



РЕСПУБЛИКА КАЗАХСТАН

(19) KZ (13) U (11) 11987
(51) H04L 9/40 (2022.01)

МИНИСТЕРСТВО ЮСТИЦИИ РЕСПУБЛИКИ КАЗАХСТАН

ОПИСАНИЕ ПОЛЕЗНОЙ МОДЕЛИ К ПАТЕНТУ

(21) 2025/1565.2

(22) 14.10.2025

(45) 03.04.2026, бюл. №13

(72) Амирханова Гульшат Аманжоловна (KZ);
Адилжанова Салтанат Альмуханбетовна (KZ);
Прокопович-Ткаченко Дмитрий Игоревич (UA);
Абдулхамит Назаргожа Хекимтулович (KZ)

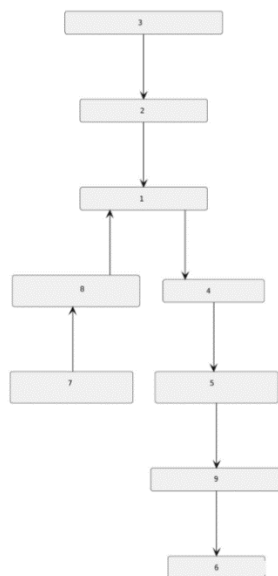
(73) Адилжанова Салтанат Альмуханбетовна (KZ)

(56) WO 2020078804 A1, 23.04.2020

(54) СИСТЕМА ЗАЩИЩЁННОГО ОБМЕНА
ПАРАМЕТРАМИ ПЕЧЕЙ В СЕТИ
ЦИФРОВОГО ДВОЙНИКА

(57) Полезная модель относится к области цифровых информационных технологий, промышленной автоматике и защиты информации и предназначена для защищённого двунаправленного обмена технологическими параметрами печей с системой цифрового двойника. Система содержит микроконтроллерный узел, коммуникационный модуль, интерфейс к цифровому двойнику, интерфейс к печам, криптографический блок

хеширования, модуль индикации, блок отказоустойчивого питания, фильтр электромагнитных помех и энергонезависимую память. Микроконтроллерный узел выполняет нормализацию и канонизацию параметров печей, формирует пакеты с меткой времени и одноразовым значением, осуществляет вычисление и проверку контрольного хеш-идентификатора содержимого пакета и управляет индикацией результата проверки. Энергонезависимая память обеспечивает журналирование событий проверки целостности. Фильтр электромагнитных помех повышает устойчивость работы модуля в производственной среде. Технический результат заключается в обеспечении достоверности и подлинности технологических параметров печей при обмене с цифровым двойником, повышении помехоустойчивости и обеспечении локальной оперативной диагностики состояния целостности данных.



Фиг. 1 – Модуль защищённого обмена параметрами печей в сети цифрового двойника

(19) KZ (13) U (11) 11987

1. Область техники

Полезная модель относится к области цифровых информационных технологий, промышленной автоматизации и защиты информации и предназначена для обеспечения достоверного двунаправленного обмена технологическими параметрами печей хлебобулочного производства с системой цифрового двойника.

2. Уровень решения и прототип)

Аналог 1. Решение контроля целостности данных цифрового двойника на основе контрольной суммы, представляющей собой хеш-значение данных цифрового двойника, с проверкой согласованности между эталонными данными и запрошенными данными цифрового двойника.

Источник: WO 2017045789 A1 (также семейство DE102015217855A1, дата публикации 23.03.2017).

Признаки аналога: формирование контрольной суммы как хеш-значения данных цифрового двойника; сравнение контрольных сумм при получении данных по каналу связи; вывод о нарушении целостности при расхождении контрольных сумм.

Совпадающие признаки: использование хеш-значения (контрольной суммы) для контроля целостности данных, передаваемых/получаемых в контуре цифрового двойника.

Причины, препятствующие получению требуемого технического результата заявляемой модели: аналог не раскрывает конструктивно выполненный модуль, обеспечивающий аппаратное подключение к печам, нормализацию/канонизацию технологических параметров печей перед формированием пакета, локальную индикацию результата проверки целостности на объекте, а также встроенную фильтрацию электромагнитных помех в составе модуля обмена.

Аналог 2. Способы и системы защищённой работы промышленного контроллера с обменом защитными данными/токенами между устройствами промышленной системы управления.

Источник: US 8,973,124 B2.

Признаки аналога: обеспечение защищённого режима функционирования промышленной системы управления, обмен защитными данными между устройствами, контроль разрешённости операций в системе.

Совпадающие признаки: обеспечение защищённого обмена между компонентами промышленной системы.

Причины, препятствующие получению требуемого технического результата заявляемой модели: аналог ориентирован на общий режим защищённой эксплуатации контроллера и политики безопасности, но не раскрывает модуль, который выполняет нормализацию и канонизацию технологических параметров печей, формирование пакетов параметров с метками актуальности, вычисление/проверку хеш-идентификатора содержимого пакета именно параметров печей и локальную индикацию результата проверки целостности, а также встроенную помехозащиту на линиях питания и сигналов.

Аналог 3. Технические решения, использующие криптографические ключи для аутентификации устройства и защиты целостности данных/программного кода для промышленных/IoT-устройств, включая IoT-шлюзы.

Источник: WO 2020078804 A1.

Признаки аналога: использование криптографических ключей для аутентификации устройства, защиты целостности хранимых данных и проверок целостности при обновлениях/обмене.

Совпадение криптографических механизмов для защиты целостности данных в устройствах промышленного/IoT-класса.

Причины, препятствующие получению требуемого технического результата заявляемой модели: аналог не раскрывает привязку к технологическим параметрам печей и к операции канонизации параметров перед контролем целостности, не содержит указания на локальную индикацию результата проверки целостности параметров печи, а также не раскрывает встроенный фильтр электромагнитных помех как функциональный блок модуля обмена параметрами печей с цифровым двойником.

Ближайший прототип.

В качестве прототипа рассматривается IoT-шлюз (модуль обмена), осуществляющий сбор технологических параметров оборудования, передачу пакетов в информационную систему и применение контрольных значений сообщений. Недостатками прототипа являются отсутствие нормализации/канонизации параметров перед контролем целостности, отсутствие встроенной фильтрации электромагнитных помех на линиях питания/сигналов и отсутствие штатной локальной индикации результата проверки целостности на объекте.

3. Сущность полезной модели

Технический результат — обеспечение достоверности и подлинности технологических параметров печей двунаправленном обмене с цифровым, повышение устойчивости к электромагнитным помехам и обеспечение локальной оперативной диагностики состояния целостности данных.

Модуль защищённого обмена параметрами печей в сети цифрового двойника содержит: микроконтроллерный узел, коммуникационный модуль, интерфейс к цифровому двойнику, интерфейс к печам, криптографический блок хеширования, модуль индикации, блок отказоустойчивого питания, фильтр электромагнитных помех и энергонезависимую память, при этом микроконтроллерный узел выполнен с возможностью нормализации и канонизации параметров печей, формирования пакета данных с меткой времени и одноразовым значением, вычисления и проверки контрольного хеш-идентификатора содержимого пакета посредством криптографического блока хеширования и формирования сигналов для модуля индикации, а энергонезависимая память с возможностью регистрации событий.

4. Краткое описание чертежей

Фиг.1 — Структурная схема модуля защищённого обмена параметрами печей в сети цифрового двойника, где показаны элементы:

- 1 — микроконтроллерный узел;
- 2 — коммуникационный модуль;
- 3 — интерфейс к цифровому двойнику;
- 4 — интерфейс к печам;
- 5 — криптографический блок хеширования;
- 6 — модуль индикации;
- 7 — блок отказоустойчивого питания;
- 8 — фильтр электромагнитных помех;
- 9 — энергонезависимая память.

5. Подробное описание реализации (по Фиг.1)

Микроконтроллерный узел 1 обеспечивает управление функционированием модуля, обработку технологических параметров печей, формирование и разбор пакетов, взаимодействие с криптографическим блоком 5 и энергонезависимой памятью 9, а также формирование сигналов состояния для модуля индикации 6.

Интерфейс к печам 4 обеспечивает получение технологических параметров печей (температура, относительная влажность, скорость конвекции) и передачу управляющих воздействий (уставок/режимов) на печи. Параметры передаются в микроконтроллерный узел 1.

В микроконтроллерном узле 1 выполняется нормализация по калибровочным коэффициентам и приведение к фиксированному формату, после чего выполняется канонизация набора параметров, включающая фиксированный порядок полей и однозначное кодирование метаданных. К канонизированному набору добавляются метка времени и одноразовое значение для контроля актуальности и исключения повторов.

Криптографирование 5 вычисляет контрольный хеш-идентификатор над канонизированным набором данных. Сформированный пакет (параметры, метаданные, хеш-идентификатор) передаётся через коммуникационный модуль 2 в интерфейс к цифровому двойнику 3.

Коммуникационный модуль 2 обеспечивает передачу пакетов в сторону цифрового двойника и приём пакетов команд/уставок от цифрового двойника через интерфейс 3. При приёме пакета команд микроконтроллерный узел 1 выполняет проверку метки времени и одноразового значения, повторно вычисляет хеш-идентификатор посредством криптографического блока 5 и сравнивает его с принятым значением. При положительном результате интерфейс к печам 4, при отрицательном результате применение команды блокируется, а событие фиксируется в энергонезависимой памяти 9.

Модуль индикации 6 обеспечивает отображение состояния: наличие связи, подтверждение целостности, ошибке актуальности пакета или повтор пакета.

Блок отказоустойчивого питания 7 обеспечивает стабилизированное питание узлов модуля и кратковременную автономность при провалах напряжения, а также защиту от импульсных

перенапряжений. Фильтр электромагнитных помех 8 обеспечивает подавление помех на линиях питания и сигнальных цепях, повышая устойчивость работы модуля в производственной среде.

Энергонезависимая память 9 хранит журнал событий проверки целостности и диагностические записи.

6. Технический результат

Реализация полезной модели обеспечивает:

- защиту технологических параметров печей от подмены за счёт контроля целостности содержимого пакетов посредством хеш-идентификатора;
- повышение достоверности обмена между цифровым двойником и печами за счёт канонизации параметров и контроля актуальности пакетов по метке времени и одноразовому значению;
- устойчивость к электромагнитным наводкам благодаря встроенному фильтру электромагнитных помех;
- локальную диагностику состояния целостности за счёт модуля индикации;
- снижение рисков сбоев электропитания за счёт блока отказоустойчивого питания.

7. Перечень

(Фиг.1)

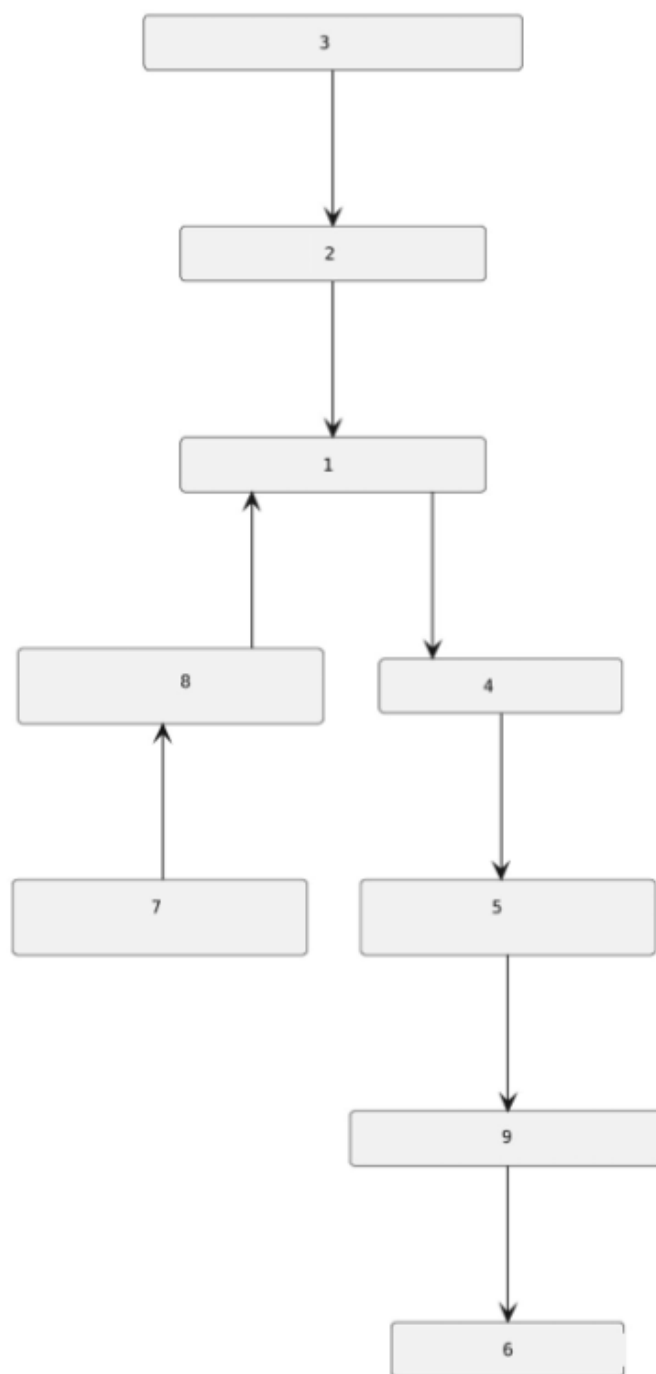
- 1 — микроконтроллерный узел;
- 2 — коммуникационный модуль;
- 3 — интерфейс к цифровому двойнику;
- 4 — интерфейс к печам;
- 5 — криптографический блок хеширования;
- 6 — модуль индикации;
- 7 — блок отказоустойчивого питания;
- 8 — фильтр электромагнитных помех;
- 9 — энергонезависимая память.

ФОРМУЛА ПОЛЕЗНОЙ МОДЕЛИ

1. Система защищённого обмена параметрами печей в сети цифрового двойника, содержащий микроконтроллерный узел, коммуникационный модуль, интерфейс к цифровому двойнику, интерфейс к печам, криптографический блок хеширования, модуль индикации, блок отказоустойчивого питания, фильтр и энергонезависимую память, **отличающийся** тем, что микроконтроллерный узел выполнен с возможностью нормализации и канонизации технологических параметров печей, формирования пакета с меткой времени и одноразовым значением, вычисления и проверки контрольного хеш-идентификатора содержимого пакета посредством криптографического блока хеширования, а модуль индикации выполнен с возможностью отображения результата проверки целостности.

2. Система защищённого обмена параметрами печей в сети цифрового двойника по п.1, **отличающийся** тем, что энергонезависимая память выполнена с возможностью регистрации событий проверки целостности, включающих отметку времени и результат проверки, а фильтр электромагнитных помех выполнен с возможностью

подавления помех на линиях питания и сигнальных цепях модуля.



Фиг. 1 – Модуль защищённого обмена параметрами печей в сети цифрового двойника