(19) Евразийское патентное ведомство

(11) 040908 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2022.08.15

(21) Номер заявки
201691185

(22) Дата подачи заявки
2015.09.24

(51) Int. Cl. ***H04L 29/06*** (2006.01)
G01D 4/00 (2006.01)

(54) ГЛОБАЛЬНАЯ СИСТЕМА УПРАВЛЕНИЯ (GMS), ИСПОЛЬЗУЮЩАЯ ЗАЩИЩЕННЫЕ ДАННЫЕ С ДОПОЛНИТЕЛЬНЫМИ АТРИБУТАМИ, И СПОСОБ ИХ СОЗДАНИЯ

(31) **62/063,534**
(32) **2014.10.14**
(33) **US**
(43) **2016.11.30**
(86) **PCT/EP2015/071967**
(87) **WO 2016/058802 2016.04.21**

(71)(73) Заявитель и патентовладелец:
СИКПА ХОЛДИНГ СА (CH)

(72) Изобретатель:
Финкель Чарльз (US), Кемпбелл Марк, Ван Нгок Ти Кристоф, Касе Джорджио, Кёблер Фридрих (CH)

(74) Представитель:
Абильманова К.С. (KZ)

(56) EP-A2-2660667
US-A1-2005039040
GB-A-2491237

(57) Изобретение относится к глобальной системе управления (GMS), использующей защищенные данные с дополнительными атрибутами, которые совместимы с внешней системой, в цепочке поставок нефтегазовых ресурсов, включая способ создания защищенных и верифицируемых данных для предотвращения фальсификации или ввода нежелательных данных, являющихся результатом несанкционированного доступа на протяжении цепочки поставок. Интерфейс создает и преобразует данные в цепочке поставок нефти и газа для совместимости с внешними системами. Датчик или устройство сбора данных промышленной системы управления получает собранные данные и передает их на защищенную промежуточную аппаратную платформу для взаимодействия с программным компонентом. Собранные данные затем модифицируются с применением обработчика бизнес-правил для создания расширенных данных и событий, созданных из расширенных данных.

040908 B1

040908 B1

Область техники

Настоящее изобретение, в общем, относится к системе и способу создания данных, совместимых с внешней системой, в цепочке поставок нефтегазовых ресурсов и, в частности, к интерфейсу и способу взаимодействия с защищенной промежуточной платформой для создания защищенных и верифицируемых данных для предотвращения фальсификации или ввода нежелательных данных, являющихся результатом несанкционированного доступа на протяжении цепочки поставок.

Уровень техники

Нефтегазовая промышленность обычно разделена на три сектора; апстрим, мидстрим и даунстрим, как изображено на фиг. 1. Сектор апстрим известен как сектор разведки и добычи. Сектор апстрим включает поиск и разведку потенциальных подземных или подводных залежей сырой нефти и природного газа (например, идентификация потенциальных запасов углеводородов), бурение разведочных скважин и, впоследствии, бурение и заканчивание скважин, извлекающих и выводящих на поверхность (добывающих) сырую нефть и/или неочищенный природный газ. Сектор мидстрим включает транспортировку (посредством трубопровода, железнодорожного транспорта, грузового транспорта и т.д.), хранение и оптовую торговлю сырыми или очищенными нефтепродуктами. Трубопроводы и другие многочисленные транспортные системы могут быть использованы для перемещения сырой нефти от мест добычи к перерабатывающим заводам и для подачи различных очищенных продуктов к дистрибьюторам в секторе даунстрим. Сектор даунстрим относится к очистке сырой нефти и к обработке и очистке неочищенного природного газа, а также к маркетингу и распределению продуктов, полученных из сырой нефти и природного газа. Сектор даунстрим предоставляет потребителям продукты, такие как бензин или моторное топливо, керосин, реактивное топливо, дизельное топливо, печное топливо, смазочные материалы, воски, асфальт, природный газ и сжиженный нефтяной газ, а также сотни нефтехимических продуктов.

В последние годы наблюдается значительное увеличение незаконной деятельности, связанной с нефтегазовыми ресурсами. Например, число хищений нефти и газа в таких регионах, как Техас и Мексика, выросло приблизительно в десять раз за последние десять лет. Коррупция, хищения, фальсификации, кражи и другая подобная незаконная деятельность происходит на всех фазах и секторах цепочки поставок, включая апстрим, мидстрим и даунстрим. Незаконные присоединения к трубопроводам, изменение маршрута транспортировки сырой нефти, угоны грузового транспорта, создание подземных туннелей и кража нефти на нефтеперерабатывающих заводах являются лишь некоторыми примерами незаконной деятельности, которые стали широко распространенными в данной промышленности. Из-за такого роста деятельности нефтегазовая промышленность столкнулась с несколькими проблемами. Например, происходящие события не всегда связаны друг с другом географически или другим образом и образуют цепочку разрозненных событий и происшествий. В настоящее время существует много разных решений и технологий для помощи в управлении, но они не являются однородными или совместимыми системами. Отсутствие координированной связи и прозрачности между регионами, функциями и командами создает различные трудности, и отсутствие возможности фиксации и отслеживания событий препятствует учету. Таким образом, становится сложно или вообще невозможно своевременно реагировать на такие события и происшествия.

Таким образом, существует потребность в предоставлении интеллектуальной системы управления, способной осуществлять контроль и отправлять отчеты или предупреждения о незаконной деятельности, направленной на нефтегазовые ресурсы, одновременно повышая надежность, безопасность, соблюдение установленных норм и ответственность за состояние окружающей среды. Дополнительно существует потребность в системе, предписывающей действия, связанные с ресурсами в секторах апстрим, мидстрим и даунстрим, путем удаленного осуществления контроля, анализа, прогнозирования событий для ресурсов и предоставления данных в качестве предупреждения для принятия решений из любого местоположения. Термин "ресурс", как определено в данном документе, включает все продукты переработки нефти и газа и инфраструктуру.

Сущность изобретения

Настоящее изобретение посредством одного или нескольких из своих различных аспектов, вариантов осуществления и/или специфических признаков или вспомогательных компонентов предоставляет различные системы, серверы, способы, носители и программы для взаимодействия с компилированными кодами, такими как, например, алгоритмы Java или интеллектуального анализа данных, или смесь аппаратных и программных элементов для создания данных с дополнительными атрибутами, применяемыми в глобальной системе управления (GMS), относящейся к управлению нефтегазовыми ресурсами. Данные с дополнительными атрибутами представляют собой расширенные данные, используемые для создания событий, применимых для создания сгруппированных событий в определенном модуле системы GMS.

Настоящее изобретение в общем относится к системе и способу для сбора данных из промышленных систем управления (ICS) и создания данных, совместимых с внешней системой, в цепочке поставок нефтегазовых ресурсов и, в частности, к интерфейсу и способу взаимодействия с защищенной промежуточной платформой для создания защищенных и верифицируемых данных для предотвращения фальсификации или введения нежелательных данных, являющихся результатом несанкционированного доступа на протяжении цепочки поставок.

В одном варианте осуществления предложен способ создания данных в цепочке поставок нефти и газа для совместимости с внешними системами, включающий получение собранных данных по меньшей мере из одного из промышленной системы управления, датчика и устройства сбора данных; хранение собранных данных в защищенной промежуточной аппаратной платформе для взаимодействия по меньшей мере с одним программным компонентом; и добавление атрибутов к собранным данным с применением обработчика бизнес-правил для создания расширенных данных, причем по меньшей мере часть собранных данных, отправленных на защищенную промежуточную платформу, принята по меньшей мере из одного из защищенного/проверенного датчика и защищенной/проверенной промышленной системы управления (ICS), соединенных с первым набором датчиков и устройств сбора данных, расположенных на протяжении цепочки поставок нефти и газа.

В другом варианте осуществления предложен интерфейс для создания данных в цепочке поставок нефти и газа для совместимости с внешними системами, включающий по меньшей мере одно из промышленной системы управления, датчика и устройства сбора данных для получения собранных данных; защищенная промежуточная аппаратная платформа для подписывания и хранения собранных данных с целью взаимодействия по меньшей мере с одним программным компонентом; и обработчик бизнес-правил для добавления атрибутов к собранным данным с целью создания расширенных данных, причем по меньшей мере часть собранных данных, отправленных на защищенную промежуточную платформу, принята по меньшей мере из одного из защищенного/проверенного датчика и защищенной/проверенной промышленной системы управления (ICS), соединенных с первым набором датчиков и устройств сбора данных, расположенных на протяжении цепочки поставок нефти и газа.

В еще одном варианте осуществления предложен постоянный машиночитаемый носитель, хранящий программу для создания данных в цепочке поставок нефти и газа для совместимости с внешними системами, причем программа при исполнении процессором включает получение собранных данных из по меньшей мере одного из промышленной системы управления, датчика и устройства сбора данных; подписывание и хранение собранных данных в защищенной промежуточной аппаратной платформе для взаимодействия по меньшей мере с одним программным компонентом; и добавление атрибутов к собранным данным с применением обработчика бизнес-правил для создания расширенных данных, причем по меньшей мере часть собранных данных, отправленных на защищенную промежуточную платформу, принята по меньшей мере из одного из защищенного/проверенного датчика и защищенной/проверенной промышленной системы управления (ICS), соединенных с первым набором датчиков и устройств сбора данных, расположенных на протяжении цепочки поставок нефти и газа.

В одном аспекте по меньшей мере часть расширенных данных, созданных с применением обработчиков бизнес-правил, преобразована в события.

В другом аспекте расширенные данные или события, основанные на расширенных данных, подписываются или шифруются по меньшей мере одним из аппаратного или программного модуля (модулей) защиты.

В еще одном аспекте способ включает защищенный сбор и верификацию собранных данных по меньшей мере из одного из промышленной системы управления, датчика и устройства сбора данных с применением по меньшей мере одного из защищенных/проверенных датчиков и ICS.

В еще одном аспекте способ включает проверку собранных и верифицированных данных для подтверждения точности информации в собранных данных перед передачей на защищенную промежуточную аппаратную платформу.

В другом аспекте способ включает обеспечение защиты защищенной промежуточной аппаратной платформы по меньшей мере от одного из фальсификации, ввода нежелательных данных и несанкционированного доступа.

В другом аспекте дополнительные атрибуты расширенных данных включают по меньшей мере один защищенный атрибут, позволяющий обнаруживать модификацию или повреждение расширенных данных и определять подлинность расширенных данных.

В одном аспекте по меньшей мере один программный компонент защищенным образом отправляет расширенные данные с дополнительными атрибутами в модуль интеграции данных.

В еще одном аспекте обработчик бизнес-правил хранит расширенные данные и создает очередь из них в зашифрованном и долгосрочном хранилище данных.

В еще одном аспекте расширенные данные с дополнительными атрибутами сообщаются с внешней системой посредством интерфейса.

В другом аспекте способ включает избыточную проверку или получение, усреднение и верификацию собранных данных по меньшей мере из одного из промышленной системы управления (ICS), датчика и устройства сбора данных с применением по меньшей мере одного из защищенных/проверенных датчиков и ICS для подтверждения точности информации.

В другом аспекте при получении и передаче собранных данных применяются системные драйвера для сбора данных по меньшей мере из одного из физического источника, датчика, программируемого логического контроллера, удаленных терминальных устройств и ICS.

В еще одном аспекте промышленные системы управления (ICS) предназначены для секторов апст-

рим, мидстрим и даунстрим цепочки поставок нефтегазовых ресурсов.

В еще одном аспекте каждая из промышленных систем управления для секторов апстрим, мидстрим и даунстрим сгруппирована в виде одного репозитория.

В еще одном аспекте собранные данные из каждой промышленной системы управления отправляются на защищенную промежуточную платформу по меньшей мере от одного из защищенных/проверенных датчиков и ICS в форме по меньшей мере одного из защищенных данных, отдельно отформатированных данных, совместно отформатированных данных, данных с защищенными атрибутами, данных, предназначенных только для чтения, и данных, защищенных от подделки.

В другом аспекте взаимодействие включает передачу собранных данных из промышленной системы управления в модуль интеграции данных посредством защищенной промежуточной аппаратной платформы по защищенной связи для обеспечения целостности собранных данных.

В другом аспекте способ включает обеспечение защиты по меньшей мере одного из защищенных/проверенных датчиков и ICS по меньшей мере от одного из фальсификации, ввода нежелательных данных и несанкционированного доступа.

В еще одном аспекте по меньшей мере одно из защищенных/проверенных датчиков и ICS включает по меньшей мере одно из самодиагностики, самопроверки достоверности, оповещения и обнаружения отклонений, а также уникальных идентификаторов для надежного шифрования собранных данных.

В одном аспекте способ включает прием защищенным образом собранных и верифицированных расширенных данных в модуле интеграции данных по меньшей мере от одного из защищенных/проверенных датчиков и ICS, и защищенной промежуточной платформы и сбор и/или организацию расширенных данных и событий, созданных из расширенных данных, в сгруппированные события в глобальной системе управления; выполнение в центре управления по меньшей мере одного из контроля предупреждений, создания предупреждений и предоставления решения на основе сгруппированных событий, созданных в системе управления данными; отображение, в центре управления, визуального представления сгруппированных событий и обеспечение взаимодействия посредством центра управления для установления сообщения по меньшей мере с одним из модуля интеграции данных, службы внешней эксплуатационной поддержки, персонала и производственного оборудования.

Краткое описание графических материалов

Настоящее изобретение далее описано в следующем подробном описании со ссылкой на упомянутое множество графических материалов путем неограничивающих примеров предпочтительных вариантов осуществления настоящего изобретения, в которых подобные условные обозначения представляют подобные элементы на нескольких видах графических материалов.

На фиг. 1 показана приведенная в качестве примера цепочка поставок для использования в нефтегазовой промышленности,

на фиг. 2 - приведенная в качестве примера система для использования согласно вариантам осуществления, описанным в данном документе,

на фиг. 3 - еще одна примерная схема глобальной системы управления согласно описанному варианту осуществления,

на фиг. 4 - приведенный в качестве примера вариант осуществления связи между системой управления данными и центром управления согласно варианту осуществления изобретения,

на фиг. 5 - примерная схема глобальной системы управления согласно описанному варианту осуществления,

на фиг. 6 - приведенная в качестве примера схема интерфейса согласно одному варианту осуществления изобретения,

на фиг. 7A-7D - приведенная в качестве примера последовательность событий, в которых получение данных происходит с течением времени для определения вероятности,

на фиг. 8 - приведенная в качестве примера схема интерфейса согласно одному варианту осуществления изобретения,

на фиг. 9 - приведенный в качестве примера вариант осуществления технологического маршрута интерфейса согласно одному варианту осуществления изобретения.

Подробное описание

Настоящее изобретение посредством одного или нескольких из своих различных аспектов, вариантов осуществления и/или специфических признаков или вспомогательных компонентов, таким образом, предназначено для предоставления одного или нескольких преимуществ, как особо указано ниже.

На фиг. 2 показана приведенная в качестве примера система для использования согласно вариантам осуществления, описанным в данном документе. Система 100 изображена в общем виде и может содержать компьютерную систему 102, обозначенную в общем виде. Компьютерная система 102 может работать в качестве автономного устройства или может быть присоединена к другим системам или периферийным устройствам. Например, компьютерная система 102 может содержать одно или несколько из следующего: компьютеры, серверы, системы, сети связи или облачная среда, или являться их частью.

Компьютерная система 102 может работать в качестве сервера в сетевой среде или в качестве пользовательского компьютера клиента в сетевой среде. Компьютерная система 102 или ее части могут быть

реализованы в виде различных устройств или встроены в различные устройства, такие как персональный компьютер, планшетный компьютер, телевизионная абонентская приставка, персональный цифровой помощник, мобильное устройство, карманный компьютер, портативный компьютер, настольный компьютер, устройство связи, беспроводной телефон, персональное доверенное устройство, веб-устройство или любая другая машина, способная выполнять набор команд (последовательных или других), определяющих действия, выполняемые этим устройством. Кроме того, хотя изображена одна компьютерная система 102, дополнительные варианты осуществления могут включать любую совокупность систем или вспомогательных систем, которые по отдельности или совместно выполняют команды или осуществляют функции.

Как изображено на фиг. 2, компьютерная система 102 может содержать по меньшей мере один процессор 104, такой как, например, центральный процессор, графический процессор или и то, и другое. Компьютерная система 102 также может содержать компьютерное запоминающее устройство 106. Компьютерное запоминающее устройство 106 может включать статическое запоминающее устройство, динамическое запоминающее устройство или и то, и другое. Компьютерное запоминающее устройство 106 в качестве дополнения или альтернативы может включать жесткий диск, оперативное запоминающее устройство, кэш-память или любую их комбинацию. Разумеется, специалистам в данной области будет очевидно, что компьютерное запоминающее устройство 106 может включать любую комбинацию известных запоминающих устройств или одно устройство хранения данных.

Как показано на фиг. 2, компьютерная система 102 может содержать компьютерный дисплей 108, такой как жидкокристаллический дисплей, дисплей на основе органических светодиодов, индикаторную панель, твердотельный индикатор, электронно-лучевую трубку, плазменный дисплей или любой другой известный дисплей.

Компьютерная система 102 может содержать по меньшей мере одно компьютерное устройство 110 ввода, такое как клавиатура, устройство дистанционного управления, содержащее беспроводную клавишную панель, микрофон, присоединенный к обработчику распознавания речи, камеру, такую как видеокамера или фотоаппарат, устройство управления курсором, сенсорный экран или любую их комбинацию. Специалистам в данной области будет очевидно, что различные варианты осуществления компьютерной системы 102 могут содержать несколько устройств 110 ввода. Более того, специалистам в данной области также будет очевидно, что вышеуказанный перечень приведенных в качестве примера устройств 110 ввода не является исчерпывающим и что компьютерная система 102 может содержать любые дополнительные или альтернативные устройства 110 ввода.

Компьютерная система 102 также может содержать устройство 112 для считывания носителей и сетевой интерфейс 114. Кроме этого, компьютерная система 102 может содержать любые дополнительные устройства, источник питания, компоненты, части, периферийные устройства, аппаратное обеспечение, программное обеспечение или любую их комбинацию, которые являются общеизвестными и расцениваются как относящиеся к компьютерной системе или включенные в нее, такие как, например, но без ограничения, устройство 116 вывода. Устройство 116 вывода может представлять собой, но без ограничения, динамик, аудиовыход, видеовыход, выход дистанционного управления или любую их комбинацию.

Все компоненты компьютерной системы 102 могут быть взаимосвязанными и обмениваться данными посредством шины 118. Как изображено на фиг. 2, все компоненты могут быть взаимосвязаны и обмениваться данными посредством внутренней шины. Тем не менее, специалистам в данной области будет очевидно, что любые из компонентов также могут быть соединены посредством шины расширения. Более того, шина 118 может позволить осуществлять обмен данными посредством любого стандарта или другой спецификации, являющейся общеизвестной и изученной, такой как, без ограничения, шина PCI, шина PCI-express, интерфейс PATA, интерфейс SATA и т.д.

Компьютерная система 102 может сообщаться с одним или несколькими дополнительными компьютерными устройствами 120 по сети 122. Сеть 122 может представлять собой, но без ограничения, локальную сеть, глобальную сеть, Интернет, телефонную сеть или любую другую сеть, хорошо известную и изученную в данной области техники. Сеть 122, изображенная на фиг. 2, представляет собой беспроводную сеть. Тем не менее, специалистам в данной области будет очевидно, что сеть 122 также может представлять собой проводную сеть.

Дополнительное компьютерное устройство 120 изображено на фиг. 2 в виде персонального компьютера. Тем не менее, специалистам в данной области будет очевидно, что в альтернативных вариантах осуществления настоящей заявки устройство 120 может представлять собой портативный компьютер, планшетный ПК, персональный цифровой помощник, мобильное устройство, карманный компьютер, настольный компьютер, устройство связи, беспроводной телефон, персональное доверенное устройство, веб-устройство, телевизор с одним или более процессорами, встроенными в него и/или присоединенными к нему, или любое другое устройство, способное исполнять набор команд, последовательных или других, определяющих действия, выполняемые этим устройством. Разумеется, специалистам в данной области будет очевидно, что вышеперечисленные устройства являются лишь приведенными в качестве примера устройствами, и что устройство 120 может представлять собой любое дополнительное устройство или приспособление, являющееся общеизвестным и изученным в данной области техники, в преде-

лах объема настоящей заявки. Более того, специалистам в данной области подобным образом будет очевидно, что устройство может представлять собой любую комбинацию устройств и приспособлений.

Разумеется, специалистам в данной области будет очевидно, что вышеперечисленные компоненты компьютерной системы 102 приведены лишь в качестве примера и не должны расцениваться как исчерпывающие и/или всеобъемлющие. Более того, примеры компонентов, перечисленных выше, также приведены в качестве примера и не должны расцениваться как исчерпывающие и/или всеобъемлющие.

На фиг. 3 показана примерная схема глобальной системы управления согласно описанному варианту осуществления. На схеме показан поток данных от начального обнаружения и сбора данных в секторах апстрим, мидстрим и даунстрим, включая любое необходимое вмешательство на месте происшествия, которое может быть выполнено в результате осуществления контроля и предупреждений, предоставленных центром командования и управления ССС. В пределах каждого потока (сектора) находятся несколько технологий, ресурсов и поколений ресурсов. Эти технологии не объединены и, следовательно, не отслеживаются вместе. Интеграция интерфейсов собранных данных между различными технологиями и системами предоставляет связь между технологиями и системами, обладающими разными протоколами, и интегрирует внешние системы, такие как ERP-системы и т.п. Интегрированные данные форматируются, хранятся и анализируются для использования центром (командования и) управления ССС. Центр управления ССС предоставляет обзор собранных данных путем осуществления контроля над данными, предоставленными системой управления данными, предупреждая на уровне центра управления (и персонала, при необходимости) о событиях или последствиях событий и осуществляя диагностику и анализ данных. В необходимой степени вмешательство со стороны персонала службы охраны и аварийной службы, БПЛА (беспилотные летательные аппараты), удаленных камер и любого другого ресурса, способного вмешиваться или осуществлять меры, направленные на вмешательство, может осуществляться после установления контакта и информирования о результатах из центра управления ССС. Данные, собранные и извлеченные БПЛА или видеокамерами, хранятся в репозитории (репозиториях) системы для использования в будущем анализе.

Более конкретно, глобальная система управления GMS (фиг. 5) управляет нефтегазовыми ресурсами защищенным образом (или незащищенным образом, при желании) путем контроля незаконной деятельности в цепочке поставок, предупреждения органов власти и/или уполномоченного персонала и реагирования на незаконную деятельность соответствующим образом. Например, система может предупреждать органы власти и/или авторизованный персонал, предоставлять письменный отчет полиции или персоналу аварийной службы, прогнозировать или предсказывать данные, автоматически предоставлять рекомендации и/или ответные действия. Следует понимать, что предоставленные примеры являются неограничивающими и что может быть предоставлено любое количество ответных действий, как предполагается в данной области техники. Также следует понимать, что глобальная система управления GMS не ограничена управлением незаконной деятельностью, но также может использоваться при подозрительной деятельности, чрезвычайных ситуациях, происшествиях, постороннем вмешательстве или для любого другого применения, обычно предусмотренного системой управления. Также следует понимать, что в ходе осуществления контроля система может обнаружить, что деятельность, оказывается, совершенно не является незаконной или подозрительной, или представляет собой результат технической проблемы, связанной с системой или событием. Дополнительно, как подробно описано ниже, центр управления ССС использует данные с течением времени для обнаружения и расчета тенденций и будущих событий в сгруппированных событиях. В связи с этим, персонал в центре управления ССС может быть предупрежден перед возникновением таких событий, по достижении определенного уровня вероятности. Также, как подробно описано ниже, центр управления ССС отображает (например, на ЖК дисплее) предупреждения (в дополнение к обычной деятельности), отражающие отслеживаемые события или происшествия. Предупреждения могут использоваться персоналом для того, чтобы связаться с персоналом аварийной службы или для осуществления вмешательства на месте происшествия, и могут автоматически подаваться центром управления ССС персоналу аварийной службы, если авторизованный персонал не отвечает на такие предупреждения в заданный период времени или после повторных предупреждений.

Глобальная система управления GMS получает информацию от датчика (датчиков) и устройства (устройств) сбора данных, расположенных в различных географических местоположениях и областях. Эти датчики могут представлять собой хорошо известный датчик или устройство сбора данных любого типа, способное воспринимать или собирать данные, при условии, что он предназначен для получения таких данных. Датчики выполнены с возможностью получения и сбора данных, связанных с нефтегазовыми ресурсами, перемещающимися по цепочке поставок, при этом данные включают, без ограничения, по меньшей мере одно из перечисленного: температуру, плотность, влажность, объем, силу тяжести, химический состав, давление, вес, изменение давления в трубопроводе, разницу в весе транспортного средства или в объеме топлива, определение местонахождения по GPS, синхронизацию местонахождения транспортного средства, географическую область, скорость потока, удельную проводимость, реологию, мутность, формирование изображений, термическое формирование изображений. Дополнительно датчики могут воспринимать и собирать информацию о состоянии датчика (т.е. о неисправной работе, отсоединении и т.д.), показаниях тензометрических датчиков, данных о погодных условиях, дорожных усло-

виях, состояниях транспортного средства или дороги, скорости ветра, барометрических условий, количестве атмосферных осадков, данных о техническом обслуживании или дате технического обслуживания, информацию о персональном местоположении (например, местоположение ближайшей пожарной станции или полицейского участка), данные из радаров, детекторов движения, радиочастотные данные, акустические данные, местоположение по GPS, данные, извлеченные из беспилотных летательных аппаратов (БПЛА), стоимость запасов нефтепродуктов и т.д. Информация также может собираться устройствами сбора данных. Например, информация и данные, содержащиеся в репозитории SAP™ или Oracle™, которые могут представлять собой любые данные, такие как прогноз, данные о покупке продуктов, налоговую ставку и т.д.

Датчики и устройства сбора данных (воспринимающие и собирающие данные в виде защищенных (или незащищенных) измерений) могут быть расположены в секторе апстрим, секторе мидстрим и/или секторе даунстрим цепочки поставок нефтегазовых ресурсов. Данные собираются и передаются в шлюз (фиг. 7). Шлюз представляет собой устройство сбора данных из различных источников (например, ICS, такой как SCADA, при этом указанная ICS использует протоколы, такие как MODBUS, AS-iOPC, EtherCAT и т.д.) и включает обработчик бизнес-правил (BRE). Шлюз также может собирать данные непосредственно из датчиков, устройств сбора данных или любого устройства, предоставляющего данные из секторов апстрим, мидстрим и даунстрим. Собранные данные могут быть преобразованы в защищенные (или дополнительно защищенные) данные, включающие, например, временную метку и различные атрибуты. Когда данные преобразованы шлюзом, данные отправляются (предпочтительно защищенным образом) в модуль интеграции данных. В качестве дополнения или альтернативы, собранные данные могут быть сохранены в репозитории или нескольких репозиториях и затем отправлены в систему управления данными, где из данных будут созданы сгруппированные события. Также следует понимать, что собранные данные не обязательно должны быть получены из источников, перечисленных выше, но могут быть получены из любого внутреннего или внешнего источников данных.

В некоторых вариантах осуществления дополнительные защищенные и проверенные датчики и/или ICS, такие как защищенные программируемые логические контроллеры (PLC) или защищенные системы SCADA используются при получении данных в секторах апстрим, мидстрим или даунстрим цепочки поставок нефти и газа, причем они могут отправлять свои данные непосредственно в шлюз (или альтернативно в модуль интеграции данных при отсутствии шлюза). Например, данные, собранные из датчиков (и/или устройств сбора данных) секторов апстрим, мидстрим и даунстрим, которые обработаны системами SCADA, также передаются на защищенные и проверенные датчики и/или ICS, а затем в интерфейс шлюза. В альтернативном варианте осуществления защищенные и проверенные датчики и/или ICS заменяют промышленную систему управления (такую как незащищенная система SCADA) и собирают данные непосредственно из датчиков секторов апстрим, мидстрим и даунстрим (фиг. 5). Хотя все датчики (и/или устройства сбора данных) секторов апстрим, мидстрим и даунстрим можно было бы заменить в системе защищенными/проверенными датчиками и/или ICS, это привело бы к очень значительным затратам денег и времени. Соответственно, в одном варианте осуществления защищенные/проверенные датчики и ICS заменяют существующие датчики и/или устройства сбора данных в заданных точках или узлах системы. В другом варианте осуществления защищенные/проверенные датчики и ICS размещают в новых местах в системе. Новые добавленные защищенные/проверенные датчики и ICS могут собирать или получать информацию от одного или более существующих датчиков или устройств сбора данных, уже установленных в системе. Защищенные/проверенные датчики и ICS имеют атрибуты, включающие, но без ограничения, защищенное аппаратное обеспечение, возможности самодиагностики, функции самопроверки достоверности, возможности оповещения, обнаружения отклонений и сообщения о них, защиту от несанкционированного доступа и уникальный идентификатор, который защищенным образом шифрует данные, принятые от стандартных или традиционных датчиков и устройств сбора данных, уже используемых в системе.

Описание не имеющих ограничительного характера примеров датчиков и ICS, которые могут быть использованы в системе, представлено ниже. Следует понимать, что описание приведено лишь в качестве пояснения, и что любое количество коммерчески доступных датчиков и/или ICS может быть представлено защищенным и проверенным образом с возможностями атрибутов (всех, некоторых и/или дополнительных), перечисленных выше.

Программируемый логический контроллер, PLC, или программируемый контроллер может быть использован в качестве ICS. PLC представляет собой компьютер промышленного применения, обычно используемый для автоматизации промышленных электромеханических процессов, таких как контроль над оборудованием на заводе. PLC применяются в различных отраслях промышленности, а также в машинах, в качестве недорогой и адаптируемой альтернативы специализированным микроконтроллерам. PLC разработаны для множества аналоговых и цифровых устройств ввода и вывода, расширенных температурных диапазонов, а также характеризуются устойчивостью к электрическому шуму, вибростойкостью и ударопрочностью. PLC непрерывно контролирует состояние подключенных устройств ввода и исполняет логические команды на основе настраиваемой программы для управления состоянием устройств вывода. Программы PLC для управления работой машин обычно хранятся в имеющем резервное

батарейное питание или энергонезависимом запоминающем устройстве. Один тип PLC представлен встроенным в ПК контроллером серий CX5010, CX5020 с процессором Intel® Atom™, изготовленный компанией Beckhoff Automation GmbH. Контроллер CX5010 имеет процессор Intel® Atom™ Z510 с тактовой частотой 1,1 ГГц, а контроллер CX5020 имеет процессор Intel® Atom™ Z530 с тактовой частотой 1,6 ГГц.

Типы датчиков могут включать, но без ограничения, акустический датчик, звуковой датчик, вибрационный датчик, автомобильный датчик, датчик обнаружения транспортных средств, химический датчик, датчик электрического тока, датчик электрического потенциала, магнитный датчик, радиодатчик, датчик для измерения условий окружающей среды, метеорологический датчик, датчик влаги, датчик влажности, датчик расхода, датчик скорости текучей среды, датчик ионизирующего излучения, датчик субатомных частиц, датчик навигационной системы, датчик положения, датчик угла поворота, датчик перемещения, датчик расстояния, датчик скорости, датчик ускорения, оптический датчик, светочувствительный датчик, датчик системы формирования изображений, датчик фотонов, датчик давления, датчик силы, датчик плотности, датчик уровня, термодатчик, тепловой датчик, датчик температуры, бесконтактный датчик, датчик обнаружения и т.д. Одним типом примерного датчика является радиолокационный датчик di-soric™ RS 40 M 6000 G8L-IBS. Датчик выполнен с возможностью бесконтактного обнаружения приближающихся и удаляющихся объектов, например продуктов на конвейере, на расстоянии до 6 м. Диапазон обнаружения и расширение импульса датчика являются регулируемыми, причем его устанавливают позади неметаллических материалов, переключающие устройства для обнаружения приближения и расстояния могут быть использованы вне помещений и размещены в надежном металлическом корпусе. В одном примерном варианте осуществления встроенный в ПК контроллер CX5010 или CX5020 может быть применен для реализации PLC или PLC/управление перемещениями (с визуальным представлением или без). Таким образом, PLC применяют в примерном варианте осуществления для логического определения (проверки) того, что датчик di-soric™ функционирует надлежащим образом и правильно обнаруживает объекты, движущиеся по конвейеру. Например, PLC может сравнивать данные, принятые от радиолокационного датчика di-soric™ RS 40 M 6000 G8L-IBS, с данными от соседнего независимого датчика обнаружения объектов, такого как фотоэлектрический датчик Tri-Tronics SMARTEYE® EZ-PRO, который обнаруживает объекты при их прохождении через излучаемый луч света или обеспечивает изменение характеристики отраженного света при их прохождении через луч. Если фотоэлектрический датчик обнаружил объекты, а радиолокационный датчик - нет, то один или оба из датчиков могут быть неисправны или неверно настроены, и может быть инициирована соответствующая система оповещения. В самом простом примерном варианте осуществления, поскольку PLC в большей или меньшей степени представляет собой выделенный контроллер, он будет многократно осуществлять внутреннюю программу. Один цикл программы включает, например, считывание входных данных с других модулей (например, датчика), исполнение логических команд на основе входных данных, а затем соответствующее обновление выходных данных. Запоминающее устройство в CPU хранит программу, а также поддерживает состояние ввода/вывода и обеспечивает средство для хранения значений. Как понятно специалисту в данной области техники, в текущей системе может быть использован любой PLC, и настоящее раскрытие не ограничено вышеописанными примерными вариантами осуществления. Дополнительно информация, собранная и выведенная защищенным датчиком или ICS, может быть защищена цифровыми средствами с применением, например, симметричных цифровых подписей. Алгоритмы с симметричным ключом представляют собой класс алгоритмов для шифрования, в котором используются одни криптографические ключи как для шифрования открытого текста, так и для расшифровывания зашифрованного текста. При практическом применении ключи представляют собой секрет, разделенный между двумя или более сторонами, который может быть использован для сохранения линии передачи конфиденциальной информации. Конечно, настоящее раскрытие не ограничено применением симметричных цифровых подписей. Скорее может быть использован любой известный метод шифрования. Например, микропроцессор Freescale™ i.MX537 предназначен для применения в перспективных промышленных и медицинских областях применения и включает криптографический ускоритель SAHARA (ускоритель генерации случайных чисел и симметричного/асимметричного хеширования). Указанный микропроцессор содержит генератор случайных чисел, защищенное запоминающее устройство, поддерживает применение различных стандартных шифров и хеш-функций, а также может защищенным образом хранить ключи AES и зашифровывать данные с их помощью.

В одном не имеющем ограничивающего характера примерном варианте осуществления защищенные/проверенные датчики и ICS выполнены с возможностью создания симметричной цифровой подписи для данных. В целях пояснения считается, что указанные устройства (например, защищенные/проверенные датчики и ICS), установленные в системе, находятся в небезопасной среде, при этом центральный сервер установлен в безопасной среде. Перед установкой создается ключ AES. Ключ AES передается в защищенный датчик или ICS и хранится в центральном сервере. Различные ключи могут быть созданы для каждого устройства. После создания ключа защищенный датчик или ICS может быть затем установлен в небезопасной среде. Для определения подлинности и предотвращения фальсифика-

ции данных, передаваемых защищенным датчиком или ICS на сервер, подпись данных создается защищенным датчиком или ICS, причем подпись может представлять собой хеш-сумму данных, которые должны быть подписаны. Указанная хеш-сумма создается в криптопроцессоре SAHARA с применением, например, стандартного алгоритма хеширования (например, SHA-224). Хеш-сумма затем шифруется с помощью криптопроцессора SAHARA с применением встроенного ключа AES. Зашифрованная хеш-сумма становится цифровой подписью. Затем данные отправляются в центральный сервер с цифровой подписью и идентификатором устройства, подписавшего данные. После того как центральный сервер получает ключ AES с применением идентификатора устройства, цифровая подпись затем расшифровывается с применением указанного ключа AES. Подпись является подлинной, если расшифрованная хеш-сумма совпадает с хеш-суммой, повторно созданной из данных, подлинность которых должна быть проверена. После того как данные подписаны, гарантируются подлинность и целостность данных. В крупномасштабных проектах, в которых объем данных, которые должны быть подписаны, слишком велик для обработки в режиме реального времени одним процессором, можно распределить вычислительную нагрузку по нескольким защищенным датчикам или ICS или хранить данные во временном буфере до наступления возможности их обработки и доставки в более позднее время. Однако следует понимать, что может быть применен любой известный метод шифрования, и система не ограничена описанными в настоящем документе методами.

Модуль интеграции данных содержит систему управления данными, которая хранит данные, получает данные из хранилища, создает структуру данных, содержащих ключевые значения, из данных, сортирует структуру данных и анализирует структурированные данные, используя вычислительные модели и алгоритмы для идентификации событий. Структурированные данные также проверяются на целостность и защищенность с целью обнаружения фальсификации. Группы связанных событий создаются системой управления данными для использования центром управления CCC. Центр управления CCC (который может содержать процессор(ы), программное обеспечение, интерфейс(ы) и несколько дисплеев, и/или персонал для управления и распоряжения информацией в глобальной системе управления GMS, и/или, например, любые из компонентов, описанных на фиг. 2, и которые могут быть расположены локально или удаленно в любом географическом местоположении, мобильным или иным образом) осуществляет контроль над событиями и предупреждениями, создает предупреждения и предоставляет решения, основанные на сгруппированных событиях, созданных в системе управления данными. Центр управления также обеспечивает связь с внешней эксплуатационной поддержкой и персоналом и ресурсами.

Вычислительные модели и алгоритмы, используемые в глобальной системе управления GMS, не ограничены любой определенной моделью или алгоритмом. Вместо этого следует понимать, что любое количество решений может использоваться в этой системе. Тем не менее, в качестве примера может быть применен алгоритм интеллектуального анализа данных, представляющий собой набор эвристических правил и вычислений, который создает из данных модель добычи данных. Для создания модели алгоритм, в первую очередь, анализирует предоставленные данные и ищет типы закономерностей или тенденций. Алгоритм использует результаты анализа для определения оптимальных параметров для создания модели интеллектуального анализа данных. Эти параметры затем применяются ко всему набору данных для извлечения закономерностей, требующих принятия мер, и подробной статистики. Модель интеллектуального анализа данных, созданная алгоритмом из собранных данных, может принимать различные формы, включая набор групп (например, сгруппированных событий), описывающих связь между случаями (например, события), в наборе данных; дерево решений, прогнозирующее результат и описывающее, как разные критерии влияют на этот результат. Используя данные, интеллектуально проанализированные алгоритмами, система способна применять исторические данные и улучшать точность с течением времени. Точности также может способствовать осуществление человеком или БПЛА, таким как дроны, верификации предупреждений, созданных системой.

На фиг. 4 показан приведенный в качестве примера вариант осуществления связи между системой управления данными и центром управления согласно варианту осуществления изобретения. Система управления данными предоставляет данные, классификацию событий и рекомендации в режиме реального времени в центр управления CCC на основании проанализированных собранных данных, как описано выше и будет описано далее. Центр управления CCC подтверждает классификации событий и отвечает отправкой уведомления в систему управления данными, которое может быть защищенным образом зарегистрировано с помощью временной метки. Центр управления CCC также обеспечивает осуществление контроля над событиями и предупреждениями, создает предупреждения и предоставляет решение на основании сгруппированных событий, созданных системой управления данными. Уведомления и предупреждения могут быть отправлены, например, персоналу, расположенному в центре управления CCC или расположенному удаленно, с помощью любого количества интерфейсов. Интерфейсы могут передавать информацию в виде зрительной информации, звуковой информации или в любой другой форме и могут передаваться с помощью мобильных устройств, а также стационарных устройств. Центр управления также обеспечивает связь с внешней эксплуатационной поддержкой и персоналом и ресурсами. Например, внешняя эксплуатационная поддержка и персонал могут обеспечивать вмешательство на месте

для верификации точности предупреждений (например, верифицировать факт взрыва, кражи материала), и БПЛА могут быть мобилизированы и отправлены с целью верификации в конкретную область, относящуюся к предупреждениям, и могут обеспечивать визуальное представление для улучшения полезности анализа сгруппированных событий.

На фиг. 5 показана примерная схема глобальной системы управления согласно описанному варианту осуществления. Глобальная система управления GMS содержит, без ограничения, центр управления CCC, систему управления данными, модуль интеграции данных, пользовательский интерфейс, интерфейс шлюза и датчики или устройства сбора данных, используемые для получения данных из секторов апстрим, мидстрим и даунстрим. Дополнительно GMS содержит защищенные/проверенные датчики и/или ICS, которые используются для дополнительной защиты и верификации данных, собранных с датчиков и устройств сбора данных, как описано выше. Глобальная система управления GMS также может содержать или охватывать внешние ресурсы, такие как ERP-системы, системы управления месторождением и ресурсами, приложения для упреждающего и предписывающего анализа, системы управления событиями, основанные на доказательном подходе, и существующие наследственные системы. Следует понимать, что глобальная система управления GMS не ограничена описанными компонентами и не обязана содержать каждый из компонентов, изображенных в неограничивающем и примерном варианте осуществления. Например, система диспетчерского управления и сбора данных (ICS, такая как SCADA) может заниматься сбором данных вместо интерфейса шлюза. Как указано выше, данные могут храниться в одном репозитории или в нескольких репозиториях.

Глобальная система управления GMS управляет нефтегазовыми ресурсами защищенным образом (или незащищенным образом, при желании) путем контроля за нелегальной деятельностью (которая может также включать, но без ограничения, подозрительную деятельность и/или технические проблемы) в цепочке поставок, предупреждения органов власти и/или уполномоченного персонала и реагирования на незаконную деятельность соответствующим образом. Глобальная система управления GMS собирает неоднородные, неструктурированные и разрозненные данные из датчиков, устройств сбора данных и вспомогательных систем наблюдения в секторах апстрим, мидстрим и даунстрим нефтегазовой инфраструктуры (трубопроводов) для хранения и обработки собранных данных, используя сведения систем нефтегазовой инфраструктуры. Данные структурированы для дополнительной обработки и анализа и целостность структурированных данных верифицируется и защищается для предотвращения фальсификации. Со временем, как описано выше, данные отправляются в центр управления CCC для того, чтобы персонал отреагировал на несанкционированное проникновение, кражу или подобные происшествия, связанные с эксплуатацией. Этот процесс позволяет быстрее реагировать по сравнению с современными системами, а также предоставлять доказательную базу, содержащую вещественное доказательство, которое может быть принято в суде общей юрисдикции для уголовного преследования в отношении правонарушителей. Например, защищенным образом собранные данные от БПЛА могут использоваться для предоставления доказательства, полученного на месте преступления, свидетельствующего о том, что событие имело место.

В частности, собранные данные будут получены и обработаны в режиме реального времени и направлены в центр управления CCC (который может иметь форму физического командного центра управления и/или приложения, функционально независимого от персонала или любой их комбинации) для соответствующего отображения персоналу командного центра. Структурированные данные будут анализироваться согласно вычислительным моделям и/или алгоритмам для идентификации событий, где события могут представлять собой происшествия, связанные с эксплуатацией, такие как незаконная деятельность, описанная выше, а также проблемы, связанные с эксплуатацией, которые могут быть идентифицированы и отображены операторам в режиме реального времени. Параллельно с этим (или в другое время), структурированные данные и события введены в модуль упреждающего и предписывающего анализа (приложение для упреждающего и предписывающего анализа), использующий машинное обучение, как описано выше, для идентификации последовательности измерений (фиг. 7A) или вычисленных данных, классифицированных как "события", требующие какого-либо действия и/или отчетности. Классификация события, ранее предоставленного системой управления данными, может быть подтверждена (человеком-оператором или машиной) и результаты отправлены в модуль упреждающего и предписывающего анализа для улучшения обучающего набора данных для алгоритма обучения, позволяя ему "обучаться" с течением времени. С помощью машинного обучения глобальная система управления GMS научится определять, какая последовательность измерений событий, взятых в совокупности, будет обозначать появление определенного события или группы событий. С помощью "выученных" событий система способна применять исторические данные и улучшать точность с течением времени. Точности также может способствовать осуществление человеком или БПЛА верификации на месте события предупреждений, созданных системой.

Система управления данными, подобно центру управления CCC, также может обмениваться данными с модулем упреждающего и предписывающего анализа, который будет применять машинное обучение на основе структурированных данных и событий в качестве обучающих наборов для классификации событий, которые могут быть расценены как последовательность измерений. Модуль упреждающего

и предписывающего анализа предоставляет информацию для идентификации вероятных событий (с переменной степенью вероятности) в будущем или происходящих событий, которые могут быть отправлены в качестве событий в центр управления ССС. Модуль упреждающего и предписывающего анализа также может предписывать ответную реакцию на событие, которая вероятнее всего приведет к положительному результату, на основании истории событий. Подобным образом, распознанные (или известные) тенденции, возникающие с течением времени, могут быть использованы для улучшения сгруппированных событий для более точного создания предупреждений в центре управления ССС.

На фиг. 6 показана приведенная в качестве примера схема интерфейса согласно одному варианту осуществления изобретения. Как изображено, интерфейс (шлюз) принимает данные из одного или более различных источников. Например, данные, собранные из датчиков в секторах апстрим, мидстрим и даунстрим и обработанные системами SCADA, передаются в интерфейс шлюза. В альтернативном варианте осуществления защищенные/проверенные датчики и PLC заменяют промышленную систему управления (такую как SCADA) и собирают данные непосредственно из датчиков секторов апстрим, мидстрим и даунстрим (фиг. 5). Интерфейс шлюза преобразовывает (например, сортирует, форматирует и модифицирует) собранные данные в защищенные и отформатированные данные, совместимые с системой и, в частности, с модулем интеграции данных, перед их отправкой в систему управления данными для анализа глобальной системы управления GMS.

На фиг. 7A-7D изображены приведенные в качестве примера измерения датчиков и датчики, собирающие данные на протяжении цепочки поставок согласно варианту осуществления изобретения. Центр управления ССС посредством интерфейса, обеспечивающего взаимодействие с системой управления месторождением и ресурсами (фиг. 5), может выполнять несколько действий на основании данных и событий в режиме реального времени, принятых от системы управления данными. После того как определенная последовательность измерений (или последовательность событий), связанная с описанием событий, стала известной (т.е. выучена приложением для упреждающего и предписывающего анализа, события могут помечаться в режиме реального времени и отправляться в центр управления ССС вместе с баллом вероятности, обозначающим вероятность того, что последовательность разворачивающихся измерений создаст в результате идентифицируемое событие. На фигурах заштрихованные прямоугольники представляют величины, полученные от заданного датчика. На фиг. 7A показано приведенное в качестве примера количество датчиков 1, ..., m, выполненных с возможностью получения последовательности событий. На фиг. 7B, 7C и 7D показана приведенная в качестве примера последовательность событий, в которой данные, полученные с течением времени t, представляют низкую вероятность, среднюю вероятность и высокую вероятность, соответственно, возникновения события (обозначенную здесь термином "вероятность события"). Изображенные датчики могут состоять из существующих в системе и/или вновь добавленных защищенных/проверенных датчиков и ICS, которые были добавлены в систему в различных местоположениях.

Вероятность события отправляется в центр управления ССС вместе с рекомендацией, такой как "На участке трубопровода 452 возможна кража, отправить команду для вмешательства в сектор D". Центр управления ССС может отреагировать различными способами, включая, без исключения, следующие: запросить отображение дополнительных данных для указанной области, в которой произошло событие (происшествие); направить дроны (БПЛА) в затронутую зону для разведки или получения информации или для визуального представления; отправить команды оперативного реагирования или людей (таких как полиция, пожарные и т.д.) в зону для проверки события или происшествия в месте эксплуатации; или отдать приказ об эвакуации персонала с места эксплуатации, в зависимости от происшествия (например, взрыв на рабочей площадке в ходе отбора моторного топлива).

Для улучшения эффективности с помощью модуля упреждающего и предписывающего анализа на основании прошлых событий, содержащихся в исторических данных измерений и событий, из исторических данных могут быть созданы модели и использованы для способствования прогнозированию будущих событий (происшествий) перед тем, как датчики и устройства сбора данных начнут регистрировать данные. Используя эти упреждающие данные, центр управления ССС и персонал, работающий в центре управления ССС, могут быть предупреждены о прогнозируемых "зонах с повышенной опасностью" возникновения кражи, идентифицированные системой, использующей данные в системе, такие как время суток, день недели, месяц или заданные даты, погодные условия, предыдущие последовательности событий и т.п. Например, на основании прогнозируемой "зоны с повышенной опасностью", БПЛА могут быть направлены для захвата и показа видеоизображения, и команды для вмешательства могут быть размещены неподалеку с целью предотвращения события. В другом случае, если, несмотря на вышеуказанные меры, событие произошло, время вмешательства будет уменьшено благодаря тому, что необходимые ресурсы находятся поблизости. Дополнительно система управления данными может приказать центру управления ССС автоматически отображать данные из "вероятных" зон, где вероятно произойдут события, таким образом, чтобы персонал мог инспектировать данные и видео из тех зон для обнаружения нарушений и деятельности, предупреждая появление какого-либо события. Глобальная система управления GMS также может использовать комбинацию алгоритмов интеллектуального анализа данных и действий персонала для обновления данных системы на основании событий и анализа, с подтверждением персона-

ла, находящегося на месте эксплуатации или на месте возникновения проблем.

Из вышеописанного становится понятно, что глобальная система управления GMS способна фиксировать развитие событий и соединять их вместе для предоставления истории для анализа и улучшения анализа данных в системе управления данными. На основании предыдущих сведений о событиях, произошедших в прошлом, исторических данных и верификации того, что события на самом деле имели место, такие как выполнение отверстия в трубопроводе с целью хищения топлива, будущие события могут быть более точно спрогнозированы и сами события могут быть лучше истолкованы при осуществлении контроля и анализа. Дополнительно благодаря тому, что глобальная система управления GMS по своей сути основана на прогнозах и предписаниях, она способна ослабить влияние коррупции людей, например рабочего персонала в центре управления CCC. Соответственно, людям, вовлеченным в незаконную деятельность, станет все сложнее избегать обнаружения путем удаления данных, изменения данных, подкупа персонала, контролирующего данные, и т.д.

В значительной степени для предотвращения таких типов ситуаций глобальная система управления предоставляет: защищенные и не поддающиеся подделке данные, которые не могут быть удалены, предупреждения, основанные на корреляции сгруппированных событий, уведомляющие о высокой вероятности незаконной деятельности, при этом указанная деятельность будет отображена оператору и зафиксирована в виде предупреждений, которые также не поддаются подделке и не могут быть удалены. В качестве альтернативы или дополнения сама система может вмешиваться вместо персонала для идентификации и отправки срочной информации внешним органам власти, таким как полиция, пожарная служба и т.д. Соответственно, роль системы заключается в предоставлении альтернативы человеческим ошибкам и некомпетентности.

Дальнейшие неограничивающие примеры глобальной системы управления GMS описаны ниже применительно к секторам мидстрим и даунстрим. В секторе мидстрим незаконная деятельность обычно представляет собой изменение маршрута транспортировки или хищение материалов. Например, в трубопроводе цепочки поставок может быть выполнено отверстие для выкачивания моторного топлива из трубопровода с целью хищения моторного топлива, часто успешного. В качестве мер противодействия и согласно целям глобальной системы управления GMS на трубопровод могут быть установлены несколько датчиков и/или устройств сбора данных, которые будут осуществлять контроль и сбор данных из трубопроводов. Например, может осуществляться контроль и сбор данных о скорости потока, температуре, давлении, объеме и т.д. Собранные данные из датчиков и устройств сбора данных будут отправлены в соответствующий шлюз (фиг. 5) или промышленную систему управления ICS с помощью защищенных/проверенных датчиков и ICS и будут переданы в систему управления данными и далее в центр управления CCC, как описано в настоящем документе выше. Дополнительно собранные данные должны быть обновлены таким образом, чтобы они могли быть истолкованы для предоставления выводов и рекомендаций. Например, если датчик(и) или устройство (устройства) сбора данных измеряют давление в трубопроводе лишь каждый час, когда топливо или сырая нефть незаконно извлекаются, датчик(и) и устройство (устройства) сбора данных могут не зафиксировать незаконную деятельность. С другой стороны, если давление в трубопроводе измеряется каждую минуту, датчик(и) и устройство (устройства) сбора данных смогут измерять любое повышение или понижение давления (или другие типы данных, такие как уменьшение объема, химическое присутствие воздуха или воды), указывающие на осуществление незаконной деятельности. БПЛА или персонал, связанные с определением местоположения датчика (датчиков) и устройства (устройств) сбора данных, могут быть автоматически отправлены в региональную область, могут захватываться изображения из локальной камеры и полиция или персонал экстренной службы могут быть уведомлены о том, что деятельность находится в процессе осуществления.

Другой неограничивающий пример данных в секторе мидстрим представляет собой автоцистерну, транспортирующую сырую нефть и нефтепродукт. В данном примере собранные данные представляют собой GPS-информацию, созданную пройденным маршрутом автоцистерны, и объем содержимого цистерны. Если данные, собранные с течением времени, указывают, например, на то, что автоцистерна стоит на месте дольше, чем ожидалось, или что объем содержимого цистерны изменился, это может указывать на осуществляемую или на осуществленную незаконную деятельность. В другом примере автоцистерна может остановиться в зоне ночного отдыха. Поскольку эти зоны являются известными, во время регулярной остановки в течение длительного периода датчики объема на автоцистерне могут быть активированы для осуществления контроля над изменением содержимого цистерны. В частности, может быть известно, что в определенной области осуществляется незаконная деятельность. В совокупности, любое изменение, обнаруженное датчиками, может быть направлено по системе управления данными в центр управления CCC, где на его основании может быть определено, что органы власти должны быть отправлены в указанное местоположение. Кроме того, данные относительно области и ожидания незаконной деятельности в указанной зоне будут переданы в обучающие механизмы системы, и такие данные будут применяться компонентом анализа данных в последующих анализах. Содержимое (ресурсы) также может быть помечено химическими маркерами или маркерами, применяемыми в судебной экспертизе, для возвращения ресурсов, например, обнаруженных в розничном магазине или органами власти.

В секторе даунстрим предоставлен неограничивающий пример, в котором собранные данные вклю-

чают объем, произведенный на перерабатывающем заводе. Данные об объеме могут быть связаны, например, с количеством автоцистерн, необходимым для транспортировки содержимого автоцистерн (топлива) в розничные магазины. Подразумевается, что после прибытия топлива в розничные магазины оно загружается в цистерны магазинов для хранения. В данном случае происходит передача объема и сбыт топлива. Датчики и устройства сбора данных в таком случае могут использоваться для измерения изменений соответствующих объемов и измерения наличных средств, полученных в результате продажи топлива. Если объемы и продажи не совпадают, это может указывать на незаконную деятельность, такую как присвоение чужих средств. Эта информация также может быть применима для повторного взимания или согласования налогов, для оценки количества топлива, требуемого в конкретном регионе, и т.д. Как следует понимать, данные не только собираются, но также хранятся в репозитории и преобразуются в сумму сгруппированных событий, которые могут быть связаны, использованы или проанализированы для предписывающего или упреждающего действия.

На фиг. 8 показана приведенная в качестве примера схема интерфейса согласно одному варианту осуществления изобретения. Интерфейс, который в данной заявке также обозначен терминами "шлюз" или "интерфейс шлюза", обеспечивает взаимодействие датчиков данных, расположенных на протяжении секторов апстрим, мидстрим и даунстрим, с внешними источниками, такими как сервисная шина предприятия ESB или глобальная система управления данными GMS, посредством защищенных/проверенных датчиков и ICS с модулем интеграции данных. Как изображено, шлюз разделен на три уровня, содержащие: (1) компьютер (для подписывания и хранения), обменивающийся данными с системами производственного управления (такими как SCADA, OPC, AS-i MODBUS и Ethercat); драйверы могут представлять собой комбинацию физических интерфейсов и программного обеспечения; (2) обработчик бизнес-правил (BRE), осуществляющий корреляцию, защиту, аутентификацию, фильтрацию, согласование, предотвращает подделывание и создает данные, содержащие ключевые значения, BRE на основании собранных данных будет создавать ассоциации с данными, собранными в объекты, создавать события, основанные на отсутствии целостности объектов, создавать предупреждения, основанные на событиях, или события, основанные на пороговых значениях, или на бизнес-правилах, или на тенденциях; и (3) интерфейсы, взаимодействующие с внешними системами с помощью, например, HTTPS, SSL или любого другого программного или аппаратного протокола.

Интерфейс шлюза предоставляет, помимо других признаков, механизм для преобразования собранных данных в формат, имеющий большую защиту и совместимый с внешней системой, в которую будут отправлены преобразованные данные или объекты или события или предупреждения, созданные в шлюзе. Например, интерфейс шлюза будет обеспечивать защиту собранных данных из датчиков и/или устройств сбора данных, а также форматирование собранных данных для придания им совместимости с защищенными/проверенными датчиками и ICS, а также системой интеграции данных перед их использованием в глобальной системе управления GMS, особенно на уровне системы управления данными (DMS). Интерфейс шлюза взаимодействует с внешними системами с помощью, например, протоколов, таких как HTTPS, SSL и т.д. Внешние интерфейсы включают, но без ограничения, сервисную шину предприятия ESB или систему производственного управления ICS. На уровне драйвера, драйверы, обменивающиеся данными с внешними системами, такими как система ICS, могут представлять собой аппаратное обеспечение, программное обеспечение или их комбинацию. Аппаратное обеспечение и программное обеспечение предпочтительно являются устойчивыми к взлому и защищенными для того, чтобы предотвратить атаки на физическое аппаратное обеспечение, а также злонамеренные атаки на программное обеспечение, например, осуществляемые хакерами, введением нежелательных данных и т.п. Данные, которые будут образованы и созданы в интерфейсе шлюза, будут более защищенными и будут обеспечивать расширенные свойства в дополнение к данным, собранным из различных репозиториев данных, таких как SCADA или ICS. Защищенные и расширенные данные затем будут предоставлены глобальной системе управления GMS и будут способствовать созданию сгруппированных событий. Шлюз также будет верифицировать подлинность данных, принятых из любого защищенного/проверенного и незащищенного/непроверенного датчика (датчиков) и устройства (устройств) сбора данных, и отсутствия их искажения внешними источниками или другим образом. Другими словами, шлюз в первую очередь будет обладать способностью определять подлинность принимаемых данных перед защитой данных и добавлением дополнительных свойств. Это будет обеспечивать определение подлинности данных, предназначенных для защиты и расширения свойств, перед их поступлением в глобальную систему управления GMS и предотвратит отправку искаженных данных в систему глобального управления GMS. Один недостаток существующих систем в цепочке поставок нефти и газа заключается в невероятно большом объеме данных. Если система становится загрязненной или зараженной поддельными, подложными, сфабрикованными или неточными данными, полученные данные не будут надежными и любые события или сгруппированные события, созданные в глобальной системе управления GMS, потенциально могут скомпрометировать предупреждения, созданные из сгруппированных событий. Соответственно, любые данные, предназначенные для доступа или использования в глобальной системе управления GMS (посредством модуля интеграции данных) с помощью шлюза, должны быть как можно более защищенными и точными. Пример определения подлинности данных, которые будут вве-

дены в шлюз, заключается в том, чтобы за короткий промежуток времени получать от датчиков в несколько раз больше информации, чем предполагается получать, и верифицировать, чтобы собранные данные всегда имели одинаковую сущность (например, данные о температуре получают десять раз в течение 30 с и величина практически не изменяется, в таком случае данные производят впечатление верных). Другой пример обеспечения подлинности данных заключается в добавлении к датчику электронной системы или механизма, защищающего его от фальсификации любыми средствами (например, ввода ошибочных данных, обеспечения ошибочных измерений, осуществляемых датчиком, и т.д.), вследствие чего данные, собранные из датчика и впоследствии отправленные в шлюз, будут насколько это возможно точными. Измерения от датчиков, сообщающие о сбоях в результате самодиагностики или самопроверок достоверности, могут не учитываться. В качестве альтернативы или дополнения вышеуказанным проверкам подлинности, данные измерений можно сравнить с данными из соседних датчиков, измеряющих аналогичные или связанные физические явления, чтобы убедиться, что они согласованы. Например, если температура повысилась в одном датчике, повысилась ли она также в соседних датчиках? Как следствие, изменяется ли давление? И так далее.

Методы машинного обучения для обнаружения отклонений также могут выполняться в отношении данных за прошедший и текущий период для обнаружения несоответствующих показаний датчиков.

Интерфейс шлюза собирает данные посредством или физических интерфейсов, взаимодействующих с промышленными датчиками, использующими промышленные протоколы связи, такие как OPC или Ethercat, или посредством виртуальных (т.е. программных) интерфейсов, взаимодействующих с существующими системам контроля или управления, таким как SCADA. Интерфейсы приводятся в действие, например, с помощью программных драйверов, которые могут быть динамически загружены или выгружены в зависимости от физических или виртуальных требований. Например, при наличии физически соединенных трех устройств, приводимых в действие протоколом OPC, и одного устройства, приводимого в действие протоколом Ethercat, будут присутствовать три драйвера OPC и один драйвер Ethercat.

Когда данные достигают интерфейса шлюза, обработчик бизнес-правил BRE создает новые данные контроля путем корреляции полученных данных, фильтрации несущественных данных, например, событий, не относящихся к безопасности, подтверждения правильности доступа для считывания/записи из/в уровень драйвера в уровень интеграции (в обоих направлениях), и применения правил безопасности/доступа/определения подлинности, при необходимости используя внешнюю систему. Тем не менее, следует понимать, что эти функции приведены лишь в качестве примера и BRE не ограничен такими функциями.

На уровне интерфейса программное обеспечение в интерфейсе шлюза также может взаимодействовать с внешними системами на основании требований контроля. Например, интерфейс может включать интерфейс электронной почты, web-интерфейс и т.д. Уровень интерфейса также может взаимодействовать с сервисной шиной предприятия ESB в качестве системы обмена сообщениями (например, использующей протокол, такой как REST по HTTPS) для интеграции данных из всех интерфейсов шлюза и внешних систем в компонент хранения данных глобальной системы управления GMS. Также следует понимать, что хотя на схеме изображен интерфейс, ведущий к интерфейсу шлюза, интерфейс шлюза также может быть непосредственно соединен или представлять собой часть глобальной системы управления GMS.

Программное обеспечение сервисной шины предприятия ESB представляет собой систему обмена сообщениями, подобную продуктам MQueue Series и BMC Control компании IBM™. Программное обеспечение шины ESB, которое в настоящем варианте осуществления обозначено термином "модуль интеграции данных", составляющий часть глобальной системы управления GMS (хотя следует понимать, что ESB также может представлять собой отдельный объект), может представлять собой приложение, такое как Open ESB, разработанное компанией Sun Microsystems™, или WSO2 ESB. Язык программирования, использующий технологию JAVA, может использоваться в качестве языка программирования для получения такого программного обеспечения.

Обработчик бизнес-правил BRE (второй уровень) выполняет функцию преобразующей обработки полученных данных и применяет правила, которые могут быть выполнены таким образом, чтобы представлять определенный интересующий элемент, такой как потенциальное нарушение безопасности. BRE контролирует всю деятельность и точки измерения загруженных драйверов, вместе с любыми физически или виртуально присоединенными устройствами. Благодаря доступу ко всем этим точкам в режиме реального времени BRE может создавать новые точки измерения или данные, применимые для создания сгруппированных событий в глобальной системе управления GMS. На основании собранных данных BRE также будет создавать ассоциации с данными, собранными в объекты, создавать события, основанные на отсутствии целостности объектов, создавать предупреждения, основанные на событиях, или события, основанные на пороговых значениях или на бизнес-правилах или на тенденциях. Например, точка измерения A на физически присоединенном устройстве (таком как датчик температуры) и точка измерения B (такая как переменная из внешней программной системы SCADA) при определенных пороговых

значениях могут создавать новые данные, основанные как на точке измерения A, так и на точке измерения B. Например, могут быть созданы новые данные C, где новые данные C представляют собой функцию от данных из точек измерения A и B и могут составлять событие. Это позволяет BRE коррелировать данные для лучшего понимания событий по мере их появления. События, созданные в шлюзе, основаны на данных, собранных из датчиков, устройств сбора данных или систем ICS. К этим данным, точность которых была проверена перед поступлением в шлюз, добавляются свойства для получения расширенных данных.

В другом варианте осуществления, если датчики, устройства сбора данных или системы ICS не являются надежными или не способны проверить точность данных, этап проверки выполняется в шлюзе. События, созданные в шлюзе, будут применимы в системе DMS системы GMS для создания сгруппированных событий. Сгруппированные события используются в GMS для создания и/или отображения предупреждений на уровне CCC и в контексте настоящего изобретения позволят эффективно мобилизовать соответствующее оперативное реагирование на месте происшествия (т.е. полицию при хищении материала, пожарных при взрыве и т.д.).

BRE также может действовать автономно, если доступно достаточно физической и/или виртуальной информации для определения на основании событий собранных данных, применимых для создания в глобальной системе управления GMS сгруппированных событий, не доверяя данным любой внешней системы, действий, таких как оповещения, для идентификации или предупреждения о нарушениях безопасности, или принятия других соответствующих действий. Определение (определения) сгруппированных событий управляется посредством модуля управления данными глобальной системы управления GMS как часть "обучающейся" сущности системы. BRE хранит эти данные и создает очередь из них, при необходимости, и шифрует или подписывает каждые данные для того, чтобы убедиться в том, что данные являются полными, аутентичными, поддающимися учету, неопровержимыми и защищенными от внешнего доступа, модификации, нарушения и уничтожения. Следует понимать, что могут использоваться один или несколько признаков, ни одного или все эти признаки в дополнение к другой форме функциональности. Зашифрованные данные потом могут быть доступны внешним системам на основании, например, профилей безопасности системы, запрашивающей информацию.

На фиг. 9 показан примерный вариант осуществления технологического маршрута интерфейса согласно одному варианту осуществления изобретения. Драйверы интерфейса шлюза собирают данные из разнообразных источников, включая, но без ограничения, физические источники, программируемые логические контроллеры (PLC) и удаленные терминальные устройства (RTU) и любой другой тип источника. Обработчик бизнес-правил BRE обрабатывает данные, коррелирует данные и создает из данных события или последовательность событий, как подробно описано выше. Данные и события необязательно подписывает аппаратный или программный модуль безопасности (HSM или SSM). События и расширенные данные могут храниться в защищенном репозитории или хранилище данных. Шлюз затем осуществляет проверку для того, чтобы определить, куда будут отправлены данные, например в глобальную систему управления GMS или в другую внешнюю систему. Если глобальная система управления GMS доступна, то данные или события могут быть отформатированы и утверждены для использования системой глобального управления. Данные, отправляемые во внешнюю систему, могут быть отформатированы и утверждены в зависимости от требований внешней системы.

Данные затем отправляются в модуль интеграции данных, который может хранить данные или события, получать данные из хранилища, создавать из данных, например структуру данных, содержащих ключевые значения, сортировать структуру данных и анализировать структурированные данные с применением вычислительных моделей и алгоритмов для идентификации корреляции между данными, применимыми для создания сгруппированных событий в глобальной системе управления GMS. Данные также проверяются на целостность структурированных данных и безопасность структурированных данных для предотвращения фальсификации. Интерфейс данных может представлять собой независимый интерфейс или часть системы управления данными. Если интерфейс является отдельным, данные затем проходят в систему управления данными для обработки согласно вариантам осуществления, описанным выше.

Соответственно, настоящее изобретение предоставляет различные системы, серверы, способы, носители и программы. Хотя изобретение было описано со ссылкой на несколько приведенных в качестве примера вариантов осуществления, следует понимать, что использованные слова являются описательными и иллюстративными, но не ограничивающими. Могут быть внесены изменения в пределах сферы действия прилагаемой формулы изобретения, в том виде, в котором она заявлена в настоящее время и в ее измененном виде, не отступая от объема и идеи изобретения в его аспектах. Хотя изобретение было описано со ссылкой на конкретные средства, материалы и варианты осуществления, изобретение не предназначено для ограничения описанными сведениями; вместо этого изобретение охватывает все функционально эквивалентные структуры, способы и применения, находящиеся в пределах объема прилагаемой формулы изобретения.

Хотя машиночитаемый носитель может быть описан как один носитель, термин "машиночитаемый носитель" включает один носитель или несколько носителей, такие как централизованная или распреде-

ленная база данных, и/или соответствующие кэш-памяти и серверы, хранящие один или более наборов команд. Термин "машиночитаемый носитель" также должен включать любой носитель, способный хранить, шифровать или содержать набор команд для исполнения процессором или обеспечивающий выполнение компьютерной системой одного или более любых вариантов осуществления, описанных в данном документе.

Машиночитаемый носитель может включать постоянный машиночитаемый носитель или носители и/или включать временный машиночитаемый носитель или носители. В определенном неограничивающем приведенном в качестве примера варианте осуществления машиночитаемый носитель может включать твердотельное запоминающее устройство, такое как карта памяти или другой модуль, вмещающий одно или более энергонезависимых постоянных запоминающих устройств. Кроме этого, машиночитаемый носитель может представлять собой оперативное запоминающее устройство или другое энергозависимое перезаписываемое запоминающее устройство. Дополнительно машиночитаемый носитель может включать магнитно-оптический или оптический носитель, такой как диск или магнитные ленты или другое устройство для хранения данных с целью получения сигналов несущей, таких как сигналы, отправленные по передающей среде. Соответственно, считается, что описание включает любой машиночитаемый носитель или другие эквиваленты и носители последующих поколений, в которых могут храниться данные или команды.

Хотя в настоящей заявке описаны конкретные варианты осуществления, которые могут быть реализованы в виде сегментов кода в машиночитаемых носителях, следует понимать, что выделенные аппаратные реализации, такие как специализированные интегральные схемы, программируемые логические матрицы и другие аппаратные устройства, могут быть предназначены для реализации одного или более вариантов осуществления, описанных в данном документе. Применения, которые могут включать различные варианты осуществления, изложенные в данном документе, могут включать большое разнообразие электронных и компьютерных систем.

Соответственно, настоящая заявка может охватывать реализации программного обеспечения, программно-аппаратного обеспечения и аппаратного обеспечения или их комбинации.

Хотя в настоящем техническом описании описаны компоненты и функции, которые могут быть реализованы в определенных вариантах осуществления, со ссылкой на определенные стандарты и протоколы, изобретение не ограничено этими стандартами и протоколами. Такие стандарты периодически замещаются более быстрыми или более эффективными эквивалентами, обладающими, по существу, теми же функциями. Соответственно, заменяющие стандарты и протоколы, обладающие такими же или подобными функциями, считаются их эквивалентами.

Изображения вариантов осуществления, описанные здесь, предназначены для предоставления общего понимания различных вариантов осуществления. Предполагается, что изображения не будут служить полным описанием всех элементов и признаков приспособления и систем, использующих структуры или способы, описанные в данном документе. Множество других вариантов осуществления могут быть очевидны специалистам в данной области после рассмотрения изобретения. Другие варианты осуществления могут быть использованы и выведены из настоящего изобретения, таким образом, чтобы структурные и логические замещения и изменения могли быть осуществлены в пределах объема изобретения. Дополнительно изображения предназначены лишь для образования представления и могут быть изображены не в масштабе. Некоторые пропорции в изображениях могут быть увеличены, в то время как другие пропорции могут быть уменьшены. Соответственно, описание и фигуры нужно расценивать как пояснительные, но не ограничивающие.

Один или более вариантов осуществления изобретения могут быть обозначены здесь, по отдельности или вместе, термином "изобретение" лишь для удобства и не предполагая добровольного ограничения объема данной заявки любым конкретным изобретением или новаторской идеей. Более того, хотя определенные варианты осуществления были изображены и описаны в данном документе, следует понимать, что любая последующая конструкция, предназначенная для достижения той же или подобной цели, может быть замещена изображенными определенными вариантами осуществления. Предполагается, что данное изобретение охватывает любые и все последующие адаптации или вариации различных вариантов осуществления. Комбинации вышеописанных вариантов осуществления и другие варианты осуществления, не описанные в данном документе особым образом, будут очевидны специалистам в данной области после рассмотрения описания.

Реферат изобретения предоставлен для того, чтобы удовлетворить требованиям 37 C.F.R. §1.72(b) и подан с пониманием того, что он не будет использован для трактовки или ограничения объема или смысла формулы изобретения. Кроме этого, в вышеизложенном подробном описании различные признаки могут быть сгруппированы вместе или описаны в одном варианте осуществления для упрощения изобретения. Данное изобретение не должно быть истолковано как подразумевающее, что заявленные варианты осуществления требуют больше признаков, чем указано в явном виде в каждом пункте формулы изобретения. Вместо этого, как отражено в следующей формуле изобретения, патентоспособный объект изобретения может относиться к не менее чем все признакам описанных вариантов осуществления. Таким образом, следующая формула изобретения включена в подробное описание, при этом каждый пункт

формулы изобретения является самостоятельным, поскольку определяет отдельно заявляемый объект изобретения.

Вышеописанный объект изобретения следует расценивать как наглядный и не ограничивающий, и предполагается, что прилагаемая формула изобретения охватывает все подобные модификации, улучшения и другие варианты осуществления, находящиеся в пределах истинной идеи и объема настоящего изобретения. Таким образом, до максимальной степени, разрешенной законом, объем настоящего изобретения должен быть определен наиболее широким из допустимых толкований следующих пунктов формулы изобретения и их эквивалентов и не должен ограничиваться вышеизложенным подробным описанием.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ создания защищенных данных с дополнительными атрибутами, применяемых в глобальной системе управления (GMS), относящейся к управлению нефтегазовыми ресурсами, включающий

получение посредством шлюза данных, связанных с нефтегазовыми ресурсами, собранных по меньшей мере из одного датчика, расположенного на протяжении цепочки поставок нефти и газа;

получение посредством шлюза по меньшей мере части данных, связанных с нефтегазовыми ресурсами, собранных по меньшей мере из одного защищенного/проверенного датчика, расположенного рядом по меньшей мере с одним датчиком, при этом по меньшей мере один защищенный/проверенный датчик выполнен с возможностью сбора и верификации данных;

проверку посредством шлюза данных, собранных по меньшей мере из одного датчика, и данных, собранных по меньшей мере из одного защищенного/проверенного датчика, для подтверждения точности информации в собранных данных перед передачей на защищенный сервер;

запись посредством шлюза полученных данных на защищенный сервер, содержащий по меньшей мере один программный компонент; и

добавление посредством шлюза атрибутов к данным, сохраненным на защищенном сервере, с применением обработчика бизнес-правил, выполненного с возможностью применения правил безопасности/доступа/определения подлинности для создания расширенных данных, причем дополнительные атрибуты расширенных данных включают по меньшей мере один защищенный атрибут, позволяющий обнаруживать модификацию или повреждение и определять подлинность расширенных данных, используемых в GMS, и

защиту посредством шлюза защищенного сервера по меньшей мере от одного из фальсификации и ввода нежелательных данных, а также несанкционированного доступа;

отличающийся тем, что проверку собранных данных для подтверждения точности информации в собранных данных осуществляют путем сравнения данных, собранных по меньшей мере из одного датчика, с данными, собранными по меньшей мере из одного защищенного/проверенного датчика, расположенного рядом по меньшей мере с одним датчиком и измеряющего аналогичные или связанные физические явления, чтобы убедиться, что они согласованы.

2. Способ по п.1, отличающийся тем, что по меньшей мере часть расширенных данных, созданных с помощью обработчика бизнес-правил, преобразована в события.

3. Способ по п.1 или 2, отличающийся тем, что расширенные данные или события, основанные на расширенных данных, подписывают или шифруют по меньшей мере одним из аппаратных или программных модулей безопасности шлюза.

4. Способ по любому из предыдущих пунктов, отличающийся тем, что по меньшей мере один программный компонент защищенным образом отправляет расширенные данные с дополнительными атрибутами в модуль интеграции данных GMS.

5. Способ по любому из предыдущих пунктов, отличающийся тем, что обработчик бизнес-правил хранит расширенные данные и создает очередь из них в зашифрованном и долгосрочном хранилище данных.

6. Способ по любому из предыдущих пунктов, отличающийся тем, что расширенные данные с дополнительными атрибутами передают на внешнюю систему посредством интерфейса.

7. Способ по п.1, отличающийся тем, что собранные данные отправляют на защищенный сервер в виде по меньшей мере одного из защищенных данных, отдельно отформатированных данных, совместно отформатированных данных, данных с защищенными атрибутами, данных, предназначенных только для чтения, и данных, защищенных от подделки.

8. Способ по любому из предыдущих пунктов, отличающийся тем, что дополнительно включает

прием защищенным образом собранных и верифицированных расширенных данных в модуле интеграции данных и сбор и/или организацию расширенных данных и событий, созданных из расширенных данных в сгруппированные события в глобальной системе управления;

выполнение в центре управления по меньшей мере одного из осуществления контроля над предупреждениями, создание предупреждений и предоставление решений на основании сгруппированных событий, созданных в системе управления данными;

отображение центром управления визуального представления сгруппированных событий и

обеспечение взаимодействия посредством центра управления для обмена данными по меньшей мере с одним из модуля интеграции данных, внешней эксплуатационной поддержки, персонала и производственного оборудования.

9. Глобальная система управления (GMS), управляющая цепочкой поставок нефти и газа и содержащая

шлюз для создания защищенных данных с дополнительными атрибутами, применяемых в GMS;

по меньшей мере один датчик, расположенный на протяжении цепочки поставок нефти и газа, выполненный с возможностью сбора данных, связанных с нефтегазовыми ресурсами;

по меньшей мере один защищенный/проверенный датчик, расположенный рядом по меньшей мере с одним датчиком, выполненным с возможностью сбора по меньшей мере части данных, связанных с нефтегазовыми ресурсами, при этом по меньшей мере один защищенный/проверенный датчик выполнен с возможностью сбора и верификации данных;

защищенный сервер, содержащий по меньшей мере один программный компонент, выполненный с возможностью хранения данных, полученных от шлюза, и защищенный посредством шлюза по меньшей мере от одного из фальсификации и ввода нежелательных данных, а также несанкционированного доступа; и

обработчик бизнес-правил шлюза, выполненный с возможностью добавления атрибутов к данным, сохраненным на защищенном сервере, для создания расширенных данных, выполненный с возможностью применения правил безопасности/доступа/определения подлинности, причем дополнительные атрибуты расширенных данных включают по меньшей мере один защищенный атрибут, позволяющий обнаруживать модификацию или повреждение и определять подлинность расширенных данных, используемых в GMS,

при этом шлюз выполнен с возможностью проверки данных, собранных по меньшей мере из одного датчика, и данных, собранных по меньшей мере из одного защищенного/проверенного датчика, для подтверждения точности информации в собранных данных перед передачей на защищенный сервер,

отличающаяся тем, что проверка собранных данных для подтверждения точности информации в собранных данных осуществлена путем сравнения данных, собранных по меньшей мере из одного датчика, с данными, собранными по меньшей мере из одного защищенного/проверенного датчика, расположенного рядом по меньшей мере с одним датчиком и измеряющего аналогичные или связанные физические явления, чтобы убедиться, что они согласованы.

10. Система по п.9, отличающаяся тем, что расширенные данные, созданные с помощью обработчика бизнес-правил, преобразованы в события.

11. Система по любому из пп.9 или 10, отличающаяся тем, что расширенные данные или события, основанные на расширенных данных, подписаны или зашифрованы по меньшей мере одним из аппаратных или программных модулей безопасности шлюза.

12. Система по пп.9-11, отличающаяся тем, что по меньшей мере один программный компонент защищенным образом отправляет расширенные данные с дополнительными атрибутами в модуль интеграции данных GMS.

13. Система по пп.9-12, отличающаяся тем, что обработчик бизнес-правил хранит расширенные данные и создает очередь из них в зашифрованном и долгосрочном хранилище данных.

14. Система по пп.9-12, отличающаяся тем, что обработчик бизнес-правил хранит события, созданные из расширенных данных, и создает очередь из них в зашифрованном и долгосрочном хранилище данных.

15. Система по пп.9-14, отличающаяся тем, что расширенные данные с дополнительными атрибутами передают на внешнюю систему посредством интерфейса.

16. Система по пп.9-15, отличающаяся тем, что события, созданные из расширенных данных, отправляют посредством интерфейса на внешнюю систему.

17. Система по пп.9-16, отличающаяся тем, что дополнительно содержит

модуль интеграции данных, принимающий расширенные данные и события, созданные из расширенных данных, в сгруппированные события в глобальной системе управления; и

центр управления, выполняющий по меньшей мере одно из осуществления контроля над предупреждениями, создания предупреждений и предоставления решений, основанных на сгруппированных событиях, созданных в системе управления данными, причем

центр управления отображает визуальное представление сгруппированных событий, и причем

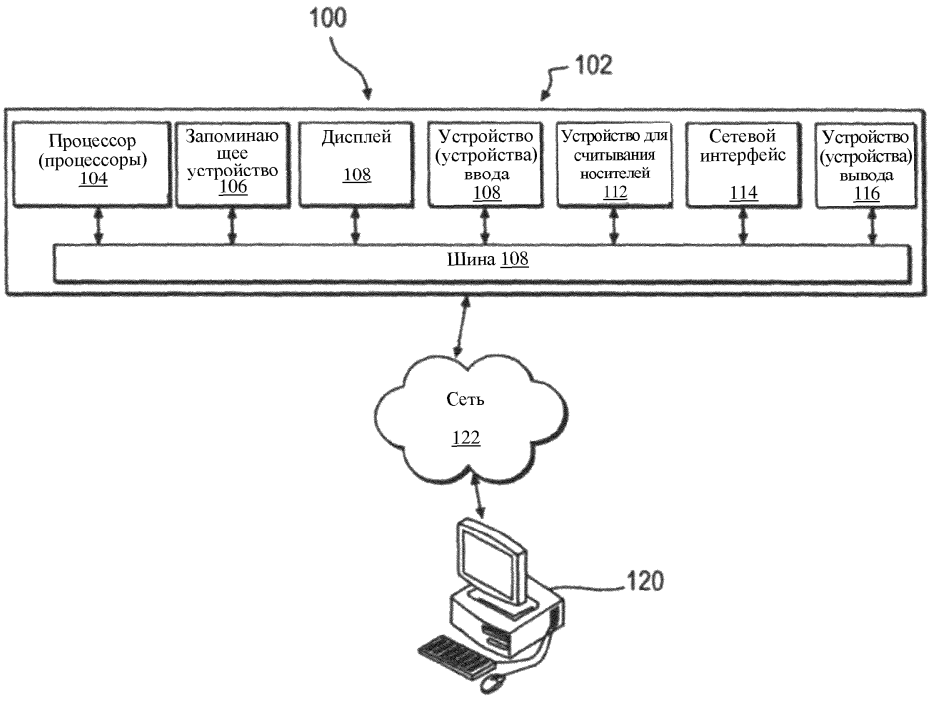
центр управления взаимодействует для обмена данными по меньшей мере с одним из модуля интеграции данных, внешней эксплуатационной поддержки, персонала и производственного оборудования.

18. Система по п.9, отличающаяся тем, что собранные данные передают на защищенный сервер в форме по меньшей мере одного из незащищенных данных, защищенных данных, отдельно отформатированных данных, совместно отформатированных данных, данных с защищенными атрибутами, данных, предназначенных только для чтения, и данных, защищенных от подделки.

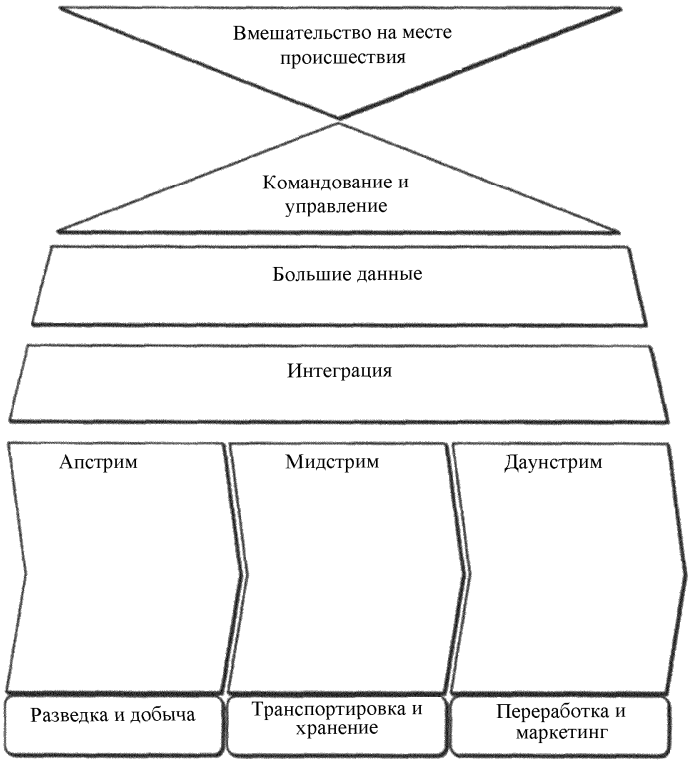
19. Постоянный машиночитаемый носитель, на котором записана программа, исполняемая процес-

сором, для осуществления способа по любому из пп.1-8.

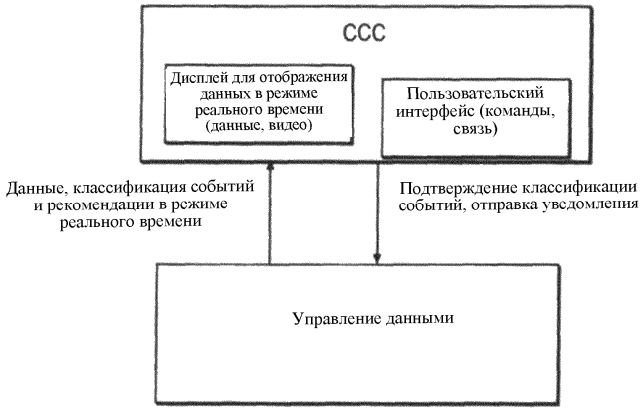
Фиг. 1



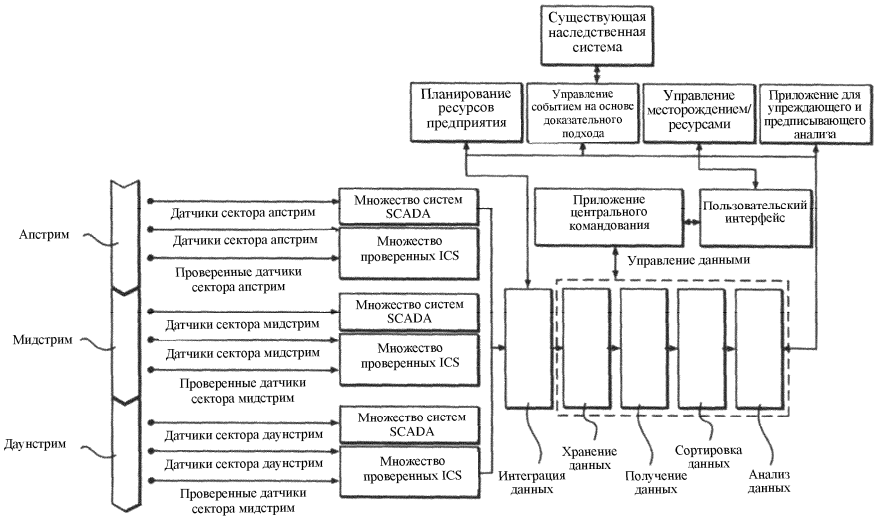
Фиг. 2



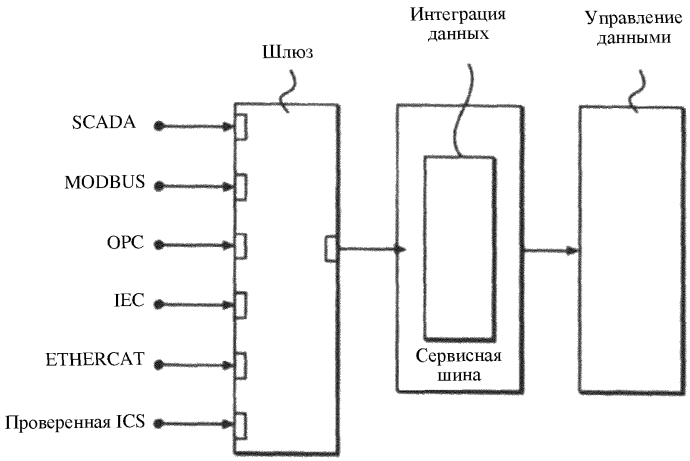
Фиг. 3



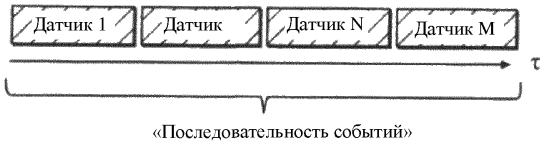
Фиг. 4



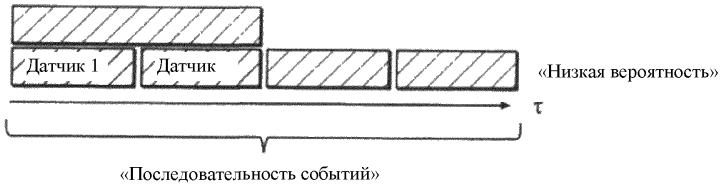
Фиг. 5



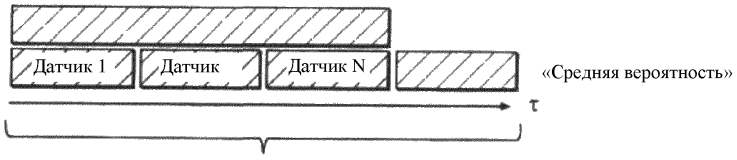
Фиг. 6



Фиг. 7A

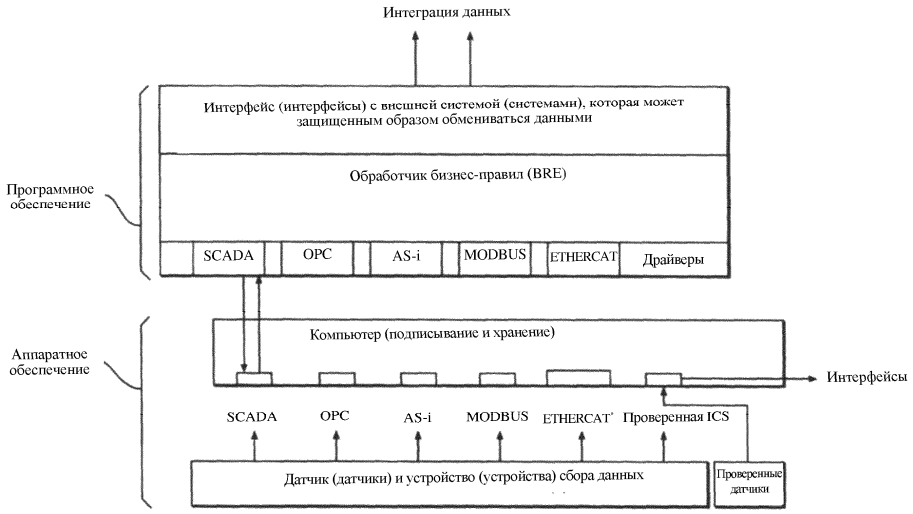


Фиг. 7B

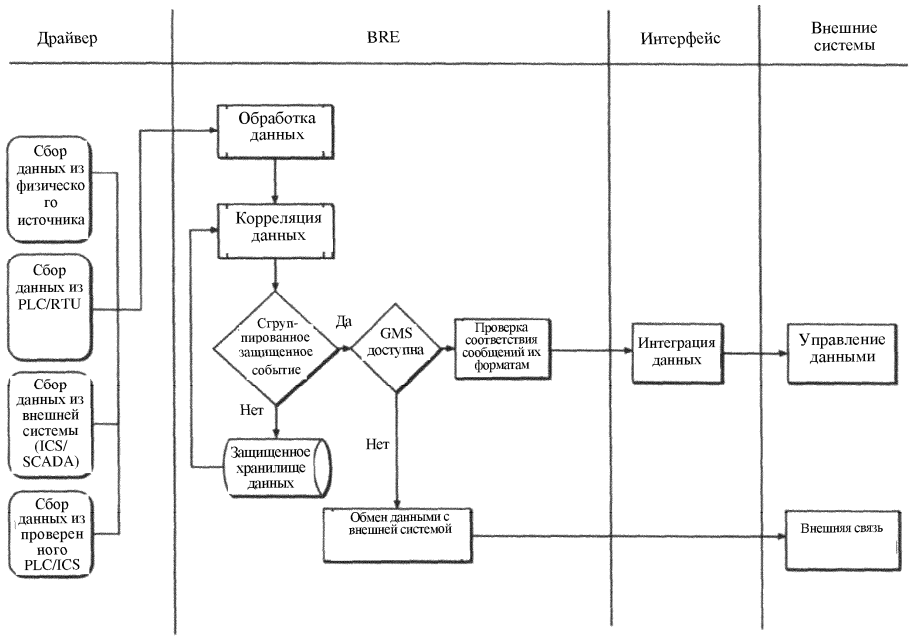


Фиг. 7C

Фиг. 7D


Интеграция данных
Интерфейс (интерфейсы) с внешней системой (системами), которая может защищенным образом обмениваться данными
Обработчик бизнес-правил (BRE)
Программное обеспечение
SCADA
OPC
AS-i
MODBUS
ETHERCAT
Драйверы
Компьютер (подписывание и хранение)
Аппаратное обеспечение
Интерфейсы
SCADA
OPC
AS-i
MODBUS
ETHERCAT
Проверенная ICS
Датчик (датчики) и устройство (устройства) сбора данных
Проверенные датчики

Фиг. 8


Драйвер
BRE
Интерфейс
Внешние системы
Сбор данных из физического источника
Сбор данных из PLC/RTU
Сбор данных из внешней системы (ICS/ SCADA)
Сбор данных из проверенного PLC/ICS
Обработка данных
Корреляция данных
Сгруп-пированное защищенное событие
Да
Нет
GMS доступна
Нет
Проверка соответствия сообщений их форматам
Защищенное хранилище данных
Обмен данными с внешней системой
Интеграция данных
Управление данными
Внешняя связь

Фиг. 9