

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 984 525**

51 Int. Cl.:

**G05B 19/418** (2006.01)

**H04L 9/40** (2012.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **22.09.2020 PCT/EP2020/076431**

87 Fecha y número de publicación internacional: **15.04.2021 WO21069207**

96 Fecha de presentación y número de la solicitud europea: **22.09.2020 E 20789457 (7)**

97 Fecha y número de publicación de la concesión europea: **10.04.2024 EP 4014467**

54 Título: **Red de datos con pasarela unidireccional**

30 Prioridad:

**10.10.2019 DE 102019215565**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:

**29.10.2024**

73 Titular/es:

**SIEMENS MOBILITY GMBH (100.0%)**

**Otto-Hahn-Ring 6**

**81739 München, DE**

72 Inventor/es:

**FALK, RAINER;**

**SELTZSAM, STEFAN;**

**SEUSCHEK, HERMANN y**

**WIMMER, MARTIN**

74 Agente/Representante:

**LOZANO GANDIA, José**

ES 2 984 525 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

## DESCRIPCIÓN

Red de datos con pasarela unidireccional

5 Antecedentes de la invención

Ámbito de la invención

10 La presente invención se refiere a una red de datos para instalaciones industriales y a un procedimiento para operar una red de datos para instalaciones industriales.

Descripción del estado de la técnica

15 Han de transmitirse datos procedentes de instalaciones industriales, para su análisis de forma protegida, a un sistema de frontera (Edge-System) de Internet de las Cosas (Internet of Things, IoT) o a un Backend (arquitectura interna) de IoT. Los datos pueden por ejemplo evaluarse para detectar a tiempo futuros defectos (Predictive Maintenance), para optimizar parámetros de máquina o para detectar ataques a un sistema de automatización o manipulaciones de la instalación industrial (Intrusion Detection System, System Integrity Monitoring).

20 Una exigencia de seguridad fundamental es proteger la propia transmisión de los datos. Para ello puede utilizarse protocolos de comunicación seguros, como por ejemplo TLS, DTLS, IPsec/IKEv2. Otra exigencia de seguridad esencial consiste en que una red de automatización (red de control) no se vea atacada o influida desde fuera. Esto es en particular importante, ya que algunas redes de automatización han de cumplir exigencias especiales en cuanto a tiempo real y a seguridad y puesto que en algunas redes de automatización se utilizan aparatos antiguos (Brownfield) con una protección insuficiente frente a accesos.

25 Una pasarela unidireccional (Data Capture Unit, One-Way Gateway, diodo de datos) hace posible al respecto una conexión de una red de automatización sin repercusiones. Así se garantiza que sólo puedan transmitirse datos de la instalación industrial hacia fuera. Se impide con fiabilidad que una red externa pueda influir o perjudicar el funcionamiento de la instalación industrial.

30 En instalaciones industriales complejas están previstas usualmente varias zonas de red/zonas de red de automatización separadas (por ejemplo en cada caso una por cada célula de fabricación, por cada línea de producción, por cada máquina). Las mismas están conectadas con una red de fábrica por ejemplo a través de un firewall (cortafuegos) industrial, que filtra el tráfico en la red. No obstante, de esta manera no queda visible en el firewall de la red de fábrica la comunicación dentro de una zona de red/célula. Cuando ha de vigilarse la comunicación dentro de una zona de red/célula, por ejemplo para detectar ataques mediante un sistema de detección de intrusión (Intrusion Detection System, IDS), debe instalarse y operarse en cada célula una respectiva One-Way-Gateway (pasarela unidireccional). La instalación y el servicio de la misma son extremadamente prolijos y por lo tanto costosos.

35 El documento EP 3 425 865 A1 describe un procedimiento y un equipo de transmisión para la transmisión unidireccional sin repercusiones de datos desde una primera zona de la red hasta una segunda zona de la red, para la evaluación en un servidor de aplicación remoto. Una unidad de transmisión unidireccional de datos está constituida para transmitir unidireccionalmente los datos en el formato de datos de transporte a la segunda zona de red (23).

Resumen de la invención

50 El objetivo de la invención consiste en especificar una solución para la transmisión de datos en redes.

La invención resulta de las características de las reivindicaciones independientes. Ventajosos perfeccionamientos y variantes de diseño son objeto de las reivindicaciones dependientes. Otras características, posibilidades de aplicación y ventajas de la invención resultan de la siguiente descripción.

55 Un aspecto de la invención consiste en proporcionar una solución económica y segura para una red de datos, para transmitir datos desde una pluralidad de zonas de la red (unidireccionalmente) sin repercusiones mediante una One-Way-Gateway.

60 La invención reivindica una red de datos para instalaciones industriales, caracterizada por:

- al menos una primera unidad de captación de datos, que está constituida para captar primeros datos generados por al menos una zona de una red de automatización asociada a la misma y transmitirlos como segundos datos a través de una conexión de red y
- 65 - una segunda unidad de captación de datos, que está constituida para recopilar los segundos datos, teniendo la zona de la red de automatización al menos un componente de automatización y

constituyendo la primera unidad de captación de datos y la segunda unidad de captación de datos conjuntamente una One-Way-Gateway.

5 La zona de la red de automatización puede denominarse también dominio de automatización y por ejemplo estar constituida como célula de fabricación, automatización de procesos, automatización de ferrocarriles, automatización de edificios, automatización de un sistema de tráfico o automatización de una red de energía.

El componente de automatización puede estar configurado por ejemplo como máquina de fabricación.

10 La One-Way-Gateway puede denominarse también vía de comunicación de un solo sentido o vía de comunicación unidireccional.

15 Los primeros datos y los segundos datos pueden ser por ejemplo datos de control y/o datos de diagnóstico y/o datos de sensor del componente de automatización.

La primera unidad de captación de datos puede denominarse también Satellite Data Capture Unit (unidad satélite de captura de datos, CDU satélite). La segunda unidad de captación de datos puede denominarse también Master Data Capture Unit (unidad maestra de captura de datos, CDU master).

20 La primera unidad de captación de datos puede ejecutar un procesamiento previo de los primeros datos antes de que se transmitan los datos previamente procesados como segundos datos. El procesamiento previo puede ser un filtrado o compresión de los primeros datos. La primera unidad de captación de datos puede otorgar una marca de tiempo (como clase especial del procesamiento previo) a los primeros datos/segundos datos. La marca de tiempo puede estar sincronizada con una información de tiempo sincronizada, por ejemplo un tiempo de GPS o una información de tiempo de un servidor NTP. Esto tiene la ventaja de que primeros datos que para una comunicación en tiempo real, por ejemplo Real-Time Ethernet o Time Sensitive Networking, están sincronizados dentro de la zona de la red de automatización con un tiempo local, pueden asociarse a una información de tiempo global. Además puede otorgarse a los primeros datos/segundos datos una información que indique si los primeros datos se han transmitido durante una franja de tiempo reservada para la transmisión de datos en tiempo real.

Pueden estar acopladas varias primeras unidades de captación de datos a una segunda unidad de captación de datos. La segunda unidad de captación de datos/master-DCU puede asumir así la función de una central.

35 La primera unidad de captación de datos puede llevar asociadas varias zonas de la red de automatización.

Las zonas de la red de automatización pueden tener subzonas, pudiéndose agregar los primeros datos generados en las subzonas y captarse agregados por la primera unidad de captación de datos.

40 La idea básica de la invención consiste en realizar jerárquicamente una solución de One-Way-Gateway: Se utilizan varias primeras unidades de captación de datos/DCUs satélite para captar sin repercusiones datos de varias zonas de la red de automatización y transmitirlos a continuación a una segunda red de captación de datos/DCU master para el subsiguiente procesamiento.

45 Este concepto puede proseguir a lo largo de varias etapas. Es decir, zonas de la red de automatización pueden a su vez dividirse en subzonas y agregarse datos de estas últimas a través del mismo mecanismo. Esto tiene la ventaja de que con poco coste pueden preverse primeras unidades de captación de datos/DCUs satélite para una mayoría/pluralidad de zonas de red de automatización en disposición jerárquica. Cada primera unidad de captación de datos/DCU satélite lleva por lo tanto asociadas varias zonas de la red de automatización.

50 La invención ofrece la ventaja de que pueden captarse datos en bruto de las zonas de la red de automatización separadas mediante el equipo y criptográficamente protegidas (a través de un túnel seguro) enviarse a la segunda unidad de captación de datos/DCU master. Así pueden transmitirse protegidos los datos interceptados a la segunda unidad de captación de datos/DCU master. En función del caso de aplicación, puede aprovecharse una infraestructura de red existente o bien constituirse una infraestructura de red separada.

55 En otra ejecución está constituida la primera unidad de captación de datos para procesar los primeros datos.

60 En otra ejecución está constituida la segunda unidad de captación de datos para controlar la primera unidad de captación de datos.

En otra ejecución determina el control de la primera unidad de captación de datos mediante la segunda unidad de captación de datos el procesamiento de los primeros datos mediante la primera unidad de captación de datos.

## ES 2 984 525 T3

El control incluye entre otros también la gestión de la primera unidad de captación de datos. La gestión se refiere a parámetros de configuración, pero en particular a aplicaciones de procesamiento previo/aplicaciones de filtrado (de datos) en las primeras unidades de captación de datos/DCUs satélite.

5 En otra ejecución, contiene el control de la primera unidad de captación de datos una configuración de la captación de los primeros datos, una configuración de una agregación de los primeros datos, una configuración de un procesamiento previo de los primeros datos (por ejemplo un acondicionamiento estadístico de datos) y/o una configuración de un filtrado (por ejemplo en función de la dirección de la red/la dirección IP, protocolo) de los primeros datos.

10 Las primeras unidades de captación de datos/DCUs satélite no tienen que configurarse con preferencia por sí mismas, ya que las mismas son configuradas por la segunda unidad de captación de datos/DCU master. Debido a ello pueden instalarse otras primeras unidades de captación de datos/DCUs satélite durante el funcionamiento.

De esta manera sigue siendo posible una fácil adaptación a nuevos patrones de ataque.

15 En otra ejecución realiza la segunda unidad de captación de datos un procesamiento de datos y un filtrado de los segundos datos.

En otra ejecución retransmite la segunda unidad de captación de datos los segundos datos recopilados a otra unidad.

20 En otra ejecución la otra unidad es un sistema backend o un servidor.

Además, se realiza en general un procesamiento y filtrado adicional en la segunda unidad de captación de datos/DCU master, que puede retransmitir los segundos datos a continuación al sistema backend/servidor. También pueden filtrarse y agregarse datos en varias etapas (es decir, tiene lugar un procesamiento previo próximo a las células, próximo a la zona de la red de automatización; entonces se realizan las transiciones sin repercusiones. Esta compresión de datos es sobre todo ventajosa para conexiones IoT y/o a la nube (cloud), ya que pueden ahorrarse costes para transmisión de datos.

25 En otra ejecución vigila la segunda unidad de captación de datos la integridad (inclusive cableado) de la primera unidad de captación de datos o bien de varias primeras unidades de captación de datos.

30 Así puede protegerse entre otros la integridad de la instalación completa. En particular puede vigilarse así también que la instalación de las primeras unidades de captación de datos/DCUs no se haya manipulado, lo cual dado el caso pondría en peligro la ausencia de repercusiones.

35 En otra ejecución tienen la primera unidad de captación de datos y la segunda unidad de captación de datos una unidad de comunicación unidireccional.

40 Se realiza entonces para una ruta de comunicación de datos de usuario una doble aplicación de la característica de comunicación unidireccional/unidad de comunicación unidireccional, por un lado a la primera unidad de captación de datos/DCU satélite y por otro lado a la segunda unidad de captación de datos/DCU master. Éstas pueden estar realizadas técnicamente idénticas.

45 En otra ejecución está realizada la unidad de comunicación unidireccional en la primera unidad de captación de datos lógicamente, basada en software y/o basada en FPGA.

En otra ejecución está realizada la unidad de comunicación unidireccional en la segunda unidad de captación de datos apoyada por hardware.

50 Con preferencia está prevista por un lado, en particular la DCU satélite, una realización fácil de llevar a cabo de la característica de comunicación unidireccional/unidad de comunicación unidireccional (por ejemplo una realización lógica, basada en software o basada en FPGA) y por otro lado una realización física/apoyada por hardware (por ejemplo utilizando una vía de comunicación unidireccional física). De esta manera se logra una doble protección unidireccional que puede realizarse eficientemente. Puesto que están implementadas realizaciones independientes tecnológicamente de la característica unidireccional, se logra una protección especialmente alta.

55 Puede estar previsto que sólo tenga que preverse una realización especial apoyada por hardware centralmente (en la segunda unidad de captación de datos/DCU master), con lo cual pueden llevarse a cabo realizaciones de la primera unidad de captación de datos/DCU satélite especialmente económicas.

60 En otra ejecución tiene la conexión a red características bidireccionales y/o unidireccionales.

65 La gestión de un equipo de comunicación unidireccional exige una comunicación bidireccional entre la segunda unidad de captación de datos/DCU master y una primera unidad de captación de datos/DCU satélite. No obstante debe ser posible en cuanto a datos de usuario interceptados sólo una comunicación unidireccional.

Para la gestión de una primera unidad de captación de datos/DCU satélite mediante la segunda unidad de captación de datos/DCU master puede estar prevista una conexión de comunicación bidireccional. La primera unidad de captación de datos/DCU satélite asegura que los datos de gestión sólo puedan alcanzar la propia primera unidad de captación de datos/DCU satélite y ser procesados por la misma, pero no pueden ser retransmitidos a la red interna (zona de la red de automatización). De esta manera se impide que puedan infiltrarse a través de la conexión bidireccional de la segunda unidad de captación de datos/DCU master a la primera unidad de captación de datos/DCU satélite de la segunda unidad de captación de datos/DCU master a través de las primeras unidades de captación de datos/DCUs satélite a la zona de la red de automatización (por ejemplo células de producción).

Esto puede lograrse por ejemplo pudiendo leer la interfaz interna de la primera unidad de captación de datos/DCU satélite sólo pasivamente.

Esto puede lograrse en otra variante no teniendo el componente de software de la primera unidad de captación de datos/DCU satélite para gestionar las primeras unidades de captación de datos ningún acceso a la interfaz de red interna, sino sólo a la interfaz de red externa. Esto puede lograrse por ejemplo en un sistema basado en Linux mediante SELinux.

Esto puede realizarse en otra variante utilizando dos canales de comunicación separados (por ejemplo VLANs) entre la primera unidad de captación de datos/DCU satélite y la segunda unidad de captación de datos/DCU master, uno para la gestión de la primera unidad de captación de datos/DCU satélite y una para la transmisión unidireccional de datos de usuario.

En otra variante esto está separado en el tiempo (bien gestión o bien transmisión de datos de usuario). Con preferencia activa una primera unidad de captación de datos/DCU satélite en la interfaz hacia la segunda unidad de captación de datos/DCU master temporalmente tras un arranque del sistema una conexión de comunicación bidireccional hacia la segunda unidad de captación de datos/DCU master, para consultar la configuración. Tras recibirse la configuración se desactiva el modo de funcionamiento bidireccional, con lo que a continuación sólo es posible una comunicación unidireccional desde la primera unidad de captación de datos/DCU satélite hacia la segunda unidad de captación de datos/DCU master.

La invención reivindica además un procedimiento para el funcionamiento de una red de datos para instalaciones industriales, caracterizado por las etapas:

- una generación de primeros datos por parte de al menos una zona de la red de automatización, teniendo la zona de la red de automatización al menos un componente de automatización,
- una captación de los primeros datos mediante una primera unidad de captación de datos y
- una transmisión de los primeros datos como segundos datos desde la primera unidad de captación de datos a una segunda unidad de captación de datos a través de una conexión de red,

constituyendo la primera unidad de captación de datos y la segunda unidad de captación de datos conjuntamente una One-Way Gateway.

En otra realización puede ejecutarse el procedimiento con la red de datos de acuerdo con la invención.

La invención ofrece las siguientes ventajas:

- Conexión segura, estrictamente unidireccional, de zonas de la red de automatización por ejemplo de instalaciones industriales a sistemas backend de IoT.
- Acceso a datos y agregación de datos (por ejemplo de subsegmentos aislados de una red de una instalación industrial) para la compresión local, filtrado y/o análisis y una retransmisión a un sistema backend de IoT.
- Fácil realización de la conexión backend de IoT (por ejemplo el menor coste posible para la gestión clave para establecer conexiones seguras) manteniendo el nivel de seguridad/protección de las redes.
- Una característica de comunicación unidireccional puede realizarse de forma practicable en sistemas de automatización con una mayoría o pluralidad de zonas de la red de automatización/células de fabricación aisladas al nivel de red.
- Puede instalarse sin poner en peligro un funcionamiento fiable, ya que ni la red interna de las células ni la red de fábrica se ven influidas. Así no puede producirse tampoco una influencia sobre la comunicación entre zonas de la red de automatización/células de fabricación a través de la red de fábrica.
- Casos de uso (use cases) de seguridad esenciales, como el establecimiento de memorias centrales de datos de registro y/o sistemas de monitorización de red para vigilar la integridad, pueden realizarse así económicamente sin influir negativamente sobre el nivel de riesgo para la instalación.
- Otra ventaja esencial de esta realización es que material clave para una conexión a sistemas backend de IoT sólo tiene que gestionarse en DCUs master/segundas unidades de captación de datos. Esto reduce el coste en gestión y ofrece una buena escalación.

Breve descripción de los dibujos

5 Las particularidades y ventajas de la invención quedarán visibles a partir de las explicaciones siguientes relativas a varios ejemplos de realización en base a dibujos esquemáticos.

Se muestra en

10 figura 1 una red de datos,  
figura 2 una red con una red de datos con dos primeras unidades de captación de datos y  
figura 3 un diagrama secuencial.

Descripción detallada de la invención

15 La figura 1 muestra una red de datos 1 para instalaciones industriales.

La red de datos 1 se caracteriza por:

- 20
- al menos una primera unidad de captación de datos S-DCU, que está constituida para captar primeros datos generados por al menos una zona de la red de automatización 2 asociada a la misma y transmitirlos como segundos datos a través de una conexión de red 4 y
  - una segunda unidad de captación de datos M-DCU, que está constituida para recopilar los segundos datos,

25 teniendo la zona de la red de automatización 2 al menos un componente de automatización 5 (sólo representado en la figura 2) y

constituyendo la primera unidad de captación de datos S-DCU y la segunda unidad de captación de datos M-DCU conjuntamente una One-Way Gateway. Así se logra evitar que influya sobre el sistema de automatización de la zona de la red de automatización 2 una red externa, es decir, a la derecha de la segunda unidad de captación de datos M-DCU. Queda garantizada así una ausencia de repercusiones (freedom of interference).

30 La zona de la red de automatización 2 está integrada en una red de orden superior 3, por ejemplo una red de fábrica 3 o una red industrial 3.

35 La One-Way Gateway puede denominarse también vía de comunicación unidireccional o vía de comunicación de un solo sentido.

40 La idea básica de la invención consiste en realizar jerárquicamente una solución One-Way Gateway. Se utilizan varias primeras unidades de captación de datos S-DCU/ DCU satélite S-DCUs para captar datos de varias zonas de la red de automatización 2 sin repercusión y transmitirlos a continuación a una segunda unidad de captación de datos M-DCU/DCU master M-DCU para el procesamiento posterior.

45 Este concepto puede proseguir a lo largo de varias etapas. Es decir, zonas de la red de automatización 2 pueden dividirse a su vez en subzonas y agregarse datos de éstas mediante el mismo mecanismo. Esto tiene la ventaja de que con poco coste pueden preverse primeras unidades de captación de datos S-DCU/ DCU satélite S-DCUs para una mayoría/pluralidad de zonas de la red de automatización 2 en configuración jerárquica. Cada primera unidad de captación de datos S-DCU/DCU satélite S-DCU lleva asociadas así varias zonas de la red de automatización 2.

50 La gestión de un equipo de comunicación unidireccional exige una comunicación bidireccional 4b entre la segunda unidad de captación de datos M-DCU/DCU master M-DCU y una primera unidad de captación de datos S-DCU/DCU satélite S-DCU. No obstante en cuanto a datos de usuario interceptados sólo debe ser posible una comunicación unidireccional 4a.

55 Para la gestión de una primera unidad de captación de datos S-DCU/DCU satélite S-DCU mediante la segunda unidad de captación de datos M-DCU/DCU master M-DCU, puede estar prevista una conexión de comunicación bidireccional 4b. La primera unidad de captación de datos S-DCU/DCU satélite S-DCU asegura que los datos de gestión sólo alcancen la propia unidad de captación de datos S-DCU/DCU satélite S-DCU y sean procesados por la misma, pero no se retransmitan a la red interna 2 (zona de la red de automatización 2). De esta manera se impide que mediante la comunicación bidireccional 4b puedan infiltrarse desde la segunda unidad de captación de datos M-DCU/DCU master M-DCU a la primera unidad de captación de datos S-DCU/DCU satélite S-DCU datos de la segunda unidad de captación de datos M-DCU/DCU master M-DCU a través de las primeras unidades de captación de datos S-DCU/DCU satélite S-DCU hasta la zona de la red de automatización 2 (por ejemplo células de producción).

60 Esto puede lograrse por ejemplo cuando la interfaz interna de la primera unidad de captación de datos S-DCU/DCU satélite S-DCU sólo puede leer pasivamente.

65

Esto puede lograrse en otra variante no teniendo el componente de software de la primera unidad de captación de datos S-DCU/DCU satélite S-DCU para la gestión de las primeras unidades de captación de datos S-DCUs ningún acceso a la interfaz de red interna, sino sólo a la interfaz de red externa. Esto puede lograrse por ejemplo en un sistema basado en Linux, mediante SELinux.

Esto se realiza en otra variante utilizando dos canales de comunicación separados (por ejemplo VLANs) entre la primera unidad de captación de datos S-DCU/DCU satélite S-DCU y la segunda unidad de captación de datos M-DCU/DCU master M-DCU, uno para la gestión de las primeras unidades de captación de datos S-DCUs y uno para la transmisión unidireccional de datos de usuario.

En otra variante esto está separado en el tiempo (bien gestión o bien transmisión de datos de usuario). Con preferencia activa una primera unidad de captación de datos S-DCU/DCU satélite S-DCU en la interfaz hacia la segunda unidad de captación de datos M-DCU/DCU master M-DCU temporalmente tras un arranque del sistema una conexión de comunicación bidireccional 4b hacia la segunda unidad de captación de datos M-DCU/DCU master M-DCU, para consultar la configuración. Tras recibir la configuración, se desactiva el modo de funcionamiento bidireccional, con lo que a continuación sólo es posible una comunicación unidireccional desde la primera unidad de captación de datos S-DCU/DCU satélite S-DCU hasta la segunda unidad de captación de datos M-DCU/DCU master M-DCU.

La figura 2 muestra una realización con dos zonas de la red de automatización 2/células de fabricación 2 en respectivas redes de células 2a (Production Cell Network 2a). Una zona de la red de automatización 2/célula de fabricación 2 puede estar prevista por ejemplo para un único componente de automatización 5, por ejemplo una máquina 5 (por ejemplo una máquina fresadora con control) o para una zona parcial de una línea de fabricación (por ejemplo una banda de varias bandas de una fábrica). Las redes de células 2a están conectadas mediante respectivas firewalls FW con una red de orden superior 3, por ejemplo una red de fábrica (Plan Network 3). De esta manera no se puede interceptar la comunicación de datos (datos de control de la célula de fabricación 2) interna de la célula en la red de fábrica 3. La red de fábrica 3 tiene un sistema Supervisory Control and Data Acquisition (control de supervisión y adquisición de datos) SCADA y un LogServer LS.

Por ello están previstos en las distintas redes de células 2a primeras unidad de captación de datos/DCU satélite S-DCU, que como interfaz unidireccional interceptan la comunicación de datos de la zona de la red de automatización 2/ célula de fabricación 2 y a través de una conexión de red unidireccional 4a/ una red de monitorización unidireccional 4a, proporcionan los datos interceptados a una segunda unidad de captación de datos/ DCU master M-DCU. Allí puede vigilarse entonces centralmente mediante una vigilancia de integridad del sistema 6 (on-premises) local la integridad de la mayoría de zonas de la red de automatización 2/ células de fabricación 2. Además pueden retransmitirse los datos de vigilancia de la integridad de la célula a través de una IoT-Gateway 7 a un IoT-Backend 8 con un sistema backend 9 (por ejemplo un Backend System Integrity Monitoring Service 9). También es posible (no se representa) proporcionar los datos de vigilancia de integridad a una infraestructura de cadenas de bloques (Blockchain, Distributed Ledger).

En el ejemplo de realización representado está prevista una red de monitorización unidireccional separada. Esta puede estar realizada por ejemplo como Ethernet, a través de conductores de fibra óptica o como red de radio (WLAN, WiMax, telefonía móvil 5G). No obstante, también es posible realizar esta red como red virtual, por ejemplo como una red separada Slice de una red de telefonía móvil 5G o a través de una VLAN (LAN virtual) o bien Software Defined Network, en base a la misma infraestructura de red básica que la red de fábrica.

La figura 3 muestra un diagrama secuencial de un procedimiento para el funcionamiento de una red de datos para instalaciones industriales, caracterizada por las etapas:

- Primera etapa S1: una generación de primeros datos mediante al menos una zona de la red de automatización, teniendo la zona de la red de automatización al menos un componente de automatización,
- segunda etapa S2: una captación de los primeros datos mediante una primera unidad de captación de datos y
- tercera etapa S3: una transmisión de los primeros datos como segundos datos desde la primera unidad de captación de datos a una segunda unidad de captación de datos a través de una conexión de red, constituyendo la primera unidad de captación de datos y la segunda unidad de captación de datos conjuntamente una One-Way Gateway.

Aun cuando la invención se ha ilustrado más en detalle y descrito mediante los ejemplos de realización, no queda limitada la invención por los ejemplos dados a conocer y el especialista puede deducir de ello otras variaciones sin abandonar el alcance de protección de la invención.

**Lista de referencias**

	1	red de datos
	2	zona de red de automatización/célula de fabricación
5	2a	red de célula/Production Cell Network
	3	red de orden superior/red de fábrica
	4	conexión de red
	4a	conexión de red unidireccional
	4b	conexión de red bidireccional
10	5	componente de automatización/máquina
	6	vigilancia de integridad del sistema
	7	IoT-gateway
	8	IoT-backend
	9	sistema backend
15	FW	firewall
	LS	Log Server
	M-DCU	segunda unidad de captación de datos/DCU master
	SCADA	Supervisory Control and Data Acquisition
20	S-CDU	primera unidad de captación de datos/DCU satélite
	S1	primera etapa
	S2	segunda etapa
	S3	tercera etapa

REIVINDICACIONES

1. Red de datos (1) para instalaciones industriales,
  - 5 -- al menos una primera unidad de captación de datos (S-DCU), que está constituida para captar primeros datos generados por al menos una zona de una red de automatización (2) asociada a la misma y transmitirlos como segundos datos a través de una conexión de red (4) y además para procesar los primeros datos y
  - una segunda unidad de captación de datos (M-DCU), que está constituida para recopilar los segundos datos, teniendo la zona de la red de automatización (2) al menos un componente de automatización (5) y constituyendo la primera unidad de captación de datos (S-DCU) y la segunda unidad de captación de datos (M-DCU) conjuntamente una One-Way-Gateway,
    - 10 caracterizada porque
    - la segunda unidad de captación de datos (M-DCU) está constituida para controlar la primera unidad de captación de datos y
    - el control de la primera unidad de captación de datos (S-DCU) mediante la segunda unidad de captación de datos (M-DCU) determina el procesamiento de los primeros datos mediante la primera unidad de captación de datos (S-DCU).
2. Red de datos (1) de acuerdo con la reivindicación 1,
  - 20 caracterizada porque el control de la primera unidad de captación de datos (S-DCU) contiene una configuración de la captación de los primeros datos, una configuración de una agregación de los primeros datos, una configuración de un procesamiento previo de los primeros datos y/o una configuración de un filtrado de los primeros datos.
3. Red de datos (1) de acuerdo con una de las reivindicaciones precedentes,
  - 25 caracterizada porque la segunda unidad de captación de datos (M-DCU) realiza un procesamiento de datos y un filtrado de los segundos datos.
4. Red de datos (1) de acuerdo con una de las reivindicaciones precedentes,
  - 30 caracterizada porque la segunda unidad de captación de datos (M-DCU) vigila la integridad de la primera unidad de captación de datos (S-DCU).
5. Red de datos (1) de acuerdo con una de las reivindicaciones precedentes,
  - caracterizada porque la segunda unidad de captación de datos (M-DCU) retransmite los segundos datos recopilados a otra unidad.
6. Red de datos (1) de acuerdo con la reivindicación 5,
  - 35 caracterizada porque la otra unidad es un sistema backend (9) o un servidor.
7. Red de datos (1) de acuerdo con una de las reivindicaciones precedentes,
  - 40 caracterizada porque la primera unidad de captación de datos (S-DCU) y la segunda unidad de captación de datos (M-DCU) tienen una unidad de comunicación unidireccional.
8. Red de datos (1) de acuerdo con una de las reivindicaciones precedentes,
  - 45 caracterizada porque la unidad de comunicación unidireccional, en la primera unidad de captación de datos (S-DCU), está realizada lógicamente, basada en software y/o basada en FPGA.
9. Red de datos (1) de acuerdo con una de las reivindicaciones precedentes,
  - caracterizada porque la unidad de comunicación unidireccional, en la segunda unidad de captación de datos (M-DCU), está realizada apoyada por hardware.
10. Red de datos (1) de acuerdo con una de las reivindicaciones precedentes,
  - 50 caracterizada porque la conexión a red (4) tiene características bidireccionales (4b) y/o unidireccionales (4a).
11. Procedimiento para el funcionamiento de una red de datos (1) para instalaciones industriales, que tiene las etapas:
  - 55 -- una generación (S1) de primeros datos por parte de al menos una zona de la red de automatización (2), teniendo la zona de la red de automatización (2) al menos un componente de automatización (5),
  - una captación (S2) de los primeros datos mediante una primera unidad de captación de datos (S-DCU) y
  - una transmisión de los primeros datos como segundos datos desde la primera unidad de captación de datos (S-DCU) a una segunda unidad de captación de datos (M-DCU) a través de una conexión de red (4), constituyendo la primera unidad de captación de datos (S-DCU) y la segunda unidad de captación de datos (M-DCU) conjuntamente una One-Way Gateway,
    - 60 caracterizado por:
    - una determinación de un control de la primera unidad de captación de datos (S-DCU) mediante la segunda unidad de captación de datos (M-DCU) en cuanto a un procesamiento de los primeros datos por parte de la primera unidad de captación de datos (S-DCU).

12. Procedimiento de acuerdo con la reivindicación 11, ejecutado mediante una red de datos (1) de acuerdo con una de las reivindicaciones 1 a 10.

FIG 1

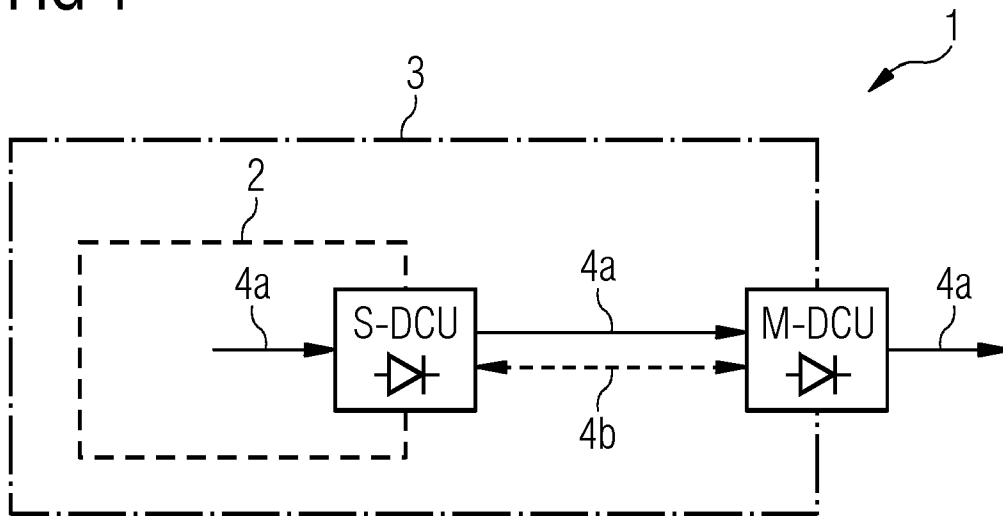


FIG 2

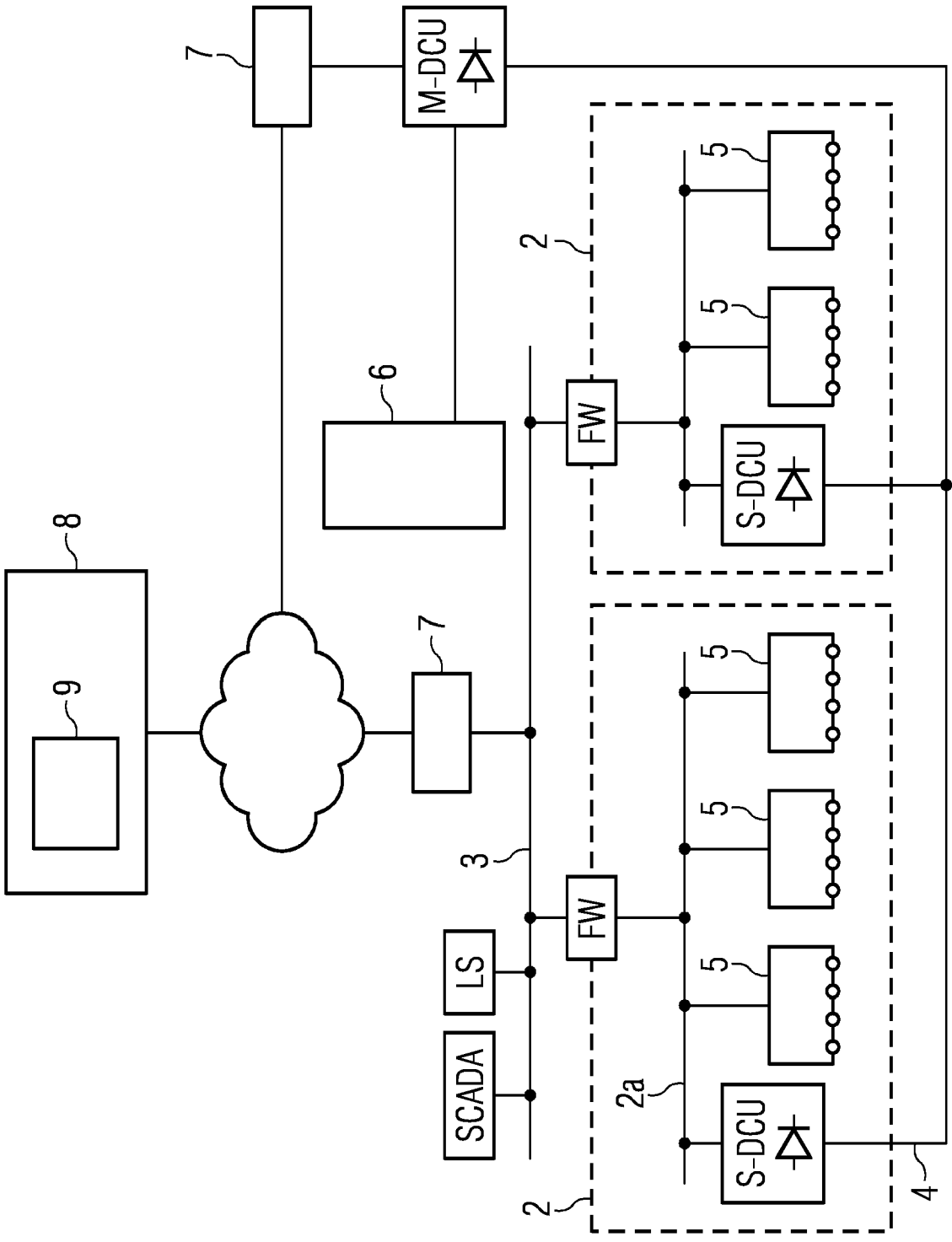


FIG 3

