РЕСПУБЛИКА КАЗАХСТАН

(19) **KZ** (13) **U** (11) **11897**
(51) ***G05B 19/00*** (2006.01)
H04L 9/00 (2022.01)

МИНИСТЕРСТВО ЮСТИЦИИ РЕСПУБЛИКИ КАЗАХСТАН

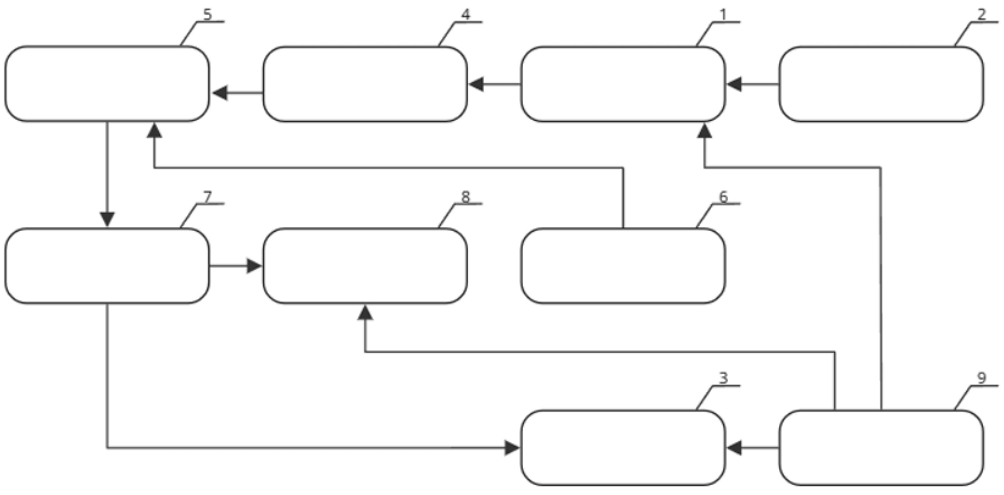
ОПИСАНИЕ ПОЛЕЗНОЙ МОДЕЛИ
К ПАТЕНТУ

(21) 2025/1569.2
(22) 15.10.2025
(45) 13.03.2026, бюл. №10
(72) Адилжанова Салтанат Альмуханбетовна (KZ); Прокопович-Ткаченко Дмитрий Игоревич (UA); Амирханова Гульшат Аманжоловна (KZ); Әліпбеки Оңғарбек Әліпбекұлы (KZ); Амирханов Алихан Бауыржанұлы (KZ)
(73) Амирханова Гульшат Аманжоловна (KZ)
(56) US 20190207944 A1, 04.07.2019

(54) **УЗЕЛ ВЕРИФИКАЦИИ КОМАНД ЦИФРОВОГО ДВОЙНИКА НА ЭТАПЕ ТЕРМООБРАБОТКИ**

(57) Полезная модель относится к области цифровых информационных технологий и промышленной автоматики пищевой промышленности, используется для контроля целостности и подлинности управляющих команд цифрового двойника при управлении печами и конвейерами выпечки. Узел включает микроконтроллерный модуль, коммуникационный модуль связи с цифровым двойником, интерфейс к термооборудованию с гальванической развязкой, модуль нормализации и канонизации команд, криптографический блок хеширования, модуль формирования временных меток и одноразовых значений, модуль сравнения и блокировки применения команды, модуль индикации состояния и блок стабилизированного питания с фильтрами электромагнитных помех. Технический результат заключается в предотвращении несанкционированных изменений управляющих сигналов за счёт обязательной хеш-верификации каждой команды с использованием алгоритма SHA-256, обеспечении отказобезопасности при сбоях питания и визуальной индикации состояния.

(19) KZ (13) U (11) 11897



Фиг. 1 - Узел верификации команд цифрового двойника на этапе термообработки

1. Область техники

Полезная модель относится к области цифровых информационных технологий, промышленной автоматики и защиты информации, а именно к средствам контроля целостности и подлинности управляющих команд, передаваемых от цифрового двойника к исполнительным устройствам линий термообработки (печам и конвейерам выпечки) пищевой промышленности.

2. Уровень техники (известные решения и прототип)

Известно техническое решение, раскрытое в публикации патентной заявки США US 2020/0128042 A1 (US20200128042A1) Communication method and apparatus for an industrial control system, Ochoa et al., дата публикации 23.04.2020, заявитель Singapore University of Technology and Design, Singapore, в котором предусмотрены модуль формирования подписи и модуль верификации для промышленной системы управления. Указанное решение осуществляет выбор критических сетевых пакетов с управляющими полезными нагрузками, формирование подписи (криптографического идентификатора) для критической полезной нагрузки и передачу комбинированного пакета, включающего полезную нагрузку и подпись, с последующей проверкой целостности критической полезной нагрузки по подписи на принимающей стороне.

Признаки аналога: выделение критических управляющих сообщений; вычисление подписи на основе содержимого критической полезной нагрузки; передача подписи совместно с сообщением; проверка целостности и подлинности критической полезной нагрузки до ее использования.

Совпадающие признаки с заявляемым решением: выполнение криптографической проверки целостности управляющей информации, поступающей по сети к исполнительным устройствам, до ее применения к объекту управления.

Недостатки аналога: проверка выполняется на уровне сетевых пакетов и не предусматривает канонизацию параметров команд в предметной области термообработки; отсутствует аппаратно реализованный узел граничной верификации, физически включенный между каналом связи и силовыми цепями исполнительных интерфейсов; отсутствуют локальная аппаратная блокировка применения несоответствующих команд, автономная индикация статуса верификации и отказобезопасное питание узла верификации.

Ближайшим аналогом (прототипом) является техническое решение, раскрытое в публикации патентной заявки США US20190207944A1 Command authentication related to the control of industrial systems, дата публикации 04.07.2019, правообладатель General Electric Company, в котором предусмотрен узел промежуточной обработки (jump host), выполняющий аутентификацию удаленно выдаваемых управляющих команд путем сопоставления поступившей команды со списком разрешенных команд (whitelist) и последующей передачи аутентифицированной команды на контроллер промышленной машины.

Признаки прототипа: наличие буферного узла между сетью и контроллером; хранение перечня разрешенных команд; проверка поступившей команды на принадлежность перечню; передача команды контроллеру при успешной проверке.

Совпадающие признаки с заявляемым решением: предварительная проверка управляющей команды до ее применения к промышленному объекту, а также реализация промежуточного узла между источником команды и исполнительным контуром.

Недостатки прототипа: аутентификация основана на принадлежности команды перечню и не обеспечивает криптографической защиты целостности параметров команды; отсутствуют процедуры нормализации и канонизации параметров, включение метки времени и одноразового значения для предотвращения повторной передачи, а также независимая аппаратная блокировка применения команды на уровне интерфейсов термооборудования; отсутствуют локальная индикация статуса верификации и меры устойчивости к кратковременным провалам питания в узле верификации.

Заявляемый узел устраняет указанные недостатки за счет аппаратно-программного контура верификации команд с хеш-контролем, независимого от транспортного уровня, с локальной индикацией состояния, стабилизированным питанием и аппаратной блокировкой применения несоответствующих команд.

3. Сущность полезной модели

Технический результат — предотвращение несанкционированных изменений управляющих сигналов на этапе термообработки за счёт обязательной хеш-верификации каждой команды до её применения к печам и конвейерам, с индикацией состояния и отказобезопасным поведением.

Суть решения: узел получает от цифрового двойника команды управления (уставки температуры, скорости конвейера, профили термообработки), выполняет их канонизацию, формирует контрольный хеш (например, по алгоритму SHA-256) с использованием метки времени и одноразового значения, сопоставляет с полученным контрольным идентификатором и, при соответствии, пропускает команду к исполнительным интерфейсам. При несоответствии выполняется аппаратная блокировка применения, фиксация события и индикация отказа.

Обрабатываемые данные: уставки температуры, влажности/пара, скорости ленты, профили нагрева/выдержки/охлаждения, служебные поля (идентификатор узла, метка времени, одноразовое значение).

Состав узлов: микроконтроллерный модуль; коммуникационный модуль связи с цифровым двойником; интерфейс к термооборудованию с

гальванической развязкой; модуль нормализации/канонизации команд; криптографический блок хеширования; модуль сравнения и блокировки; модуль индикации; блок стабилизированного и отказоустойчивого питания; фильтры электромагнитных помех; сторожевой таймер и аппаратный межблокировочный выход.

Реализуемые принципы: канонизация представления команд; включение метки времени и одноразового значения; вычисление хеш-идентификатора; сравнительная верификация; аппаратная блокировка и безопасное состояние при несоответствии или сбоях питания; визуальная индикация.

4. Краткое описание чертежей

Фиг.1 — Структурная схема узла верификации команд цифрового двойника.

На схеме показаны:

1 — микроконтроллерный узел;

2 — коммуникационный модуль связи с цифровым двойником (WiFi/Ethernet/промышленный шлюз);

3 — интерфейс к термооборудованию (печи, конвейеры) с опторазвязкой;

4 — модуль нормализации и канонизации команд;

5 — криптографический блок хеширования;

6 — модуль временных меток и одноразовых значений;

7 — модуль сравнения и блокировки применения команды;

8 — модуль индикации состояния;

9 — блок стабилизированного и отказоустойчивого питания с фильтрами ЭМП.

5. Подробное описание реализации

Микроконтроллерный узел (1) является центральным элементом управления потоками данных и координации верификации. Он связан с коммуникационным модулем (2), обеспечивающим обмен с цифровым двойником по проводному или беспроводному каналу. На входе от (2) команды поступают в модуль нормализации и канонизации (4), который:

— проверяет структуру сообщения и допустимость параметров;

— удаляет избыточные представления (например, незначащие пробелы, различия форматов чисел);

— сортирует поля в предопределённом порядке и формирует канонизированный буфер данных для хеширования.

Модуль временных меток и одноразовых значений (6) формирует высокоточные временные отметки (синхронизация по сетевому времени/внутреннему источнику) и одноразовые значения (nonce), исключающие повторное использование ранее валидных команд.

Криптографический блок (5) выполняет вычисление контрольного хеша над конкатенацией: идентификатор узла, канонизированный набор параметров команды, метка времени, одноразовое значение. В типовой реализации применяется алгоритм SHA-256. В альтернативном варианте допускается использование HMAC-SHA-256 с предраспределённым ключом для повышения стойкости к коллизиям и подмене.

Модуль сравнения и блокировки (7) сопоставляет локально вычисленный хеш с контрольным идентификатором, полученным вместе с командой от цифрового двойника. При полном совпадении разрешается передача управляющих сигналов на интерфейс к термооборудованию (3). При несоответствии инициируется:

— аппаратная блокировка применения команды (разрыв разрешающих цепей через силовое реле/транзисторный ключ);

— запись события отказа в энергонезависимой памяти микроконтроллера;

— выдача сигнала на модуль индикации (8).

Интерфейс к термооборудованию (3) содержит цепи гальванической развязки (оптроны/драйверы), формирователи уровней для входов печей и конвейеров, а также обратные сигналы состояния (готовность, авария), используемые для диагностики.

Модуль индикации (8) реализует визуальную (многоцветный индикатор/сегментный дисплей) и, при необходимости, звуковую индикацию трёх состояний: готовность к приёму команд, верификация успешна/команда применена, несоответствие/блокировка. Дополнительно предусмотрен выход типа сухой контакт для передачи статуса в систему мониторинга линии.

Блок стабилизированного и отказоустойчивого питания (9) включает входные фильтры ЭМП, стабилизатор напряжения, цепи подавления бросков и кратковременных провалов, а также буфер накопителя (суперконденсатор/аккумулятор малой ёмкости), обеспечивающий корректное завершение операций верификации и безопасное удержание блокировки при кратковременных перебоях. Сторожевой таймер реализуется внутри (1) с внешним аппаратным сбросом на случай зависаний.

Алгоритм работы узла:

1. приём команды от цифрового двойника через (2);

2. нормализация и канонизация представления в (4);

3. дополнение меткой времени и одноразовым значением из (6);

4. вычисление хеша в (5);

5. сравнение с полученным контрольным идентификатором в (7);

6а) при совпадении — разрешение применения команды через (3) и фиксация успешного события;

6б) при несоответствии — аппаратная блокировка, запись отказа, индикация несоответствия.

Аппаратная реализация не содержит исполняемого пользователем программного кода на уровне интерфейсов — только функциональные блоки, алгоритмические операции и физические соединения, обеспечивающие независимость контура верификации от транспортного протокола и ПО верхнего уровня.

6. Технический результат

— защита управляющих команд от подмены и повторной передачи;

— повышение достоверности и отказобезопасности управления термообработкой;

— автоматическая индикация состояния верификации для оперативного контроля;

— устойчивость к электромагнитным помехам и кратковременным перебоям питания за счёт стабилизации и резервирования;

— локальная аппаратная блокировка применения несоответствующих команд.

7. Перечень условных обозначений (Фиг.1)

1 — микроконтроллерный узел;

2 — коммуникационный модуль связи с цифровым двойником;

3 — интерфейс к термооборудованию с опторазвязкой;

4 — модуль нормализации и канонизации команд;

5 — криптографический блок хеширования;

6 — модуль временных меток и одноразовых значений;

7 — модуль сравнения и блокировки применения команды;

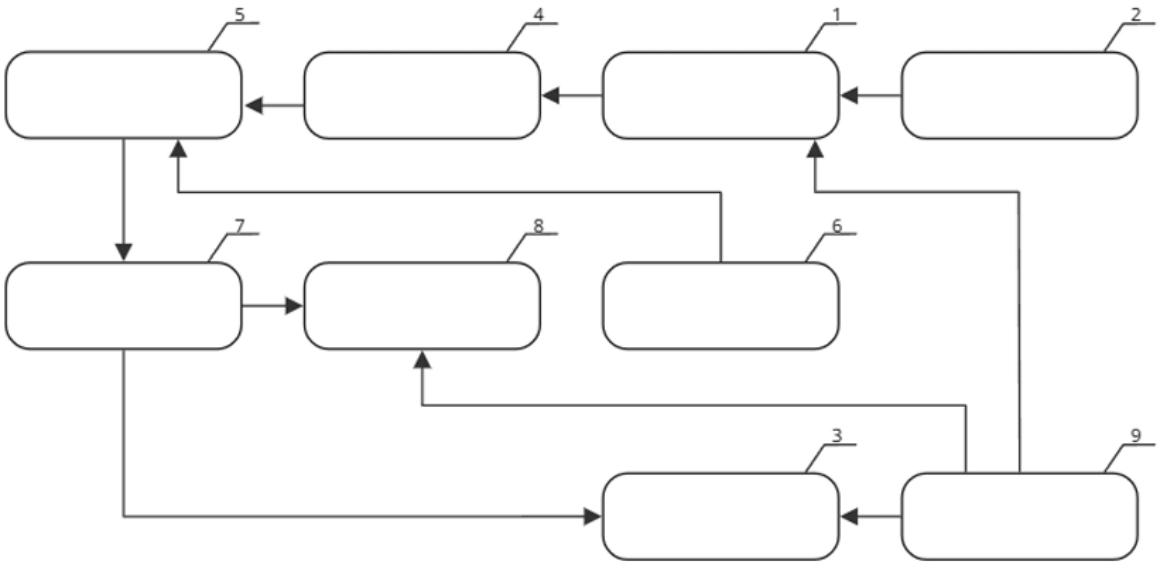
8 — модуль индикации состояния;

9 — блок стабилизированного и отказоустойчивого питания с фильтрами ЭМП.

ФОРМУЛА ПОЛЕЗНОЙ МОДЕЛИ

1. Узел верификации команд цифрового двойника на этапе термообработки, содержащий микроконтроллерный узел, коммуникационный модуль связи с цифровым двойником, интерфейс к термооборудованию с гальванической развязкой, модуль нормализации и канонизации команд, криптографический блок хеширования, модуль временных меток и одноразовых значений, модуль сравнения и блокировки применения команды, модуль индикации состояния и блок стабилизированного и отказоустойчивого питания с фильтрами ЭМП, ***отличающийся*** тем, что микроконтроллерный узел выполнен с возможностью формирования канонизированного набора параметров команды и вычисления контрольного хеша по криптографическому алгоритму над канонизированным набором параметров совместно с идентификатором узла, меткой времени и одноразовым значением, при этом модуль сравнения и блокировки выполнен с возможностью разрешения передачи команды на интерфейс к термооборудованию только при совпадении вычисленного контрольного хеша с контрольным идентификатором, полученным от цифрового двойника, и с возможностью аппаратной блокировки применения команды при несоответствии.

2. Узел по п.1, ***отличающийся*** тем, что блок стабилизированного и отказоустойчивого питания содержит накопитель энергии в виде суперконденсатора или аккумулятора малой емкости для удержания блокировки и корректного завершения операций верификации при кратковременных провалах питания, а модуль индикации выполнен с возможностью выдачи визуального сигнала состояния верификации и дискретного выхода состояния для системы мониторинга.



Фиг. 1 - Узел верификации команд цифрового двойника на этапе термообработки

Верстка Д. Женысова
Корректор Г. Косанова