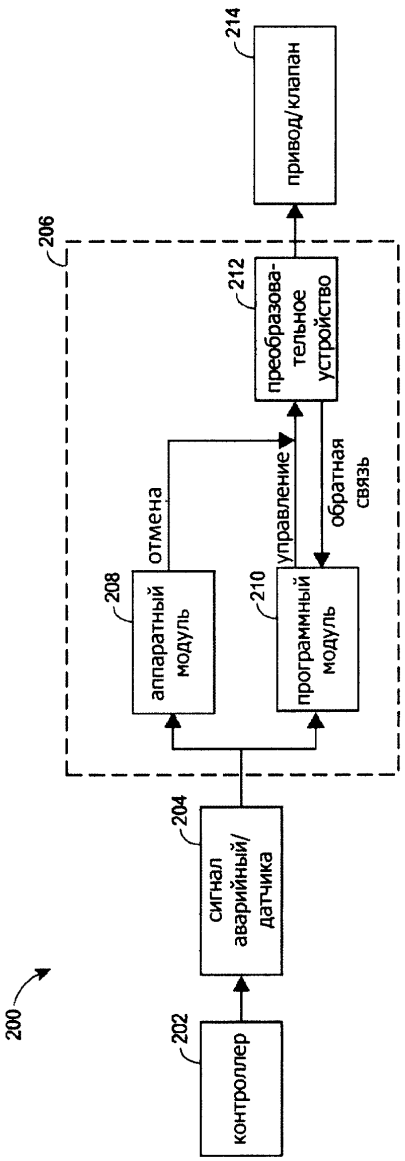
1


44
Дисплейное приложение
Диагностическое приложение
38
10
16
20
38
16
34
36
22
18
56
28 29 30 31 32 38 50 54 51 54 52 53
26
38
24 46
33
35
58 58 56 38 55 57
12
40 40 40
40
40
40
60
60
60
14
62
62
62
62
41 41 41 41
47
42
45
42
43
42
42
42
37
48
67
65
69
65
63
65
65
65
59
66

Фиг. 1

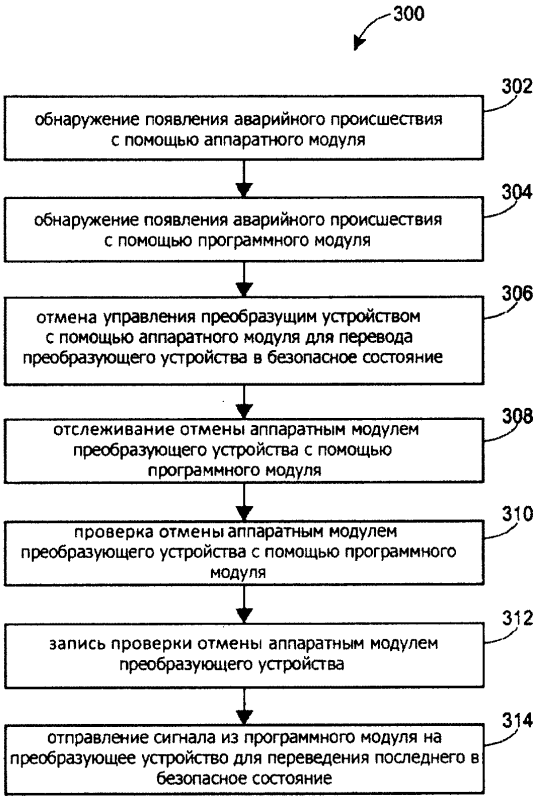
2

2


200
202
контроллер
204
сигнал аварийный/ датчика
206
208
аппаратный модуль
210
программный модуль
212
преобразова-тельное устройство
214
привод/клапан
отмена
управление
обратная связь

Фиг. 2

3


300
302
обнаружение появления аварийного происшествия с помощью аппаратного модуля
304
обнаружение появления аварийного происшествия с помощью программного модуля
306
отмена управления преобразущим устройством с помощью аппаратного модуля для перевода преобразующего устройства в безопасное состояние
308
отслеживание отмены аппаратным модулем преобразующего устройства с помощью программного модуля
310
проверка отмены аппаратным модулем преобразующего устройства с помощью программного модуля
312
запись проверки отмены аппаратным модулем преобразующего устройства
314
отправление сигнала из программного модуля на преобразующее устройство для переведения последнего в безопасное состояние

Фиг. 3