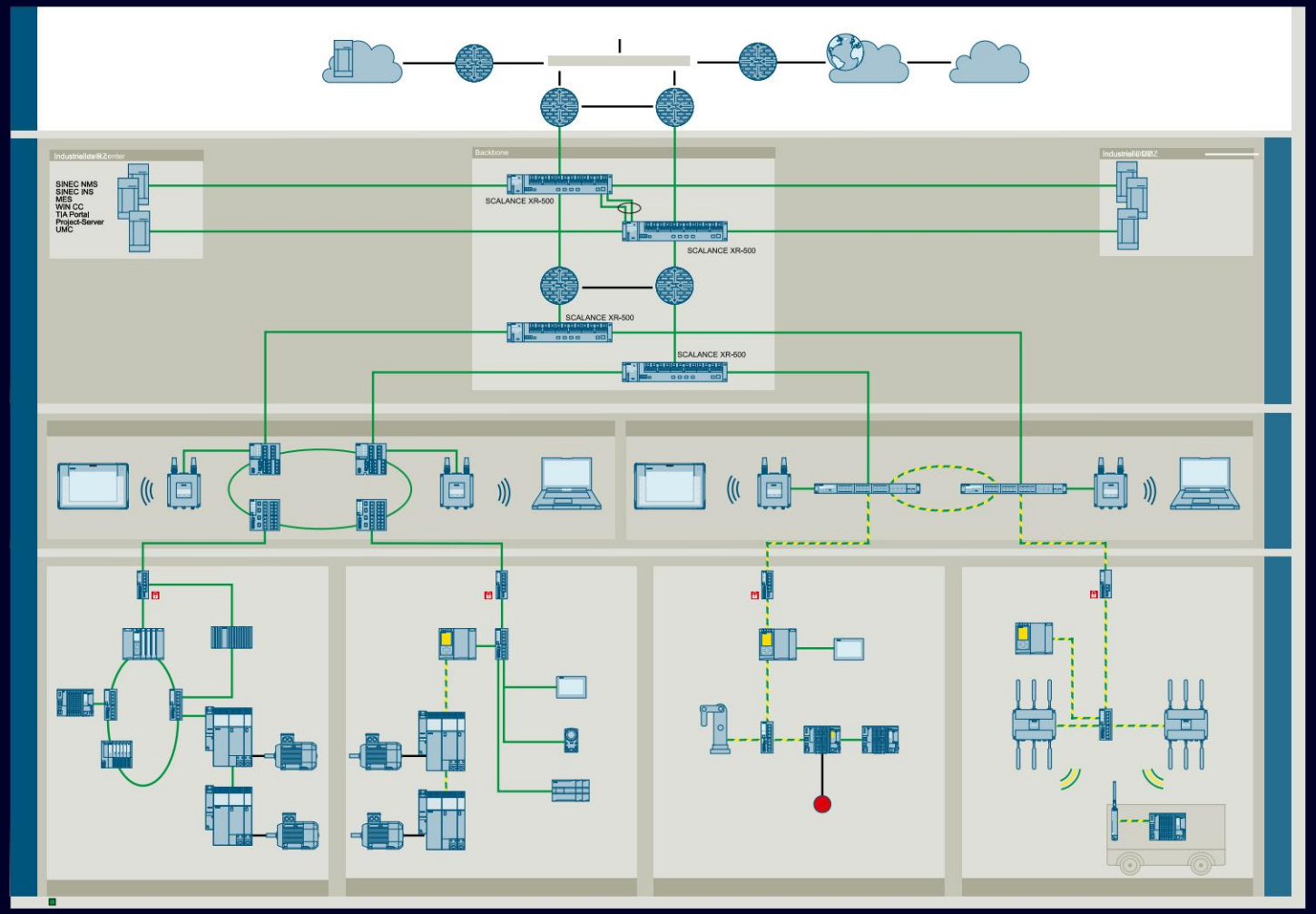
Concepto de red para Factory Automatización

Diseño de red probado, seguro y confiable como base para una producción exitosa

SIEMENS

Concepto de red para la automatización de fábricas
Base para una producción exitosa



Proven, secure and reliable network design

Desafío La digitalización y la creciente conexión en red de máquinas y sistemas industriales también implican una creciente complejidad de las redes industriales.
Los sistemas de OT, TI, lago de datos, nube y producción tienen sus requisitos individuales para las redes. Para cumplir con todos estos requisitos, considerando también la seguridad, la protección, la disponibilidad, la transparencia y el rendimiento, las redes deben diseñarse específicamente para esos usos.
casos.

Solución

En esta implementación de un concepto de red para la automatización de fábricas, se recomienda un concepto de protección de celdas. Este concepto de red muestra un ejemplo de cómo configurar una red industrial basada en casos de uso del cliente. (más información en SIOS)

Valor •

Crear una red estructurada y fiable que satisfaga las demandas de comunicación tanto de OT como de TI • Fácil adaptación

gracias a los ejemplos de configuración preparados

productos y servicios

TIA Portal V18 – CPU S7 – Paneles HMI
– SCALANCE X/S/W – Edge – SINEC – Consultoría de redes

SIEMENS

Agenda

1. Descripción general del concepto de red para la automatización de fábricas
2. Detalles zonas de red
3. Tema – Solución para células
4. Tema: OT frente a redes de TI
5. Tema: comunicación de máquina a máquina
6. Tema: acceso remoto (p. ej., servicio)

SIEMENS

Agenda

1. Descripción general del concepto de red para la automatización de fábricas
2. Detalles zonas de red
3. Tema – Solución para células
4. Tema: OT frente a redes de TI
5. Tema: comunicación de máquina a máquina
6. Tema: acceso remoto (p. ej., servicio)

SIEMENS

Contenidos del concepto de red

SIEMENS

Descripción general del concepto de red
Consideraciones de diseño

Best practice in OT

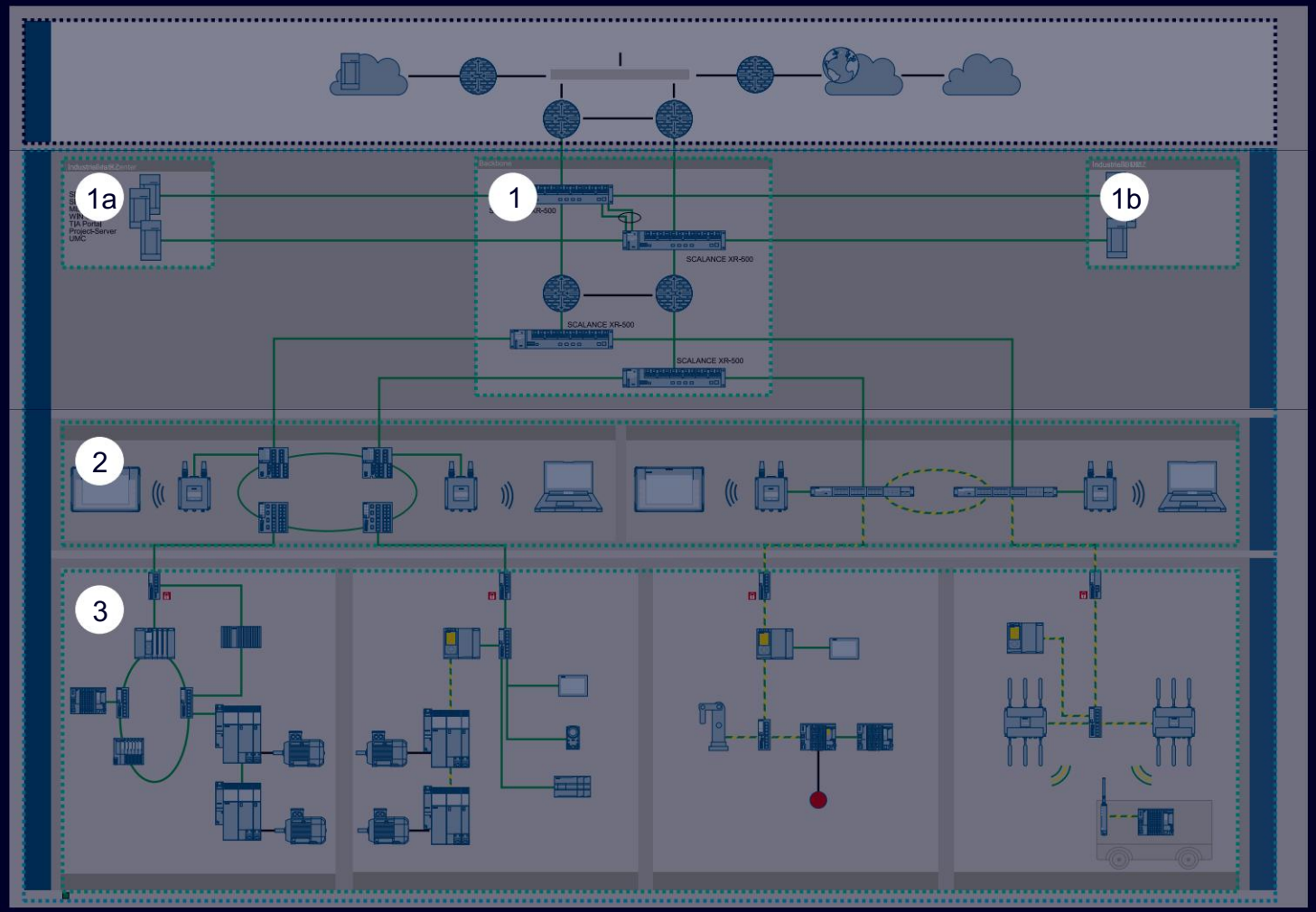
Elegido por el concepto de red
para Factory Automation

Commonly used by IT

SIEMENS

Descripción general del concepto de red para la automatización de fábricas

Zonas de red – Capa 2



Enterprise network – globally connected company solutions and systems

Red industrial – red de plantas

1 Red troncal : red de planta central que conecta TI IDC e IDMZ a la red TO

1a Centro de datos industriales (IDC)

1b Zona Industrial Desmilitarizada (IDMZ)

2 Agregación : acumulación de celdas y posibilidad de funcionalidad adicional

3 Red de celdas : una máquina o grupo funcional de la producción en una celda

SIEMENS

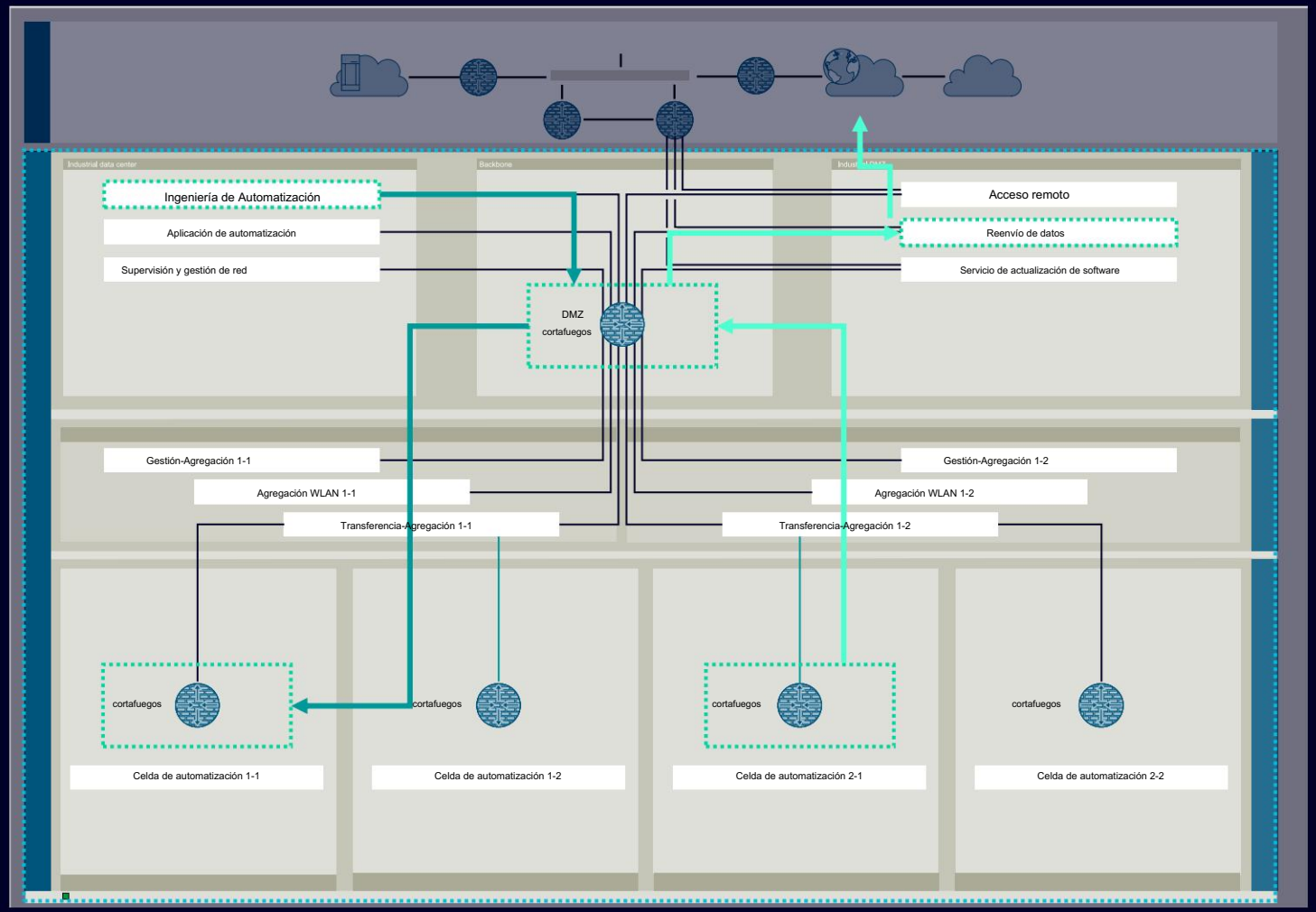
Agenda

1. Descripción general del concepto de red para la automatización de fábricas
2. Detalles zonas de red
3. Tema – Solución para células
4. Tema: OT frente a redes de TI
5. Tema: comunicación de máquina a máquina
6. Tema: acceso remoto (p. ej., servicio)

SIEMENS

Descripción general del concepto de red para la automatización de fábricas

Zonas de red – Capa 3 – red lógica



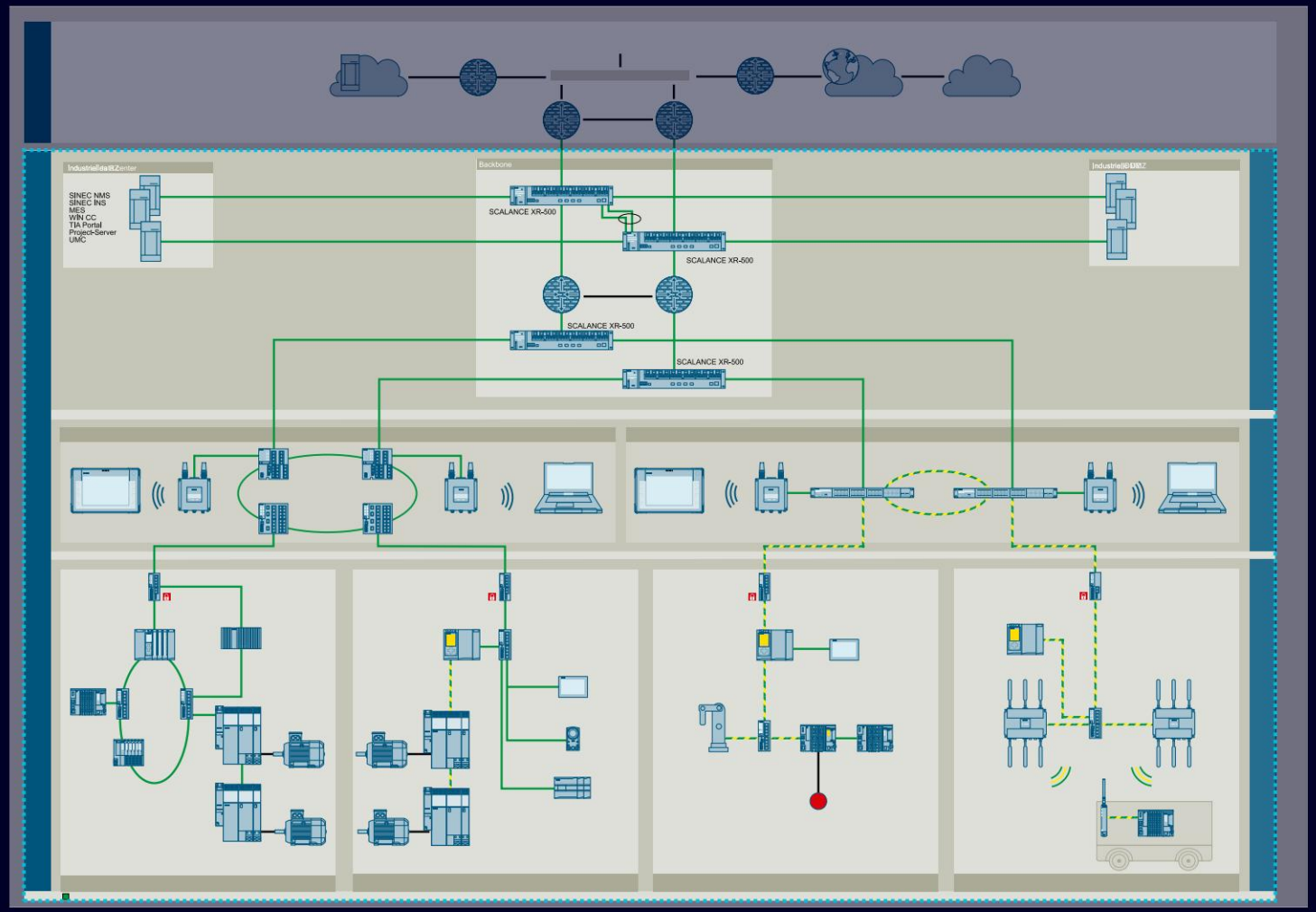
Logical network

- La red está separada en diferentes zonas para aplicaciones específicas basadas en VLAN
- Cada zona está protegida perimetralmente por firewalls que también son responsables del enrutamiento general
- La comunicación entre zonas es posible a través de los cortafuegos y debe permitirse explícitamente (p. ej., descarga de PLC)
- Se requiere que toda la comunicación externa se transfiera a través de sistemas ubicados en la IDMZ (p. ej., acceso a Internet)

SIEMENS

Descripción general del concepto de red para la automatización de fábricas

Red industrial



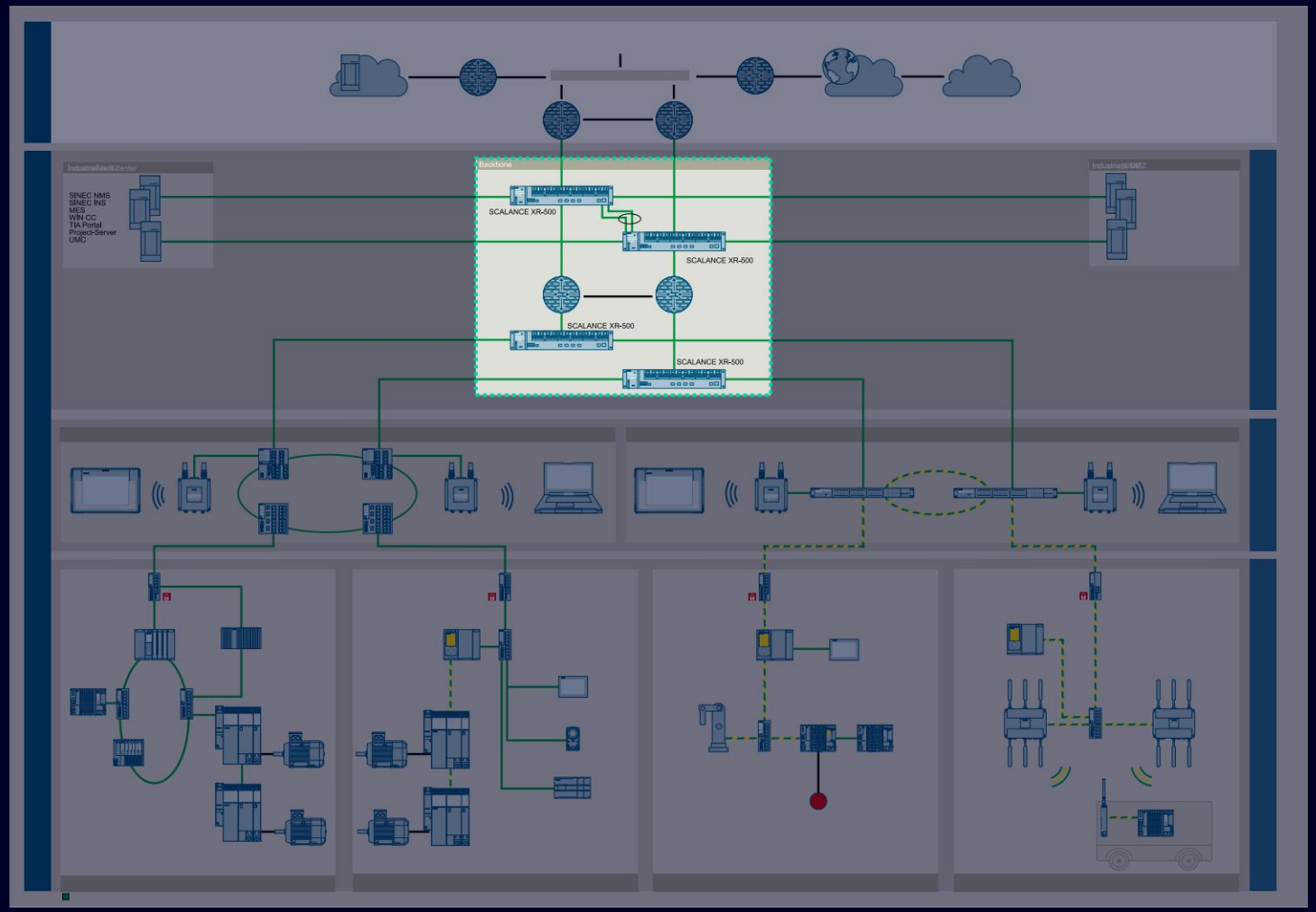
Industrial network

- Construye la base para todas las necesidades de comunicación relevantes para la producción del cliente.
- Está físicamente separado de la red empresarial para cumplir con IEC 62443 (SL2) debido a la seguridad
- Tiene un punto de traspaso definido y controlado a la red empresarial
- Está bajo la responsabilidad de OT mientras está alineado con las operaciones de TI

SIEMENS

Descripción general del concepto de red para la automatización de fábricas

capa de la columna vertebral

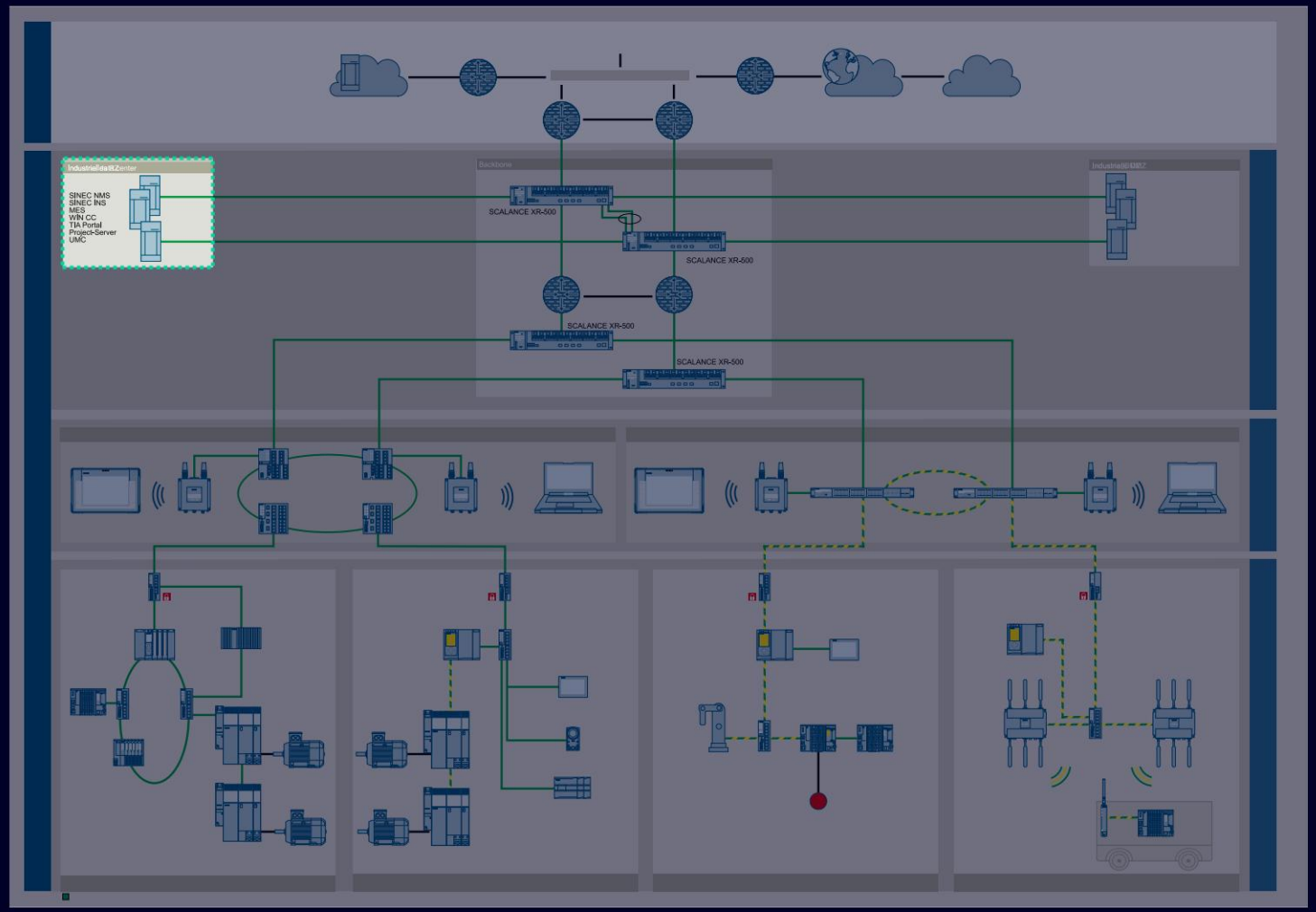


Backbone layer

- Proporciona conectividad entre la red empresarial, IDMZ, IDC y la capa de agregación
- Está construido en base a dispositivos de red y firewall con características de alta disponibilidad y protocolos de redundancia
- Las zonas de seguridad de la red se implementan en función de las VLAN donde el acceso está controlado por políticas de firewall.

SIEMENS

Descripción general del concepto de red para la automatización de fábricas
Centro de datos industriales



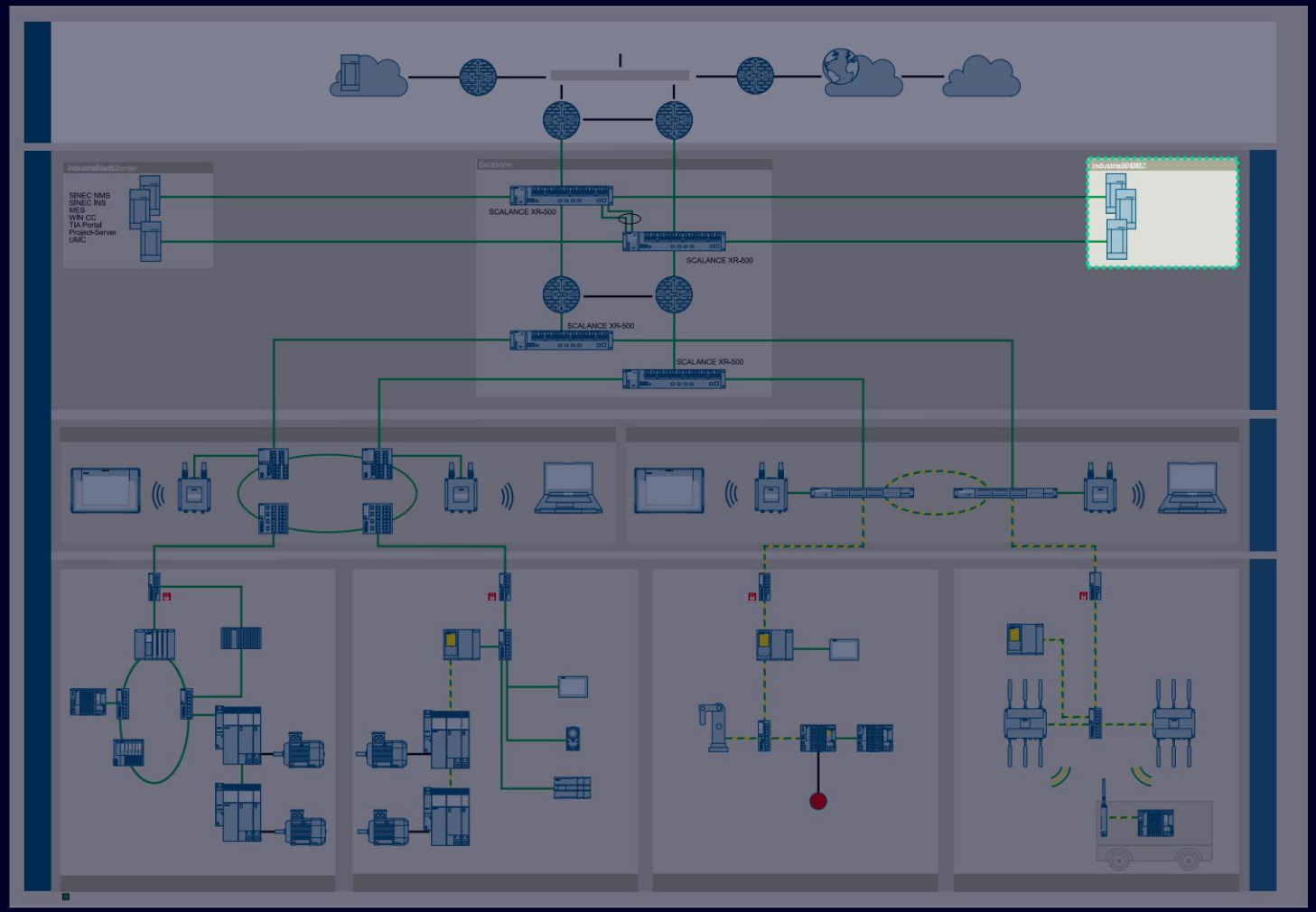
Industrial data center

- Zonas de red seguras donde se encuentran las aplicaciones relevantes para la producción
- Contiene herramientas de automatización como el portal TIA, WinCC, EDGE Management y el sistema MES
- Gestión y servicio de red de hosts Herramientas como SINEC NMS y SINEC INS
- La comunicación es principalmente interna y dirigida a través de la red troncal y la agregación en las células/máquinas.

SIEMENS

Descripción general del concepto de red para la automatización de fábricas

Zona desmilitarizada industrial



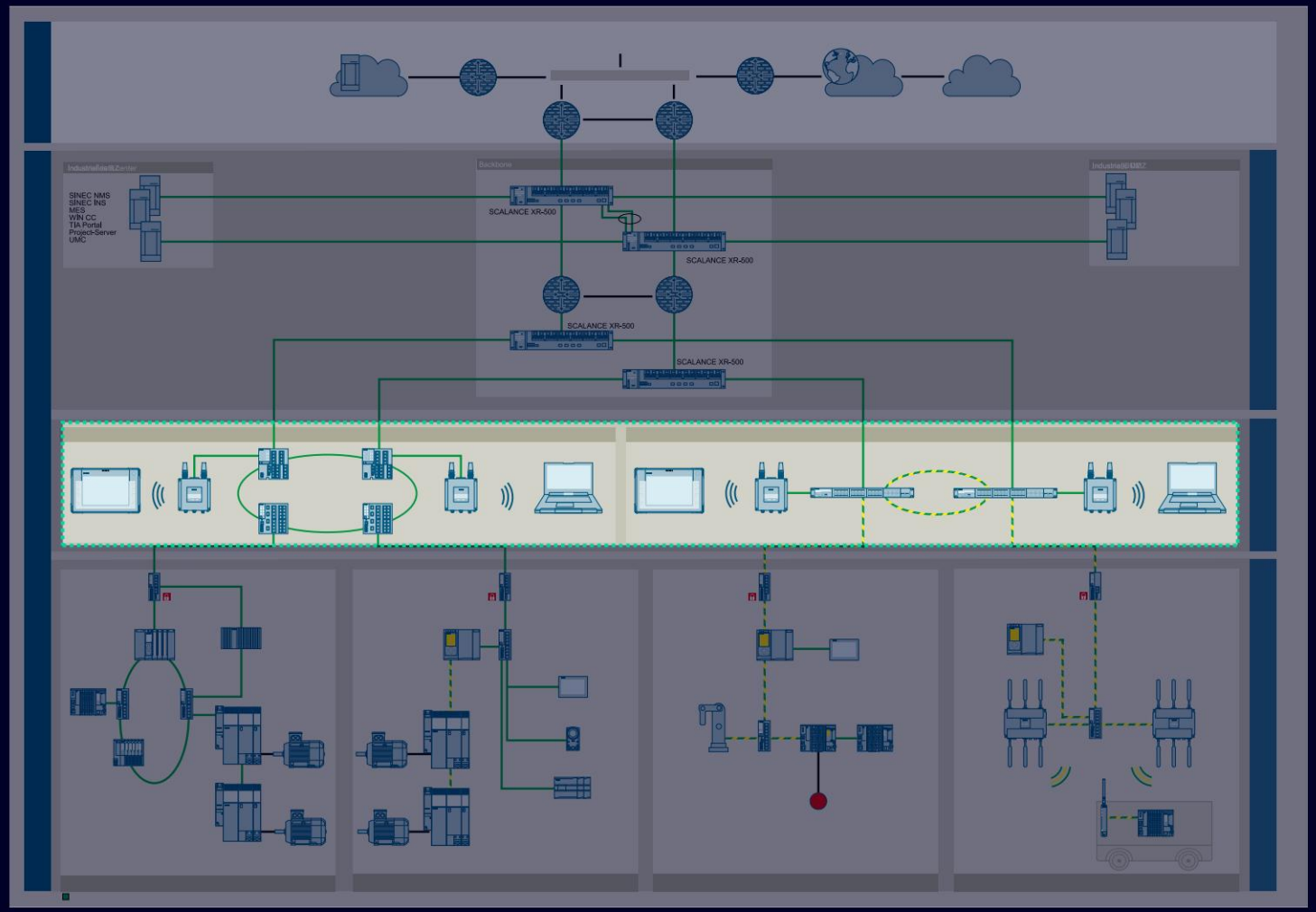
Industrial DMZ

- Zonas de red seguras donde se ubican las aplicaciones y los sistemas para la comunicación entrante/saliente
- SINEMA Remote Connect para remoto
  Acceso con Jump Host para uso interno y Usuarios externos
- WSUS para actualizar Windows,
  Proxy para acceso general a Internet si es necesario
- Active Directory para fines de autenticación y autorización, especialmente pero no solo con Windows

SIEMENS

Descripción general del concepto de red para la automatización de fábricas

Capa de agregación



Aggregation layer

- Proporciona conectividad entre la capa troncal y la capa celular.
- Zonas de red seguras donde se ubican las aplicaciones y los sistemas para el taller (p. ej., WLAN industrial)
- Según el tamaño de la fábrica, la agregación se puede integrar en una sola capa de red troncal

SIEMENS

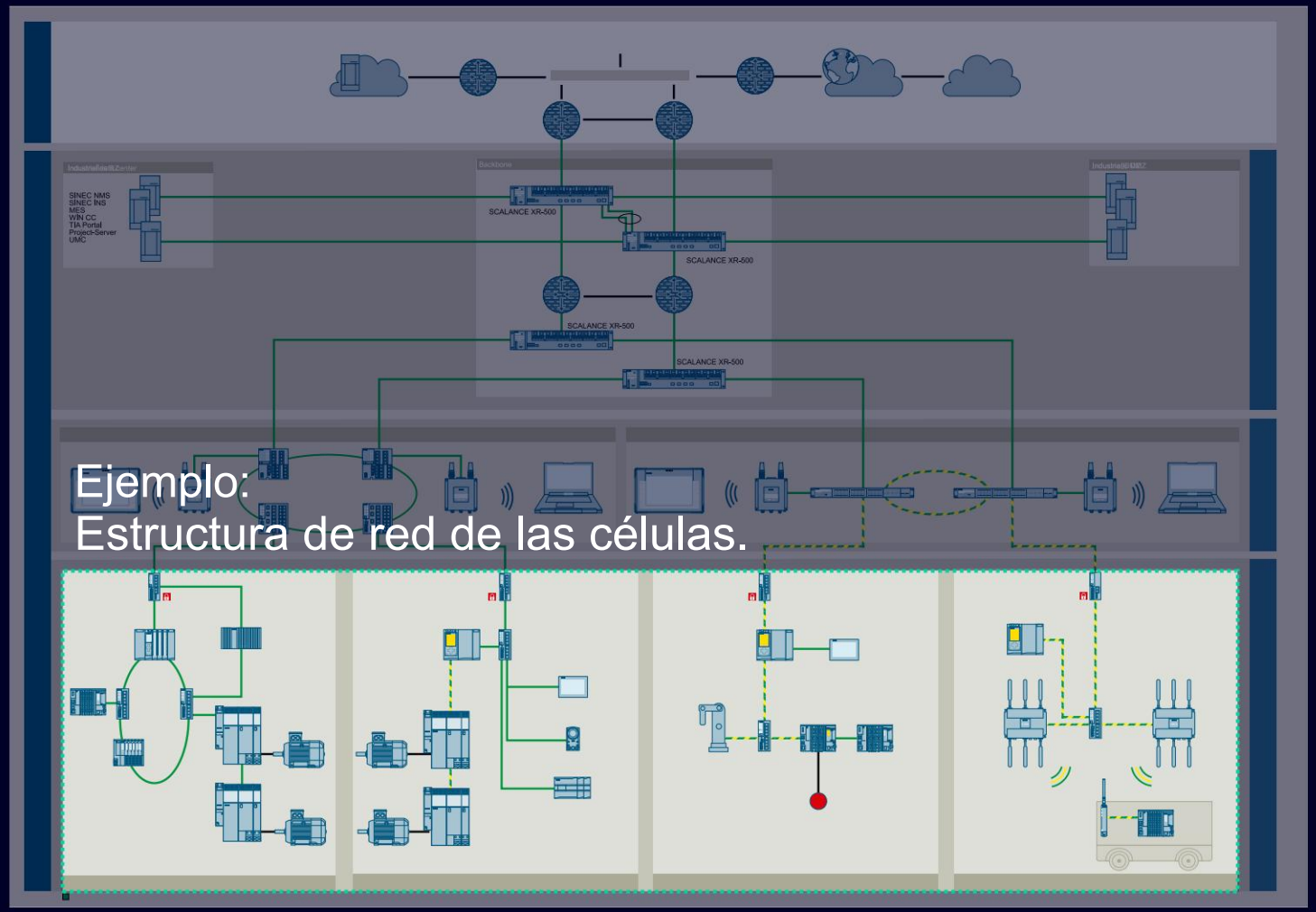
Agenda

1. Descripción general del concepto de red para la automatización de fábricas
2. Detalles zonas de red
3. Tema – Solución para células
4. Tema: OT frente a redes de TI
5. Tema: comunicación de máquina a máquina
6. Tema: acceso remoto (p. ej., servicio)

SIEMENS

Estructura de la red a nivel celular

Resumen de soluciones de ejemplo para el nivel de celda



Ejemplo:
Estructura de red de las células.

Cells – Where the production takes place

Máquinas o grupos funcionales: • Es necesaria la comunicación en tiempo real:
PROFINET RT/IRT

• Las aplicaciones basadas en la seguridad son comunes • Las condiciones ambientales pueden ser adversas

Las redes son simples y generalmente se basan en topologías de estrella, árbol o línea, mientras que la redundancia se puede alcanzar con anillos y protocolos especiales.

Las conexiones a redes externas se pueden realizar a través de PLC o un dispositivo de red dedicado

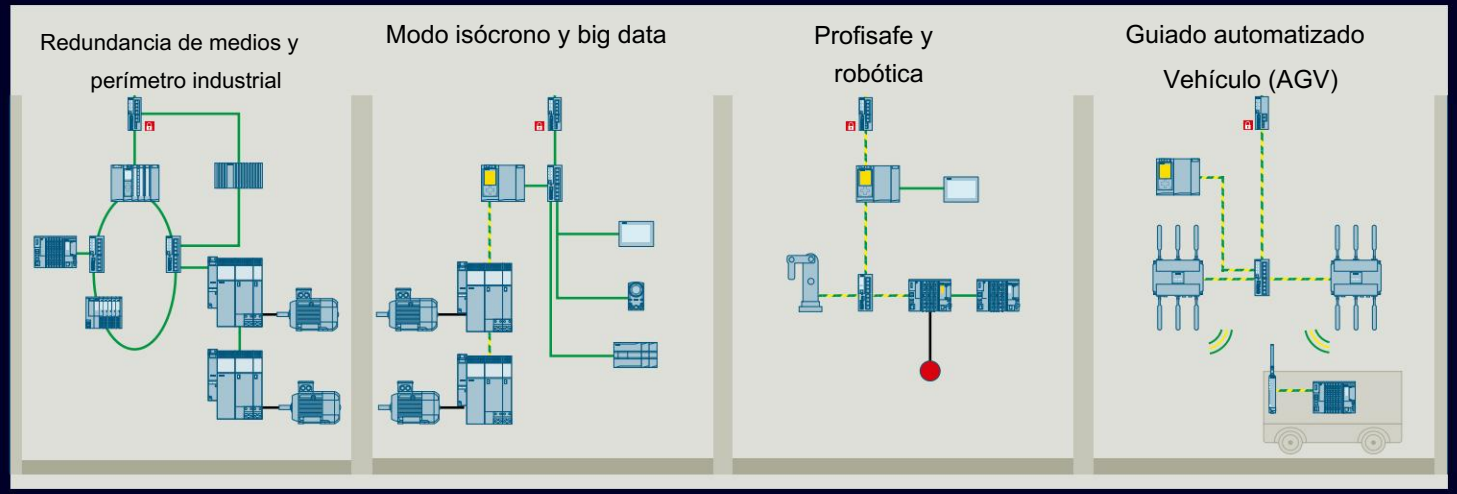
SIEMENS

Estructura de la red a nivel celular

Resumen de soluciones de ejemplo para el nivel de celda

Ejemplo:

Estructura de red de las células.



Cells –
Where the production takes place

Use celdas basadas en casos:

Descripción detallada de cada celda basada en casos de uso

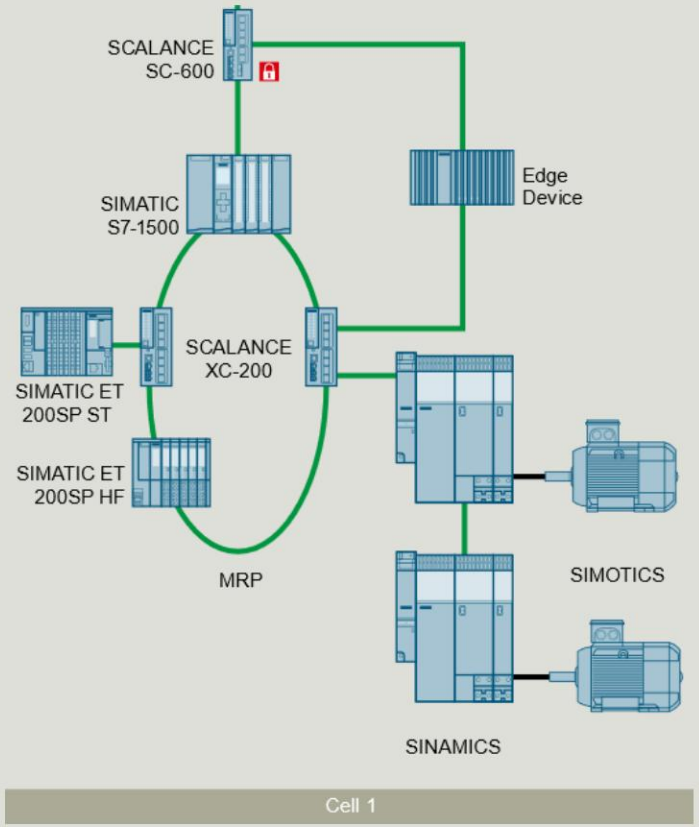
- Requisitos de las celdas en la red
- Propuestas explícitas de implementación
- Documentar enlaces internos/externos para mayor información

SIEMENS

Estructura de la red a nivel celular

Celda 1: redundancia de medios y perímetro industrial

Redundancia de medios
y borde industrial



Availability

- Protocolo de redundancia de medios (MRP) a través de PROFINET
- Controlador de conexión de topología en anillo y conmutadores compatibles
- Stubs PROFINET que conectan dispositivos no compatibles con MRP

Reachability of cell controller and field devices

- Industrial Edge Device •

Interfaz entre los datos de la máquina de nivel inferior y la gestión de la planta de nivel superior

Datos secundarios MRP

- Máx. 50 dispositivos
- Tiempo de reconfiguración inferior a 200 ms
- Admite PROFINET RT •

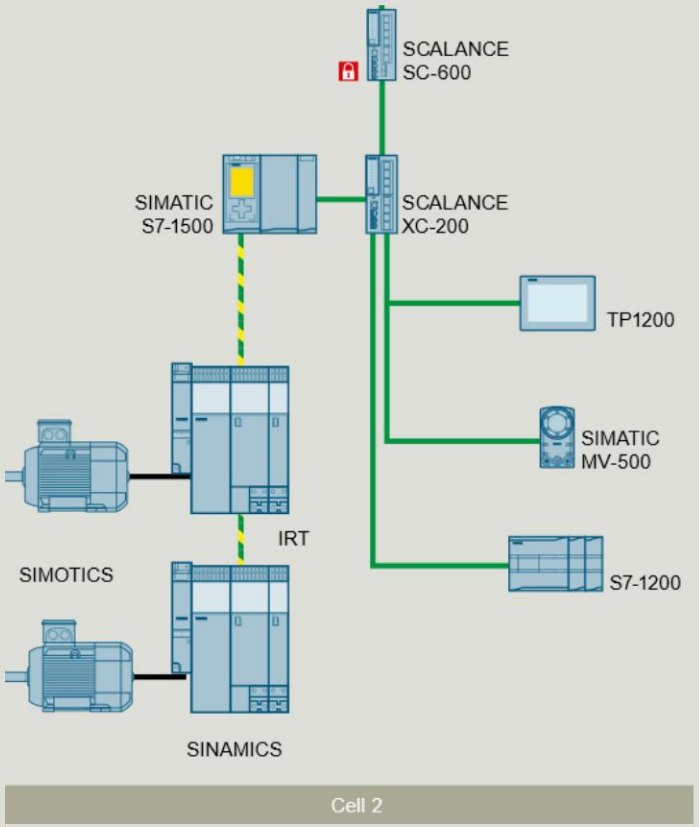
PROFINET IRT es posible con la extensión MRPD

SIEMENS

Estructura de la red a nivel celular
Celda 2: Modo Isócrono y Big Data

Modo isócrono

y grandes datos



Realtime communication

• PROFINET Isochronous Realtime IO Communication (IRT) • Caso de uso: aplicaciones de movimiento

Big Data

• Conmutador compatible con Gigabit • Manejo confiable de altas velocidades de datos • Caso de uso: flujos de video detallados

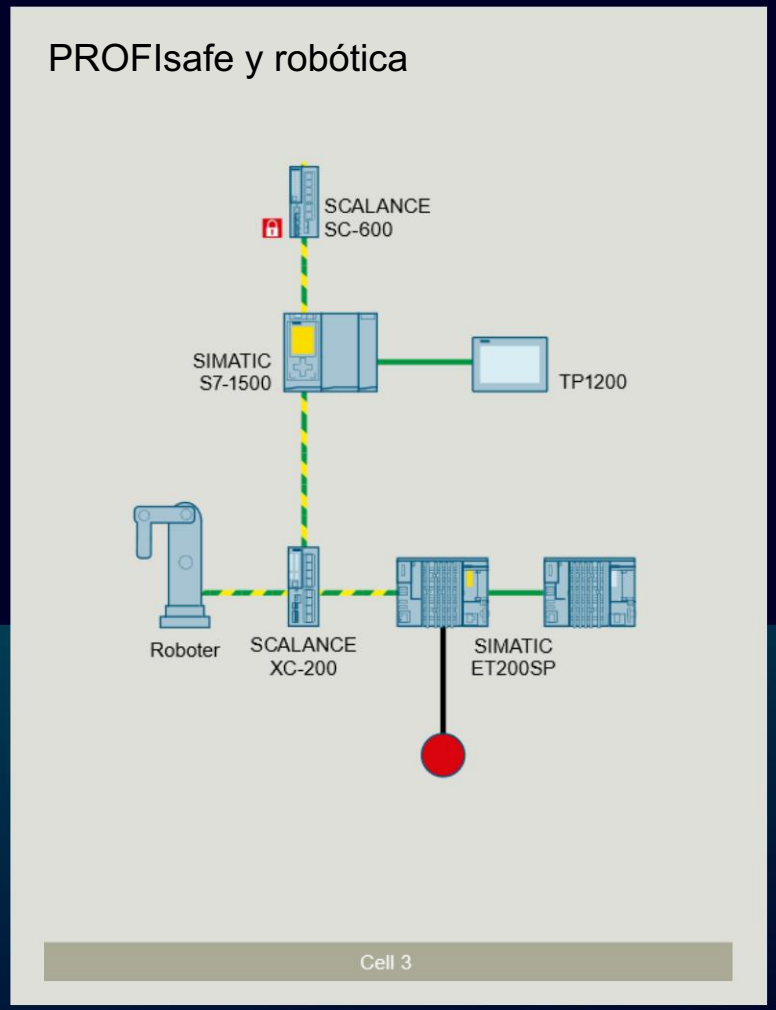
Datos secundarios IRT •

Topología lineal • Los dispositivos deben estar en el mismo dominio de sincronización • El proceso de diseño debe considerar:

Ancho de banda de la red, reloj de envío, longitud del cable, ciclo de aplicación • Separación de dispositivos Big Data de la red RT

SIEMENS

Estructura de la red a nivel celular
Celda 3: PROFIsafe y robótica



Safety

• Corrección y actualización de los datos •
Entrega oportuna de los datos
• Garantía del receptor correcto • El
cruce de los límites de celda/subred está habilitado por F-Link flexible a través de Open
Usuario Comunicación entre CPU

Robotics

• El robot debe cumplir los requisitos de PROFINET, por ejemplo, el ciclo de actualización de E/S •
La instalación y el mantenimiento se realizan normalmente a través de la interfaz
local → Debe tenerse en cuenta durante el proceso de diseño de la celda

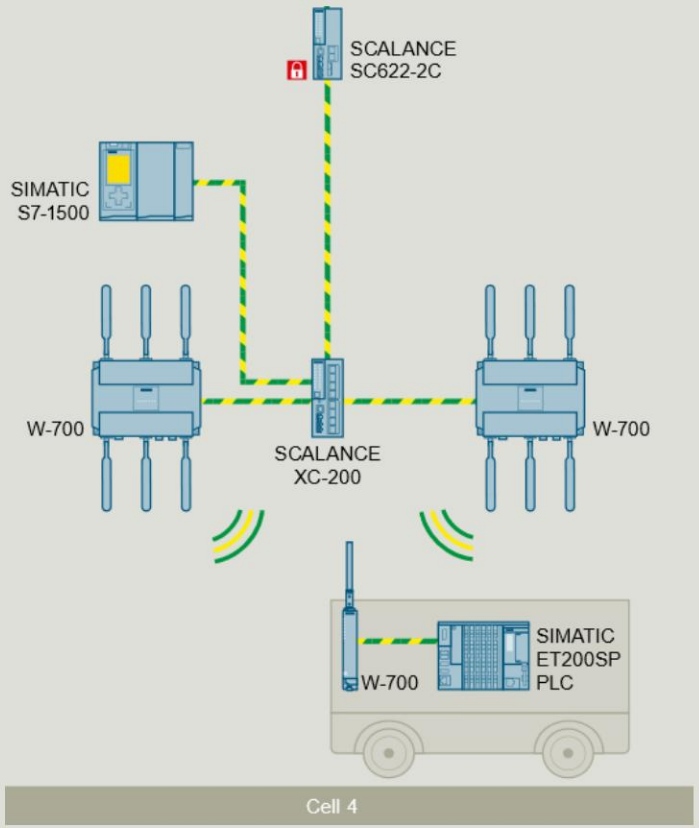
Datos secundarios SEGURIDAD

• Direcciones PROFIsafe únicas debido a la separación de capa
2 • Comunicación entre celdas a través de F-Link flexible

SIEMENS

Estructura de la red a nivel celular
Celda 4: Vehículo de guiado automático (AGV)

Vehículo guiado automatizado



Mobile automation solution

• Red de área local inalámbrica industrial (IWLAN) y PROFIsafe trabajando juntos • Vehículo guiado automatizado (AGV) con funciones de seguridad integradas independientes • Comunicación centrada en la seguridad con la unidad de control central • Direcciones únicas de dispositivos PROFIsafe a nivel de celda son cruciales para una funcionalidad segura

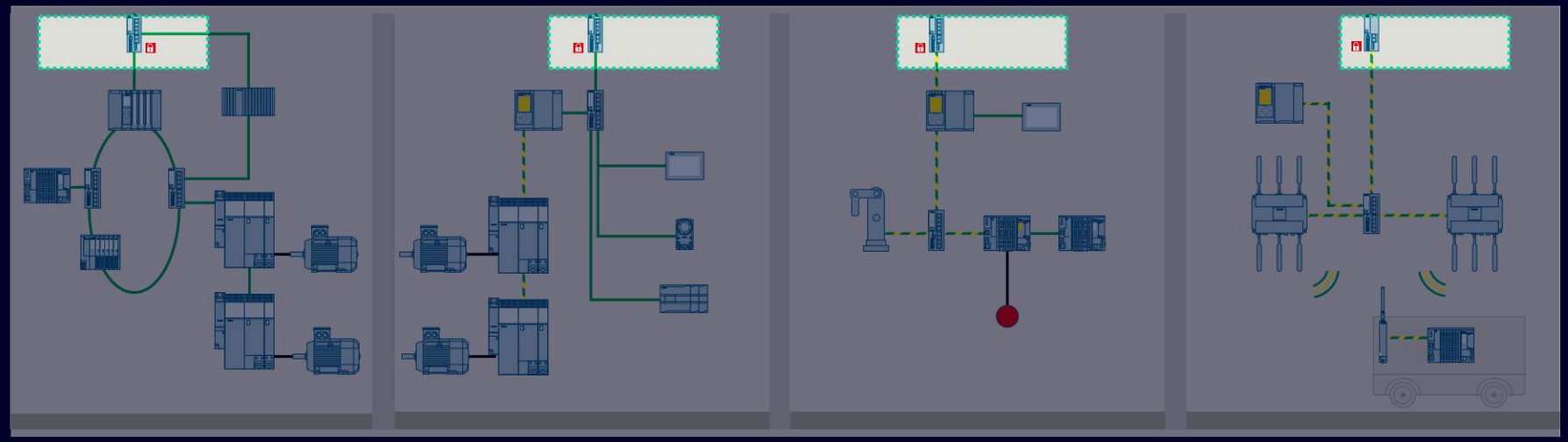
Datos secundarios

• Separación de capa 2 a través de SCALANCE SC622-2C • SCALANCE SC626-2C con 6 puertos para mayor flexibilidad • RT y PROFIsafe también a través de redes inalámbricas • Wi-Fi 6 y bajo consumo de energía

SIEMENS

Estructura de la red a nivel celular

Acceso a la celda a través de un firewall dedicado



Common cell access point: Firewall

• Único punto de acceso a nivel de celda • Stateful Packet Inspection • La seguridad surge de la separación de la capa 3 de las celdas • Mayor escalabilidad debido a la configuración independiente de las celdas • Los dispositivos SCALANCE SC622-2C y SC626-2C cumplen los requisitos de la especificación PROFIsafe

Contains

• Cortafuegos recomendado reglas para cumplir con los requisitos de los temas técnicos “configuración con TIA”

• Descripción de los requisitos para cada diseño de celda de ejemplo, por ejemplo, PROFIsafe

SIEMENS

Agenda

1. Descripción general del concepto de red para la automatización de fábricas
2. Detalles zonas de red
3. Tema – Solución para células
4. **Tema: OT frente a redes de TI**
5. Tema: comunicación de máquina a máquina
6. Tema: acceso remoto (p. ej., servicio)

SIEMENS

Seguridad de la red
Enfoque diferente en OT y TI

Disponibilidad | Integridad | Confidencialidad

Bajo — **Prioridad** — Alto

Confidencialidad | Integridad | Disponibilidad

¡ IEC 62443 es uno de los estándares líderes para la seguridad de redes y sistemas en la industria!

Los riesgos de seguridad pueden surgir debido a la conectividad a Internet

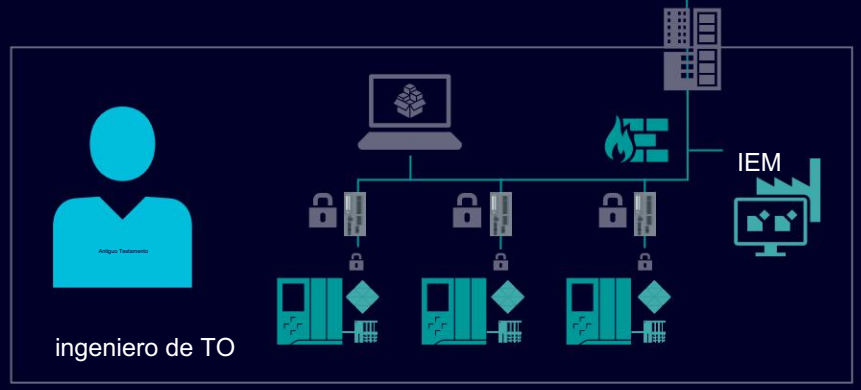
Daily business!

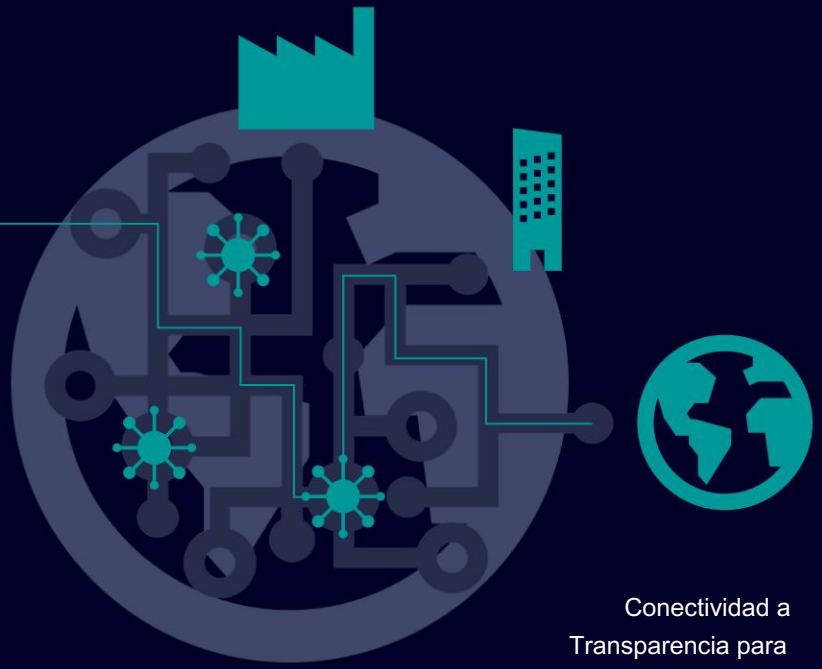
Muchas medidas para evitar hilos de seguridad. →

“Just” need to extend?

Nunca he oído hablar
de: •

Cortafuegos • PKI • Servidores proxy





Conectividad a
Transparencia para
componentes
externos

Desafío: cumplir con los estándares utilizados en la infraestructura de TI

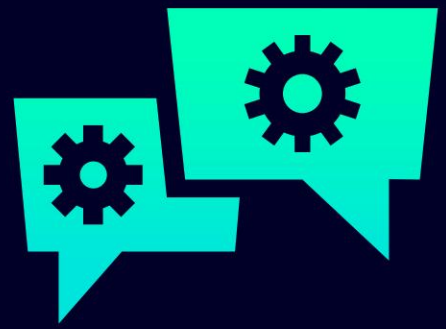
SIEMENS

Agenda

1. Descripción general del concepto de red para la automatización de fábricas
2. Detalles zonas de red
3. Tema – Solución para células
4. Tema: OT frente a redes de TI
5. Tema: comunicación de máquina a máquina
6. Tema: acceso remoto (p. ej., servicio)

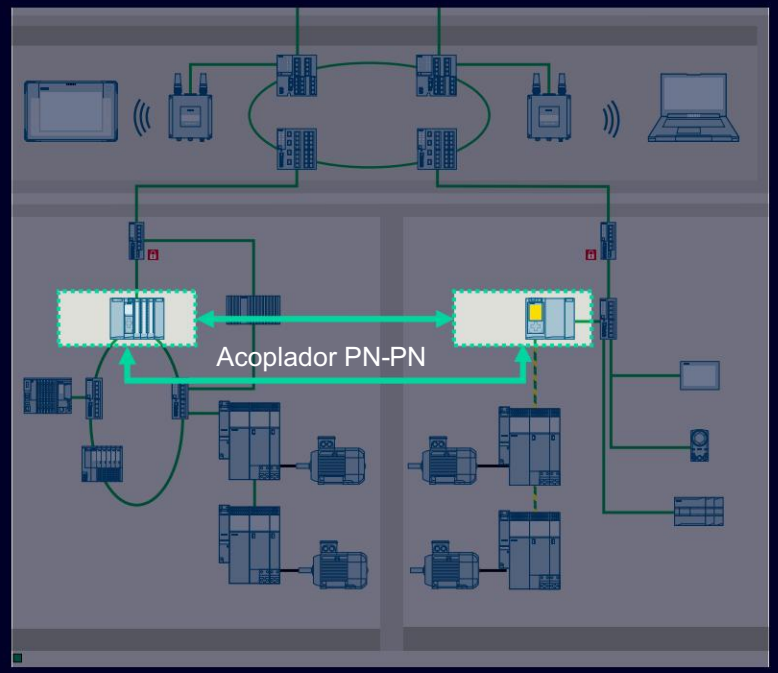
SIEMENS

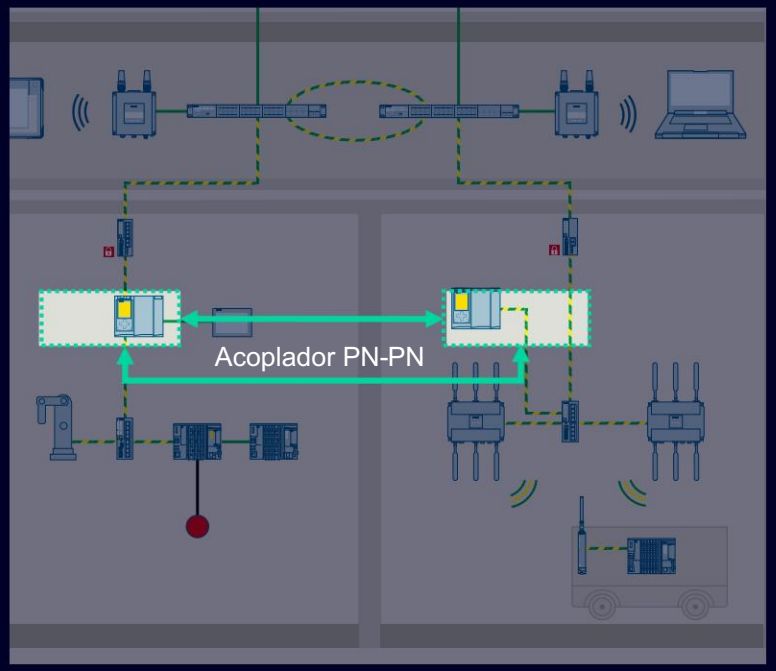
¿Cómo puede la comunicación entre las máquinas a configurar con respecto a los diferentes requisitos?



SIEMENS

Tema: comunicación de máquina a máquina (M2M)
¿Cómo se comunican las células entre sí?





Se describen múltiples métodos de comunicación a través de sus casos de uso.

Descripción de los requisitos para cada protocolo con respecto a las reglas del firewall y las condiciones de seguridad

Descripción detallada de las tres formas recomendadas de comunicación M2M

Requirements on M2M communication in consideration shown use cases

General •

Capacidad de enrutamiento

• Mecanismos de seguridad •

Capacidad en tiempo real

Avanzado •

Apertura •

Estandarización •

Seguridad

Tema: comunicación de máquina a máquina (M2M)
Tipos de comunicación máquina a máquina recomendados

Servidor/Cliente OPC UA

Routing capable, secure, open, standardized

Solución preferida para comunicación estandarizada

El modelado de interfaz también es posible de acuerdo con las especificaciones complementarias

Transferencia de datos consistente a través de métodos

Acoplador PROFINET PN/PN

Realtime capable, standardized, safety capable

Diseñado para cumplir con requisitos estrictos en tiempo real

Se puede implementar como medida de seguimiento

Dispositivo dedicado para la transferencia de datos

Enlace F flexible

Routing capable, secure, safety-focused

Especialmente diseñado para requisitos de SEGURIDAD incluso sobre enrutadores

El protocolo se puede elegir dependiendo ( )

No se requiere hardware adicional para la comunicación SAFETY M2M

TCP

UDP

S7

SIEMENS

Agenda

1. Descripción general del concepto de red para la automatización de fábricas
2. Detalles zonas de red
3. Tema – Solución para células
4. Tema: OT frente a redes de TI
5. Tema: comunicación de máquina a máquina
6. Tema: acceso remoto (p. ej., servicio)

SIEMENS

¿Cómo puedo garantizar la disponibilidad y un servicio rápido con una configuración de red tan segmentada?

SIEMENS

Servicio en-sitio
Consumidor de tiempo y costoso

constructor de maquinas

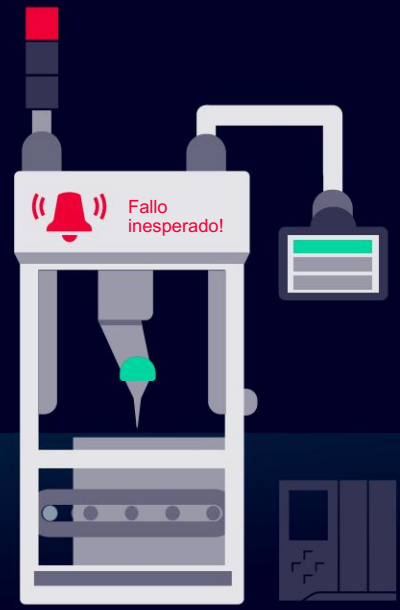
What kind of trouble?

We send someone
out tomorrow.
Next week he will arrive on-site.

We are having trouble with a machine

Unexpected Fault

Cliente final



Falta del tiempo

Reprogramación necesaria

El servicio in situ consume mucho tiempo

SIEMENS

Solución posible

Utilice la conexión a Internet para llegar a la máquina

Desafío: ¡ Establezca conexiones remotas seguras!

SIEMENS

Conectividad remota
Riesgos y requisitos

Risks

Fácil descubrimiento de equipos „OT

Acceso no autorizado

Espionaje y ataques
man-in-the-middle

Ataques de denegación de servicio

Remote access requirements

Alta protección necesaria -de-
la-

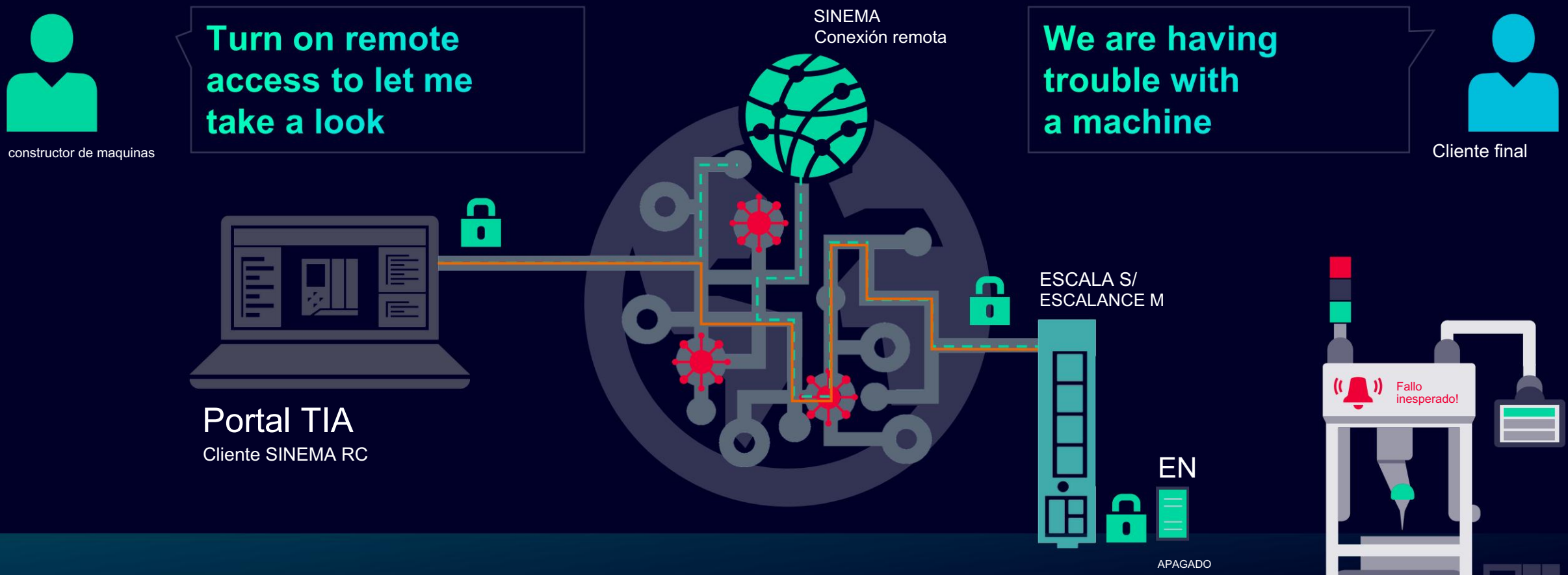
Limite y gestione el acceso con una gestión de usuarios eficiente

Optimice la usabilidad, por ejemplo, mediante una integración perfecta en la cartera SIMATIC

Configuración rápida y fácil
sin conocimientos de TI

SIEMENS

Servicio remoto con SINEMA Remote Connect

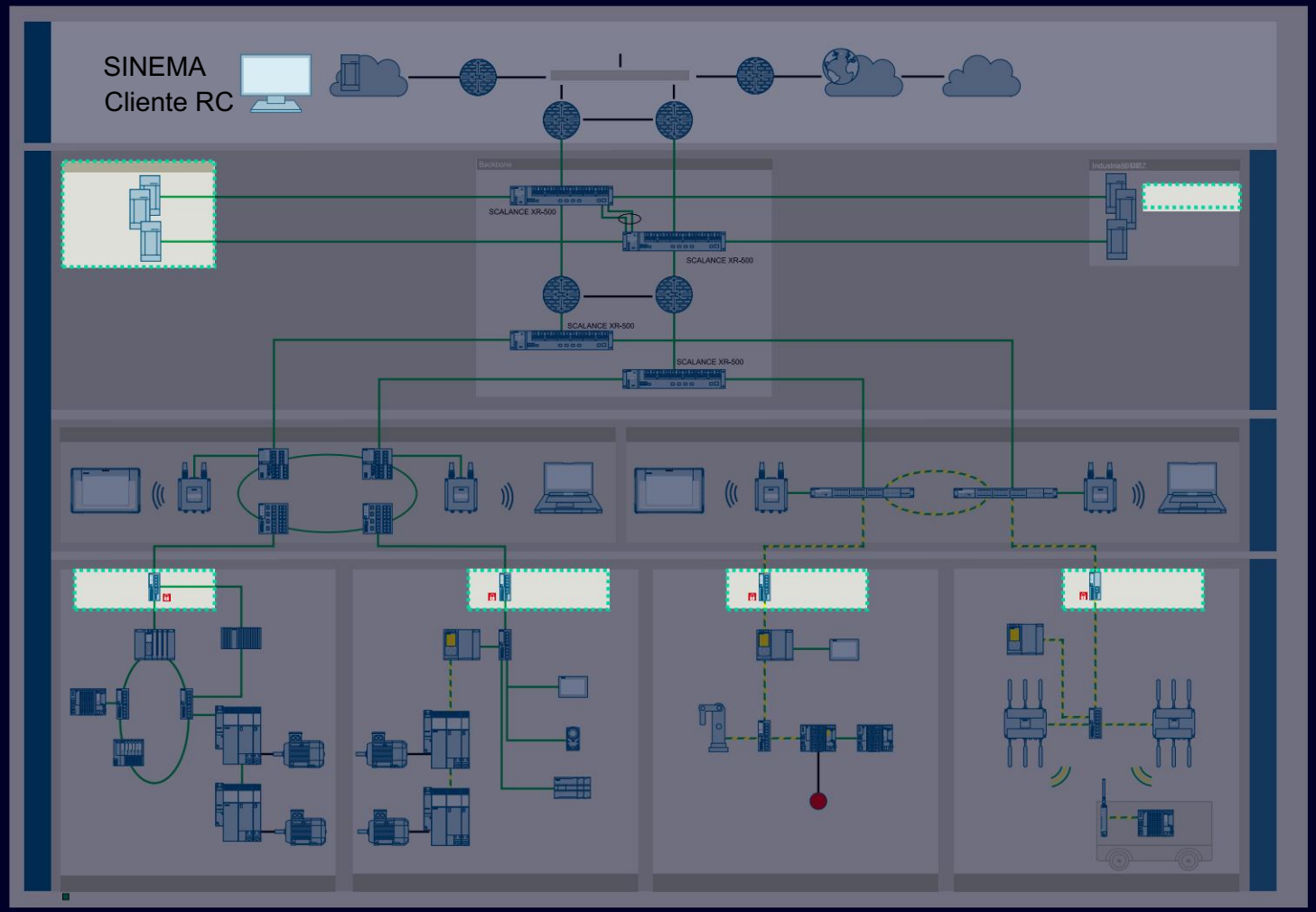


Solución: SINEMA Remote Connect ofrece una plataforma de acceso remoto segura y fácil de usar

SIEMENS

Caso de uso: acceso remoto

Descripción general de los componentes dentro del concepto de red



Enterprise network

Cliente SINEMA RC/Escritorio remoto
Protocolo (RDP)

Industrial network – plant network

IDMZ
• Servidor SINEMA Remote Connect •
Jump Host (interno y externo)

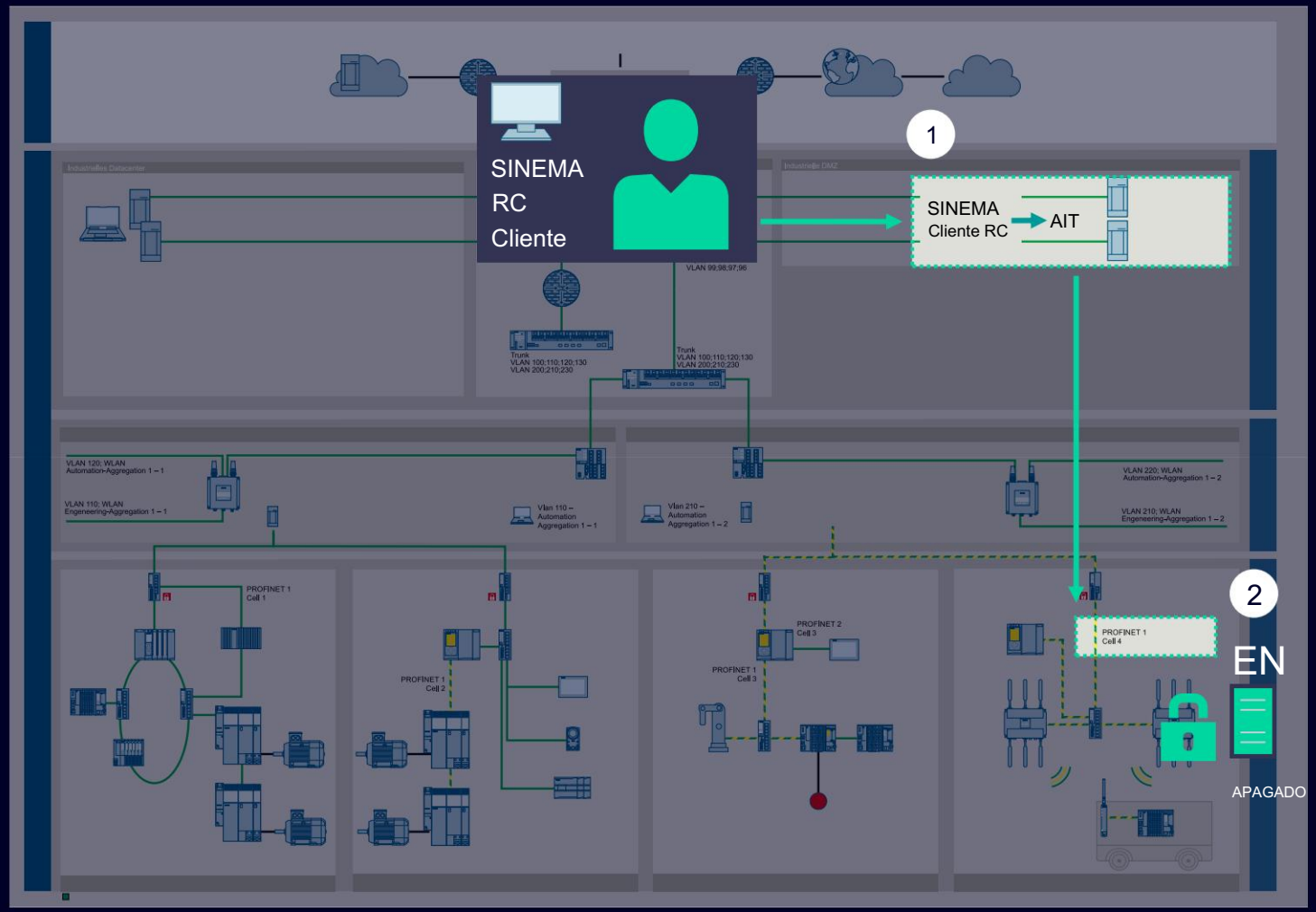
Herramientas de gestión de red y automatización de IDC (p. ej., TIA Portal, SINEC NMS)

Cell network

SCALANCE SC-600/S615

SIEMENS

Caso de uso: acceso remoto
Acceso externo



- Fabricante de la máquina (a través de jump host external)
  Proveedor externo se conecta a través de internet

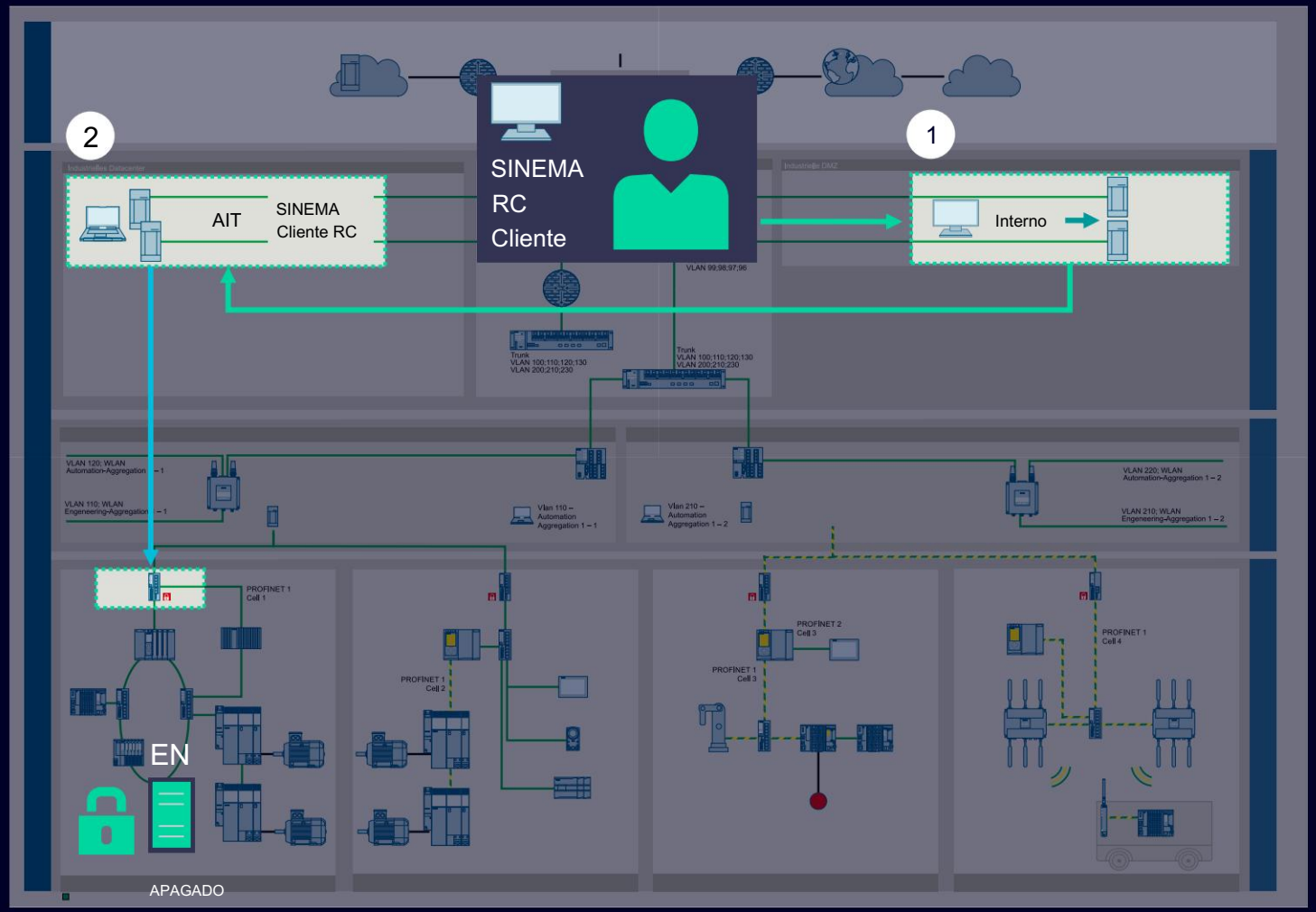
1 Conexión a través del cliente SINEMA RC a SINEMA Remote Connect Server en IDMZ, que se encarga del reenvío de datos junto con un Jump Host

El cortafuegos de celdas permite la conexión vía SINEMA Remote Connect Server vía interruptor de llave

- Todas las tareas requeridas se pueden realizar a través de aplicaciones instaladas en la PC/PG del fabricante de la máquina

SIEMENS

Caso de uso: acceso remoto
Acceso interno



- Técnico de servicio (a través de host de salto interno)
  Empleado interno a través de Internet/ red empresarial

1 Conéctese a través de SINEMA RC Client a
SINEMA Remote Connect Server en IDMZ,
que se encarga de los Datos
Reenvío junto con un Jump Host

2 Conéctese a la máquina virtual requerida
(MV) en el IDC

- Tareas sencillas (p. ej., descarga de PLC,
  servidor web) sin medidas adicionales de seguridad.
  Todas las aplicaciones necesarias están alojadas en
  IDC

- Las tareas críticas para la seguridad deben ser
  habilitadas por el cortafuegos celular
  SCALANCE SC-600 a través
  de un interruptor de llave (p. ej., acceso no autorizado con SNMP

SIEMENS

Contacto

Publicado por Siemens XX
Nombre Apellido
Título profesional
Grupo/Región/Departamento XY
calle 123
12345 ciudad
País
Teléfono +49 123 45 67 89
Móvil +49 123 45 67 89 0
Correo electrónico nombre.apellido@siemens.com

SIEMENS

Sujeto a cambios y errores. La información proporcionada en este documento solo contiene descripciones generales y/o características de rendimiento que pueden no siempre reflejar específicamente las descritas, o que pueden sufrir modificaciones en el curso del desarrollo posterior de los productos. Las características de rendimiento solicitadas son vinculantes solo cuando se acuerdan expresamente en el contrato celebrado.

Informacion de seguridad

Para proteger plantas, sistemas, máquinas y redes contra amenazas cibernéticas, es necesario implementar, y mantener continuamente, un sistema industrial holístico y de última generación.

.

concepto. Para obtener más información sobre seguridad industrial, visite https://www.siemens.com/industrialsecurity.

SIEMENS