(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 613 701**

(51) Int. CI.:

G05B 9/02 (2006.01)
F03D 7/04 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.03.2012 PCT/DK2012/050097**

(87) Fecha y número de publicación internacional: **04.10.2012 WO2012130246**

(96) Fecha de presentación y número de la solicitud europea: **29.03.2012 E 12713867 (5)**

(97) Fecha y número de publicación de la concesión europea: **14.12.2016 EP 2691819**

(54) Título: **Sistema de control y protección distribuido tolerante a fallos**

(30) Prioridad:

30.03.2011 DK 201170152 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.05.2017

(73) Titular/es:

VESTAS WIND SYSTEMS A/S (100.0%)
Hedeager 42
8200 Aarhus N, DK

(72) Inventor/es:

BENGTSON, JOHN

(74) Agente/Representante:

ARIAS SANZ, Juan

DESCRIPCIÓN

Sistema de control y protección distribuido tolerante a fallos

Campo de la invención

La presente invención se refiere a sistemas de control de instalaciones de energía eólica que utilizan nodos de control distribuidos con propiedades de tolerancia a fallos y relacionadas con la seguridad. Los nodos de control distribuidos se conectan mediante una red de comunicación determinista tolerante a fallos. Los nodos de control distribuidos comprenden esquemas de votación descentralizada, apuntando dichos esquemas de votación descentralizada a la selección de los puntos de consigna de control o valores de datos más fiables entre una pluralidad de puntos de consigna de control o valores de datos disponibles. Los nodos de control distribuidos comprenden funciones de votación inherentes en términos de circuitos electrónicos, eléctricos o hidráulicos.

Antecedentes de la invención

Las turbinas eólicas modernas se diseñan para producción en serie. Se usa la modularización como un medio para establecer una producción de subconjuntos ajustada. Es deseable, por lo tanto, dividir en módulos el sistema de control de acuerdo con la modularización de la turbina eólica para permitir la fabricación y ensayos de subconjuntos en una instalación de producción ajustada.

Las plantas modernas de generación de energía comprenden no solamente turbinas eólicas, sino también otras instalaciones tales como, por ejemplo, sistemas de medición de potencia, sistemas de compensación de fase, sistemas de metrología, sistemas de interruptores de potencia y sistemas de almacenamiento de energía. Dichos sistemas también se pueden dividir en módulos para permitir la fabricación y ensayo de subconjuntos en una instalación de producción ajustada. Los sistemas en sí mismos pueden considerarse módulos en una planta de energía eólica y, por ello, contener nodos de control distribuidos. Se considera beneficioso dividir en módulos el sistema de control de acuerdo con la modularización del sistema.

Las turbinas eólicas modernas y otros sistemas de plantas de generación de energía están sometidos a elevados requisitos de disponibilidad y producción de energía y, en consecuencia, las paradas de producción provocadas por el sistema de control se consideran inaceptables. Los requisitos de fiabilidad para los sistemas de control de turbinas eólicas son, por lo tanto, muy altos. Sistemas de control basados en tolerancia a fallos son medios para obtener los requisitos de fiabilidad y seguridad deseados.

Las turbinas eólicas modernas están sometidas a elevados requisitos de seguridad. Las grandes turbinas eólicas modernas tienen elevadas demandas en cuanto a seguridad funcional. El sistema de control debe tener propiedades de seguridad funcional para soportar las demandas. Las instalaciones de almacenamiento de energía, sistemas de convertidores de potencia, sistemas de interruptores de potencia y otros sistemas de plantas de generación de energía pueden presentar también elevadas demandas en cuanto a seguridad funcional, dado que el impacto de las averías puede ser grave tanto en relación con la salud humana como con respecto a daños a los activos.

Los sistemas de control tolerantes a fallos para plantas de energía eólica se implementan típicamente como sistemas redundantes que comprenden duplicados de varios módulos/dispositivos críticos de la planta. En caso de que un módulo/dispositivo crítico de la planta falle, su funcionalidad es asumida por un módulo/dispositivo similar de la planta.

Los documentos US 2009/0309360 y US 2009/0309361 explican ambos un método y un sistema para el control de un parque de energía eólica. En los documentos US 2009/0309360 y US 2009/0309361, una unidad de comunicación principal controla varias unidades de control priorizadas. En caso de que una unidad de control dada con una prioridad dada falle, la unidad de comunicación principal selecciona una unidad de control de prioridad más baja para hacerse cargo de la funcionalidad de la unidad de control defectuosa.

Es una desventaja del método y sistema sugeridos en los documentos US 2009/0309360 y US 2009/0309361 que la unidad de comunicación principal selecciona qué unidad de control ha de hacerse cargo en caso de que otra unidad de control se averíe o funcione defectuosamente de cualquier otro modo. Sin embargo, en caso de que se averíe la unidad de comunicación principal en sí, no hay unidad de sustitución disponible.

Por ello, el método de control y el sistema de control sugeridos en los documentos US 2009/0309360 y US 2009/0309361 no pueden considerarse un método/sistema de control tolerante a fallos —al menos no en el nivel del controlador principal—. Más aún, el método de control y el sistema de control sugeridos en los documentos US 2009/0309360 y US 2009/0309361 no pueden considerarse seguros, dado que no se implementan características de seguridad.

Puede verse como un objeto de las realizaciones de la presente invención proporcionar un sistema de control distribuido con propiedades inherentes de tolerancia a fallos y relacionadas con la seguridad para aplicaciones de

plantas de energía eólica.

Descripción de la invención

El objeto anteriormente mencionado puede cumplirse proporcionando, en un primer aspecto, un sistema de control distribuido tolerante a fallos para una instalación de energía eólica modularizada que comprende subconjuntos, comprendiendo el sistema de control

- medios de control tolerantes a fallos adaptados para generar puntos de consigna de control y/o valores de datos, estando dichos medios de control tolerantes a fallos distribuidos en subconjuntos de acuerdo con la modularización de la instalación de energía eólica y

- una red de comunicación tolerante a fallos para la transmisión de los puntos de consigna de control y/o valores de datos esencialmente al mismo tiempo a una pluralidad de nodos en el sistema de control distribuido, siendo capaz dicha pluralidad de nodos distribuidos de seleccionar un paquete de transmisión válido de entre dos o más paquetes de transmisión proporcionados en la red de comunicación tolerante a fallos.

Se asocian las siguientes ventajas con el primer aspecto de la presente invención:

1. La arquitectura del sistema de control distribuido de la presente invención está de acuerdo con la modularización de las instalaciones modernas de energía eólica, tales como turbinas eólicas modernas y plantas de energía eólica modernas.

2. La arquitectura del sistema de control distribuido tolerante a fallos de la presente invención satisface los elevados requisitos de disponibilidad y fiabilidad que se plantean a las turbinas eólicas modernas y los sistemas de control de las plantas de energía eólica.

3. La arquitectura del sistema de control distribuido tolerante a fallos de la presente invención permite la integración de funciones de votación electrónica, eléctrica e hidráulica que soportan beneficiosamente series de producción de subconjuntos.

4. La arquitectura del sistema de control distribuido de la presente invención integra la seguridad funcional y es capaz de soportar las clases de modo de baja demanda, modo de alta demanda y modo continuo de las funciones relacionadas con la seguridad definidas en la norma IEC61508.

5. La arquitectura del sistema de control distribuido de la presente invención es escalable y flexible de tal forma que permite la adaptación de la funcionalidad a varias plataformas de turbina eólica y aplicaciones de planta de energía eólica.

La arquitectura del sistema de control de la presente invención refleja en general el principio de diseño establecido de “la forma sigue a la función”. Como se ha mencionado anteriormente, la arquitectura del sistema de control de la presente invención es aplicable en turbinas eólicas, plantas de energía eólica, subestaciones eléctricas, sistemas de almacenamiento de energía, estaciones metrológicas y en otras aplicaciones relacionadas con la energía.

La arquitectura del sistema de control puede comprender controladores primarios tales como, por ejemplo, Controladores Principales (MC), Controladores de Turbina (TC), Controladores de Seguridad (SC), Controladores de Potencia (PC), Controladores de Diagnóstico (DC).

Más aún, el sistema de control puede comprender Nodos de Control Distribuidos (DCN) que se interrelacionan con sensores y actuadores. Los DCN pueden servir como nodos de adquisición de datos, nodos de salida de control para uno o más controladores primarios o como controladores autónomos del sistema. Los DCN pueden tener funciones integradas relacionadas con la seguridad que soportan la seguridad funcional a nivel del sistema. Las funciones relacionadas con la seguridad pueden ser autónomas o pueden controlarse desde uno o más SC.

Los controladores primarios y DCN pueden ser tolerantes a fallo simple, doble o múltiple para dar soporte a la estructura del sistema y fiabilidad deseada. Más aún, los controladores primarios y los nodos de control distribuidos pueden ser réplicas deterministas para dar soporte a la tolerancia a fallos a nivel del sistema.

La arquitectura del sistema de control de la presente invención puede aplicarse a una red de comunicación en tiempo real (RTCN) tolerante a fallos determinista con elevada fiabilidad y propiedades relacionadas con la seguridad.

Como ya se ha mencionado, la red de comunicación puede comprender una red de comunicación en tiempo real, tal como una Ethernet de activación por tiempo. La red de comunicación Ethernet de activación por tiempo puede implementarse como una red tolerante a fallo simple, una red tolerante a fallo doble o incluso una red tolerante a fallo múltiple. Más aún, la red de comunicación Ethernet de activación por tiempo puede estar certificada para

seguridad.

La red de comunicación puede soportar clases de seguridad funcional en modo de baja demanda, modo de alta demanda y modo continuo, tal como se define en la norma IEC61508.

Las funciones de seguridad funcional cumplen con los requisitos para Nivel de Integridad de Seguridad 2 (SIL 2) o Nivel de Integridad de Seguridad 3 (SIL 3).

El sistema de control distribuido tolerante a fallos puede comprender adicionalmente sistemas de sensores tolerantes a fallos que comprenden una pluralidad de sensores. La pluralidad de sensores puede disponerse de una forma redundante. La pluralidad de sensores está adaptada para medir al menos un parámetro relevante para el control de al menos un subsistema de la instalación de energía eólica.

Ejemplos de subconjuntos de turbina eólica son sistemas de paso de pala, sistemas de orientación, sistemas de árbol principal, sistemas de engranajes, sistemas de generador, sistemas de convertidor de potencia y sistemas de interruptores de potencia.

El sistema de control distribuido tolerante a fallos, y en particular los nodos de control distribuidos, pueden comprender adicionalmente medios de votación adaptados para votar entre valores de datos entre una pluralidad de fuentes, estando adaptados dichos medios de votación para votar de acuerdo con el principio de votación 1 de 2 (1oo2), 2 de 2 (2oo2), 2 de 3 (2oo3) u otro principio de votación adecuado. Las fuentes para proporcionar valores de datos pueden incluir uno o más controladores primarios.

Pueden disponerse al menos dos controladores primarios redundantes en una configuración de réplica determinista. Los al menos dos controladores primarios redundantes pueden comprender un controlador primario activo y uno o más controladores de reserva en caliente. Como alternativa, los al menos dos controladores primarios redundantes pueden comprender un controlador primario activo y uno o más controladores de reserva en frío.

En un segundo aspecto, la presente invención se refiere a un sistema de control distribuido tolerante a fallos para el control de uno o más objetos de una instalación de energía eólica, comprendiendo el sistema de control

- medios de control tolerantes a fallos que presenten un comportamiento de fallo seguro adaptado para controlar uno o más objetos,

- medios de votación electrónicos, eléctricos o hidráulicos para el control tolerante a fallos de los uno o más objetos y

- medios para la supervisión y/o el diagnóstico de los medios de votación.

De modo similar al primer aspecto, la expresión instalación de energía eólica cubre turbinas eólicas individuales o grupos de turbinas eólicas que forman una planta de energía eólica.

Los uno o más objetos a ser controlados pueden implicar sistemas de paso de palas, sistemas de orientación, sistemas de árbol principal, sistemas de engranajes, sistemas de generador, sistemas de convertidor de potencia y sistemas de interruptores de potencia.

El sistema de control distribuido tolerante a fallos de acuerdo con el segundo aspecto puede comprender adicionalmente un esquema de control de réplica determinista. De modo similar al primer aspecto de la presente invención, el sistema de control distribuido puede soportar tolerancia a fallo simple, tolerancia a fallo doble o tolerancia a fallo múltiple.

Pueden proporcionarse asimismo unidades de fuente de alimentación distribuidas adaptadas para soportar una partición de entre una pluralidad de particiones. Más aún, puede soportarse desacoplamiento en el dominio del fallo entre particiones.

Un tercer aspecto la presente invención se refiere a un método para el control de una instalación de energía eólica modularizada que comprende subconjuntos, comprendiendo el método las etapas de

- generación de puntos de consigna de control y/o valores de datos usando medios de control tolerantes a fallos, estando distribuidos dichos medios de control tolerantes a fallos en subconjuntos de acuerdo con la modularización de la instalación de turbina eólica,

- transmisión de los puntos de consigna de control y/o valores de datos generados esencialmente al mismo tiempo a una pluralidad de nodos en el sistema de control distribuido a través de una red de comunicación tolerante a fallos y

- selección, usando la pluralidad de nodos distribuidos, de un paquete de transmisión válido de entre dos o más paquetes de transmisión proporcionados en la red de comunicación tolerante a fallos.

En un cuarto aspecto final, la presente invención se refiere un método para el control de uno o más objetos de una instalación de energía eólica, comprendiendo el método las etapas de:

- proporcionar un medio de control tolerante a fallos que presente un comportamiento de fallo seguro adaptado para el control de uno o más objetos,
- proporcionar medios de votación electrónicos, eléctricos o hidráulicos para el control tolerante a fallos de los uno o más objetos y
- supervisar y/o diagnosticar los medios de votación.

El método de acuerdo con el tercer y cuarto aspectos puede ser aplicable en turbinas eólicas, plantas de energía eólica, subestaciones, sistemas de almacenamiento de energía, estaciones de metrología y otras aplicaciones de planta de energía eólica.

Es una ventaja de los métodos anteriormente mencionados que están de acuerdo con la modularización de las instalaciones de energía eólica modernas, tales como las turbinas eólicas modernas y las plantas de energía eólica modernas. Más aún, los métodos, si se ejecutan en un sistema de control distribuido tolerante a fallos, cumplen con los elevados requisitos de disponibilidad y fiabilidad que se plantean a las turbinas eólicas modernas y los sistemas de control de las plantas de energía eólica.

Además, los métodos permiten que las arquitecturas de sistema de control distribuido sean escalables y flexibles de forma tal que permitan la adaptación de la funcionalidad a varias plataformas de turbina eólica y aplicaciones de planta de energía eólica.

Breve descripción de los dibujos

La presente invención se explicará ahora con detalles adicionales con referencia a las figuras adjuntas, en las que

La Fig. 1 muestra una primera realización de un sistema de control distribuido genérico,

La Fig. 2 muestra una red de comunicación tolerante a fallo simple ejemplificada,

La Fig. 3 muestra una red de comunicación tolerante a fallo doble ejemplificada,

La Fig. 4 muestra un escenario de fallo simple ejemplificado en un subsistema tolerante a fallo simple genérico,

La Fig. 5 muestra un escenario de fallo doble ejemplificado en un subsistema tolerante a fallo doble genérico,

La Fig. 6 muestra un subsistema redundante n+m genérico ejemplificado,

La Fig. 7 muestra una vista genérica de un dominio de ejecución del controlador principal,

La Fig. 8 muestra una vista genérica de un dominio de ejecución del controlador de seguridad,

La Fig. 9 muestra una vista genérica de un dominio de ejecución sin maestro y

La Fig. 10 muestra una vista genérica de un dominio del tiempo global de precisión.

Aunque la invención es susceptible de varias modificaciones y formas alternativas, se han mostrado realizaciones específicas por medio de ejemplos en los dibujos y se describirán en detalle en el presente documento. Debería entenderse, sin embargo, que la invención no se pretende que esté limitada a las formas particulares divulgadas. Por el contrario, la invención ha de cubrir todas las modificaciones, equivalentes y alternativas que caen dentro del espíritu y alcance de la invención tal como se define por las reivindicaciones adjuntas.

Descripción detallada de la invención

En general, la presente invención se dirige a proporcionar un sistema de control distribuido para instalaciones de energía eólica, tales como turbinas eólicas y/u otros sistemas en una planta de energía eólica. En realizaciones preferidas de la invención, el sistema de control distribuido tiene propiedades tolerantes a fallos que dan soporte a alta fiabilidad y seguridad.

De acuerdo con la presente invención, el control tolerante a fallos en el sistema de control distribuido se lleva a cabo

mediante funciones redundantes que permiten la operación continuada en caso de que una o más funciones en un conjunto redundante de funciones falle(n). Las funciones redundantes se establecen mediante dos o más particiones físicas. Las particiones físicas pueden ser unidades completamente separadas o pueden ser unidades físicas únicas con partición interna o una combinación de los mismos.

En una realización de la invención, las particiones físicas forman dominios de fallos separados en donde un único fallo en un dominio no puede comprometer la función de la otra partición redundante o cualquier otra parte del sistema de control. También, cada función redundante puede tener fuentes de alimentación locales que dan soporte a la función de control y sensores y actuadores conectados. Esto asegura que una avería en un dominio de la fuente de alimentación no puede influir en la función de otros dominios en el sistema de control.

Controladores primarios dispuestos de modo redundante proporcionan un método y un sistema que da soporte a la votación entre valores de datos. Unos DCN dispuestos de modo redundante controlando objetos de una instalación de energía eólica proporcionan un método y un sistema que da soporte a la votación descentralizada entre valores de datos. La votación puede ser en términos de circuitos de votación dedicados o en términos de control simultáneo del objeto controlado por las funciones redundantes.

En una realización de la invención, los DCN que contienen las funciones redundantes integran funciones de votación en términos de circuitos de votación electrónicos, eléctricos o hidráulicos. Los nodos pueden integrar también circuitos de supervisión y funciones de diagnóstico para los circuitos de votación que soportan la fiabilidad y seguridad deseadas de las funciones. La integración de las funciones de votación puede ser una propiedad deseada en relación con la seguridad, tolerancia a fallos, fabricación y ensayos.

En una realización de la invención, los controladores primarios son réplicas deterministas, lo que significa que producen la misma salida esencialmente al mismo tiempo. Esta propiedad permite un control continuado en caso de una avería simple en un controlador primario. La propiedad es especialmente deseable en funciones relacionadas con la seguridad de modo continuo en donde la pérdida temporal del control se considera crítica o en funciones en donde se requiere una muy alta disponibilidad. Más aún, las funciones redundantes que controlan objetos de la instalación de energía eólica pueden ser réplicas deterministas, lo que significa que las funciones producen la misma salida esencialmente al mismo tiempo. Esta propiedad impide la votación errónea provocada por diferentes trayectorias de cálculo en las funciones. Las funciones redundantes pueden tener propiedades de fallo seguro, también denominadas a veces propiedades de fallo silencioso, lo que significa que las funciones fallarán a un estado pasivo en caso de avería interna. Esta propiedad impide que un controlador en fallo comprometa el funcionamiento de controladores no defectuosos. La propiedad de fallo seguro se impone por el diseño y tiene una alta probabilidad de función correcta. En las funciones relacionadas con la seguridad, la propiedad de fallo seguro tiene un nivel de integridad de seguridad (SIL) que cumple con los requisitos de seguridad globales para la función de control.

De acuerdo con la presente invención, un control tolerante a fallos en el sistema de control distribuido se lleva a cabo proporcionando un método y sistema que dan soporte a votación descentralizada entre puntos de consigna de control o valores de datos —es decir, en donde la selección de un punto de consigna o valor de datos se realiza en el nodo de consumo—. Un punto de consigna de control puede reflejar datos de control lógico de un Controlador Principal, Controlador de Turbina, Controlador de Seguridad, Controlador de la Planta de Generación o cualquier otro controlador. Un valor de datos puede reflejar datos medidos de una función de adquisición de datos o desde cualquier otra fuente de datos en el sistema.

Debe señalarse que los controladores y nodos pueden residir en una planta de energía eólica completa y por ello la presente invención no está limitada a comprender controladores y nodos dentro de una única turbina eólica.

Con referencia ahora a la Fig. 1, los sistemas de sensores 108, 109, 113, 114, 138, 139, 143 y 144 para la medición de, por ejemplo, potencia, frecuencia, tensión, corriente, presión o temperatura se conectan a los DCN replicados 110, 111, 117, 118, 136, 137, 141 y 142 respectivos, o bien directamente u, opcionalmente, a través de por ejemplo buses de campo, trayectorias de comunicación entre pares o cualquier otro tipo de interfaz. Los sistemas de sensores se posicionan en conjuntos de subsistemas (SSA) 112, 115, 140 y 145 junto con los DCN asociados. Otros SSA 107, 127, 131 y 135 comprenden DCN 104, 105, 124, 125, 128, 129, 132 y 133 para el control de objetos 106, 126, 130, 134 respectivos de la instalación de energía eólica.

Los DCN replicados adquieren datos de los sistemas de sensores y publican los datos adquiridos en la RTCN 103, poniendo así los datos a disposición de otros DCN en el sistema a través de conmutadores de RTCN 101, 102 replicados.

Los sensores que se replican con la finalidad de tolerancia a fallos o seguridad se conectan más preferentemente a diferentes DCN para conseguir el nivel más alto de tolerancia a fallos y fiabilidad.

Cualquier DCN puede tener la capacidad de votar entre valores de punto de consigna o valores de datos proporcionados por los controladores primarios u otros conmutadores de la RTCN en el sistema. Los puntos de consigna y valores de datos pueden representar lógica de control, datos de sensores u otras fuentes de datos.

Un posible escenario podría ser que un votador vote de acuerdo con el principio “2 de 3” (2oo3) —es decir, si uno de los valores de punto de consigna o valores de datos se desvía significativamente de los otros 2, el valor de punto de consigna o valor de datos desviado es ignorado—. Debería señalarse, sin embargo, que el proceso de votación no está limitado al esquema de votación 2oo3, es decir son aplicables asimismo otros esquemas de votación.

Con referencia todavía a la Fig. 1 se representa una disposición de una RTCN 103 genérica tolerante a fallo simple de acuerdo con una realización de la presente invención. La propiedad de tolerancia a fallo simple de la RTCN 103 se ilustra por las trayectorias de comunicación continua y discontinua entre los conmutadores de la RTCN 101, 102 replicados y los diversos DCN de la RTCN 103.

Como se ve en la Fig. 1, los Controladores Principales 118, 119 del SSA 120, los Controladores de Seguridad 121, 122 del SSA 123 y los DCN de otros SSA se interconectan conectados a través de la RTCN 103 que utiliza conmutadores de la RTCN 101, 102. Los conmutadores de la RTCN 101, 102 replicados se conectan en una topología de estrella-rama-estrella. Sin embargo, son también aplicables otras tecnologías de red.

La RTCN 103 sirve como la infraestructura de comunicación que conecta todos los DCN en el sistema. La RTCN 103 puede tener una conexión a la red de comunicación de la planta de generación a través de otros conmutadores de la RTCN 146. La RTCN 103 puede ser no tolerante a fallos, tolerante a fallo simple o tolerante a fallo doble dependiendo de los requisitos de fiabilidad.

La RTCN 103 podría basarse en una red de comunicación industrial tal como Ethernet/IP, Ethernet POWERLINK, PROFInet-IRT u otras redes de comunicación con propiedades similares.

En una realización preferida, la RTCN es una red de comunicación altamente determinista con propiedades de activación por tiempo. Dicha red podría ser TTEthernet u otras redes de comunicación que tengan propiedades similares. Este tipo de RTCN pone los datos a disposición esencialmente al mismo tiempo en los canales de la RTCN redundantes y por ello proporciona un soporte fuerte para tolerancia a fallos a nivel del sistema.

La TTEthernet combina las ventajas del paradigma de comunicación activado por tiempo con la flexibilidad de la ampliamente distribuida Ethernet. Soporta el tráfico Ethernet estándar, lo que asegura no interferencias con tráfico de datos crítico. En dichos paradigmas de comunicación, la comunicación de datos en tiempo real en la RTCN se planifica en la fase de diseño y los nodos asociados tienen un conocimiento *a priori* de cuándo están disponibles los datos. La TTEthernet también proporciona un tiempo global de precisión tolerante a fallos a todos los nodos del sistema. Estas propiedades permiten que dos o más nodos replicados por suscripción a los mismos datos puedan garantizarse que funcionan sobre los mismos datos al mismo tiempo y, debido al tiempo global de precisión, se diseñan para ejecutar las mismas funciones esencialmente al mismo tiempo, y por ello son réplicas deterministas.

Preferentemente, la RTCN tiene propiedades específicas que dan soporte a funciones relacionadas con la seguridad en “modo continuo” tal como se define en la norma IEC61508. Las funciones de seguridad en modo continuo dependerían de datos relativos a la seguridad comunicados entre nodos en la RTCN para realizar la función de seguridad. TTEthernet soporta inherentemente funciones de seguridad en modo continuo por su tolerancia a fallos y sus propiedades relacionadas con la seguridad. El sistema de comunicación TTEthernet es certificable respecto a seguridad. Mediante la utilización de este tipo de red de comunicación, la capacidad de la arquitectura tolerante a fallos de la presente invención puede extenderse para comprender todas las clases de funciones de seguridad: funciones de seguridad en modo de baja demanda, modo de alta demanda y modo continuo de acuerdo con las definiciones en la norma IEC61508.

La arquitectura de comunicación descansa preferentemente sobre la confiable red de comunicación TTEthernet mencionada anteriormente. En dicha realización, el tráfico de datos de diferente criticidad puede coexistir en la RTCN. La arquitectura de comunicación da soporte a la coexistencia de diferentes dominios de ejecución en la misma RTCN sin interferencia mutua. Dichos dominios de ejecución podrían ser:

- dominio de ejecución maestro centralizado no relacionado con la seguridad, consúltese la Fig. 7,
- dominio de ejecución maestro centralizado relacionado con la seguridad, consúltese la Fig. 8,
- dominio de ejecución sin maestro, consúltese la Fig. 9,

Las Figs. 7, 8 y 9 se explicarán con detalle adicional a continuación.

En un sistema de control distribuido, la tolerancia a fallos puede obtenerse por réplica de canales de comunicación, incluyendo los conmutadores de la RTCN, y de los DCN.

Las Figs. 2 y 3 muestran redes de comunicación tolerantes a fallo simple ejemplificadas y redes de comunicación tolerantes a fallo doble ejemplificadas, respectivamente.

Con referencia ahora a la Fig. 2, los conmutadores de la RTCN 201, 202 replicados están en comunicación con los DCN 205-210. De modo similar, los conmutadores de la RTCN 203, 204 replicados están en comunicación con los DCN 211-214. Como puede verse en la Fig. 2, cada DCN se conecta a dos conmutadores de la RTCN. Se proporciona una única trayectoria de comunicación RT 200 tolerante a fallos entre los conmutadores de la RTCN 201, 202 y 203, 204. Más aún, está disponible una trayectoria de comunicación RT 215 para la conexión a otros conmutadores de la RTCN.

En referencia ahora a la Fig. 3, los conmutadores de la RTCN 301-303 replicados están en comunicación con los DCN 304-309 formando de ese modo una RTCN 300 tolerante a fallo doble. Como puede verse, cada DCN se conecta a tres conmutadores de la RTCN formando de ese modo la configuración tolerante a fallo doble. Está también disponible una conexión 310 a otros conmutadores de la RTCN.

Las RTCN mostradas en las Figs. 2 y 3 son tolerantes a fallo simple y doble, respectivamente. Debería señalarse, sin embargo, que son asimismo aplicables RTCN redundantes triples o incluso múltiples.

Los controladores distribuidos pueden replicarse en dos, tres o más dependiendo del requisito de fiabilidad de cada subsistema y de la arquitectura tolerante a fallos elegida para el subsistema. En caso de que los controladores distribuidos sean inherentemente tolerantes a fallo no se requiere la réplica física.

Los DCN presentan preferentemente un comportamiento “de fallo silencioso” para permitir al o a los nodos replicados mantener el control sobre el objeto controlado. En caso de que falle un DCN que presente un comportamiento de fallo silencioso, no perturbará el funcionamiento de la turbina eólica ni provocará posiblemente una avería crítica del sistema. En consecuencia, un DCN de fallo silencioso tendrá un riesgo muy bajo de provocar una avería crítica del sistema.

La propiedad de fallo silencioso deberá permanecer estable hasta que el servicio en la unidad defectuosa, tal como un DCN, haya restaurado el sistema. Esto significa que el comportamiento de fallo silencioso debe mantenerse con una muy alta probabilidad en caso de una segunda avería en el nodo ya defectuoso. En caso contrario, el nodo defectuoso puede perturbar el funcionamiento de la turbina eólica y provocar posiblemente una avería crítica del sistema.

Tolerancia a fallo simple

La Fig. 4 muestra una vista de la implementación genérica de un subsistema tolerante a fallo simple. La propiedad de tolerancia a fallo simple se ilustra por las trayectorias de comunicación continua y discontinua entre los conmutadores de la RTCN 403, 411 replicados y los DCN 404, 405, 412, 413.

Los DCN 404, 405, 412, 413 pueden implementarse como nodos replicados activos o como nodos de reserva pasivos o en frío. Preferentemente, los DCN funcionan como nodos replicados activos. Los DCN tienen comportamiento de fallo seguro en caso de una avería interna. Los valores de los sensores están disponibles para los DCN como datos en la RTCN y opcionalmente también como datos de sensores locales. Los datos pueden utilizarse por los controladores en esquemas de redundancia 1oo2 (1 de 2), 2oo2 (2 de 2) o 2oo3 (2 de 3) dependiendo de la criticidad de la función. Sin embargo, son aplicables asimismo otros esquemas de redundancia.

El dibujo superior en la Fig. 4 muestra un subsistema que funciona en condiciones de trabajo normales. Los sensores 406, 408 proporcionan señales del sensor a los DCN 404, 405 para controlar el objeto 407. Más aún, el sensor 401 proporciona señales del sensor al DCN 402 que está en comunicación con los DCN 404, 405 a través del conmutador de la RTCN 403 replicado.

En caso de avería en un DCN 412, se asegura la operación continuada por el DCN 413 replicado, en comparación con el dibujo inferior en la Fig. 4. De ese modo, el control del objeto 415 se mantiene con entradas desde los sensores 409, 416 y el control apropiado de los DCN 410, 413 y el conmutador de la RTCN 411 replicado.

Si ambos DCN 404, 405 o 412, 413 funcionan sobre los mismos datos al mismo tiempo, puede soportarse el determinismo de la réplica.

Tolerancia a fallo doble

La Fig. 5 muestra una vista de implementación genérica con un subsistema tolerante a fallo doble. La propiedad de tolerancia a fallo doble se ilustra por las trayectorias de comunicación continua y las dos discontinuas entre los DCN y los conmutadores de la RTCN replicados.

Los DCN pueden implementarse como nodos replicados activos o como nodos de reserva pasivos o en frío. Más preferentemente, los DCN funcionan como nodos replicados activos. Los DCN tienen comportamiento de fallo seguro en caso de una avería interna. Los valores de los sensores están disponibles para los DCN como datos sobre la RTCN y opcionalmente también como datos de sensor local. Los datos de sensores pueden utilizarse por

los controladores en esquemas de redundancia 1oo2 (1 de 2), 2oo2 (2 de 2) o 2oo3 (2 de 3) dependiendo de la criticidad de la función. Como se ha mencionado anteriormente, son aplicables asimismo otros esquemas de redundancia.

El dibujo superior en la Fig. 5 muestra un subsistema que funciona en condiciones de trabajo normales. Los sensores 507, 509 proporcionan señales del sensor a los DCN 504, 505, 506 para controlar el objeto 508. Más aún, el sensor 501 proporciona señales del sensor al DCN 502 que está en comunicación con los DCN 504, 505, 506 a través del conmutador de la RTCN 503 replicado.

En caso de avería en un DCN 513, se asegura la operación continuada por los DCN 514, 515 restantes, compárese con el dibujo medio en la Fig. 5. De ese modo, el control del objeto 517 se mantiene con entradas desde los sensores 510, 518 y el control apropiado de los DCN 511, 514, 515 y el conmutador de la RTCN 512 replicado.

En caso de avería en dos DCN 522, 523, aún se asegura la operación continuada por el DCN 524 restante, compárese con el dibujo inferior en la Fig. 5. Por ello, el control del objeto 526 se mantiene con entradas desde los sensores 519, 527 y el control apropiado de los DCN 520, 524 y conmutador de la RTCN 521 replicado.

Si los DCN de la Fig. 5 funcionan sobre los mismos datos al mismo tiempo, puede soportarse el determinismo de la réplica.

La arquitectura de control mostrada en la Fig. 5 satisface el requisito de tolerancia a fallo para la fiabilidad del sistema muy alta en, por ejemplo, sistemas de misión crítica, posiblemente con largo tiempo medio para la reparación después de la primera avería. Dichos sistemas podrían ser sistemas de seguridad de “modo continuo” o sistemas de alta disponibilidad.

Tolerancia a fallos que utiliza redundancia n+m

Los sistemas de control pueden beneficiarse de una arquitectura de tolerancia a fallos que utilice una redundancia n+m, consúltese la Fig. 6, en donde m DCN son reserva para n DCN. La Fig. 6 muestra una RTCN 600 tolerante a fallo doble (indicada por las líneas continua y discontinua) en donde un conmutador de la RTCN 601 replicado está en comunicación con seis DCN de fallo silencioso 602-607. Los seis DCN de fallo silencioso 602-607 se configuran para controlar un objeto dado 620 de una turbina eólica en respuesta a entradas de sensores desde los sensores 608-619.

Los DCN 602-607 de réplica determinista n+m ejecutan conjuntamente el control sobre el objeto controlado 620. De nuevo, en caso de que un DCN 602-607 con comportamiento de fallo seguro falle no perturbará el funcionamiento del objeto controlado y en consecuencia tendrá muy poca probabilidad de provocar una avería crítica del sistema. Posibles áreas de aplicación para este tipo de redundancia podrían ser el sistema de orientación de la turbina eólica y los sistemas de convertidor de potencia modulares.

Como se ha mencionado previamente, el Dominio de Ejecución no Relacionado con la Seguridad Maestro Centralizado comprende funciones relacionadas con el control normal de la turbina eólica. La ejecución en este dominio se caracteriza por un paradigma maestro-esclavo replicado que utiliza uno o más controladores principales 701 y DCN 705, 707, 710, 714 y 716 replicados interconectados por la RTCN 700 replicada, consúltese los elementos de línea continua de la Fig. 4. Los elementos en línea discontinua son inactivos en este dominio. Cuando se utiliza una RTCN 700 determinista, este dominio soporta la tolerancia a fallos mediante DCN deterministas replicados redundantes 705, 707, 710, 714 y 716. La réplica de la RTCN 700 y los DCN 705, 707, 710, 714 y 716 se ilustran como estructuras apiladas (de RTCN y DCN) en la Fig. 7.

El Dominio de Ejecución de Control de Seguridad Maestro Centralizado comprende funciones relacionadas con la seguridad, relativas a la protección de personas o activos. La ejecución en este dominio se caracteriza por un paradigma de maestro centralizado que utiliza controladores de seguridad maestro replicados 802 (línea continua) y DCN relacionados con la seguridad replicados 806, 808, 811, 813 y 815 asociados (línea continua), consúltese la Fig. 8. Los controladores replicados 802 y los DCN 806, 808, 811, 813 y 815 replicados se interconectan mediante la RTCN 800 replicada (línea continua). Los elementos en línea discontinua son inactivos en este dominio. Cuando se utiliza una RTCN determinista, este dominio soporta la tolerancia a fallos mediante DCN deterministas replicados redundantes.

El Dominio de Ejecución de Control Distribuido permite un enfoque sin maestro para el control. El enfoque soporta la tolerancia a fallos mediante réplica determinista redundante de los DCN 903, 904, 907, 909, 910, 916 interconectados a través de la RTCN 900 replicada, consúltense los elementos en línea continua de la Fig. 9. Los elementos en línea discontinua son inactivos. Este dominio se aplica a controlador o controladores no maestros y el área primaria de aplicación de este dominio es el control relacionado con la seguridad en modo continuo. Sin embargo, el paradigma también puede usarse en otros controles relacionados con la seguridad y no relacionados con la seguridad.

En la Fig. 9, un grupo de DCN 903, 904, 907, 909, 910, 916 relacionados con la seguridad funcionan como publicadores y suscriptores de datos. Los DCN 903, 904, 907, 909, 910, 916 adquieren datos desde por ejemplo sistemas de sensores y publican los datos resultantes sobre la RTCN 900 replicada. Los otros DCN se suscriben a los datos publicados que necesitan para realizar su función. Un DCN dado puede ser tanto un publicador como un suscriptor. Como el intercambio de datos es directo entre los DCN, no se requiere un controlador principal.

En sistemas de control distribuido, la tolerancia a fallos y propiedades en tiempo real pueden soportarse por el establecimiento de un tiempo global preciso en donde los nodos tienen una noción común del tiempo que se desvía muy poco —típicamente en el intervalo de un microsegundo o menos, sin embargo no limitado a esta precisión—. El tiempo global da soporte a:

- Sincronización de la adquisición de datos a través de los controladores y nodos distribuidos
- Sincronización de los procesos a través de los controladores y nodos distribuidos
- Sincronización de la comunicación de datos (comunicación de activación por tiempo)
- Determinismo de la réplica en controladores tolerantes a fallos y nodos distribuidos

El tiempo global puede establecerse mediante la implementación de un protocolo de tiempo de precisión compatible con IEEE-1588. Como alternativa, el tiempo global puede establecerse utilizando el soporte inherente para un tiempo global de precisión que es parte de muchas redes de comunicación industriales. En sistemas en donde el tiempo global de precisión es crítico para la disponibilidad y/o seguridad del sistema, debe establecerse un nivel suficiente de tolerancia a fallos y fiabilidad en la distribución del tiempo global de precisión.

Una versión de dominio de tiempo global de la RTCN genérica mostrada en la Fig. 1 se ilustra en la Fig. 10, en la que sensores de sistemas 1008, 1009, 1013, 1014, 1038, 1039, 1043 y 1044 para la medición de por ejemplo, potencia, frecuencia, tensión, corriente, presión o temperatura se conectan a unos DCN replicados 1010, 1011, 1017, 1018, 1036, 1037, 1041 y 1042 respectivos, o bien directamente u opcionalmente a través de por ejemplo buses de campo, trayectorias de comunicación entre pares o cualquier otro tipo de interfaz. Los sistemas de sensores se posicionan en conjuntos de subsistemas (SSA) 1012, 1015, 1040 y 1045 junto con los DCN asociados. Otros SSA 1007, 1027, 1031 y 1035 comprenden unos DCN 1004, 1005, 1024, 1025, 1028, 1029, 1032 y 1033 para el control de objetos 1006, 1026, 1030, 1034 respectivos de la instalación de energía eólica. Los DCN replicados adquieren datos de los sistemas de sensores y publican los datos adquiridos sobre la RTCN 1003, poniendo los datos a disposición de otros DCN en el sistema través de conmutadores de la RTCN 1001, 1002 replicados. El tiempo global es indicado por 1047.

La Fig. 10 representa una RTCN genérica 1003 tolerante a fallo simple de acuerdo con una realización de la presente invención. La propiedad de tolerancia al fallo simple de la RTCN 1003 se ilustra por las trayectorias de comunicación continuas y discontinuas entre los conmutadores de la RTCN 1001, 1002 replicados y los diversos DCN de la RTCN 1003.

Los controladores principales 1018, 1019 del SSA 1020, controladores de seguridad 1021, 1022 del SSA 1023 y los DCN de otros SSA se interconectan conectados a través de la RTCN 1003 que utiliza conmutadores de la RTCN 1001, 1002 replicados. Los conmutadores de la RTCN 1001, 1002 replicados se conectan en una topología de estrella-rama-estrella. Sin embargo, son también aplicables otras tecnologías de red. La RTCN 1003 sirve como la infraestructura de comunicación que conecta todos los DCN en el sistema de control. La RTCN 1003 puede tener una conexión a la red de comunicación de la planta de generación a través de otros conmutadores de la RTCN 1046 replicados. La RTCN 1003 puede ser no tolerante a fallos, tolerante a fallo simple o tolerante a fallo doble dependiendo de los requisitos de fiabilidad.

En implementaciones tolerantes a fallos, los controladores primarios/principales y los DCN tienen generalmente la capacidad recibir datos desde dos o más canales RTCN redundantes y realizar la selección de un paquete de datos válido de entre los paquetes de datos redundantes disponibles. Los controladores y los DCN también tienen la capacidad de publicar los mismos datos al mismo tiempo sobre dos o más canales RTCN redundantes y por ello poner estos datos a disposición de otros DCN en el sistema para la selección de datos válidos. Esta propiedad da soporte a la fiabilidad y seguridad del sistema.

Más aún, en implementaciones tolerantes a fallos, los controladores primarios/principales y los DCN en el sistema pueden soportar tolerancia a fallos bien mediante “reserva en frío”, “reserva en caliente” o “réplica activa”.

En un sistema tolerante a fallo simple, dos controladores forman un par redundante en una función de control. En reserva en frío, un controlador es activo y el otro está desconectado. En caso de avería en el primer controlador, el segundo controlador se hace cargo de la función del controlador en fallo después de su arranque e inicialización. En reserva en caliente, un controlador está activo y el segundo controlador es observador pasivo. En caso de avería en el primer controlador, el segundo controlador se hace cargo de la función. En replica activa, ambos controladores

están activos, funcionan en sincronismo sobre los mismos datos, y producen así la misma salida al mismo tiempo. En caso de que falle el controlador, el segundo controlador preserva un control sin saltos de la turbina. Los tres principios pueden utilizarse en la presente invención.

En un sistema tolerante a fallo múltiple, se utilizan más controladores redundantes. Los principios de redundancia son los mismos que para los sistemas tolerantes a fallo simple.

Diferentes niveles de tolerancia al fallo pueden aplicarse a la red de comunicación y nodos dependiendo de los requisitos de fiabilidad y seguridad. La presente invención no está limitada a los ejemplos mostrados.

REIVINDICACIONES

1. Una instalación de energía eólica modularizada que comprende subconjuntos, que tiene un sistema de control distribuido tolerante a fallos, comprendiendo el sistema de control:

- medios de control tolerantes a fallos adaptados para generar puntos de consigna de control y/o valores de datos, estando dichos medios de control tolerantes a fallos distribuidos en subconjuntos de acuerdo con la modularización de la instalación de energía eólica y

caracterizada por

- una red de comunicación tolerante a fallos para la transmisión de puntos de consigna de control y/o valores de datos esencialmente al mismo tiempo a una pluralidad de nodos en el sistema de control distribuido a través de dos o más conmutadores de la red de comunicación en tiempo real replicados, siendo capaz dicha pluralidad de nodos distribuidos de seleccionar un paquete de transmisión válido de entre dos o más paquetes de transmisión proporcionados en la red de comunicación tolerante a fallos, en el que la red de comunicación comprende una red de comunicación en tiempo real que comprende una Ethernet de activación por tiempo.

2. Una instalación de energía eólica modularizada de acuerdo con la reivindicación 1, en la que la red de comunicación Ethernet de activación por tiempo se implementa como una red tolerante a fallo simple.

3. Una instalación de energía eólica modularizada de acuerdo con la reivindicación 1, en la que la red de comunicación Ethernet de activación por tiempo se implementa como una red tolerante a fallo doble.

4. Una instalación de energía eólica modularizada de acuerdo con la reivindicación 1, en la que la red de comunicación Ethernet de activación por tiempo está certificada respecto a seguridad.

5. Una instalación de energía eólica modularizada de acuerdo con cualquiera de las reivindicaciones precedentes, en la que la red de comunicación soporta las clases de seguridad funcional en el modo de baja demanda, modo de alta demanda y modo continuo de acuerdo con la norma IEC61508.

6. Una instalación de energía eólica modularizada de acuerdo con la reivindicación 5, en la que las funciones de seguridad funcional cumplen con los requisitos para Nivel de Integridad de Seguridad 2.

7. Una instalación de energía eólica modularizada de acuerdo con la reivindicación 5, en la que las funciones de seguridad funcional cumplen con los requisitos para Nivel de Integridad de Seguridad 3.

8. Una instalación de energía eólica modularizada de acuerdo con cualquiera de las reivindicaciones precedentes, que comprende adicionalmente sistemas de sensores tolerantes a fallos que comprenden una pluralidad de sensores.

9. Una instalación de energía eólica modularizada de acuerdo con la reivindicación 8, en la que la pluralidad de sensores se dispone de una forma redundante.

10. Una instalación de energía eólica modularizada de acuerdo con la reivindicación 8 o 9, en la que la pluralidad de sensores está adaptada para medir al menos un parámetro relevante para el control de al menos un subconjunto.

11. Una instalación de energía eólica modularizada de acuerdo con cualquiera de las reivindicaciones precedentes, que comprende adicionalmente medios de votación adaptados para votar entre valores de datos de entre una pluralidad de fuentes, estando adaptados dichos medios de votación para votar de acuerdo con el principio de votación 1oo2, 2oo2, 2oo3 u otro principio de votación adecuado.

12. Una instalación de energía eólica modularizada de acuerdo con cualquiera de las reivindicaciones precedentes, que comprende adicionalmente al menos dos controladores primarios redundantes dispuestos en una configuración de réplica determinista.

13. Una instalación de energía eólica modularizada de acuerdo con la reivindicación 12, en la que los al menos dos controladores primarios redundantes comprenden un controlador primario activo y uno o más controladores de reserva en caliente.

14. Un sistema de control distribuido tolerante a fallos de acuerdo con la reivindicación 12, en el que los al menos dos controladores primarios redundantes comprenden un controlador primario activo y uno o más controladores de reserva en frío.

15. Un método para el control de una instalación de energía eólica modularizada que comprende subconjuntos, comprendiendo el método las etapas de

- generar puntos de consigna de control y/o valores de datos usando medios de control tolerantes a fallos, estando distribuidos dichos medios de control tolerantes a fallos en subconjuntos de acuerdo con la modularización de la instalación de turbina eólica,

caracterizado por

- transmitir los puntos de consigna de control y/o valores de datos generados esencialmente al mismo tiempo a través de dos o más conmutadores de la red de comunicación en tiempo real replicados a una pluralidad de nodos en el sistema de control distribuido a través de una red de comunicación en tiempo real tolerante a fallos que comprende una Ethernet de activación por tiempo y
- seleccionar, usando la pluralidad de nodos distribuidos, un paquete de transmisión válido de entre dos o más paquetes de transmisión proporcionados en la red de comunicación tolerante a fallos.

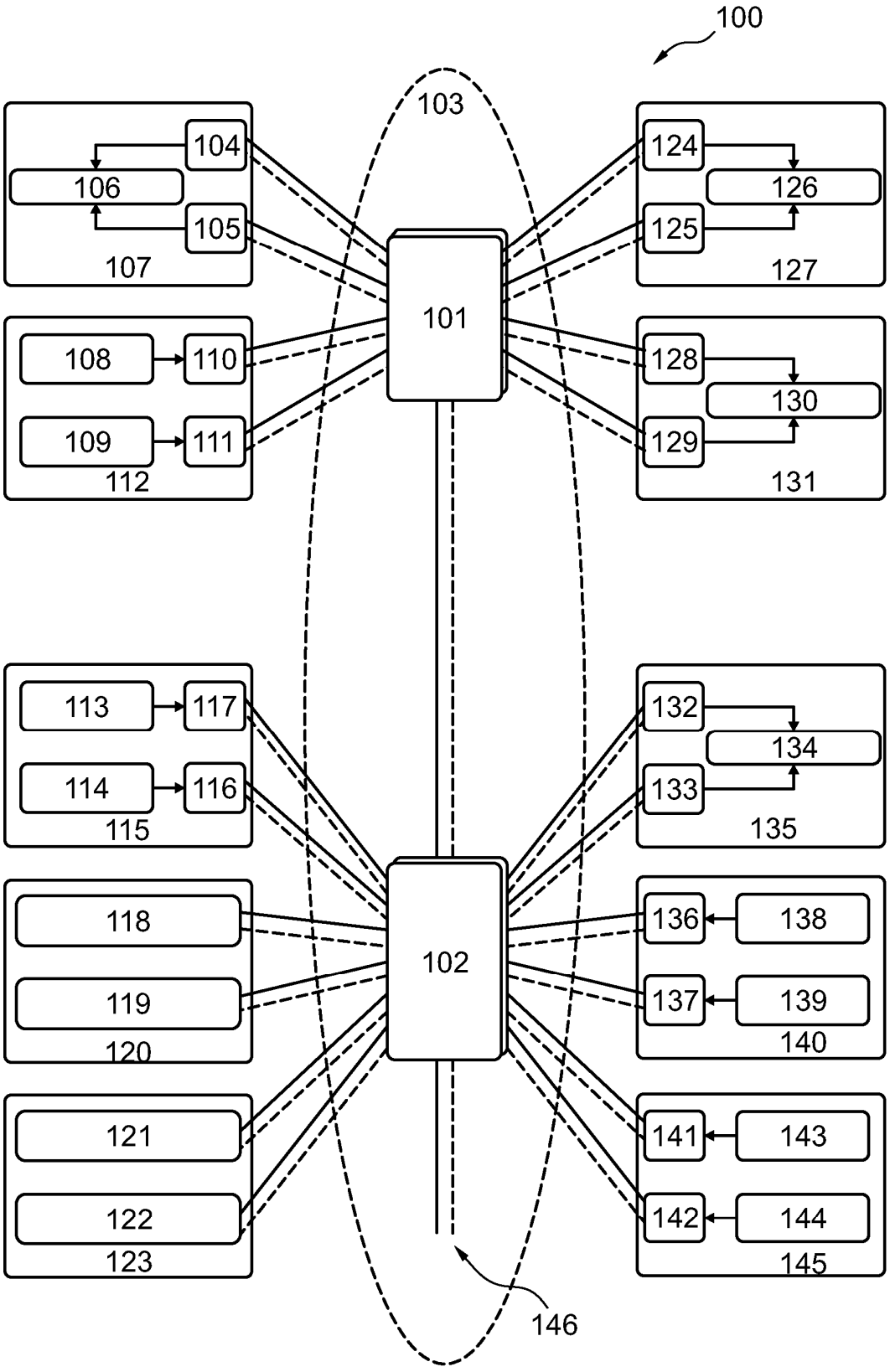
100
103
104
106
105
107
124
126
125
127
101
108
110
109
111
112
128
130
129
131
113
117
114
116
115
132
134
133
135
118
119
120
102
136
138
137
139
140
121
122
123
141
143
142
144
145
146

Fig. 1

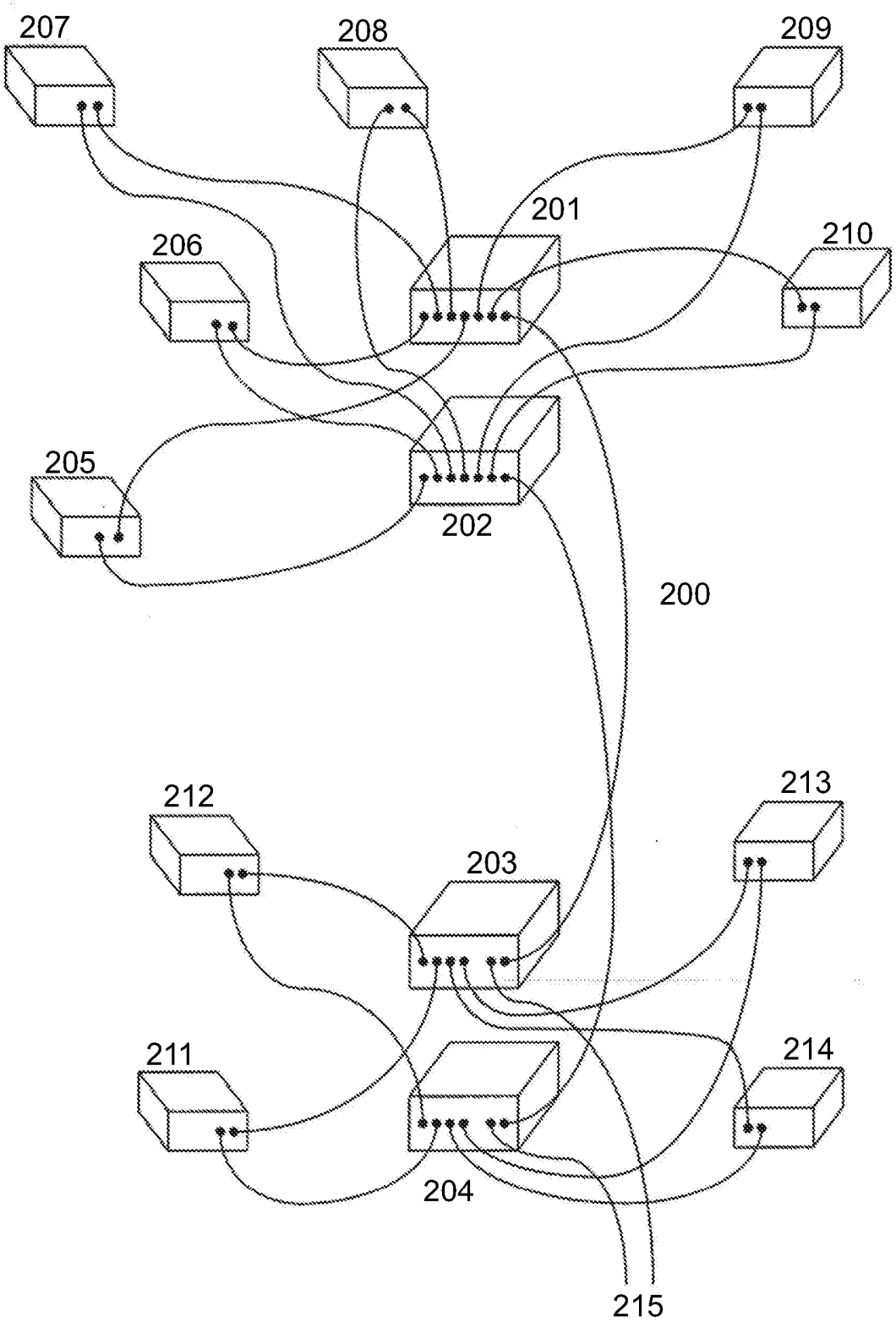

FIG. 2

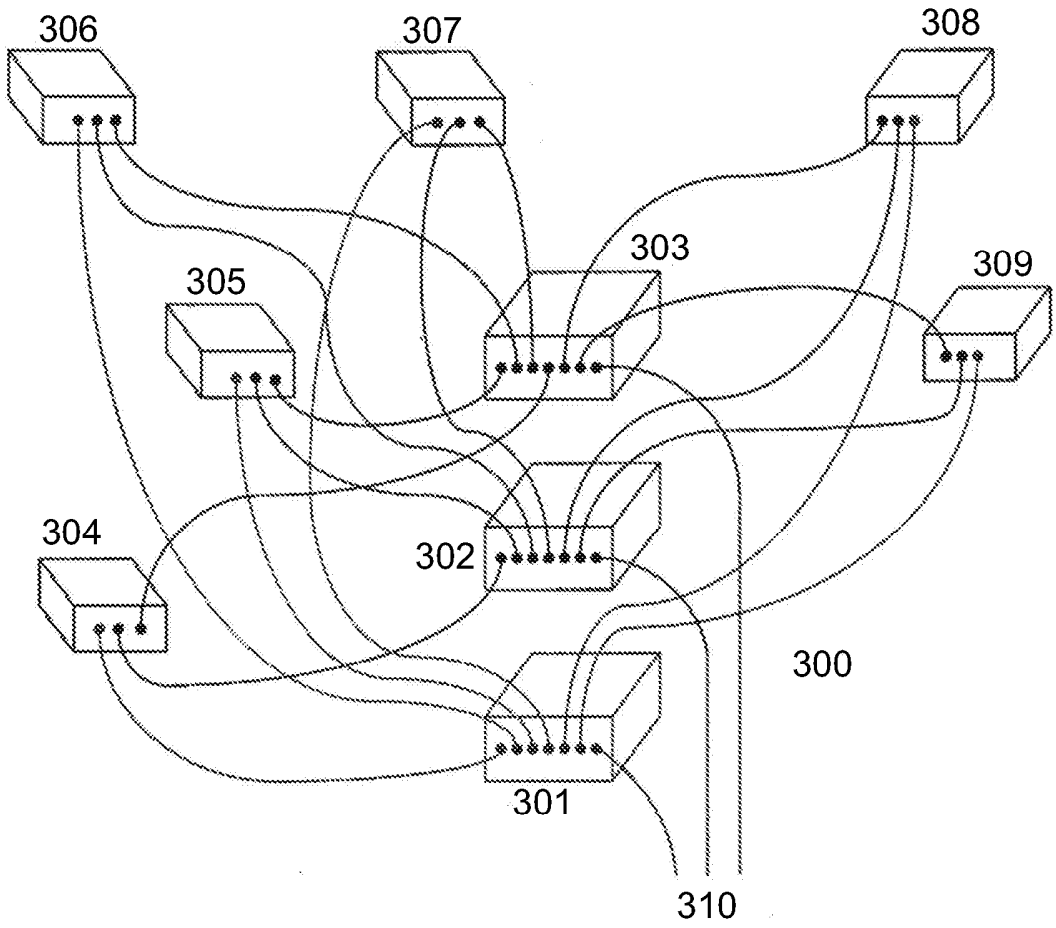

FIG. 3

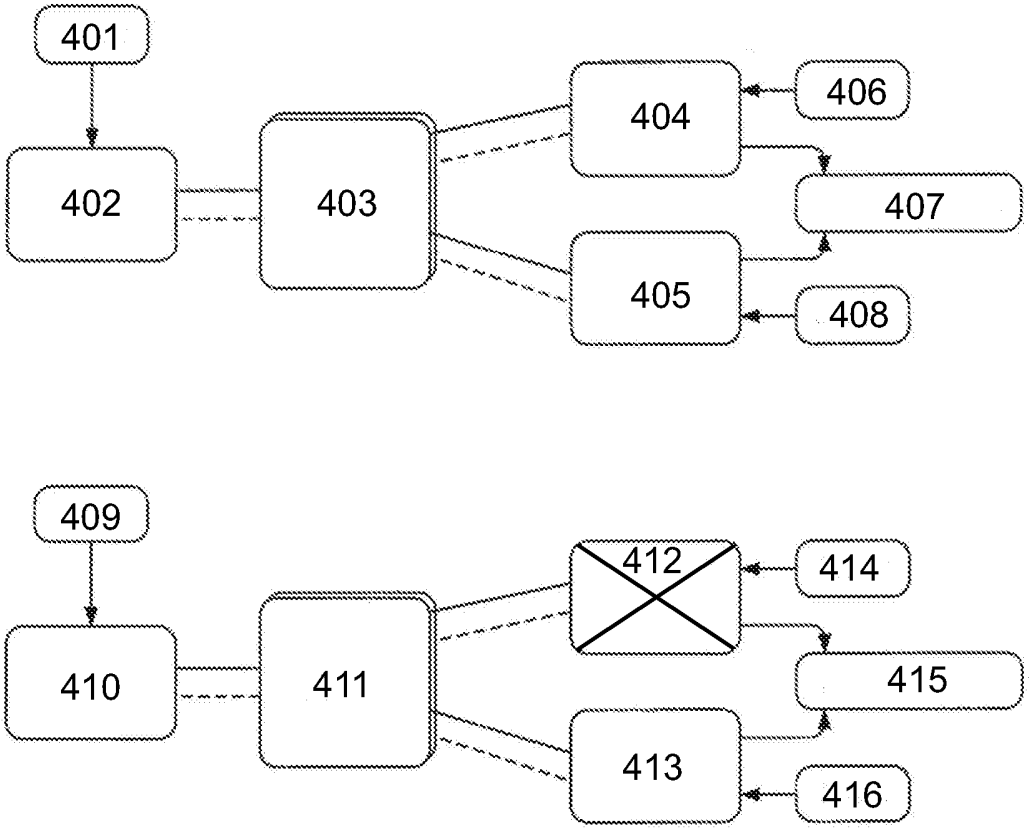

FIG. 4

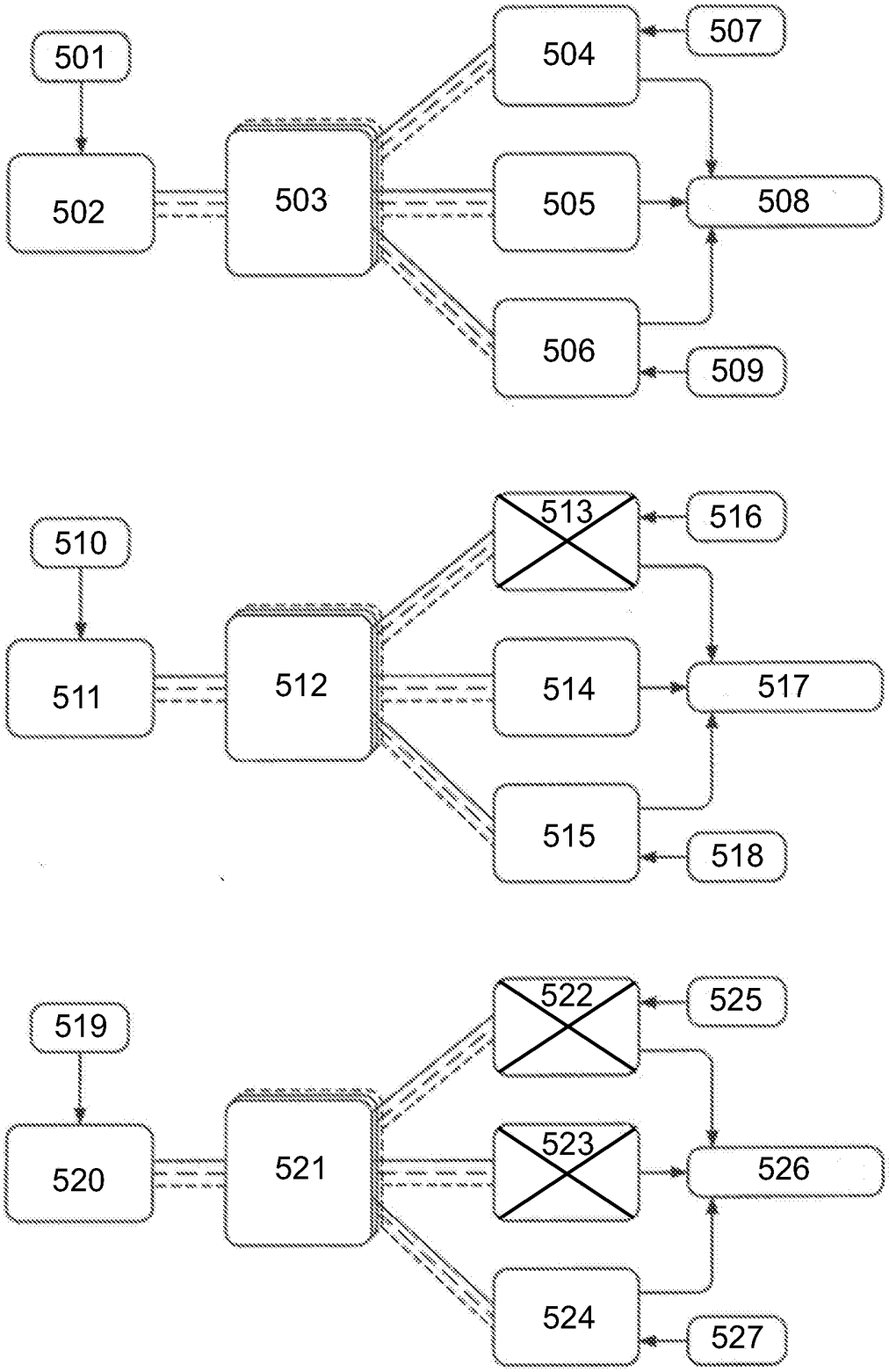
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527

FIG. 5

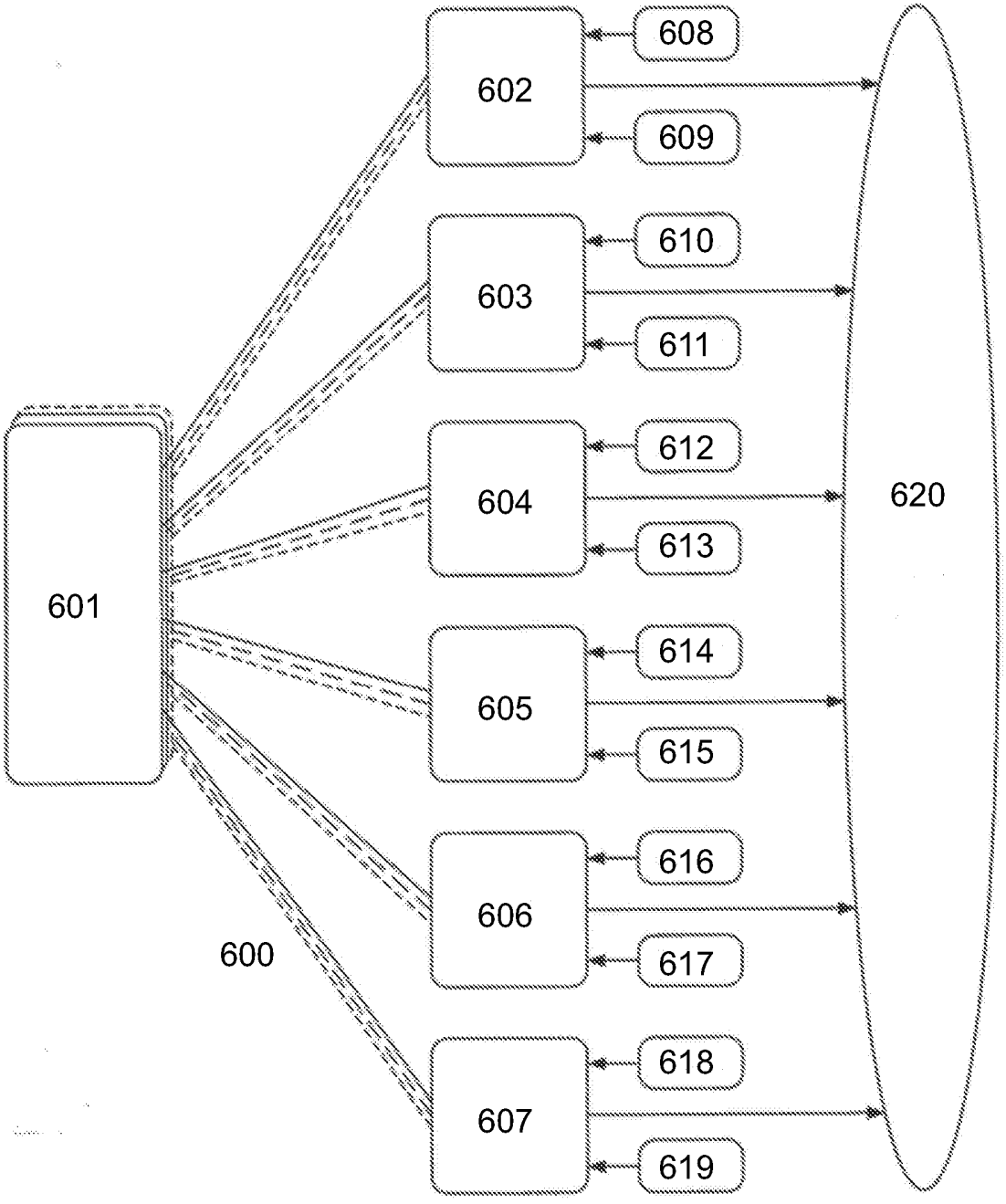
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
600

FIG. 6

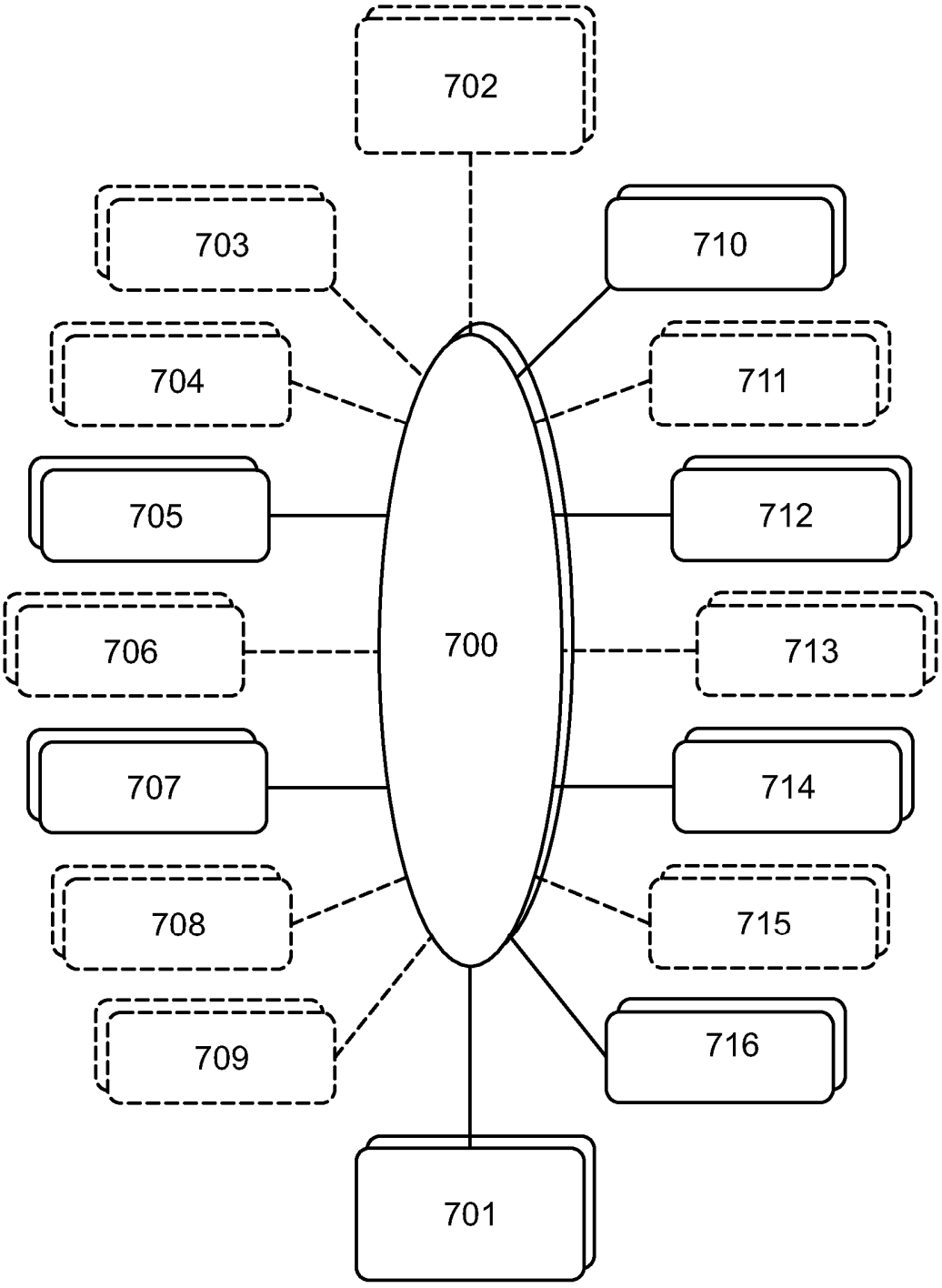
702
703
710
704
711
705
712
706
700
713
707
714
708
715
709
716
701

Fig. 7

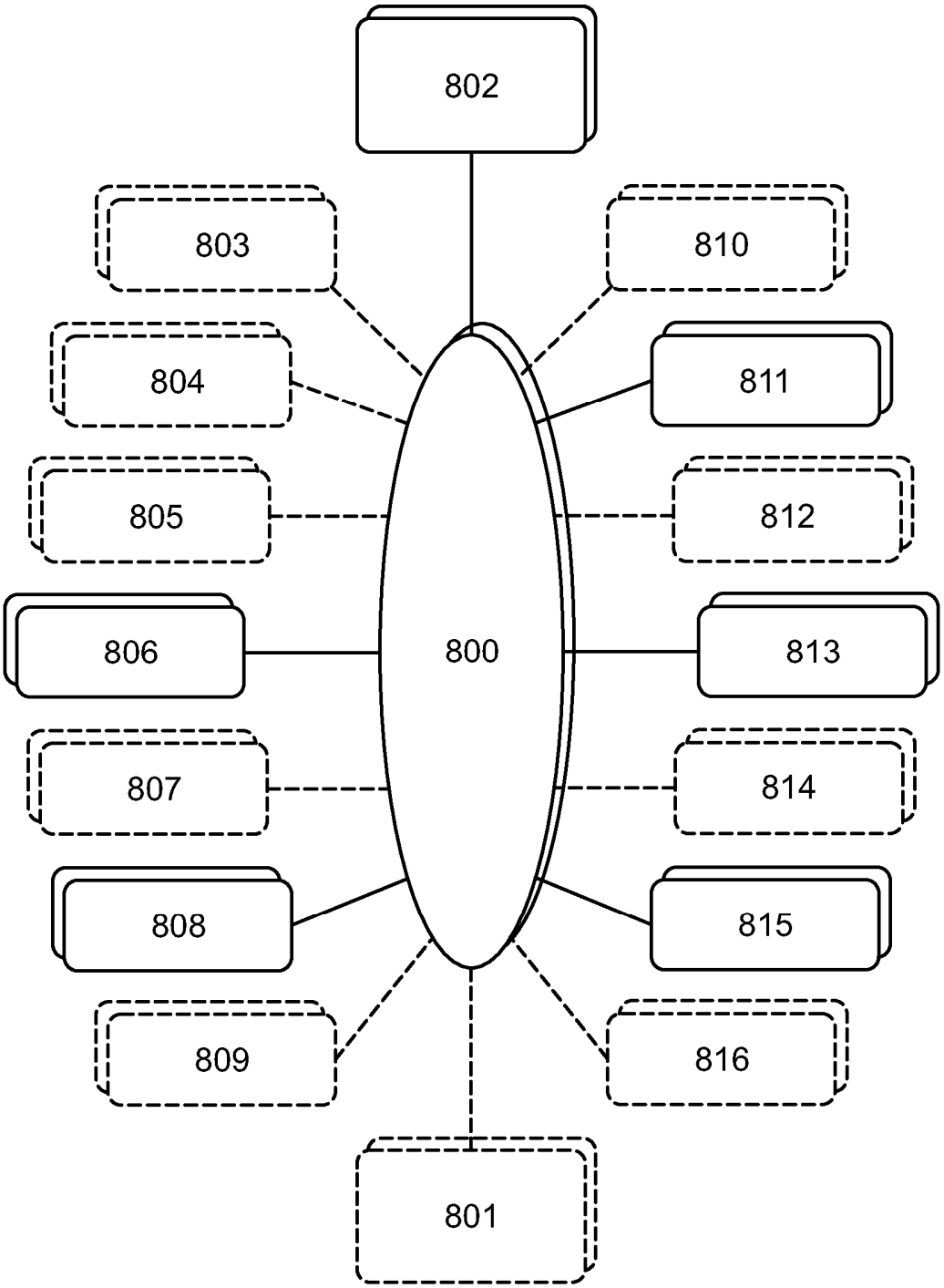
802
803
810
804
811
805
812
806
800
813
807
814
808
815
809
816
801

Fig. 8

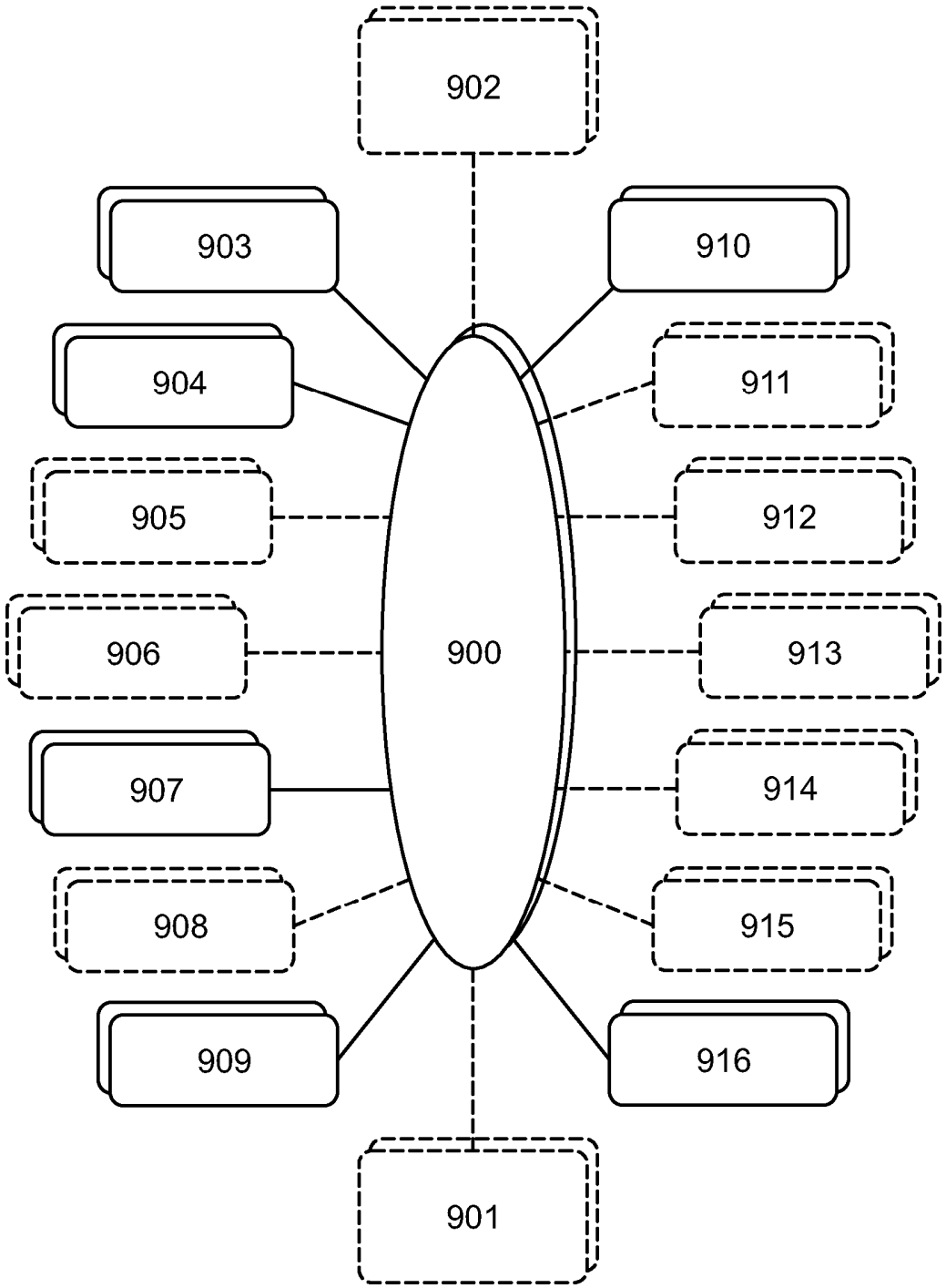
902
903
910
904
911
905
912
906
900
913
907
914
908
915
909
916
901

Fig. 9

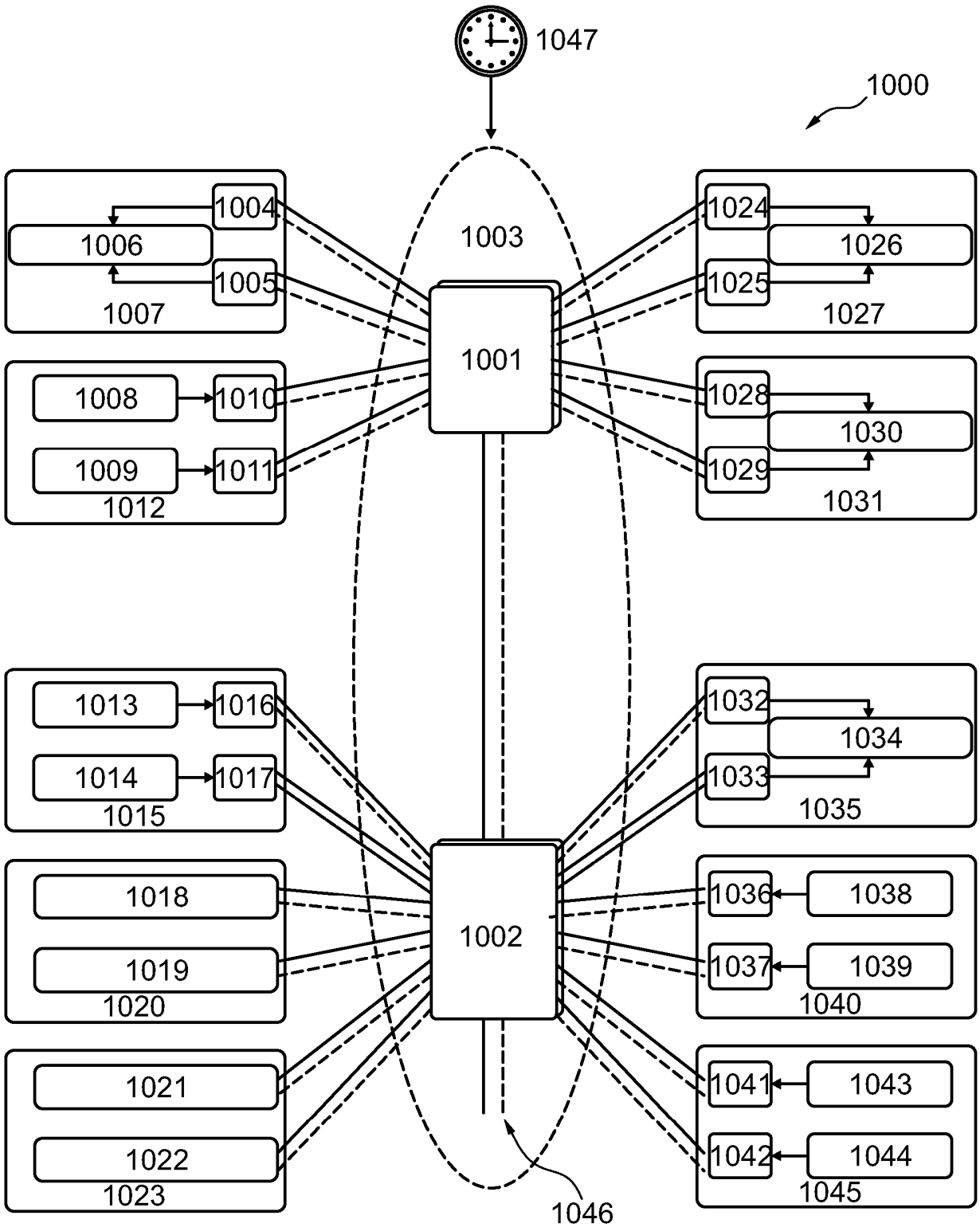
1047
1000
1003
1001
1002
1004
1006
1005
1007
1008
1010
1009
1011
1012
1024
1026
1025
1027
1028
1030
1029
1031
1013
1016
1014
1017
1015
1018
1019
1020
1021
1022
1023
1032
1034
1033
1035
1036
1038
1037
1039
1040
1041
1043
1042
1044
1045
1046

Fig. 10