(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **1 197 111**

(21) Número de solicitud: 201731292

(51) Int. CI.:

G05B 23/02 (2006.01)

(12) SOLICITUD DE MODELO DE UTILIDAD U

(22) Fecha de presentación:

25.10.2017

(43) Fecha de publicación de la solicitud:

08.11.2017

(71) Solicitantes:

UNIVERSIDAD DE LEÓN (100.0%)
Avenida de La Facultad 25
24071 LEÓN ES

(72) Inventor/es:

DOMÍNGUEZ GONZÁLEZ, Manuel;
FUERTES MARTÍNEZ, Juan José ;
PRADA MEDRANO, Miguel Ángel ;
ALONSO CASTRO, Serafín;
MORÁN ÁLVAREZ, Antonio;
REGUERA ACEVEDO, Perfecto y
SANTALLA FERNÁNDEZ, Roberto

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

(54) Título: **DISPOSITIVO PARA LA REALIZACIÓN DE PRÁCTICAS EN CIBERSEGURIDAD INDUSTRIAL**

ES 1 197 111 U

DISPOSITIVO PARA LA REALIZACIÓN DE PRÁCTICAS EN CIBERSEGURIDAD INDUSTRIAL

DESCRIPCIÓN

Campo de la invención

La presente invención se engloba en el campo de la ciberseguridad, y más concretamente se refiere a un dispositivo para realizar actividades formativas en el ámbito de la ciberseguridad industrial. La presente invención ha sido especialmente concebida para satisfacer las necesidades formativas en ciberseguridad de dichas infraestructuras en todos los niveles educativos, especialmente aquellos de grado superior (ciclos formativos de grado superior, ingenierías, licenciaturas, grados o másteres en ingeniería). Por lo tanto, la invención se refiere al campo de los dispositivos de aprendizaje para las citadas técnicas.

Antecedentes de la invención

Actualmente la formación práctica en ciberseguridad de infraestructuras críticas, además de estar poco desarrollada, se realiza manejando dispositivos tales como PLCs, DCSs, routers, switches, firewalls, etc., y su software asociado, de forma aislada, o a través de simulaciones, por ejemplo, del tráfico de red. Cuando se trabaja con los dispositivos industriales de esta forma, sin estar instalados en un sistema completo de automatización, el alumno solamente puede aprender de forma parcial su utilidad, vulnerabilidades y/o aseguramiento, ya que no es posible considerar las interacciones que se producen entre el dispositivo industrial y el proceso o con otros dispositivos industriales. De esta forma, obtiene solamente una vaga idea de la correcta configuración del sistema. Lo mismo se produce cuando se recurre a la simulación virtual, que sólo hace una representación limitada y simplificada del funcionamiento del sistema. El alumno no llega a conocer en su totalidad el funcionamiento de un dispositivo real y su comportamiento dentro de la industria, dando lugar a configuraciones erróneas y falsas ideas. La presente invención resuelve de forma plenamente satisfactoria esta problemática, ya que se trata de un dispositivo de prácticas formado por equipos presentes en todos los niveles de un sistema de automatización: campo, control y supervisión. Además, dispone de un sistema auxiliar de comunicaciones que permite hacer diferentes configuraciones seguras enlazando de diversos modos los diferentes niveles.

Descripción de la invención

La invención se refiere a un dispositivo para prácticas en ciberseguridad industrial, con finalidad didáctica. El dispositivo representa un sistema de automatización completo que contiene los tres niveles principales definidos en la pirámide de automatización: campo, control y supervisión; así como las comunicaciones y enlaces que se establecen entre ellos. En particular, el dispositivo está formado por cuatro sistemas principales (campo, control industrial, control eléctrico y supervisión) y otros dos auxiliares (alimentación y comunicaciones). Combinando estos sistemas se pueden realizar diversas configuraciones seguras orientadas a la formación en ciberseguridad para infraestructuras críticas.

El dispositivo para prácticas en ciberseguridad industrial comprende:

- Un armario de soporte de los distintos componentes del dispositivo.
- Un sistema de campo que comprende un variador de frecuencia trifásico y también puede comprender una botonera.
- Un sistema de control industrial que comprende un PLC con conectividad a una estación remota.
- Un sistema de supervisión que comprende una interfaz de usuario, preferentemente una pantalla de visualización táctil.
- Un sistema de control eléctrico que comprende un medidor del consumo eléctrico y unos contactores e interruptores telecontrolados a través de un enlace de control remoto.
- Un sistema de comunicaciones que comprende un switch que interconecta distintos equipos según una configuración de red, un router que gestiona el enrutado de paquetes entre las distintas redes, y un firewall que bloquea los accesos no permitidos entre redes y equipos.
- Un sistema de alimentación eléctrica de los componentes electrónicos del dispositivo. En una realización, el sistema de alimentación eléctrica comprende un transformador de corriente por cada fase, un primer bornero que alimenta directamente a un interruptor unido a un conector de potencia, y una fuente de alimentación de corriente continua.

Con todo lo expuesto, las ventajas que aporta la presente invención con respecto al estado del arte, a título meramente enunciativo y no limitativo, son las siguientes:

- Es un dispositivo que reproduce las condiciones reales de sistema de automatización, lo que permite a los alumnos obtener una idea real de configuraciones industriales inadecuadas, desde el punto de vista de la seguridad

informática, como las que se pueden encontrar a lo largo de su carrera profesional, y su utilización les aporta conocimientos para asegurarlas.

- En el armario-soporte de la presente invención se distribuyen los diferentes dispositivos industriales, eléctricos y de comunicaciones, con una disposición que dota el sistema de flexibilidad tanto desde el punto de vista de la configuración de las comunicaciones como de la manipulación y parametrización de los dispositivos, gracias al acceso directo y sencillo a los mismos.
- El dispositivo didáctico tiene un espectro de operación muy amplio ya que con él se pueden realizar desde experiencias de ciberseguridad básicas hasta avanzadas y desde configuraciones inseguras, en las que todos los elementos forman parte de la misma red de comunicaciones y no disponen de ningún mecanismo de seguridad, hasta configuraciones seguras, en las que se realiza una segmentación total y se incluyen medidas de seguridad, como cortafuegos, entre los diferentes niveles.
- Por la disposición de los elementos y la configuración del armario-soporte, se ha previsto que la presente invención sea portable y autónoma.

Breve descripción de los dibujos

A continuación se pasa a describir de manera muy breve una serie de dibujos que ayudan a comprender mejor la invención y que se relacionan expresamente con una realización de dicha invención que se presenta como un ejemplo no limitativo de ésta.

La Figura 1 muestra una vista en perspectiva de una posible realización del dispositivo para prácticas en ciberseguridad industrial.

La Figura 2 representa una vista frontal del dispositivo para prácticas en ciberseguridad industrial de la Figura 1 donde únicamente se muestran los componentes ubicados en la parte más anterior del dispositivo, mientras que en la Figura 3 se representa también una vista frontal del dispositivo de la Figura 1 pero donde se muestran solo el resto de componentes (esto es, aquellos que están ubicados en la parte posterior).

La Figura 4 muestra una vista en planta superior del dispositivo para prácticas en ciberseguridad industrial de la Figura 1.

Descripción detallada de la invención

La **Figura 1** representa una vista en perspectiva del dispositivo (20) para prácticas en ciberseguridad industrial de acuerdo a una posible realización. Una vista frontal del dispositivo (20) de la Figura 1 se muestra repartido en dos figuras, **Figuras 2** y **3**, para una mejor visualización de los componentes individuales. En la Figura 2 se muestra únicamente los componentes ubicados en la parte más anterior del dispositivo (elementos 3, 8, 10 y 14), mientras que en la Figura 3 se muestran el resto de componentes, los cuales están ubicados en una parte más trasera. La **Figura 4** muestra una vista superior del dispositivo (20) de la Figura 1. El dispositivo (20) está formado por cuatro módulos o sistemas principales -campo, control industrial, control eléctrico y supervisión- y otros dos módulos o sistemas auxiliares -alimentación y comunicaciones-.

El dispositivo (20) para prácticas en ciberseguridad industrial, cuya finalidad es presentar condiciones industriales reales, comprende un armario de soporte (17) de los distintos componentes del dispositivo (20). En la parte superior del armario de soporte (17) se ubica el sistema de alimentación que alimenta al sistema de comunicaciones y a los sistemas de campo, control industrial, supervisión y control eléctrico.

El sistema de campo está ubicado en la parte inferior del armario de soporte (17) y sus principales componentes son un variador de frecuencia trifásico (4) y una botonera (15). Los elementos del sistema de campo representan el nivel de sensores y actuadores del dispositivo para prácticas. El sistema de control industrial se ubica encima del nivel de campo y se compone de un PLC (6) con conectividad a una estación de ingeniería para programación externa (e.g. una estación de trabajo tipo PC donde se instala el software de configuración de los equipos). La botonera (15) está cableada a las entradas digitales del PLC (6). El variador de frecuencia trifásico (4), que se puede conectar a un motor de corriente alterna, se comunica con el PLC (6) mediante un bus de comunicaciones industrial. En la parte intermedia del armario de soporte (17) se encuentra el sistema de comunicaciones que comprende un switch (11) que interconecta distintos equipos según la configuración de red que se realice, un router (12) encargado de gestionar el enrutado de paquetes entre las distintas redes, y un firewall (13) que bloquea los accesos no permitidos entre redes y equipos. En la zona superior y posterior del dispositivo (20) se encuentra la entrada de alimentación tanto de corriente continua como de alterna trifásica.

En cuanto a los elementos ubicados en la parte anterior del dispositivo (20), mostrados en la vista frontal de la Figura 2, a una altura central del armario de soporte (17) se encuentra una

interfaz de usuario, implementada preferentemente mediante una pantalla de visualización táctil (10), perteneciente al sistema de supervisión. Por último, ubicado en la zona superior y anterior del armario de soporte (17) se encuentra el sistema de control eléctrico que comprende un medidor del consumo eléctrico (3) proveniente de las fases de alimentación externa para la tensión y la corriente, unos contactores e interruptores (8) telecontrolados y un enlace de control remoto (14), que dispone de un puerto ethernet, con comunicación modbus TCP/IP, a través del cual recibe las órdenes del estado que deben tener los contactores e interruptores.

La disposición de los diferentes elementos del dispositivo permite la sencilla manipulación del armario de soporte (17), con lo que se pueden realizar distintas configuraciones de ciberseguridad, permitiendo o impidiendo los enlaces entre los diferentes sistemas.

En relación al sistema de alimentación, la corriente trifásica, que proviene de una red externa al dispositivo (20), pasa primero a través de una serie de transformadores de corriente (1), uno por cada fase. La corriente de cada fase sin transformar se conduce a un primer bornero (2) que alimenta directamente al variador de frecuencia trifásico (4) y a un interruptor (5), el cual está unido a un conector de potencia (16) que, conectado a un segundo bornero (9), mantiene la alimentación del PLC (6), una fuente de alimentación de corriente continua (7) y el propio medidor de consumo eléctrico (3), así como los contactores e interruptores (8).

La fuente de alimentación de corriente continua (7) pasa por un tercer bornero (18), el cual alimenta al resto de dispositivos: pantalla de visualización (10), switch (11), router (12), firewall (13), enlace de control remoto (14) y la botonera (15).

A modo de ejemplo, se describe a continuación una posible configuración para hacer una práctica con el dispositivo. El primer objetivo de la práctica es observar las diferencias, desde el punto de vista de la ciberseguridad, que se manifiestan al dividir una red ethernet en dos diferentes mediante un router. Para ello, en primer lugar, se configura el switch (11) del armario para que todas las bocas pertenezcan a la misma VLAN, y se deja el router (12) desconectado. Se hacen a continuación pruebas de escaneo y descubrimiento ARP, observando que todos los dispositivos conectados a la red son descubribles, incluso aunque presenten sus puertos cerrados. A continuación, se configuran dos VLANs en el switch (11), y se conectan mediante el router (12). Se repite la prueba de descubrimiento, observando

esta vez que, dado que las peticiones ARP no son propagadas por el router (12), los dispositivos de una red no son directamente visibles desde la otra.

A continuación, con el objetivo de mostrar las ventajas de usar cortafuegos que realicen una inspección a fondo de los paquetes (DPI) se configura el firewall (13) para controlar el acceso al PLC (6) desde una estación de ingeniería, la pantalla de visualización táctil (10) y el resto de la red. Para ello, se conecta el firewall (13) directamente al PLC (6), por una de sus interfaces, uniendo la otra al switch (11). En la interfaz de configuración del firewall (13), se permite todo el tráfico MODBUS entrante desde la estación de ingeniería, sólo el tráfico que realice operaciones de lectura desde la pantalla de visualización (11), y ningún tipo de tráfico desde cualquier otro dispositivo. Se asegura así que ningún dispositivo extraño de la red puede conectarse al PLC (6) y reprogramarlo.

REIVINDICACIONES

1. Dispositivo para la realización de prácticas en ciberseguridad industrial, caracterizado por que comprende:

- un armario de soporte (17);
- un sistema de campo que comprende un variador de frecuencia trifásico (4);
- un sistema de control industrial que comprende un PLC (6) con conectividad a una estación remota;
- un sistema de supervisión que comprende una interfaz de usuario;
- un sistema de control eléctrico que comprende un medidor del consumo eléctrico (3) y unos contactores e interruptores (8) telecontrolados a través de un enlace de control remoto (14);
- un sistema de comunicaciones que comprende un switch (11) que interconecta distintos equipos según una configuración de red, un router (12) que gestiona el enrutado de paquetes entre las distintas redes, y un firewall (13) que bloquea los accesos no permitidos entre redes y equipos;
- un sistema de alimentación eléctrica.

2. Dispositivo según la reivindicación 1, caracterizado por que la interfaz de usuario comprende una pantalla de visualización táctil (10).

3. Dispositivo según cualquiera de las reivindicaciones anteriores, caracterizado por que el sistema de alimentación eléctrica comprende:

un transformador de corriente (1) por cada fase;

un primer bornero (2) que alimenta directamente a un interruptor (5) unido a un conector de potencia (16);

una fuente de alimentación de corriente continua (7).

4. Dispositivo según cualquiera de las reivindicaciones anteriores, caracterizado por que el sistema de campo comprende una botonera (15).

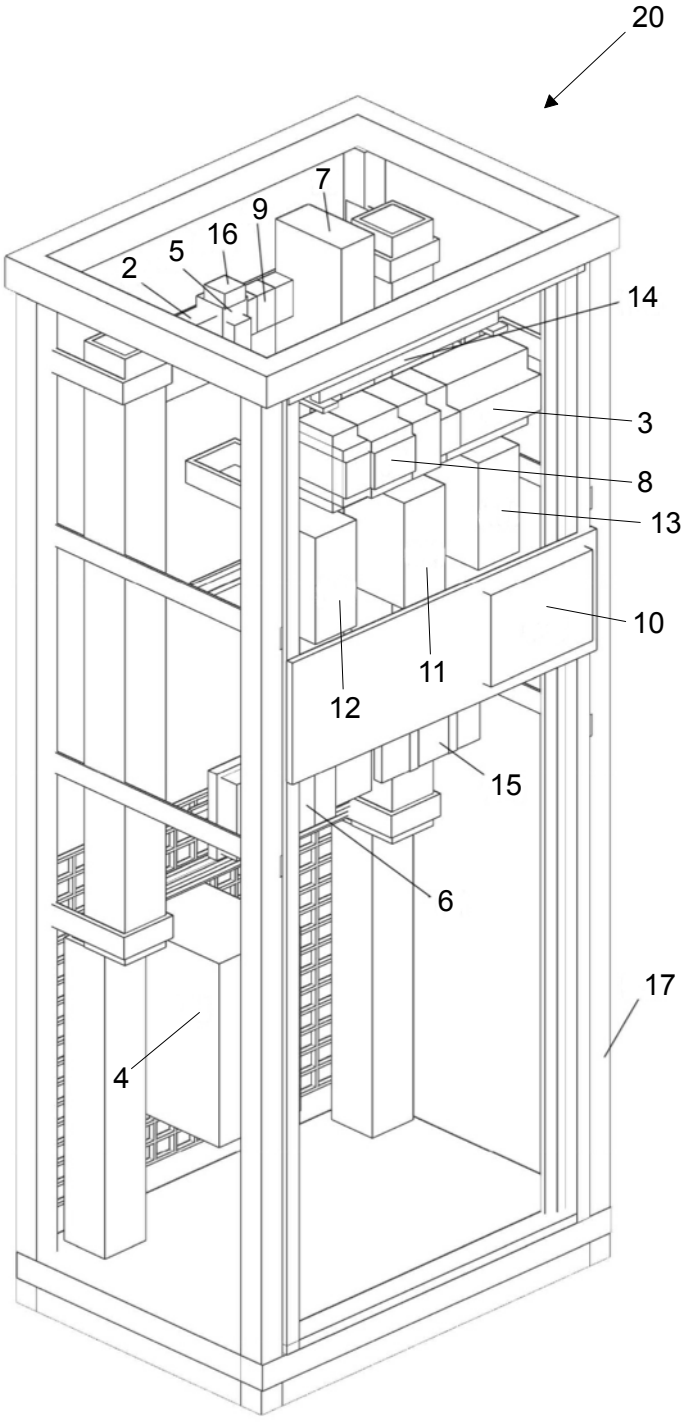

FIG. 1

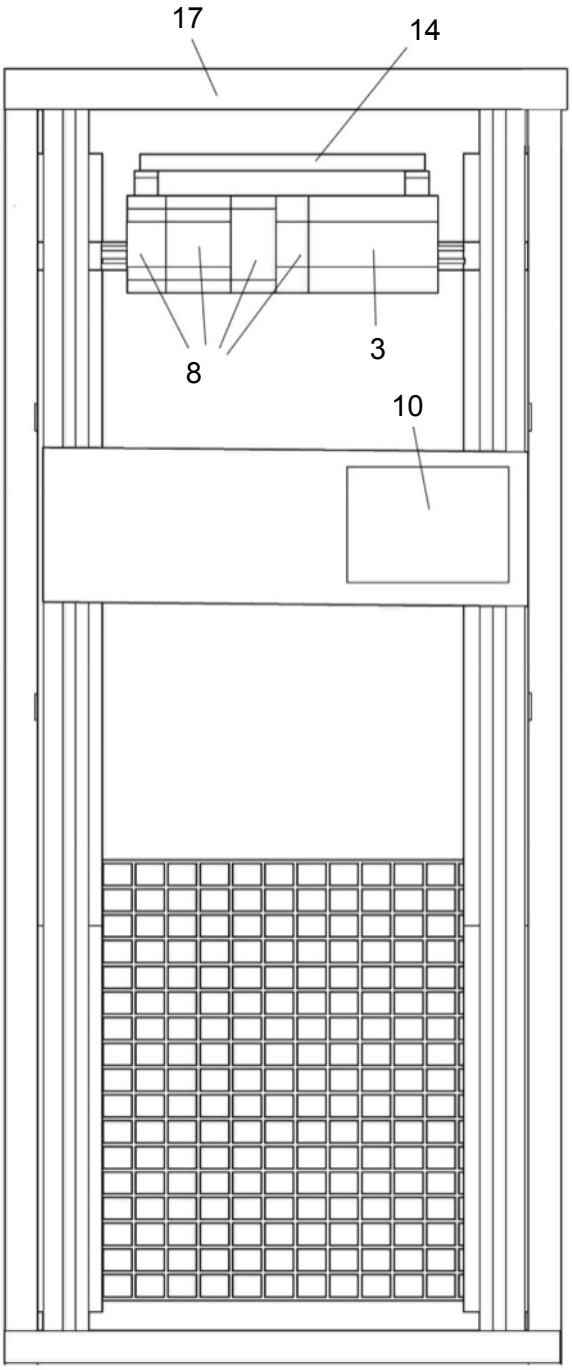

FIG. 2

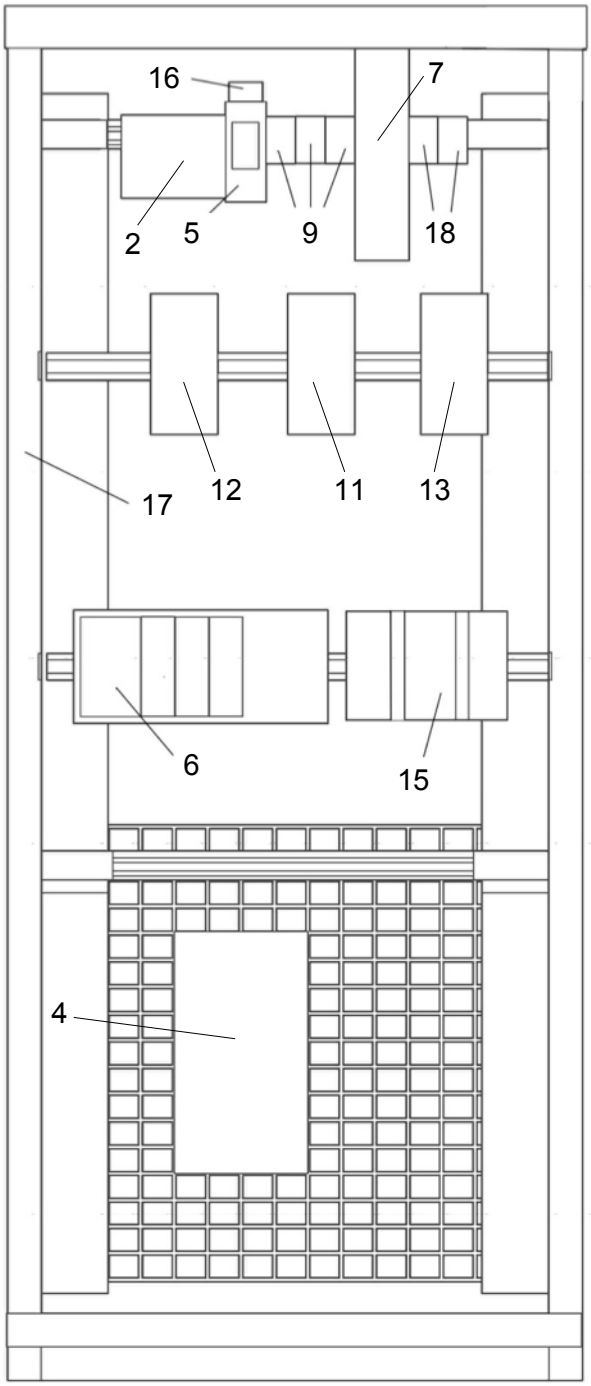

FIG. 3

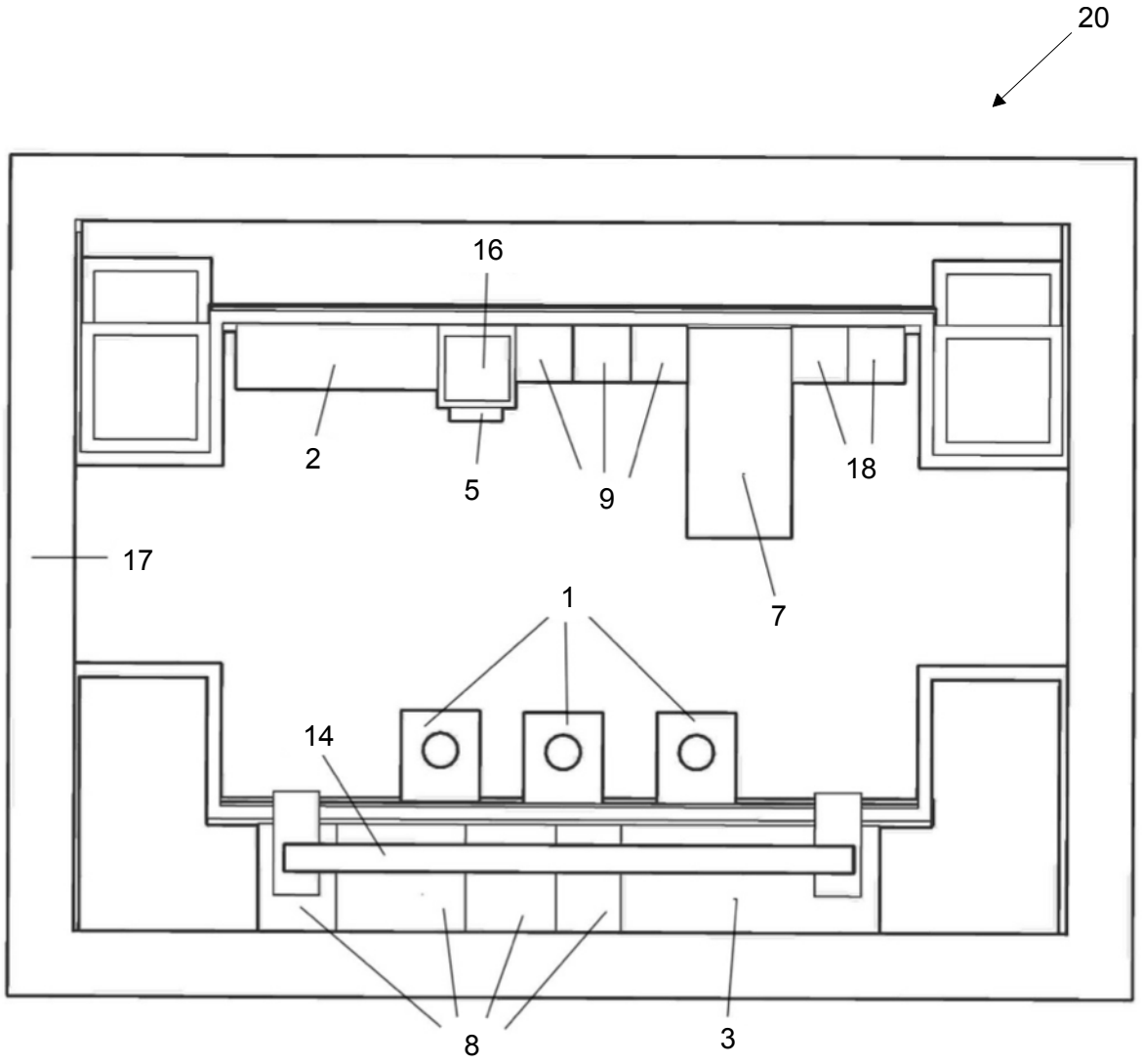

FIG. 4