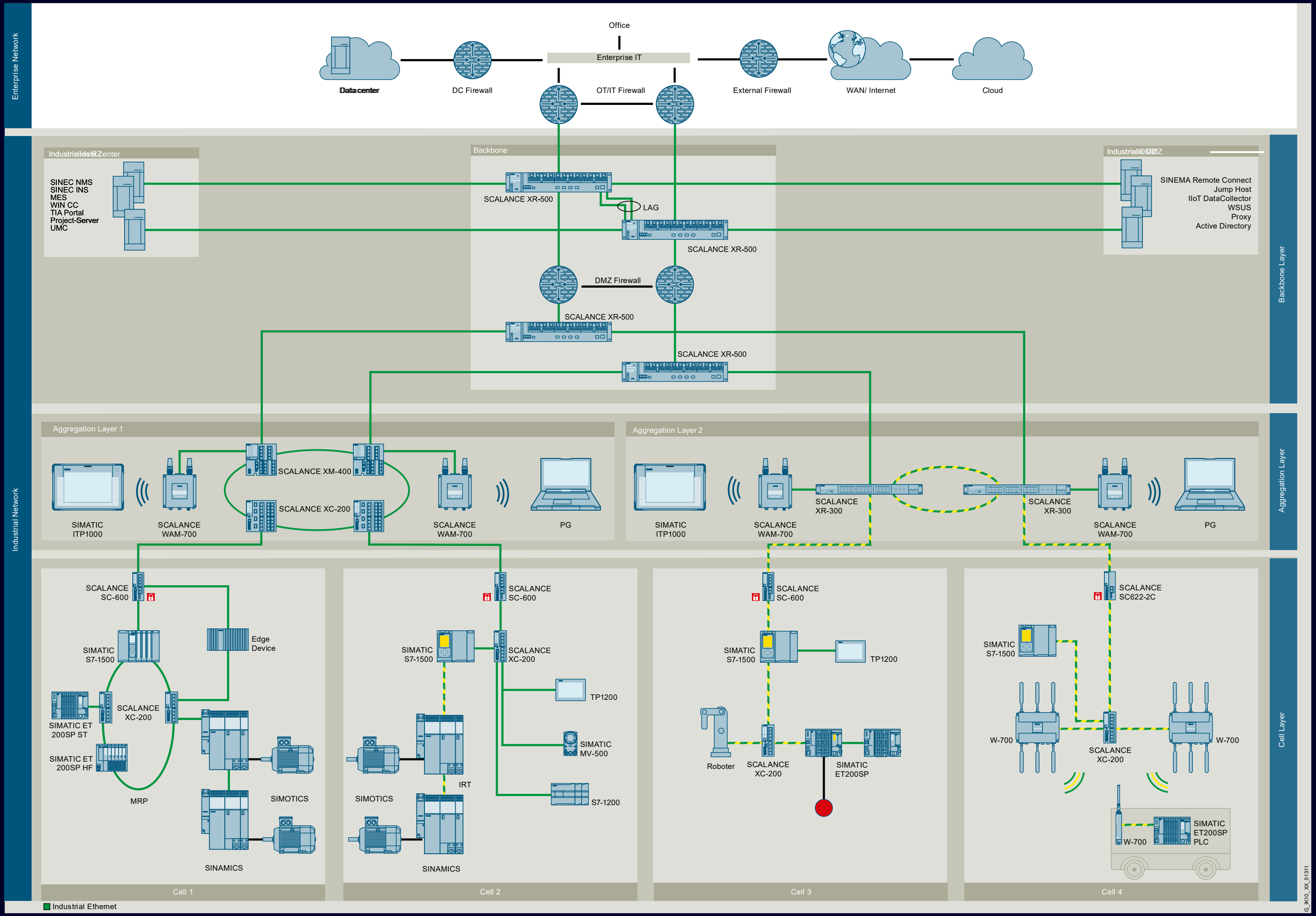
Network concept for Factory Automation

Proven, secure and reliable network design as foundation
for a successful production

SIEMENS

Network concept for Factory Automation
Foundation for successful production



Proven, secure and reliable network design

Challenge

Digitalization and the growing networking of machines and industrial systems also entail an increasing complexity of industrial networks. OT-, IT-, data lake, cloud and production systems all have their individual requirements to networks. To meet all these requirements, also considering security, safety, availability, transparency and performance, networks have to be designed specifically for those use cases.

Solution

In this implementation of a network concept for factory automation, a cell protection concept is recommended. This network concept shows an example of how to set up an industrial network based on customer use cases. (more information s. SIOS)

Value

- Creating a structured and reliable network that meets the communication demands of both OT and IT
- Easy adaption thanks to prepared configuration examples

Products & Services

TIA Portal V18 – S7 CPUs – HMI panels – SCALANCE X/S/W – Edge – SINEC – Network consulting

Agenda

1 Overview network concept for Factory Automation

2 Details network zones

3 Topic – Solution for cells

4 Topic – OT vs. IT networks

5 Topic – Machine to machine communication

6 Topic – Remote access (e.g., service)

Agenda

1 **Overview network concept for Factory Automation**

2 Details network zones

3 Topic – Solution for cells

4 Topic – OT vs. IT networks

5 Topic – Machine to machine communication

6 Topic – Remote access (e.g., service)

Overview network concept for Factory Automation

Contents of the network concept

02 | Solution details

2.1 | Overview of layer 2

2.2 | Overview of layer 3

2.3 | Network structure in the cell level

2.4 | Network structure in the aggregation level

2.5 | Network structure in the backbone level

2.6 | Central network services

03 | Technical topics

3.1 | Visualization

3.2 | Network management

3.3 | Engineering and configuration with TIA Portal

3.4 | Update management

3.5 | Virtualization

3.6 | User management

3.7 | PROFINET communication

3.8 | Safety-related communication

3.9 | M2M communication

3.10 | Communication to clouds

3.11 | Certificate management

3.12 | Security

3.13 | WLAN

3.14 | Edge computing

04 | Use cases

4.1 | Backup restore

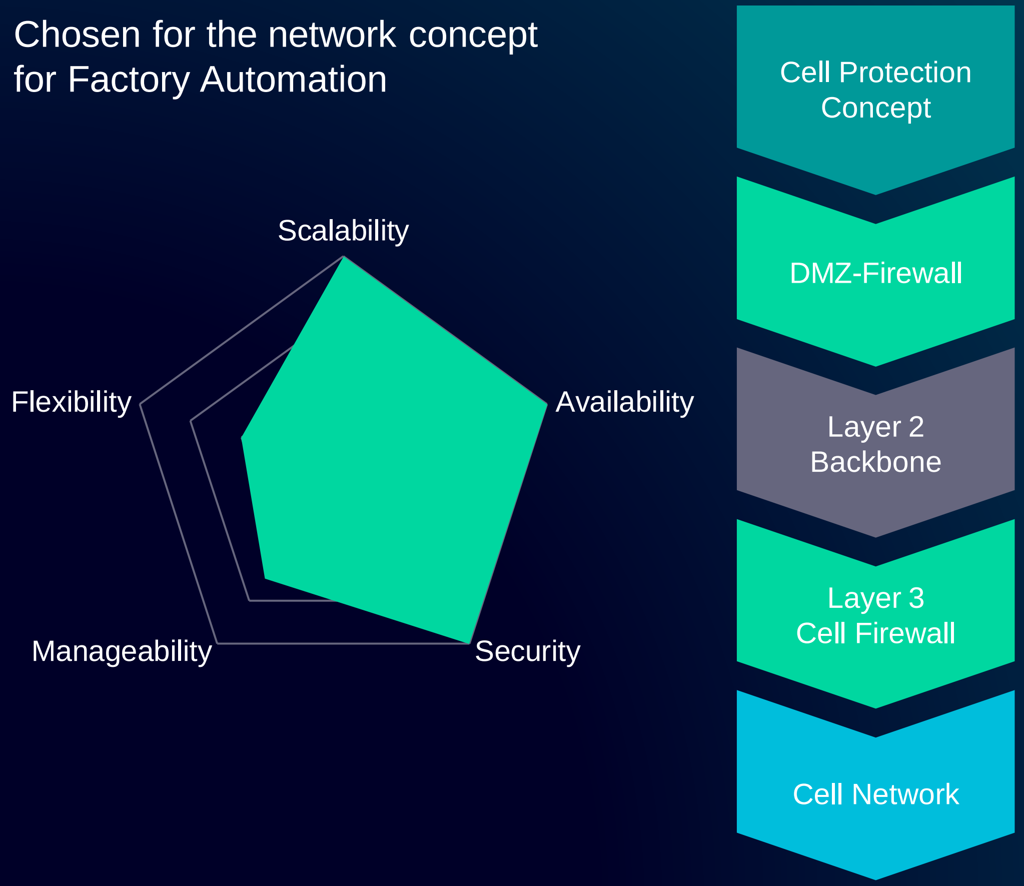
4.2 | Remote access

4.3 | Connecting serial machines

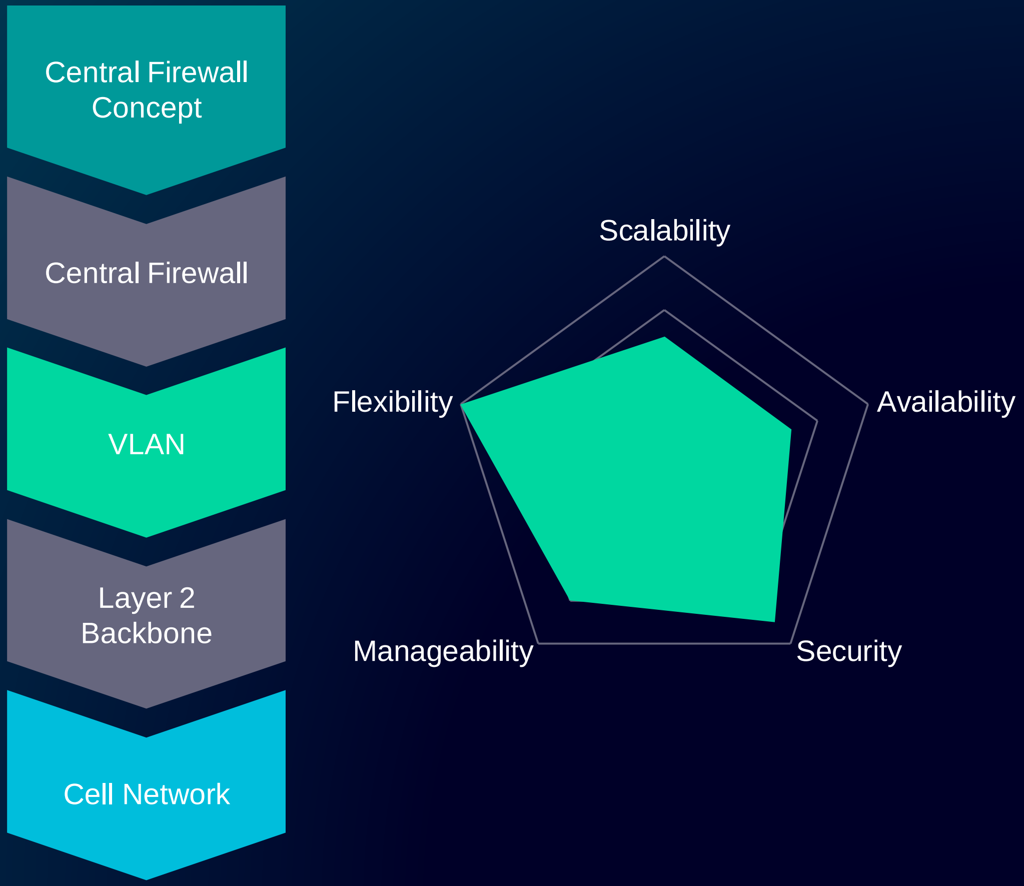
Overview network concept
Design considerations

Best practice in OT

Chosen for the network concept for Factory Automation

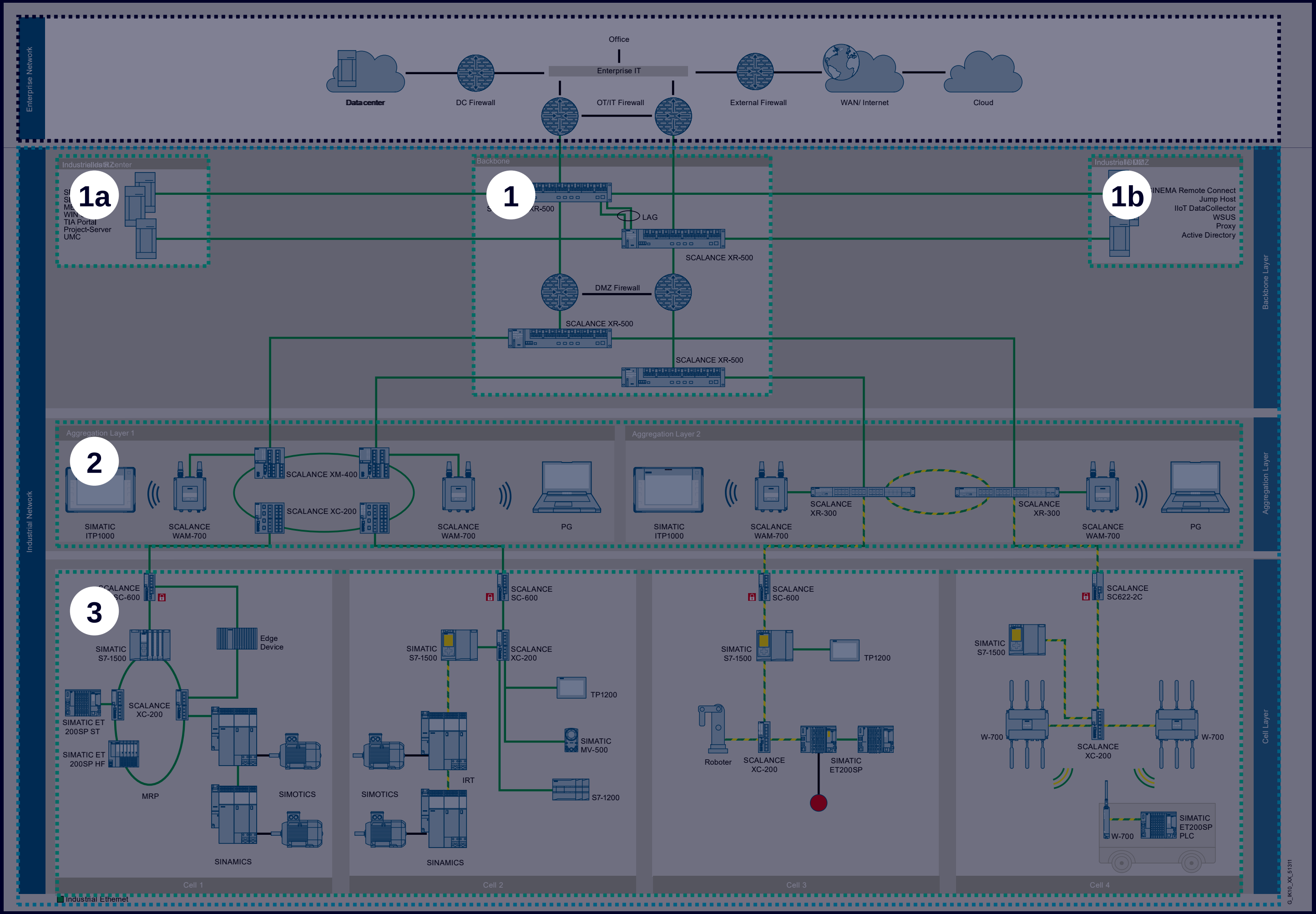


Commonly used by IT



SIEMENS

Overview network concept for Factory Automation
Network zones – Layer 2



Enterprise network – globally connected company solutions and systems

Industrial network – plant network

IT

1. **Backbone** – central plant network connecting IT IDC & IDMZ to the OT network

IT OT

1a Industrial data center (IDC)

1b Industrial Demilitarized Zone (IDMZ)

2. **Aggregation** – cumulating cells and possibility of added functionality

IT OT

3. **Cell network** – one machine or functional group of the production in one cell

OT

SIEMENS

Agenda

1 Overview network concept for Factory Automation

2 Details network zones

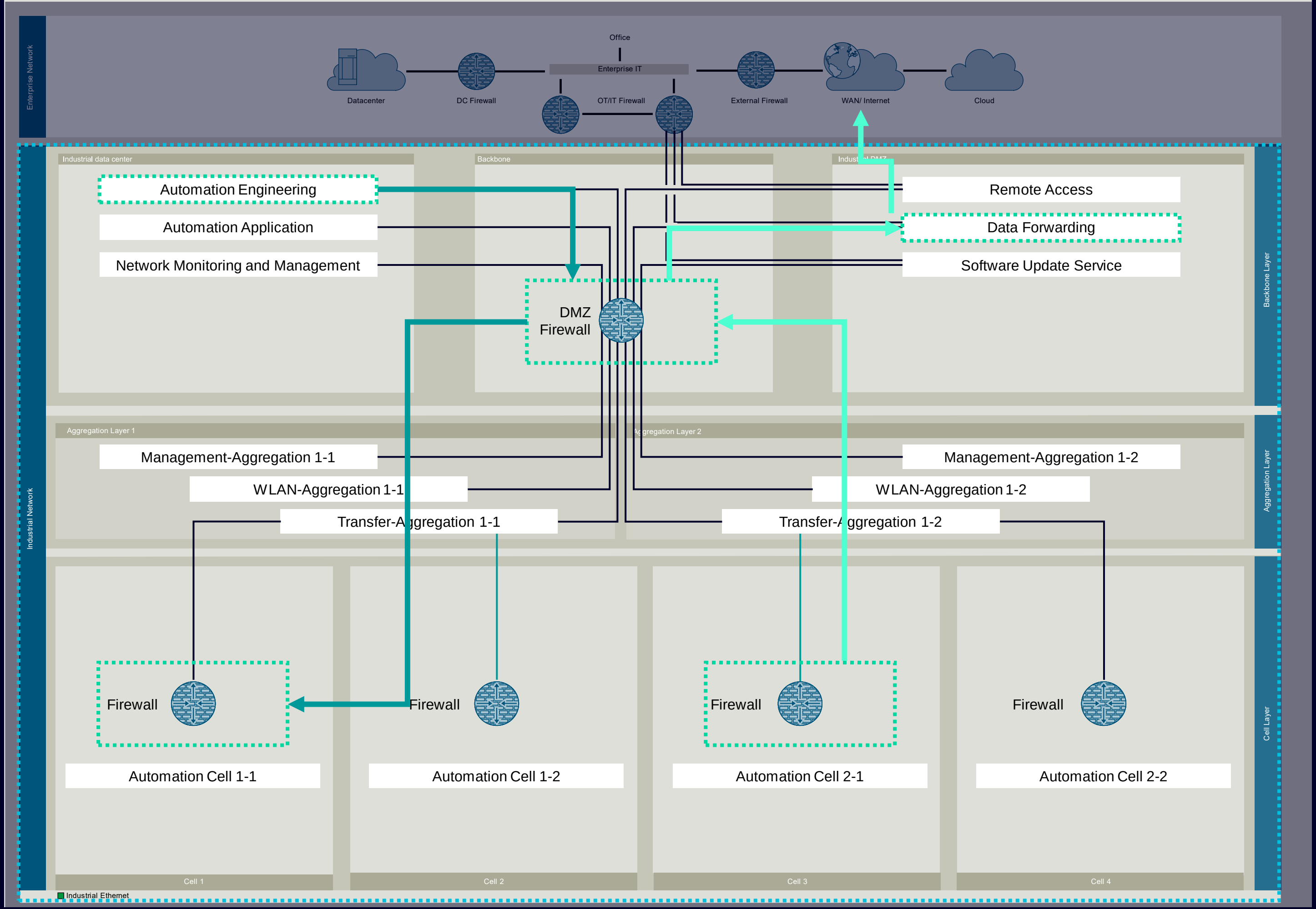
3 Topic – Solution for cells

4 Topic – OT vs. IT networks

5 Topic – Machine to machine communication

6 Topic – Remote access (e.g., service)

Overview network concept for Factory Automation
Network zones – Layer 3 – logical network

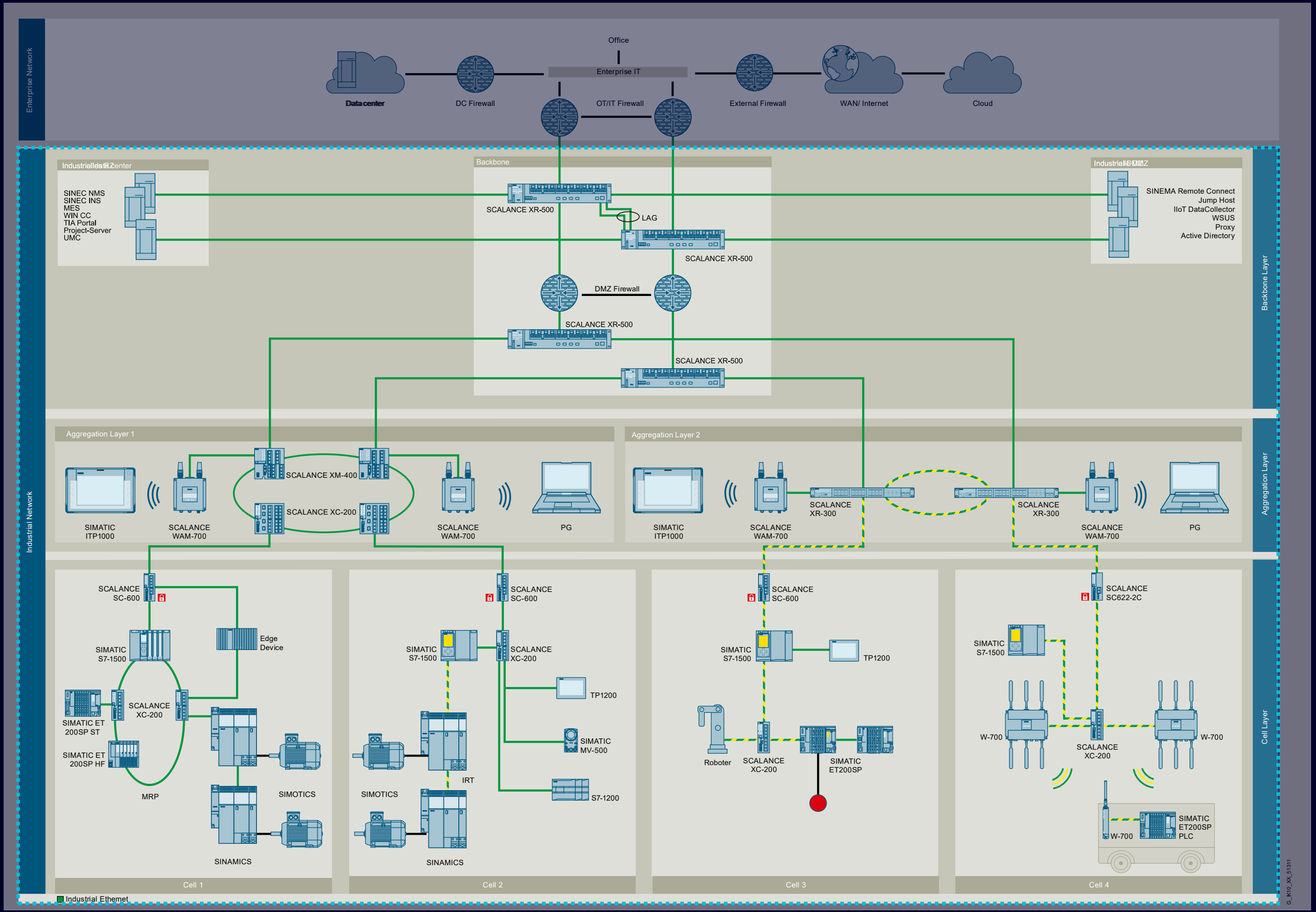


Logical network

- The network is separated in different zones for specific applications based on VLANs
- Each zone is perimeter protected by firewalls which are also responsible for general routing
- Communication between zones is possible across the firewalls and has to be explicitly allowed (e.g., PLC-Download)
- All external communication is required to be transferred across systems located in the IDMZ (e.g., Internet access)

SIEMENS

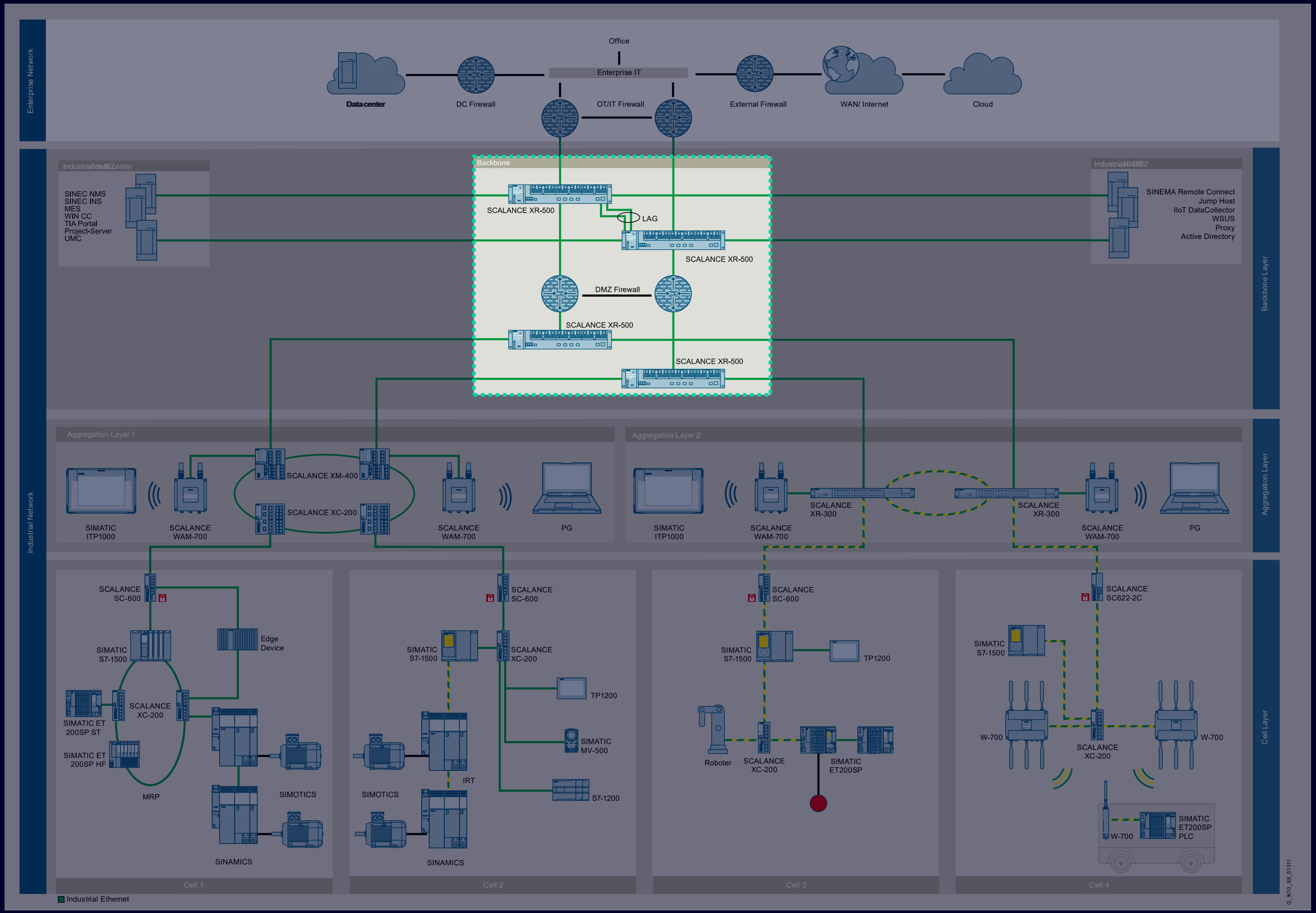
Overview network concept for Factory Automation
Industrial network



Industrial network

- Builds the basis for all production relevant communication needs of the customer
- Is physically separated from the enterprise network to comply with IEC 62443 (SL2) because of security
- Has a defined and controlled handover point to the enterprise network
- Is in responsibility of OT while aligned with IT operations

Overview network concept for Factory Automation
Backbone layer

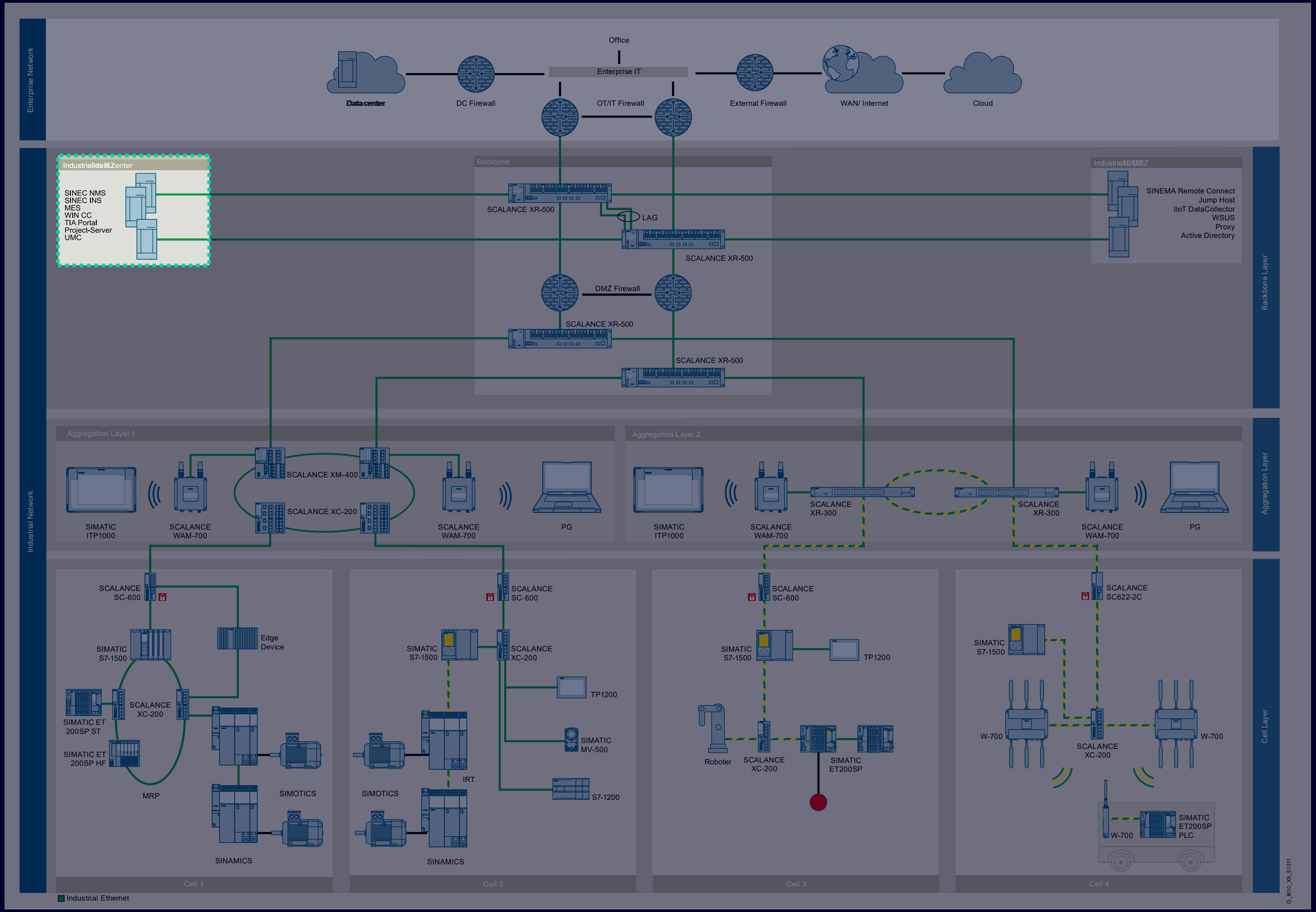


Backbone layer

- Provides connectivity between enterprise network, IDMZ, IDC and aggregation layer
- Is build based on network and firewall devices with high availability features and redundancy protocols
- Network security zones are implemented based on VLANs where the access is controlled by firewall policies

Overview network concept for Factory Automation

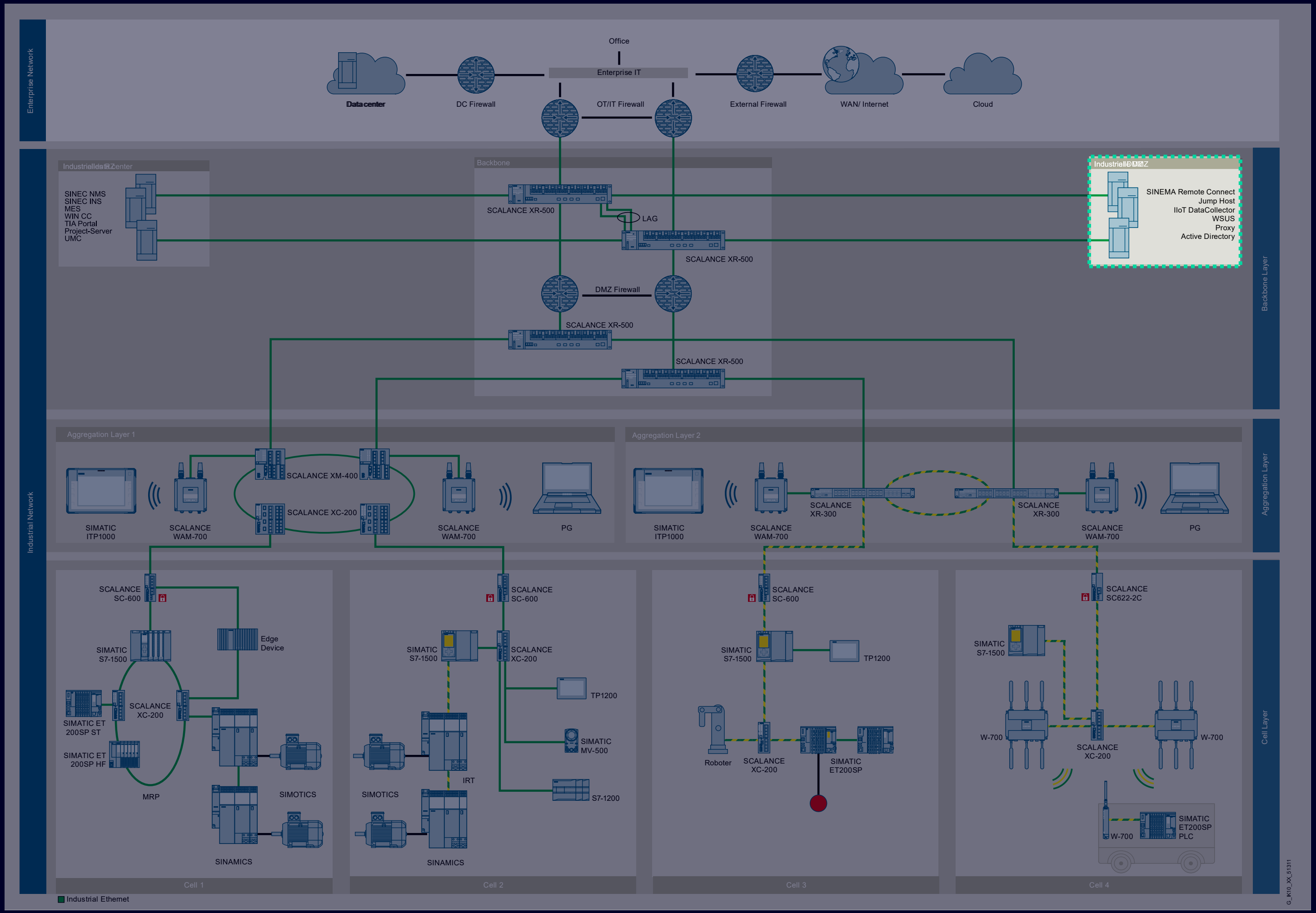
Industrial data center



Industrial data center

- Secured network zones where production relevant applications are located
- Contains Automation tools like TIA portal, WinCC, EDGE Management and the MES system
- Hosts Network Management and Service Tools like SINEC NMS and SINEC INS
- Communication is mainly internal and directed across backbone and aggregation into the cells/machines

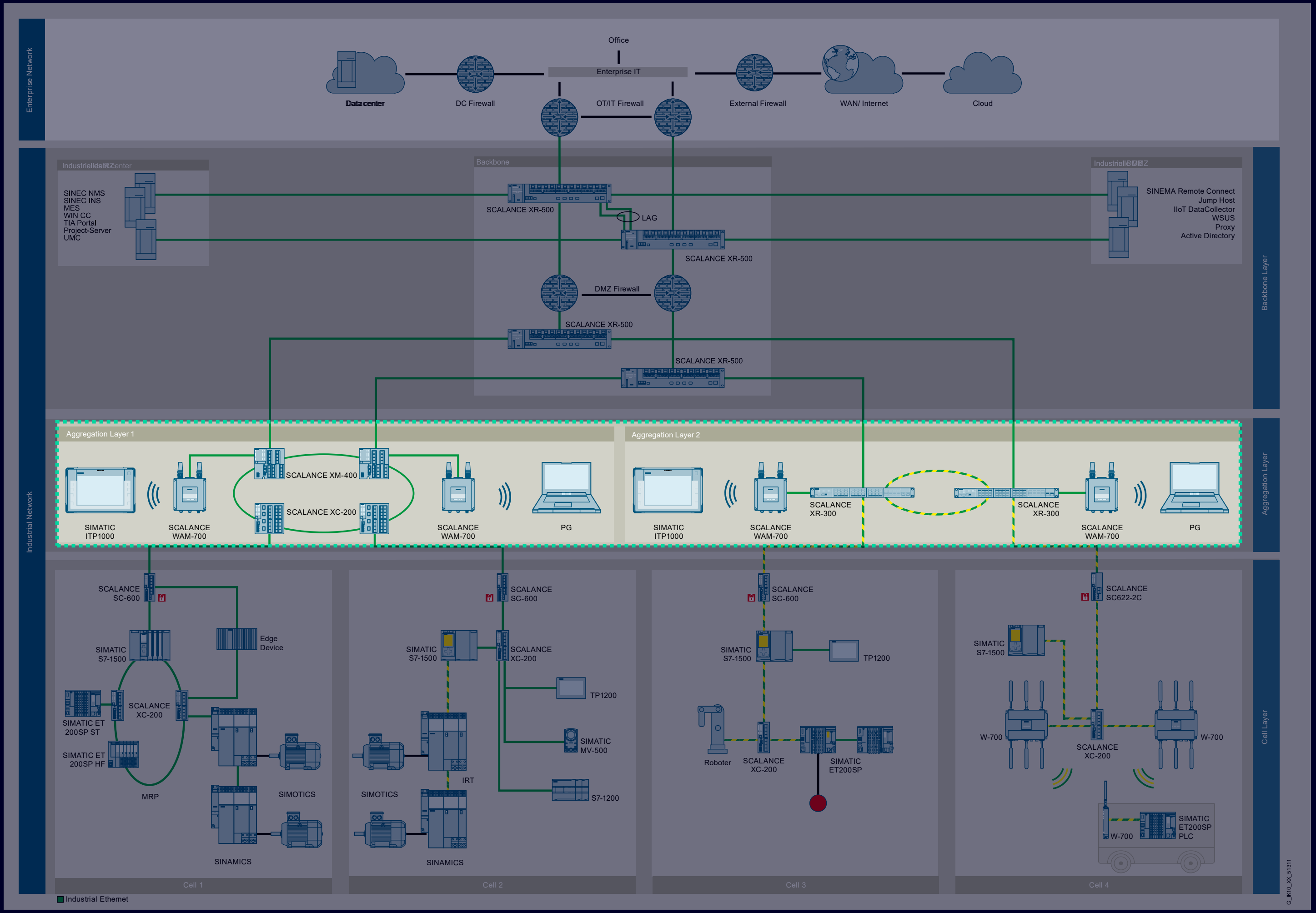
Overview network concept for Factory Automation
Industrial DMZ



Industrial DMZ

- Secured network zones where applications and systems are located for incoming/outgoing communication
- SINEMA Remote Connect for Remote Access with Jump Host for Internal and External users
- WSUS for getting Windows up to date, Proxy for general internet access if required
- Active Directory for authentication and authorization purposes especially but not only with windows

Overview network concept for Factory Automation
Aggregation layer



Aggregation layer

- Provides connectivity between backbone layer and cell layer
- Secured network zones where applications and systems are located for the shopfloor (e.g., Industrial WLAN)
- Depending on the factory size aggregation can be integrated into a single backbone layer

Agenda

1 Overview network concept for Factory Automation

2 Details network zones

3 **Topic – Solution for cells**

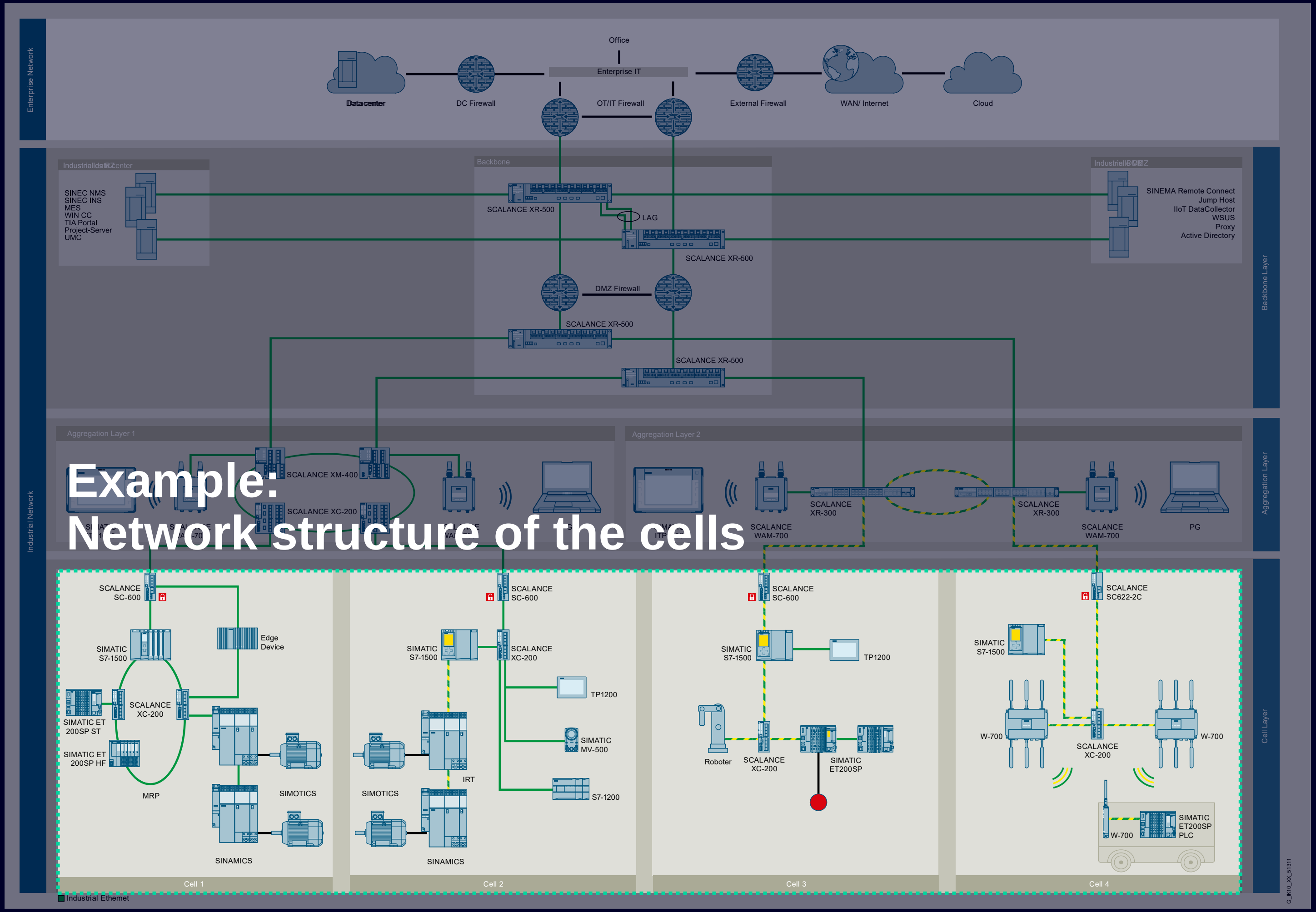
4 Topic – OT vs. IT networks

5 Topic – Machine to machine communication

6 Topic – Remote Access (e.g., Service)

Network structure in the cell level

Overview of example solutions for cell level



Example: Network structure of the cells

Cells – Where the production takes place

Machines or functional groups:

- Realtime communication is necessary: PROFINET RT/IRT
- Safety-based applications are common
- Environmental conditions may be rough

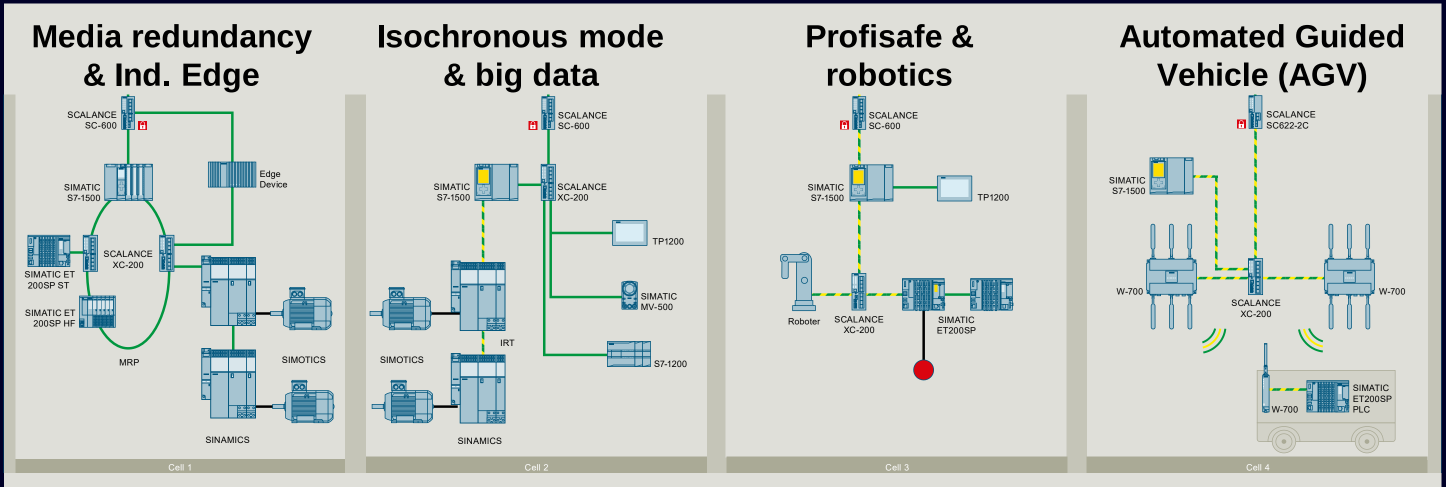
Networks are simple and usually based on star, tree or line topologies, while redundancy can be reached with rings and special protocols

Connections to external networks can be done through PLC or a dedicated network device

Network structure in the cell level
Overview of example solutions for cell level

Example:

Network structure of the cells



Cells –
Where the production takes place

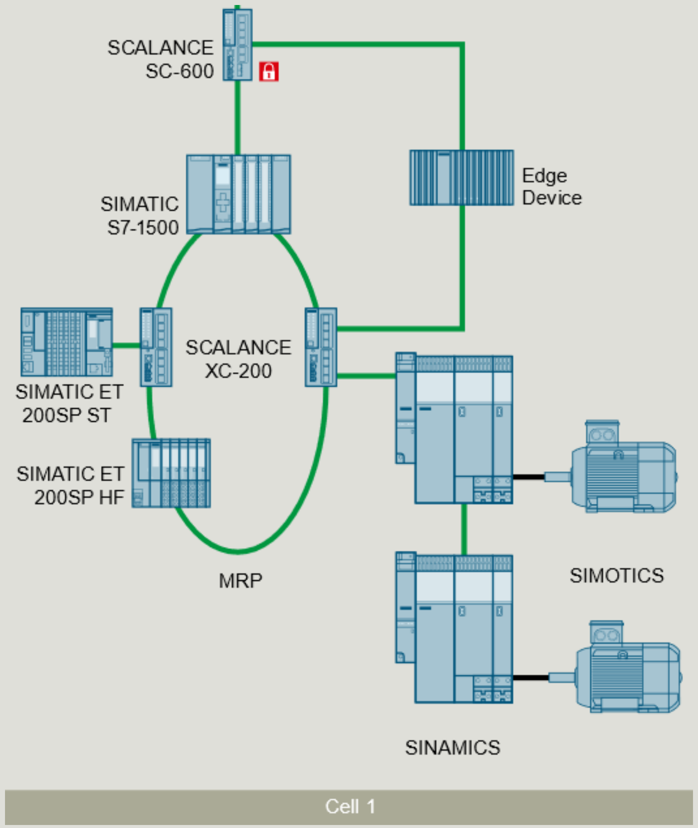
Use case-based cells:
Detailed description for each use case-based cell

- Requirements of the cells on the network
- Explicit proposals for implementation based on “real” models
- Document internal/external links for further information

Network structure in the cell level

Cell 1: Media redundancy & Industrial Edge

Media redundancy & Industrial Edge



Availability

- Media Redundancy Protocol (MRP) via PROFINET
- Ring topology connecting controller and capable switches
- PROFINET stubs connecting non-MRP-capable device

Reachability of cell controller and field devices

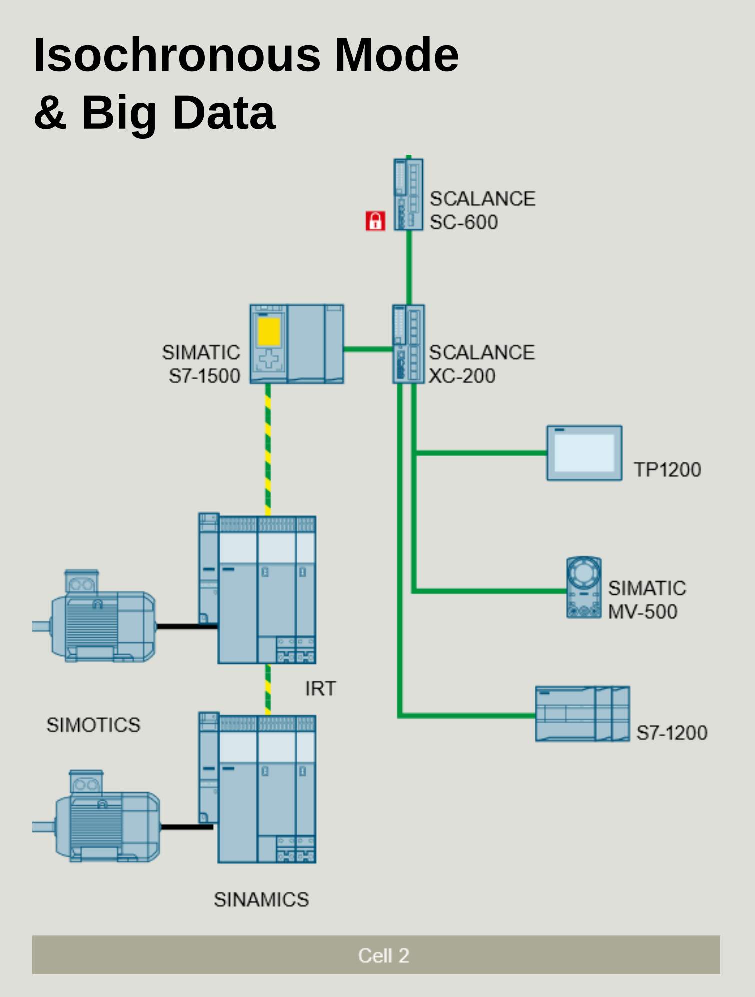
- Industrial Edge Device
- Interface between lower-level machine data and higher-level plant management

Side facts MRP

- Max. 50 devices
- Reconfiguration time less than 200 ms
- Supports PROFINET RT
- PROFINET IRT is possible with MRPD extension

Network structure in the cell level

Cell 2: Isochronous Mode & Big Data



Realtime communication

- PROFINET Isochronous Realtime IO Communication (IRT)
- Use case: motion applications

Big Data

- Gigabit-capable switch
- Reliable handling of high data rates
- Use case: Detailed video streams

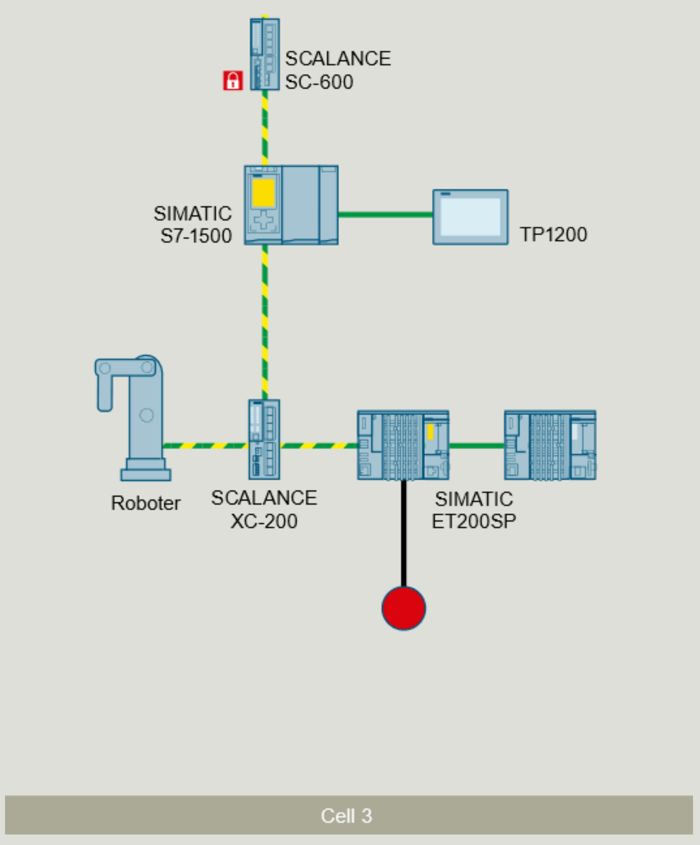
Side facts IRT

- Linear topology
- Devices must be in the same sync domain
- Design process must consider:
  Network bandwidth, send clock, cable length, application cycle
- Separation of Big Data devices from RT network

SIEMENS

Network structure in the cell level
Cell 3: PROFIsafe & Robotics

PROFIsafe & Robotics



Safety

- Correctness & up-to-dateness of data
- Timely delivering of data
- Assurance of the correct receiver
- Crossing cell/subnet boundaries is enabled by flexible F-Link via Open User Communication between CPUs

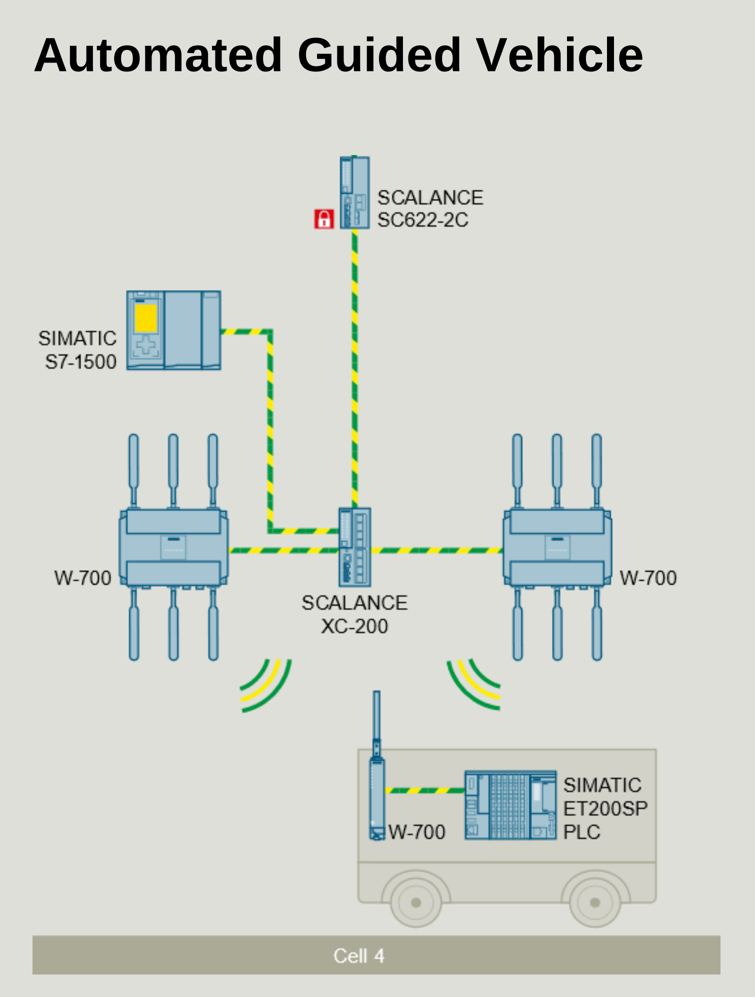
Robotics

- PROFINET requirements need to be met by robot, e.g. I/O-update cycle
- Installation & maintenance is typically done via local interface
  → Should be considered during cell design process

Side facts SAFETY

- Unique PROFIsafe addresses due to layer 2 separation
- Communication between cells over Flexible F-Link

Network structure in the cell level
Cell 4: Automated Guided Vehicle (AGV)



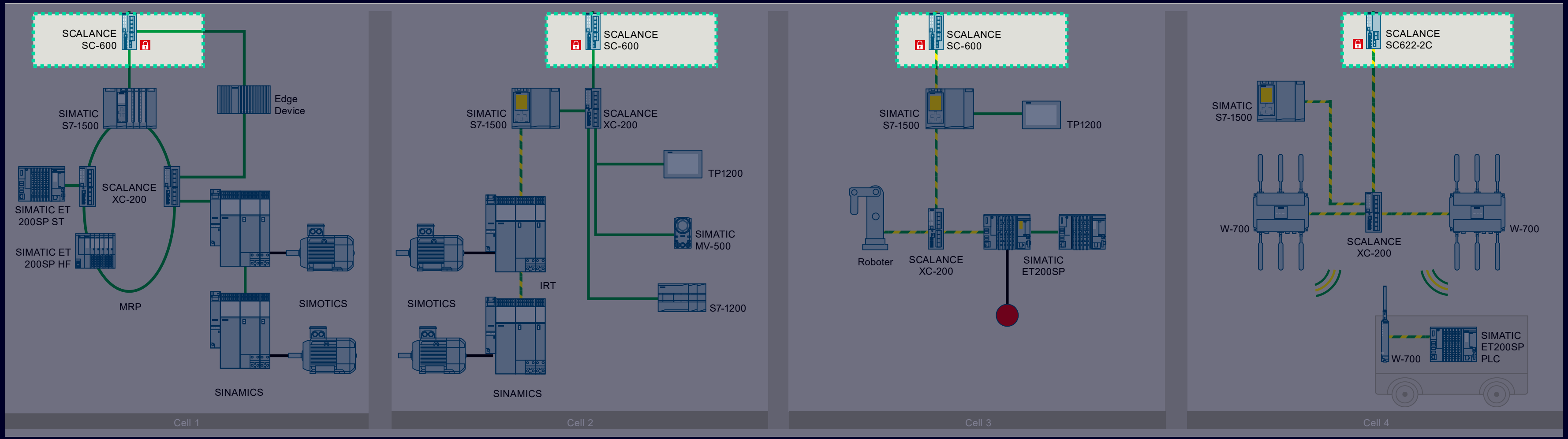
Mobile automation solution

- Industrial Wireless Local Area Network (IWLAN) & PROFIsafe working together
- Automated Guided Vehicle (AGV) with independent onboard safety functions
- Safety-focused communication to central control unit
- Unique addresses of PROFIsafe devices on cell level are crucial for safe functionality

Side facts

- Layer 2 separation via SCALANCE SC622-2C
- SCALANCE SC626-2C with 6 ports for more flexibility
- RT & PROFIsafe also over wireless networks
- Wi-Fi 6 and low power consumption

Network structure in the cell level
Cell access through dedicated firewall



Common cell access point: Firewall

- Only access point to cell level
- Stateful Packet Inspection
- Security arises from layer 3 separation of the cells
- Increased scalability due to independent setup of the cells
- SCALANCE SC622-2C and SC626-2C appliances meets the requirements of the PROFIsafe specification

Contains

- Recommended firewall rules to fulfill requirements of technical topics e.g., “Engineering and configuration with TIA Portal”
- Description of requirements for each example cell layout e.g., PROFIsafe

SIEMENS

Agenda

1 Overview network concept for Factory Automation

2 Details network zones

3 Topic – Solution for cells

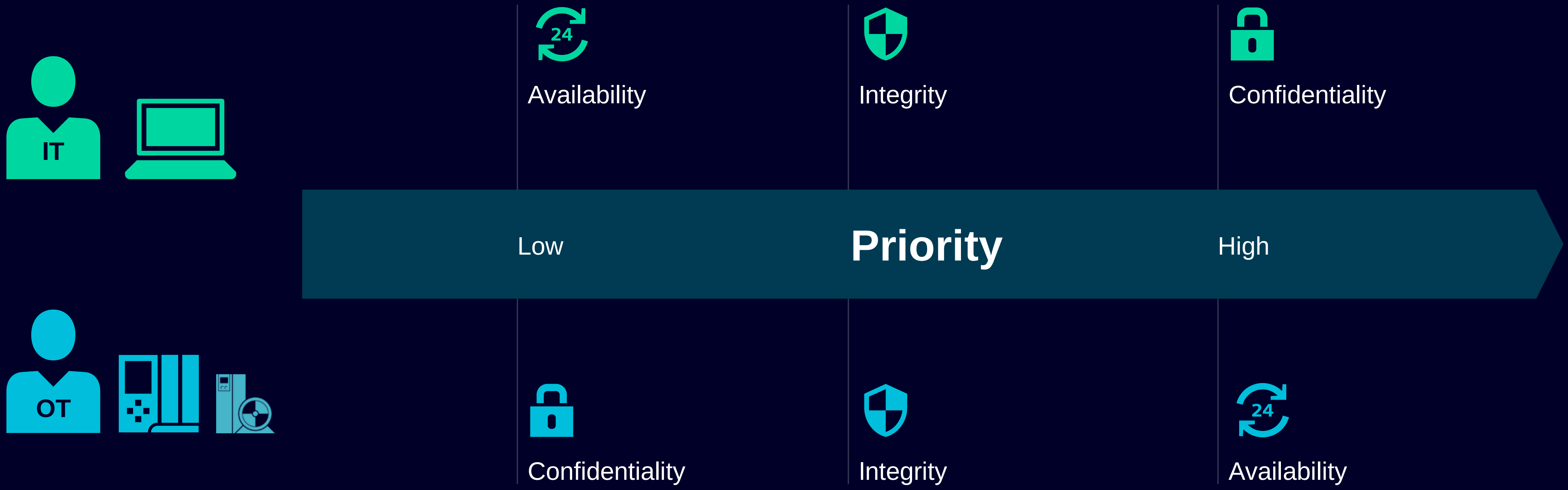
4 Topic – OT vs. IT networks

5 Topic – Machine to machine communication

6 Topic – Remote access (e.g., service)

Network security

Different focus in OT and IT



	Low	Priority	High
IT	Availability	Integrity	Confidentiality
OT	Confidentiality	Integrity	Availability

IEC 62443 is one of the leading standards for network and system security in industry!

Security risks potentially arise due to internet connectivity

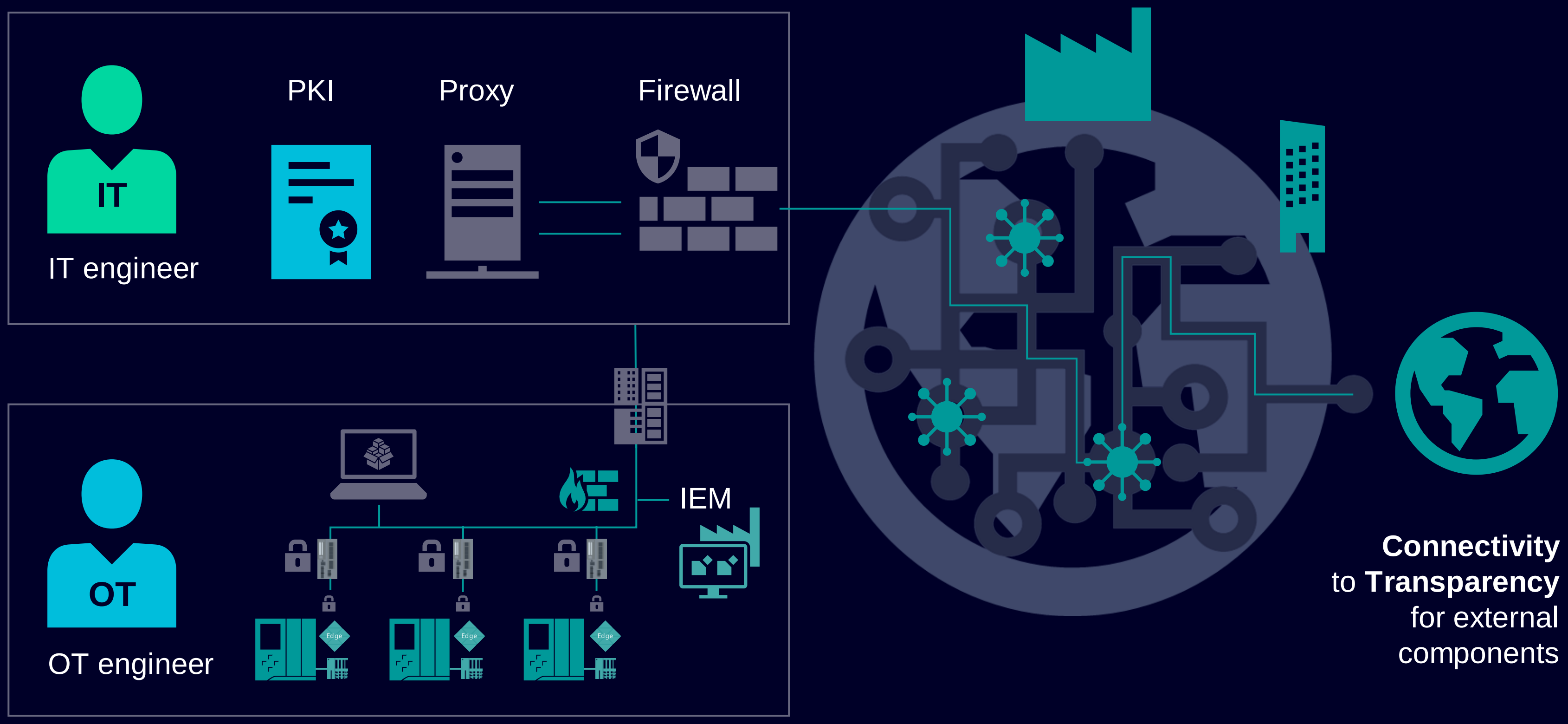
Daily business!

Lots of measures to avoid security threads.
→ “Just” need to extend this to shop floor

“Just” need to extend?

Never heard about:

- Firewalls
- PKI
- Proxy servers



Connectivity to **Transparency** for external components

Challenge – Comply with standards used in IT infrastructure

Agenda

1 Overview network concept for Factory Automation

2 Details network zones

3 Topic – Solution for cells

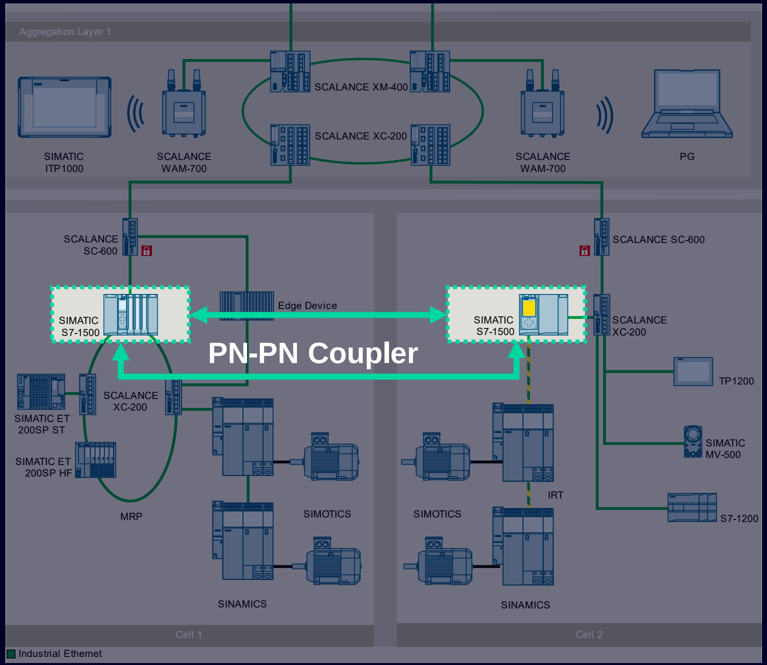
4 Topic – OT vs. IT networks

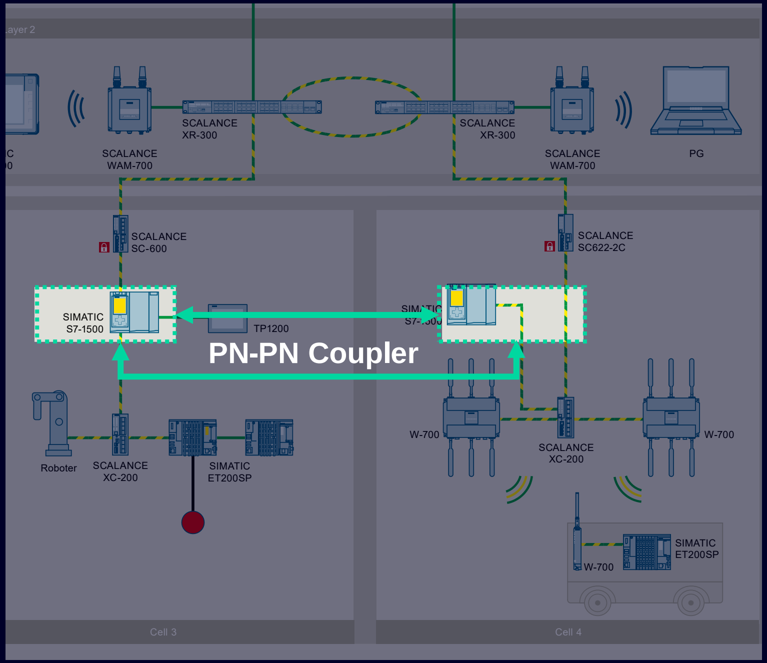
5 Topic – Machine to machine communication

6 Topic – Remote access (e.g., service)

How can the **communication between machines** to be set up in **regards of the different requirements**?

Topic – machine to machine (M2M) **communication**
How do cells communicate to each other?





Requirements on M2M communication in consideration shown use cases

General
- Routing capability
- Security mechanisms
- Realtime capability

Advanced
- Openness
- Standardization
- Safety

Multiple communication methods are described through their use cases

Description of requirements for each protocol in regards of firewall rules and security conditions

Detailed description for the three recommended ways of M2M communication

Topic – machine to machine (M2M) communication

Recommended machine to machine communication types

OPC UA Server/Client

Routing capable, secure, open, standardized

Preferred solution for standardized communication

Interface modelling is possible also according to companion specifications

Consistent data transfer via Methods

PROFINET PN/PN coupler

Realtime capable, standardized, safety capable

Designed to meet hard realtime requirements

Can be implemented as follow up measure

Dedicated device for data transfer

Flexible F-Link

Routing capable, secure, safety-focused

Specially Designed for SAFETY requirements even over routers

Protocol can be chosen depending on the application’s needs (OUC)

No additional hardware is required for SAFETY M2M communication

TCP

UDP

S7

Agenda

1 Overview network concept for Factory Automation

2 Details network zones

3 Topic – Solution for cells

4 Topic – OT vs. IT networks

5 Topic – Machine to machine communication

6 Topic – Remote access (e.g., service)

How can I **guarantee availability** and **fast service** with such a segmented network set up?

On-site service
Time consuming and expensive

Machine builder

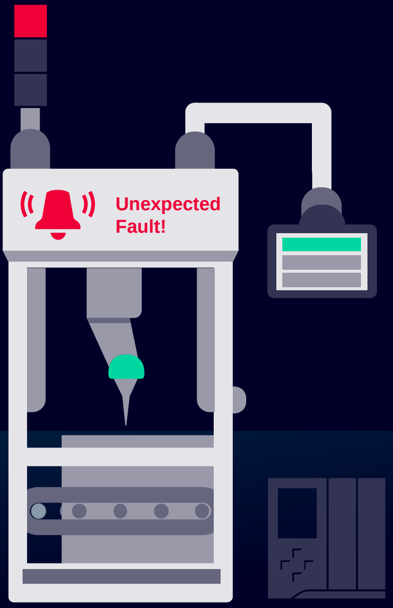
What kind of trouble?

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

**We are having
trouble with
a machine**

Unexpected Fault

End customer

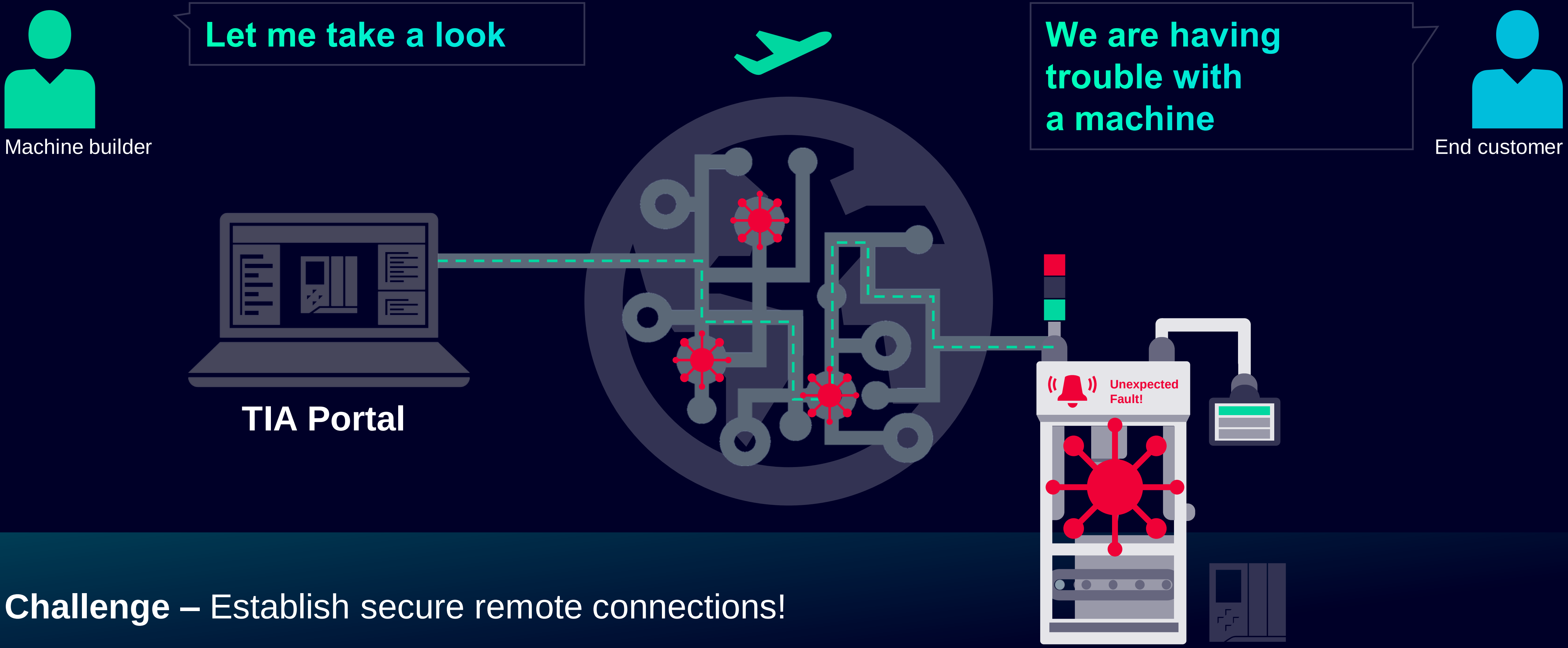


**Rescheduling
necessary**

Downtime

On-site service is time consuming

Possible solution
Use internet connection to reach the machine



Challenge – Establish secure remote connections!

Remote connectivity
Risks and requirements

Risks

- Easy discovery of OT equipment e.g., by tools like “Shodan.io”
- Unauthorized access
- Eavesdropping and man-in-the-middle attacks
- Denial-of-service attacks

Remote access requirements

- High protection necessary with “state-of-the-art” security
- Limit and manage access with efficient user management
- Optimize usability e.g., by seamless integration in SIMATIC portfolio
- Fast and easy configuration without IT Know-how

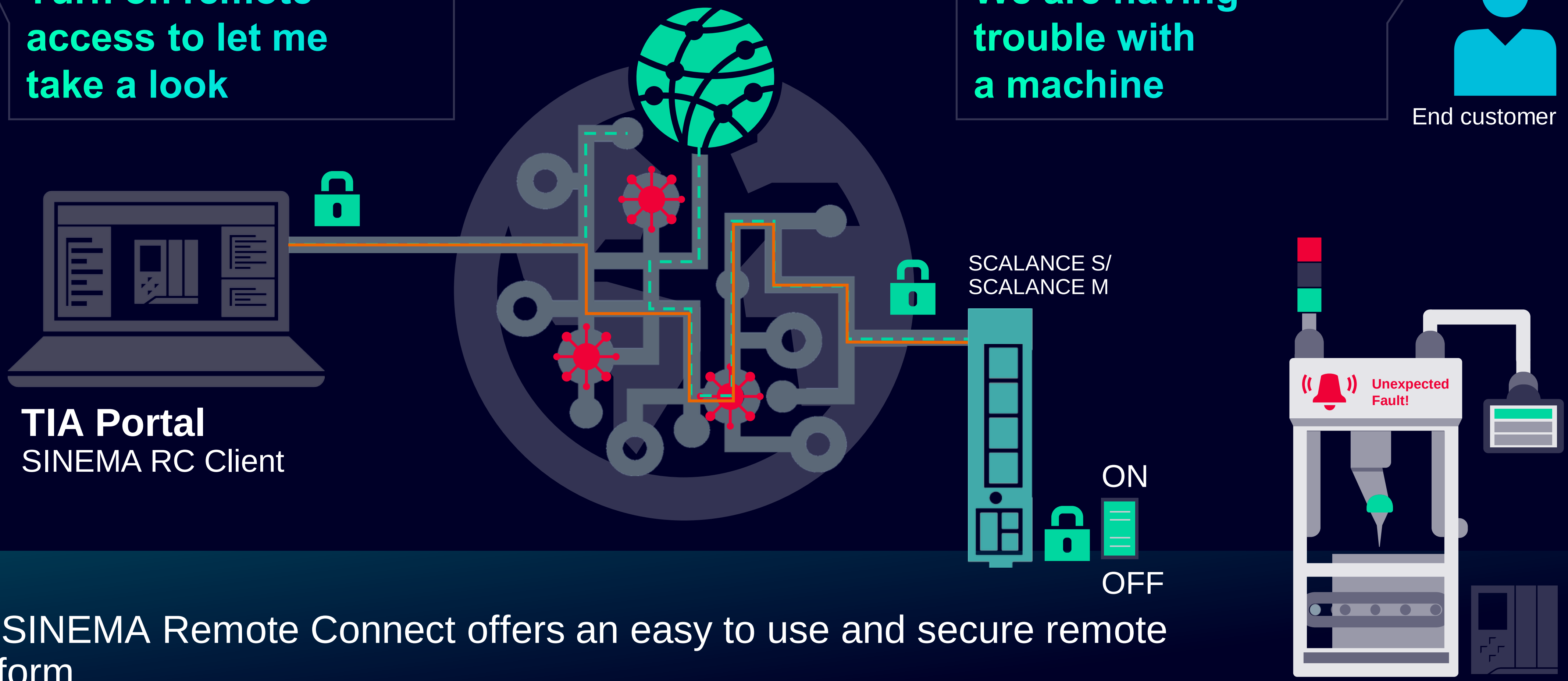
Remote service with SINEMA Remote Connect

Machine builder

Turn on remote access to let me take a look

We are having trouble with a machine

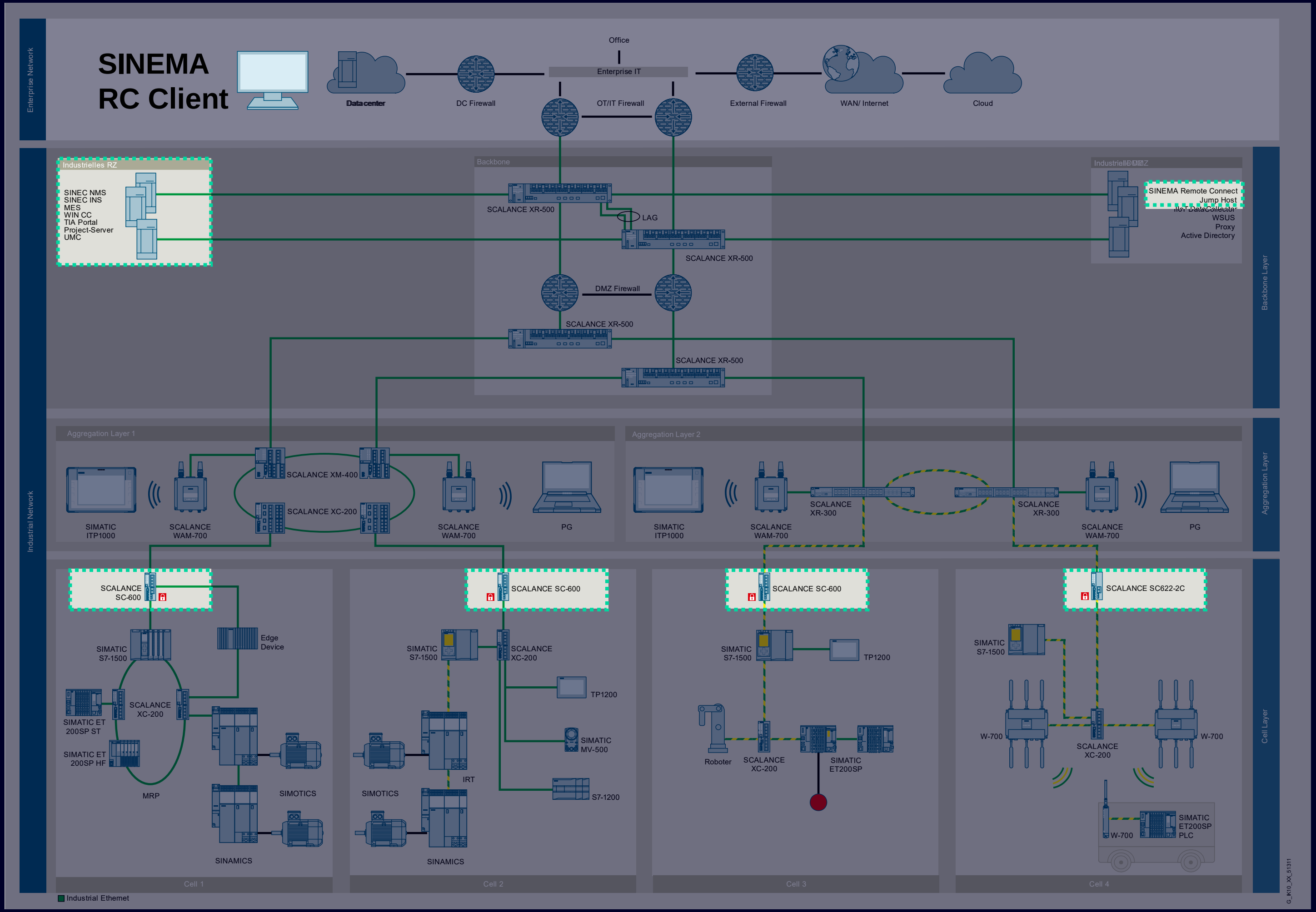
End customer



Solution – SINEMA Remote Connect offers an easy to use and secure remote access platform

Use Case: Remote access

Overview of components inside the network concept



Enterprise network

SINEMA RC Client/Remote Desktop Protocol (RDP)

Industrial network – plant network

IDMZ

- SINEMA Remote Connect Server
- Jump Host (internal & external)

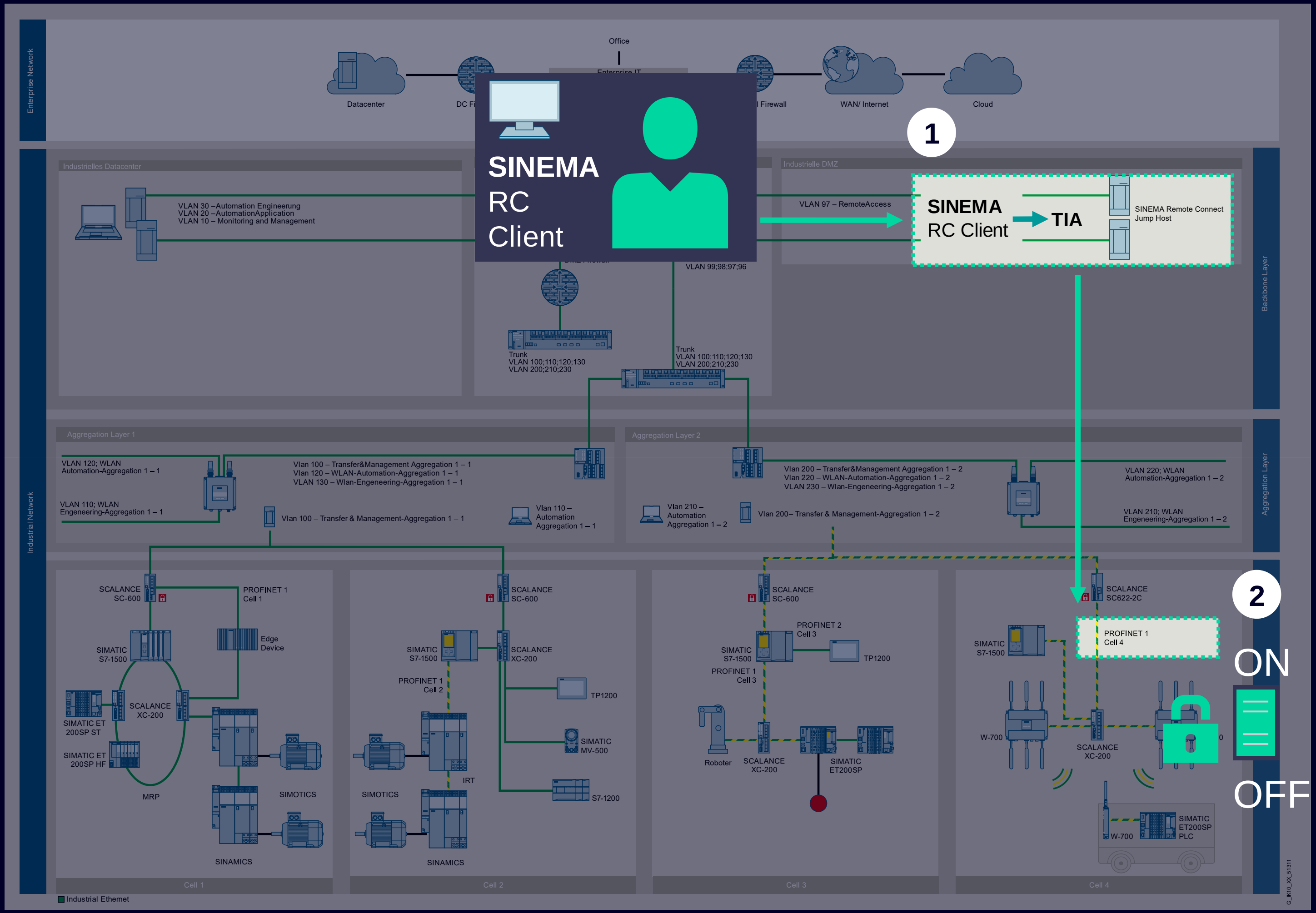
IDC

Automation & Network management Tools (e.g., TIA Portal, SINEC NMS)

Cell network

SCALANCE SC-600/S615

Use Case: Remote access
External access



- Machine manufacturer (via jump host external) External supplier connects via internet

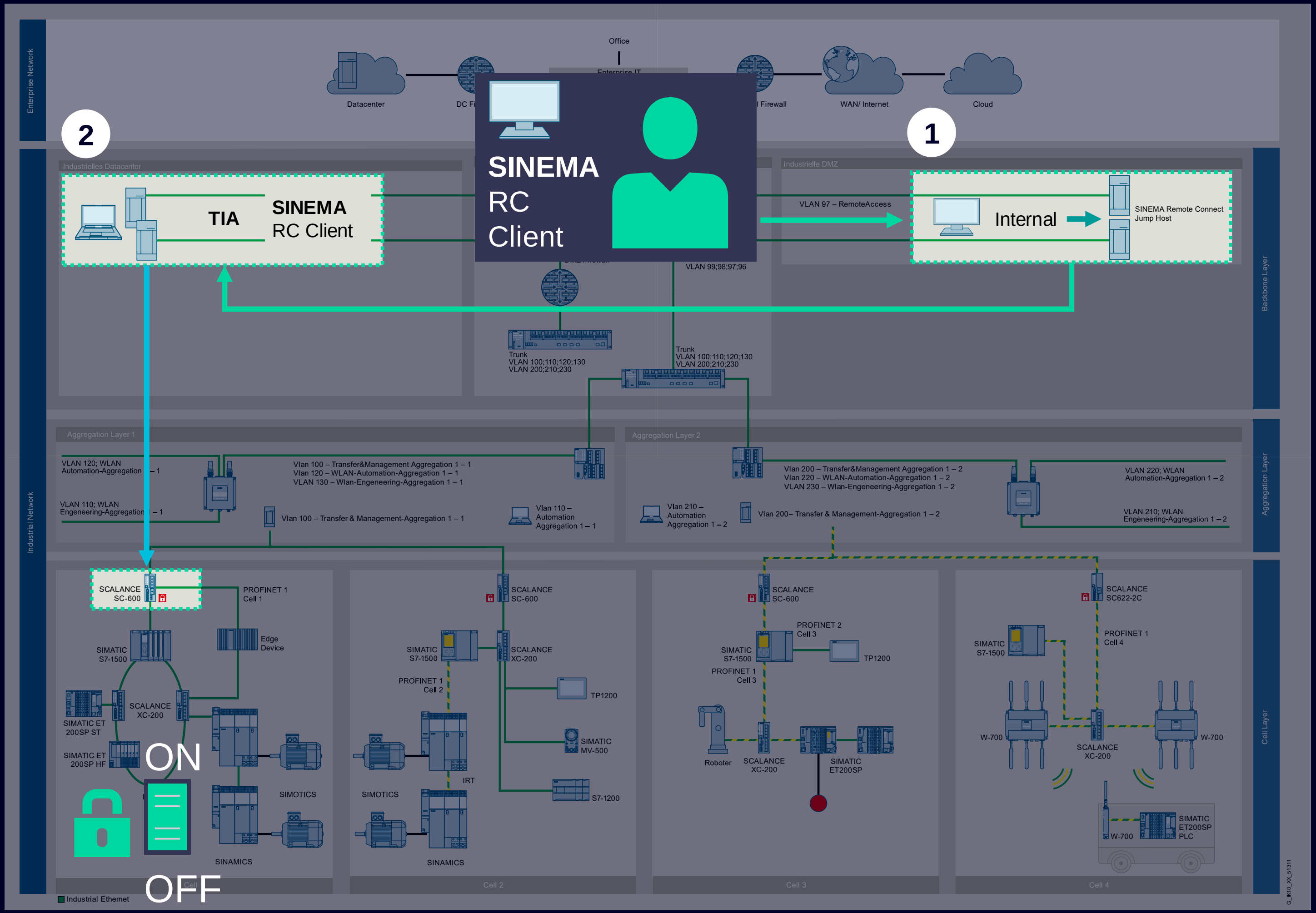
1 Connect via SINEMA RC Client to SINEMA Remote Connect Server in IDMZ, that takes care of data forwarding together with a Jump Host

2 Cell firewall enables connection via SINEMA Remote Connect Server via key-operated switch

- All required tasks can be fulfilled via applications installed on the PC/PG of the machine manufacturer

SIEMENS

Use Case: Remote access
Internal access



- Service Technician (via jump host internal) Internal employee via Internet/Enterprise network

1. Connect via SINEMA RC Client to SINEMA Remote Connect Server in IDMZ, that takes care of Data Forwarding together with a Jump Host

2. Connect to required virtual machine (VM) in the IDC

- Simple tasks (e.g., PLC-download, Webserver) without additional measures regarding security. All needed applications are hosted in IDC
- Security critical tasks have to be enabled by cell firewall SCALANCE SC-600 via key-operated switch (e.g., unauthorized access with SNMPv1)

Contact

Published by Siemens XX

First name Last name
Job title
Group/Region/Department XY
Street 123
12345 City
Country

Phone +49 123 45 67 89
Mobile +49 123 45 67 89 0

E-mail firstname.lastname@siemens.com

Disclaimer

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations may be trademarks or other rights of Siemens AG, its affiliated companies or other companies whose use by third parties for their own purposes could violate the rights of the respective owner.

Security information

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept. For more information about industrial security, please visit https://www.siemens.com/industrialsecurity.