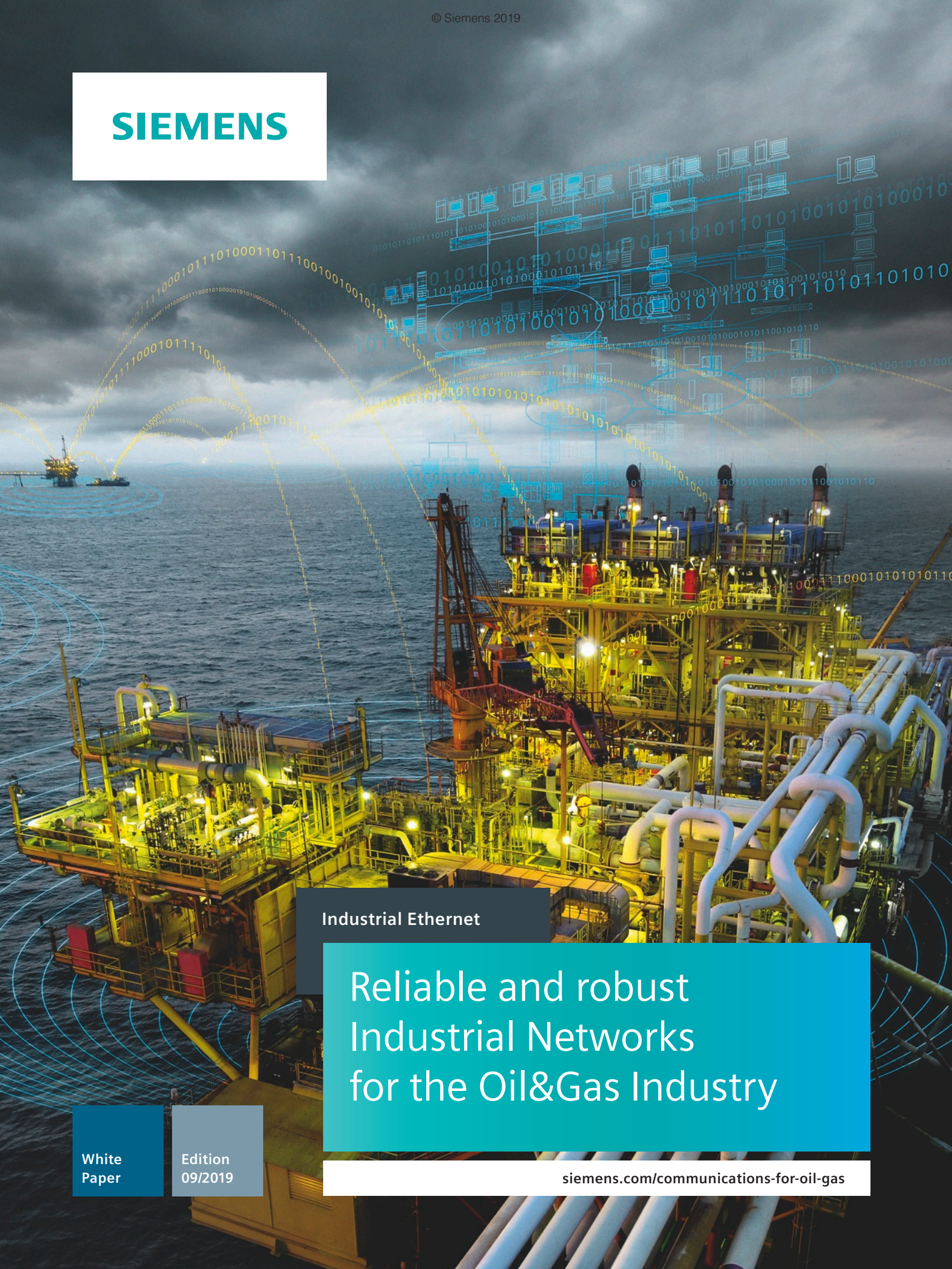
SIEMENS



Industrial Ethernet

Reliable and robust Industrial Networks for the Oil&Gas Industry

White Paper

Edition 09/2019

siemens.com/communications-for-oil-gas

Content

Reliable and robust Industrial Networks for the Oil&Gas Industry

Basics and requirements for networks in the Oil & Gas industry

There is now a wealth of information, trade fairs, conferences and training courses on the subject of communications and networking for Oil and Gas. This white paper will specifically address the necessary basics and requirements of network technology, whether the network is located on an offshore oil platform, drilling rig in a barren desert, at a depth of 3,000 m on the seabed, or on a gas tanker. The wide-ranging environments and applications result in a wide variety of requirements for the products used. These include, for example:

- Redundant communication
- Shipbuilding certifications
- Long product life cycle
- Long mean time between failures (MTBF)
- Sealing of the electronic circuit boards (conformal coating)
- Wide operating temperature range
- Explosion protection up to hazardous zone 1+2

In addition to the technical basics, the examples (see page 5 et seq.) also provides user with detailed guidance for use in the respective application areas.

Safety first

The safety and security of the business activities and the various technologies used is a priority for all users in the O&G industry. There are no visits to facilities without safety training and appropriate protective equipment.

This principle should also be considered when setting up communication networks. Does the supplier have the right products with the appropriate certifications? Have they introduced a complete quality standard in production? Are the products produced according to current cybersecurity standards and is there also an incident management system in place? Are there appropriate training and certification programs available to train employees on the products used in deployment? Is the supplier a long-standing and trustworthy partner?

If so, the operator of the plant should seek advice from these specialists.

Ethernet networks for communication in the Oil & Gas industry

In classic O&G systems, there are a multitude of requirements on the networks for industrial communication. This starts with simple line/star structures and ends with rings and redundant network structures. A diverse combination of communication mediums (copper cable, glass fiber, wireless) are used these solutions. PLCs, DDCs, PACs, cameras, flow meters, gas analyzers, intrusion detection systems, SCADA systems and many more are the start or end points of communication. All these devices require networks customized for its specific application to ensure fast and secure data communication.

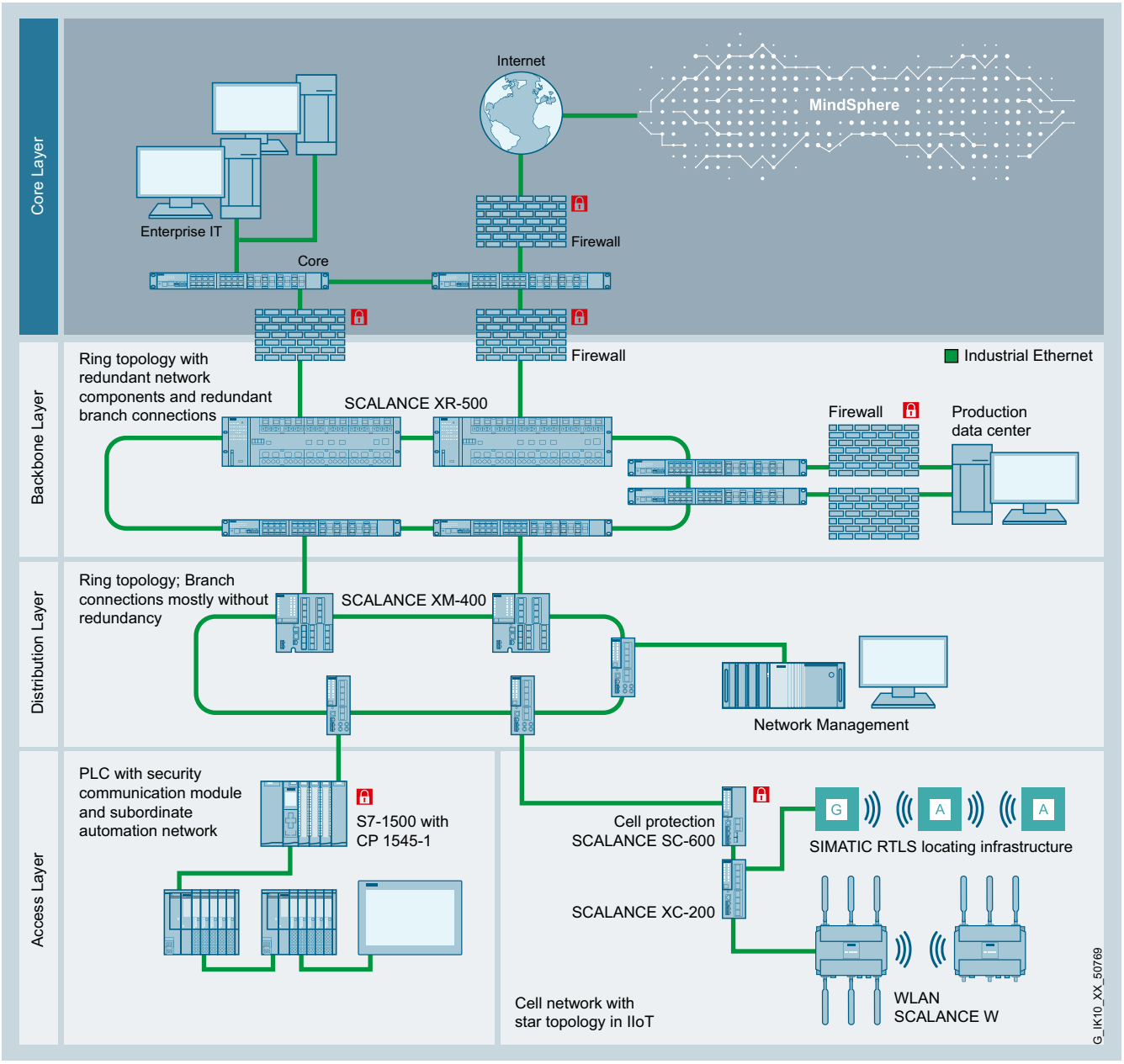
Since there is no “standard network” for these different applications, this paper will use the following network concept as a reference.

Here is a brief explanation:

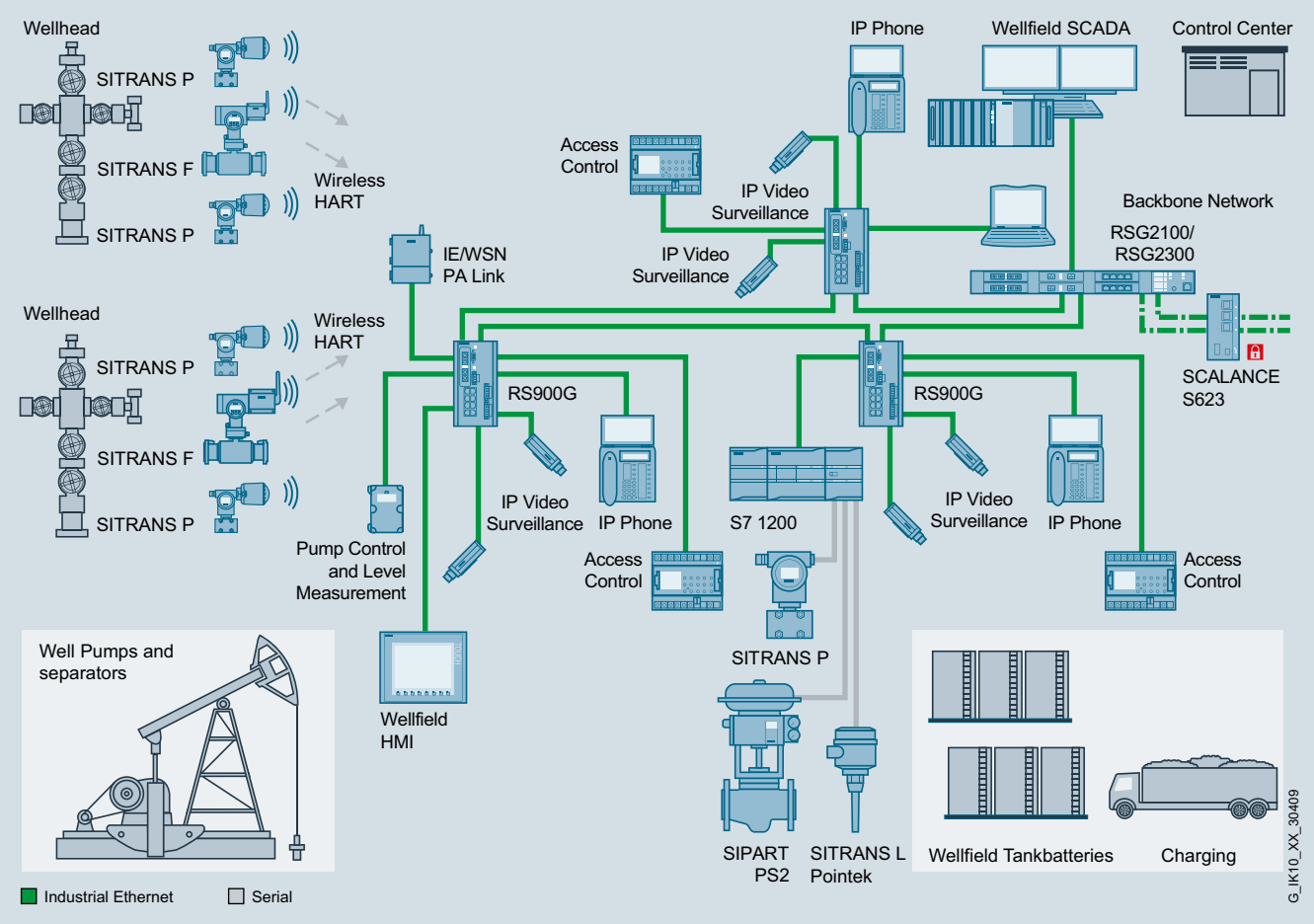
- The core layer establishes the connection to the customer’s IT and other systems. The transitions to the production networks must be secured with a firewall.
- The redundant backbone layer connects the subordinate distribution layers with a production data center or SCADA systems.
- In the distribution layer, the individual islands of automation are connected by a single connection or redundantly in the case of fault-tolerant automation devices.
- The access layer establishes the connection to the automation systems, the distributed I/O devices and the mobile terminals in the system. High precision locating technology (such as SIMATIC RTLS) can be used to protect employees in oil or gas fields.

The most common applications in the Oil & Gas sector are presented and explained in the following examples (see page 5 et seq.).

Reliable and robust Industrial Networks for the Oil&Gas Industry



Network concept for Oil & Gas



DDC/PLC/PAC/cameras/sensors on a SCADA system

Example with DCS/PLC/PAC on a SCADA system

Depending on environmental conditions and customer requirements, the right and most cost-effective combination for communication can be selected from the Siemens portfolio. The DDC/PLC/PAC are usually connected to the network via a copper or fiber-optic cable with Fast Ethernet (10/100 Mit/s). The field devices on a DDC/PLC/PAC can be conventionally connected to the I/O modules via serial connections or integrated via Ethernet (such as Modbus TCP protocol). For IP telephony or video surveillance, it is important to consider the available bandwidth on the local system bus. Here you should use the Gigabit Ethernet ports provided by the devices shown. The connection to higher-level backbone networks is usually designed in ring topology so that a single fault in the network does not shut down the entire system. After detecting the error, the Ring Manager can switch to an alternative communication path within a few milliseconds.

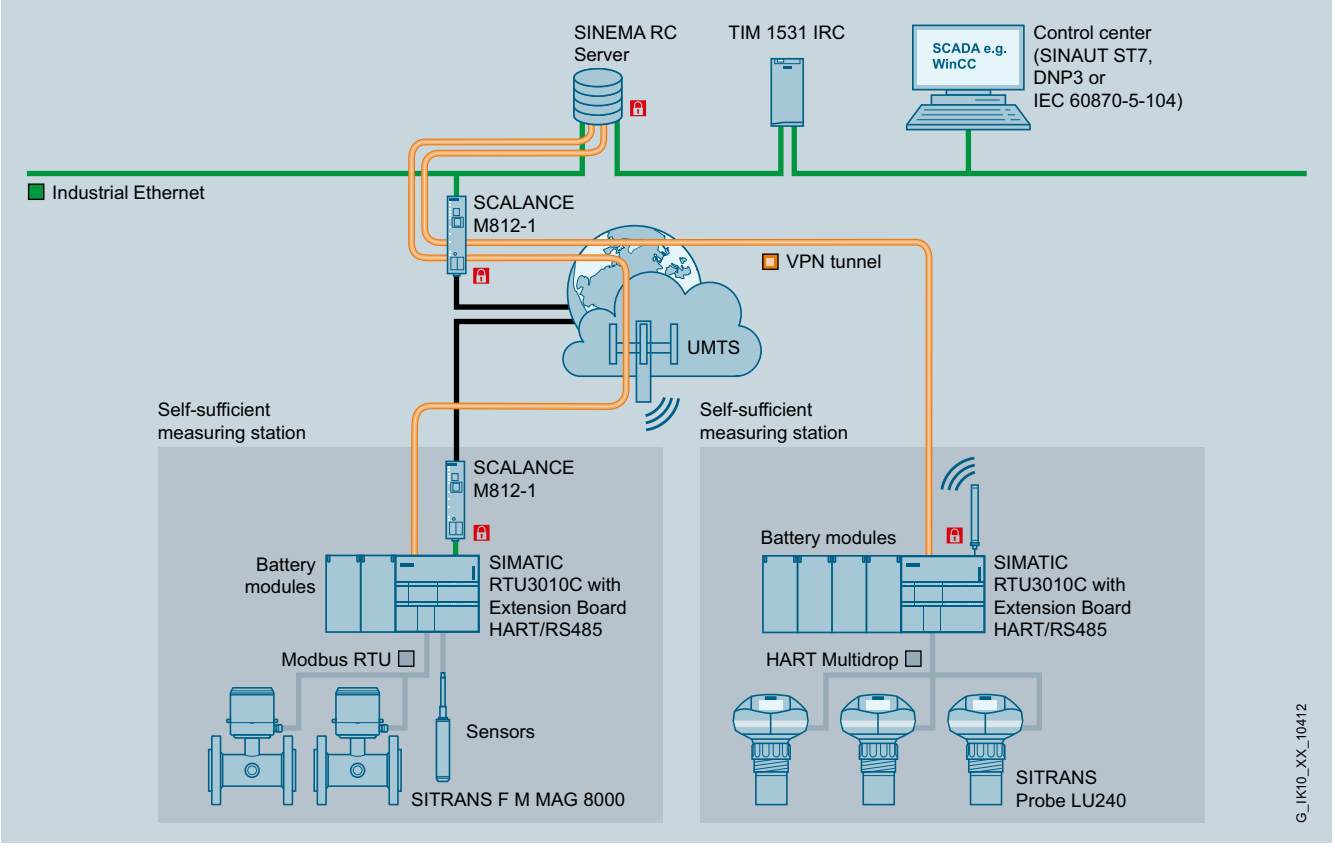
Remote maintenance or remote access to such systems should always take place via secured paths and specially developed security components. SCALANCE S or SCALANCE M offer a multitude of possibilities and, with SINEMA Remote Connect, access to different systems can be managed easily and, above all, securely.

RTU with low power consumption (battery operation)

For an RTU, other networks topologies are required than those used for PLCs/DDCs. The RTU, which is to be operated with one battery for years, must use an extremely efficient and energy-saving method, otherwise the battery will require frequent maintenance, which could lead to high costs in the O&G industry.

2G/3G or 4G radio technology is usually used for this purpose. However, this also depends on the availability existing communication infrastructure in the field.

Reliable and robust Industrial Networks for the Oil&Gas Industry



Configuration: RTU 3010C with battery supply

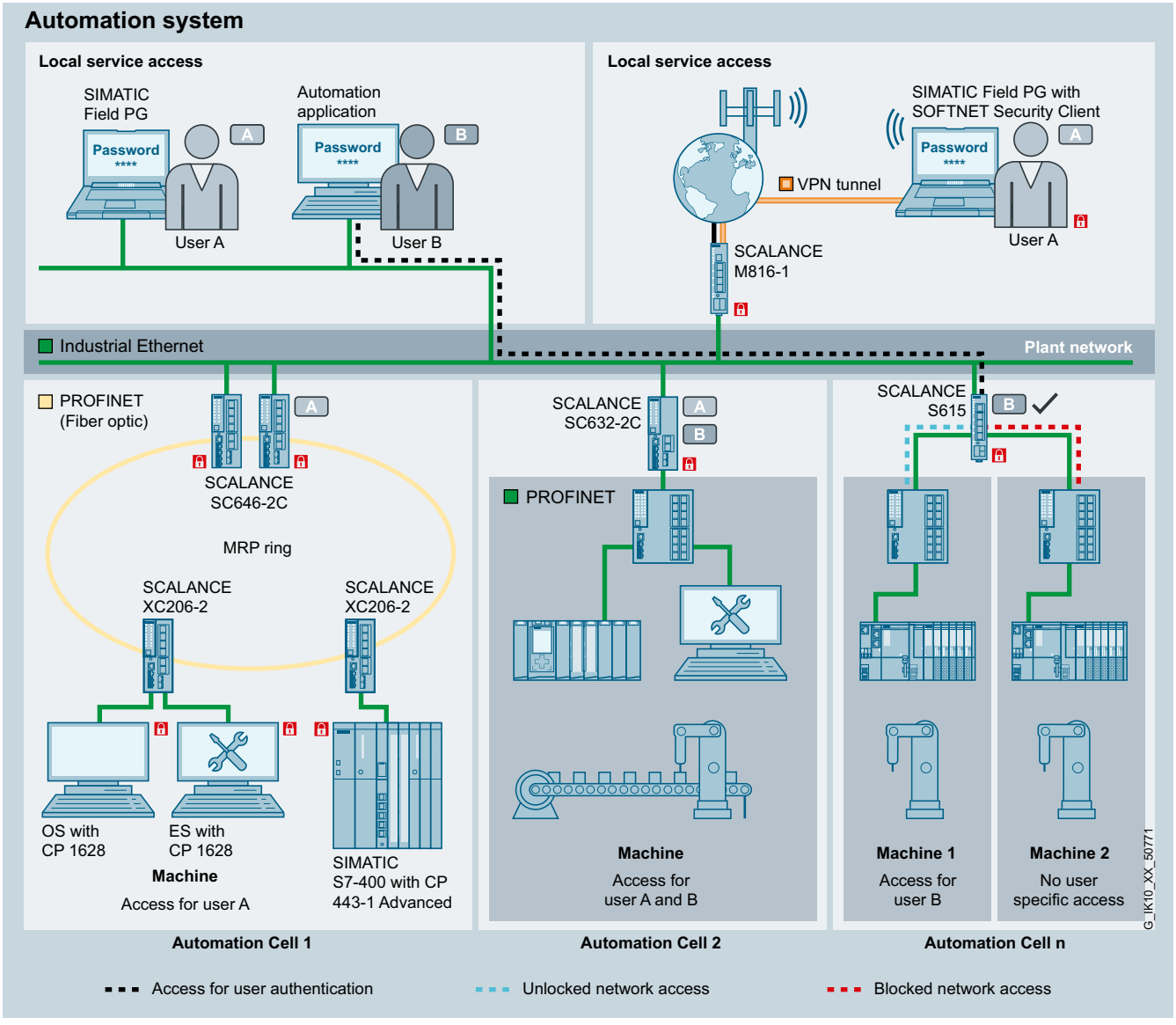
The configuration shows a SIMATIC RTU 3030C from Siemens with battery modules, which can operate connected sensors directly via the RTU battery. Various telecontrol protocols such as IEC 60870-5-104, DNP3, Telecontrol Basic and SINAUT ST7 can be supported on the radio interface. Devices with Modbus RTU and HART (wired) can also be addressed via a pluggable additional module. When communication is interrupted, all RTU data is stored locally with a time stamp and can also be transmitted securely via a VPN tunnel. Power can be supplied via battery modules or solar panels. The permissible ambient conditions are within the usual O&G temperature range of -40°C to +70°C.

Industrial Security

Digitalization increasingly interconnects industrial facilities. On the one hand this enables numerous new insights based on analyzed data. On the other hand, this leads to a higher risk of cyber-attacks, which requires an effective protection concept that consists of multiple layers and protects industrial facilities against any threats. To provide an industrial plant with comprehensive industrial security protection against such attacks, appropriate measures must be taken. It is essential in such cases to protect production against sabotage or espionage without having a negative impact on availability.

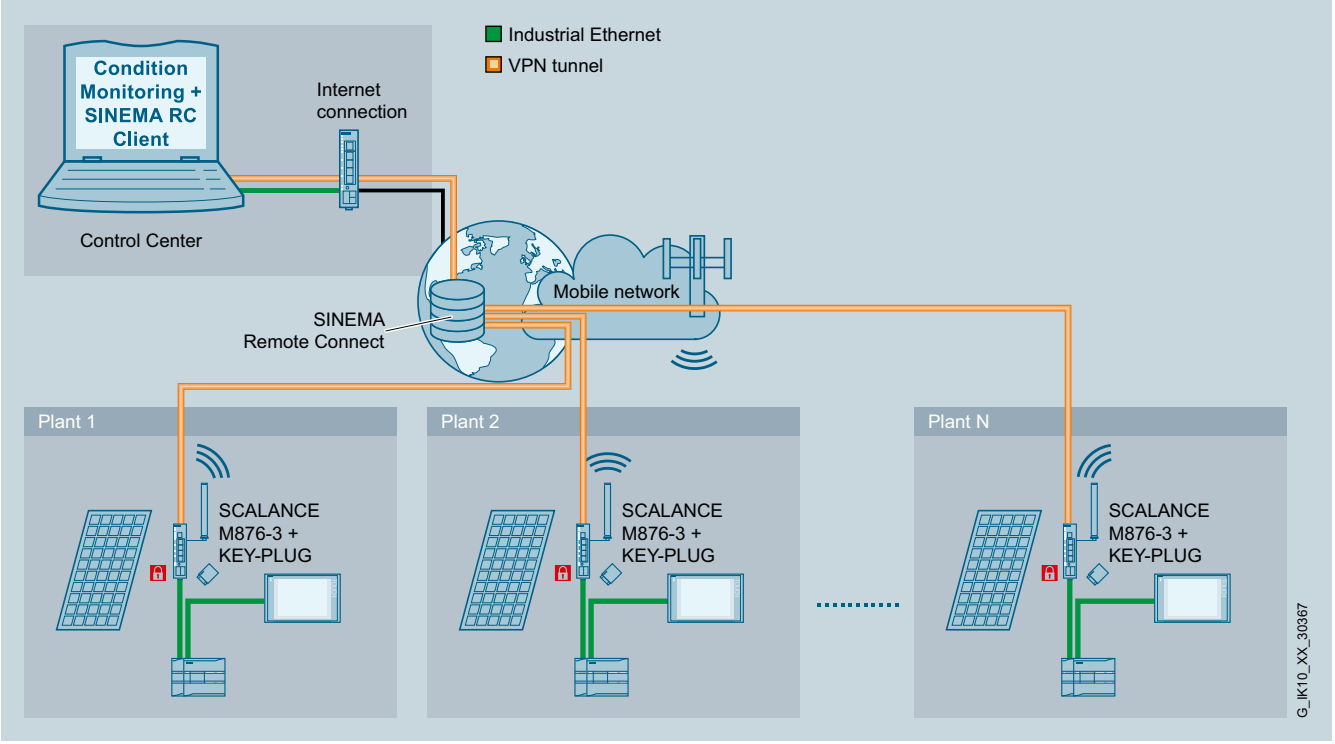
Overview of Industrial Security products

Siemens helps you to achieve this aim by providing support in reaching a common understanding of the general threat situation and implementing suitable protective measures in a targeted manner as part of an integrated industrial security concept. An essential part of such a concept deals with network security. Put simply, this includes the monitoring of all interfaces such as the interfaces between office and plant networks, and remote maintenance access to the Internet. Security can be implemented by means of firewalls and, if applicable, by establishing a secured and protected demilitarized zone (DMZ). The DMZ is used for making data available to other networks without granting them direct access to the automation network itself. The additional segmentation of the plant network into individual, protected automation cells is used to minimize risks, for example against the horizontal spread of malware, and thus also contributes to enhancing security. Division into cells and the assignment of the associated devices take place based on communication and protection requirements.



User-specific firewall for personalized and role-dependent network access

Reliable and robust Industrial Networks for the Oil&Gas Industry



Remote monitoring of distributed RTUs

The transfer of data between the cells can be encrypted using virtual private networks (VPNs) and can thus be protected against data espionage and tampering, with the communication partners being securely authenticated beforehand. The cell protection concept can be implemented as needed and communication protected using Security Integrated network components from Siemens, such as SCALANCE S Industrial Security Appliances, SCALANCE M Internet and mobile wireless routers, or security communications processors for SIMATIC. SINEMA Remote Connect, the management platform for remote networks, can be added for protected and convenient remote access to widely distributed machinery and plants.

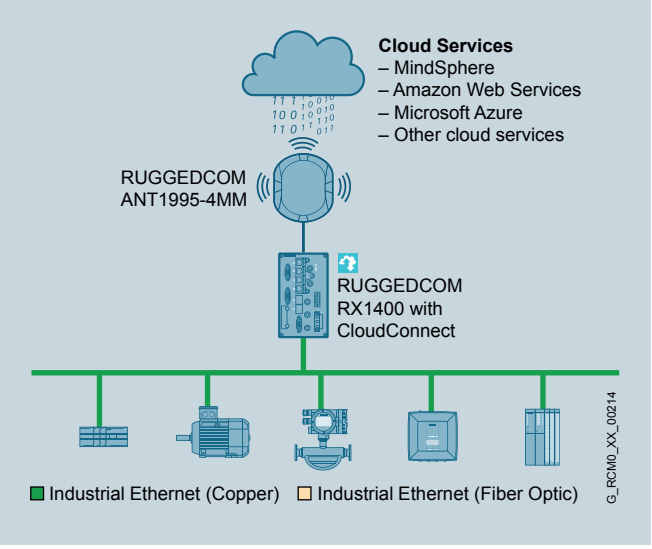
Secure remote monitoring

SCALANCE M routers for wire-based communication are available for the secure connection of Ethernet-based networks and automation devices to the hard-wired broadband network, or for secure connection via existing two-wire or multi-wire cables. These ADSL, SHDSL and PROFIBUS/ MPI routers feature integrated firewalls and VPN functionalities to protect against unauthorized access, data tampering or espionage. Depending on the device version, one or more network segments can be set up with a device.

For protected remote access to plants via mobile wireless networks, for example via 2G, 3G or 4G, we offer SCALANCE M mobile wireless routers, which also feature these integrated security functions.

With the advent of 5G networks in the near future, the corresponding devices will also be available with increased download and upload speed.

The SINEMA Remote Connect software allows secure management of VPN tunnel connections to plants and machines distributed around the world. Communication takes place exclusively via a rendezvous server. The service technician and the machine to be serviced establish separate connections to the SINEMA Remote Connect server. This then verifies the identity of the devices by an exchange of certificates before access to the machine takes place.



CloudConnect: Connection of field devices with RUGGEDCOM RX1400

CloudConnect: the transitions from field to cloud services

With the all-in-one router RUGGEDCOM RX1400, in addition to Siemens' own cloud solution MindSphere, all other large providers such as IBM Cloud, Amazon Web Services, Microsoft Azure and other cloud services based on the MQTT protocol can be connected to the system.

With the help of appropriate applications in the cloud, customers can use their data to optimize the flow rate of oil through the pipeline, energy consumption, predictive maintenance and much more.

IEC 62443: safety begins in the development stage

A reliable and integrated industrial security solution can only be successfully established and maintained if it is based on a holistic and continuous approach. This means, among other things, that it must be possible to adapt the overall solution to constantly changing threats, and that the interplay between plant operators, system integrators, service providers and product suppliers always must be taken into consideration. The issue of cyber security must be considered right from the development phase for all components used in production.

Reliable and robust Industrial Networks for the Oil&Gas Industry

CERTIFICATE

No. Q4B 076903 0003 Rev. 00

Holder of Certificate: Siemens AG
DF TI QM
Östliche Rheinbrückenstr. 50
76187 Karlsruhe
Germany

Certification Mark:

Scope of certificate: Secure Product Development Lifecycle - Product Lifecycle Management Reference Process for Division of Digital Factory (DF) and Process Industries and Drives (PD)

The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report. See also notes overleaf.

Report No: SK89768C

Valid until: 2021-07-26

Date, 2018-07-30

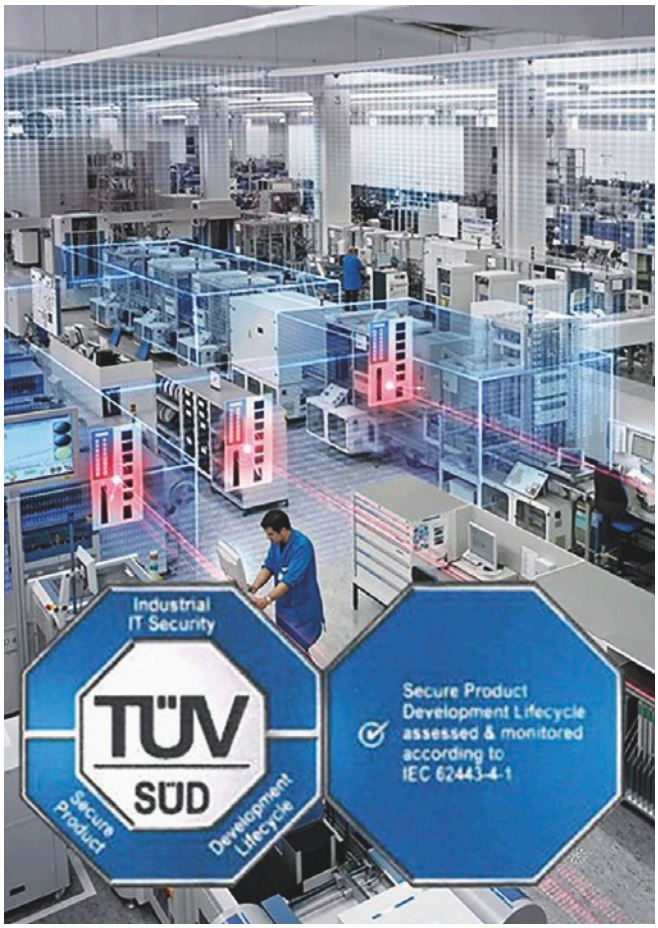
(Christian Dirmeier)

Page 1 of 3
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

TÜV®

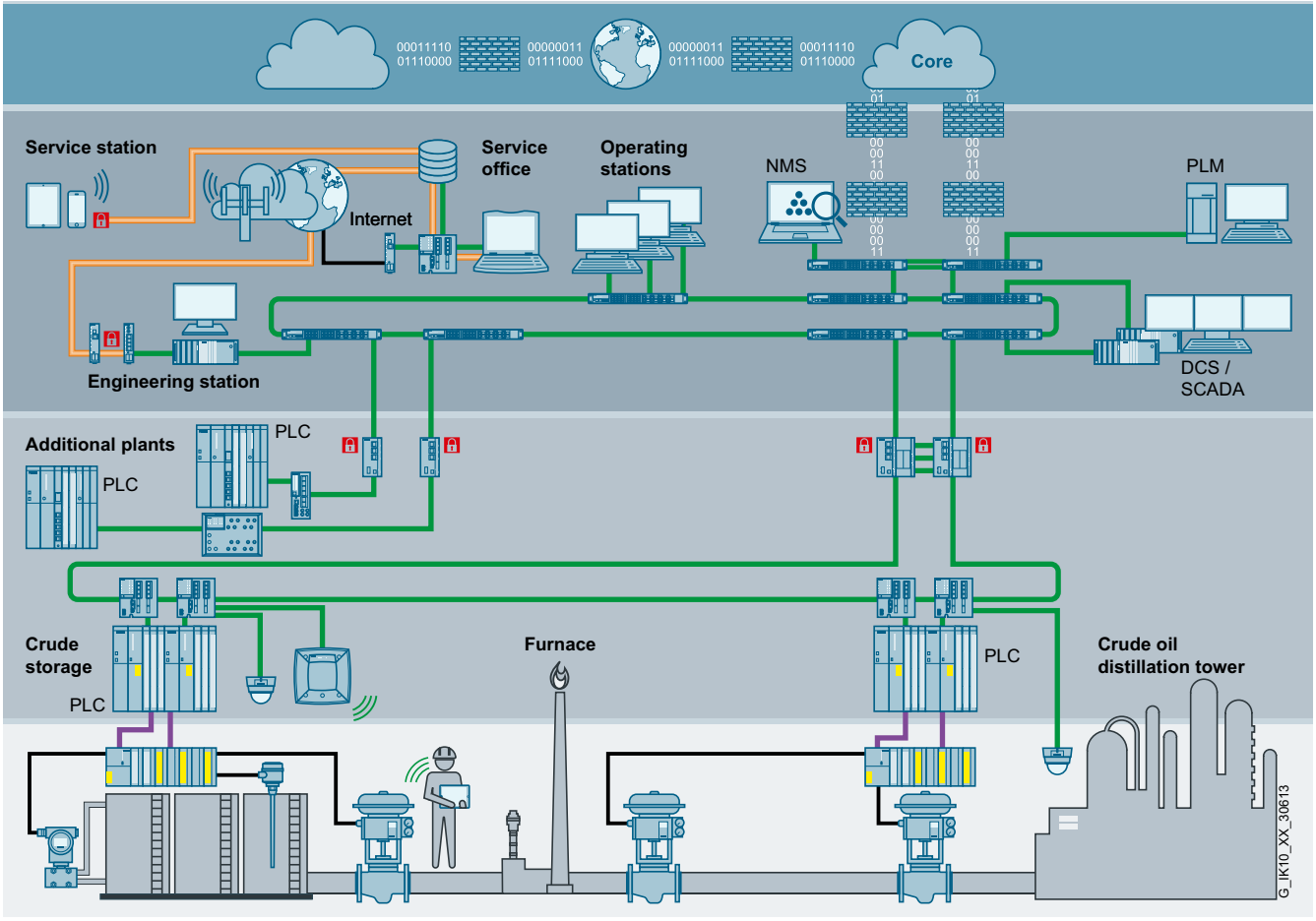
ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Certificate for the PLM Process



With the aim of taking a further step toward a secure digital world, Siemens is the first company to receive TÜV SÜD (German Technical Inspectorate/South) certification based on IEC 62443-4-1 for the interdisciplinary process of developing Siemens automation and drive products, and is also the initiator of the “Charter of Trust”.

Based on 10 key principles, the members of the “Charter of Trust” set themselves the three goals of protecting the data of individuals and companies, preventing harm to people, companies and infrastructures, and creating a reliable basis upon which trust is established and can grow in a connected, digital world.



Safety functions via Industrial Ethernet and PROFIBUS

WLAN and Safety, an example

Many process plants in the O&G industry have mixed structures of PROFIBUS and PROFINET networks. In recent times, mobile devices, which are also approved within the hazardous zone, are being used more and more frequently.

Using these mobile devices (usually tablets or smartphones), operators of a plant can directly access the data assigned to them in real time or check it by means of an on-site inspection.

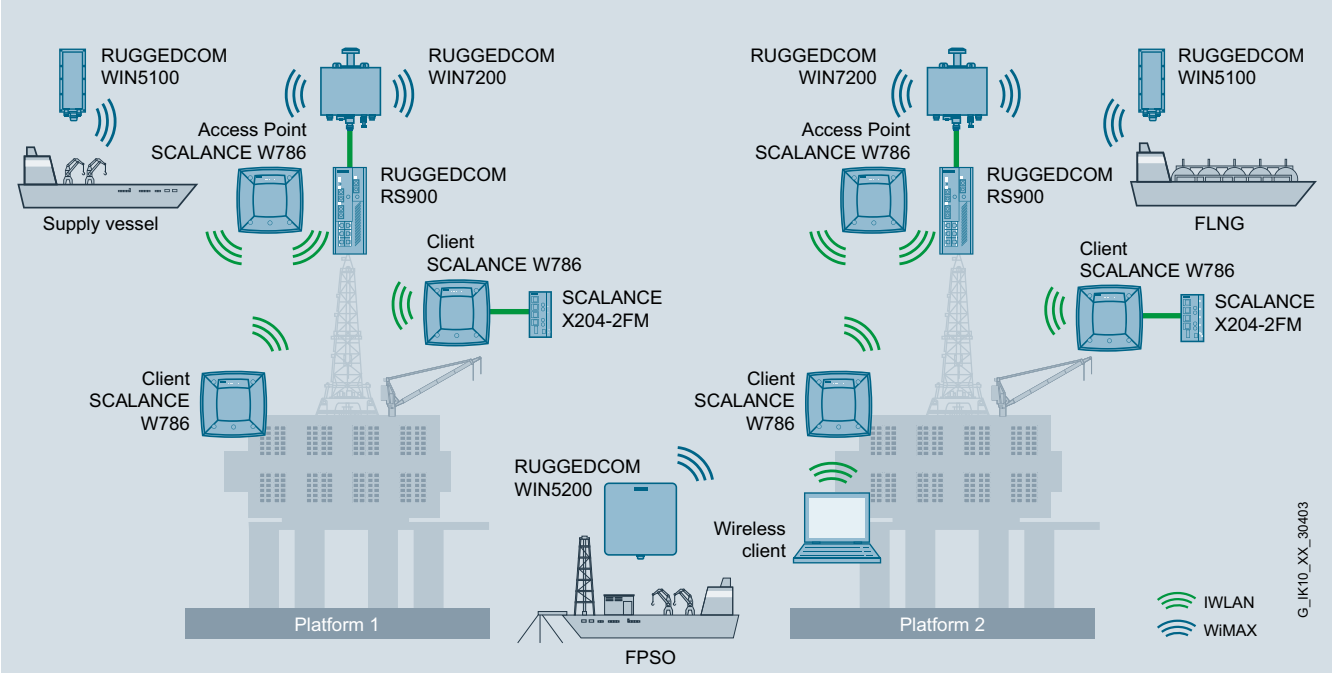
This wireless communication in combination with SCALANCE W components with PROFIsafe (Safety via IWLAN) can even be used to switch off critical parts of the system or to make an “EMERGENCY STOP”.

In addition to the protocols used in process automation, voice transmission, a video image or even data glasses can of course also be integrated in the network. With this “Augmented Reality”, system repairs or inspections have become even easier.

Creating and using private networks

In order to maintain control over network access, many customers rely on wireless networks or wired networks, that they themselves operate and maintain. With RUGGEDCOM WIN, customers have the possibility to operate their very own private broadband wireless network. The RUGGEDCOM WIN 7200 shown here is an IEEE 802.16e-compliant wireless broadband base station that has been specially developed for use in harsh environments. The data transmission rate is usually 10-20 times higher (up to 40 Mbps) than using expensive satellite transmission. The reach of such radio cells can be up to 40 km. Since the Industrial Wireless LAN (IWLAN) components and the RUGGEDCOM WIN components operate in different frequency ranges, the two technologies can also coexist.

Reliable and robust Industrial Networks for the Oil&Gas Industry



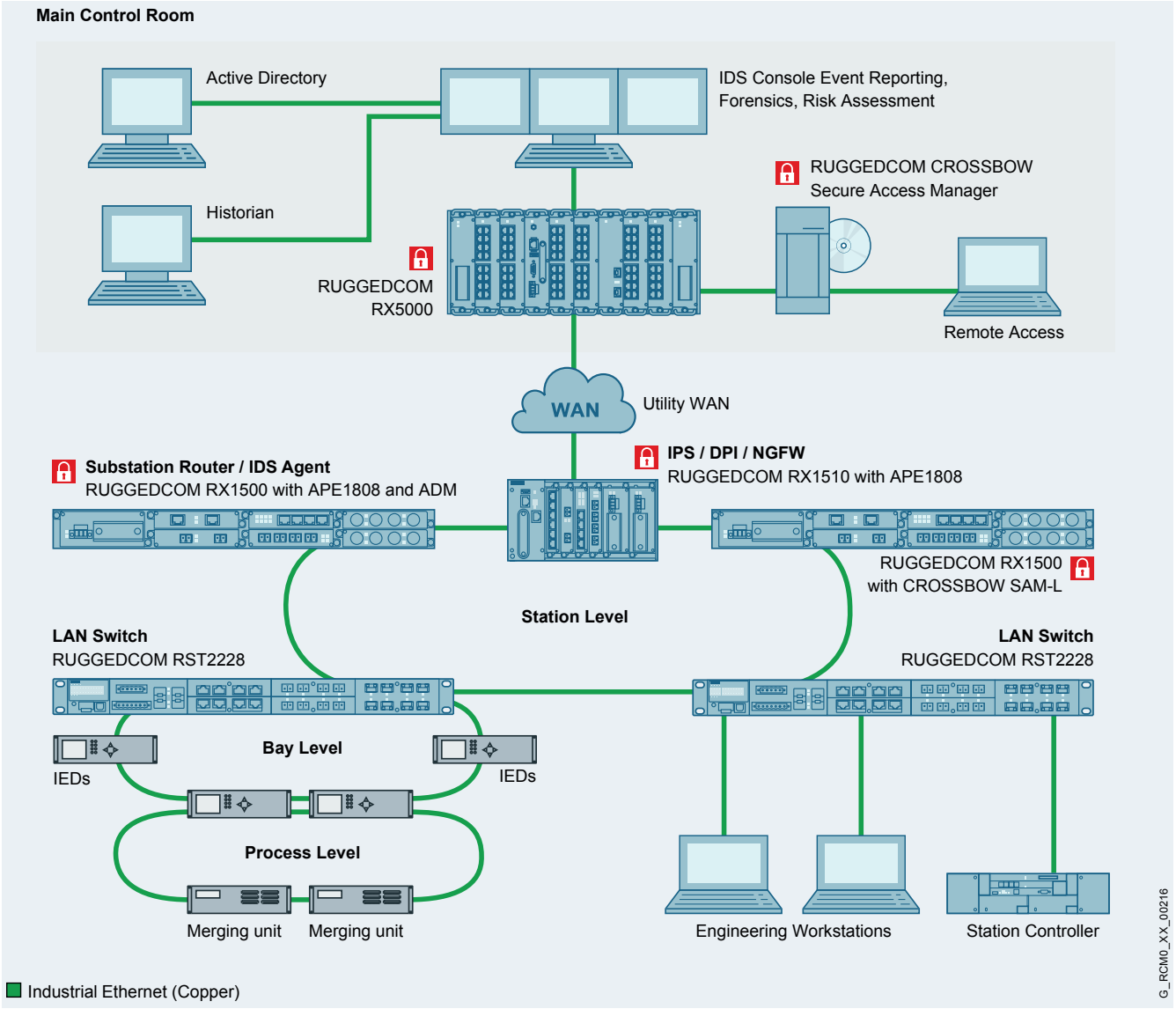
Coexistence of IWLAN and RUGGEDCOM WIN

Important note:

Suggest removing this as it gives negative impression on LPWAN tech. It is often discussed whether the applications described here can also be implemented with Narrowband IoT or LoRaWAN. From our experience, we would strongly advise against this, especially because of the significantly poorer access technology to the network and the much lower bandwidth. In addition, such networks are primarily intended for stationary sensors.

Supported software from third-party developers
By using the multiservice platform RUGGEDCOM RX1500 with RUGGEDCOM Application Processing Engine (APE), it is now possible to install and run 3rd party software applications.

With a choice of either a Debian LINUX or Windows Embedded operating system implementing software-based firewalls, intrusion detection systems or in-house softwares for your specific application – allowing greater flexibility and adding new capabilities on a single platform.



Using third-party software

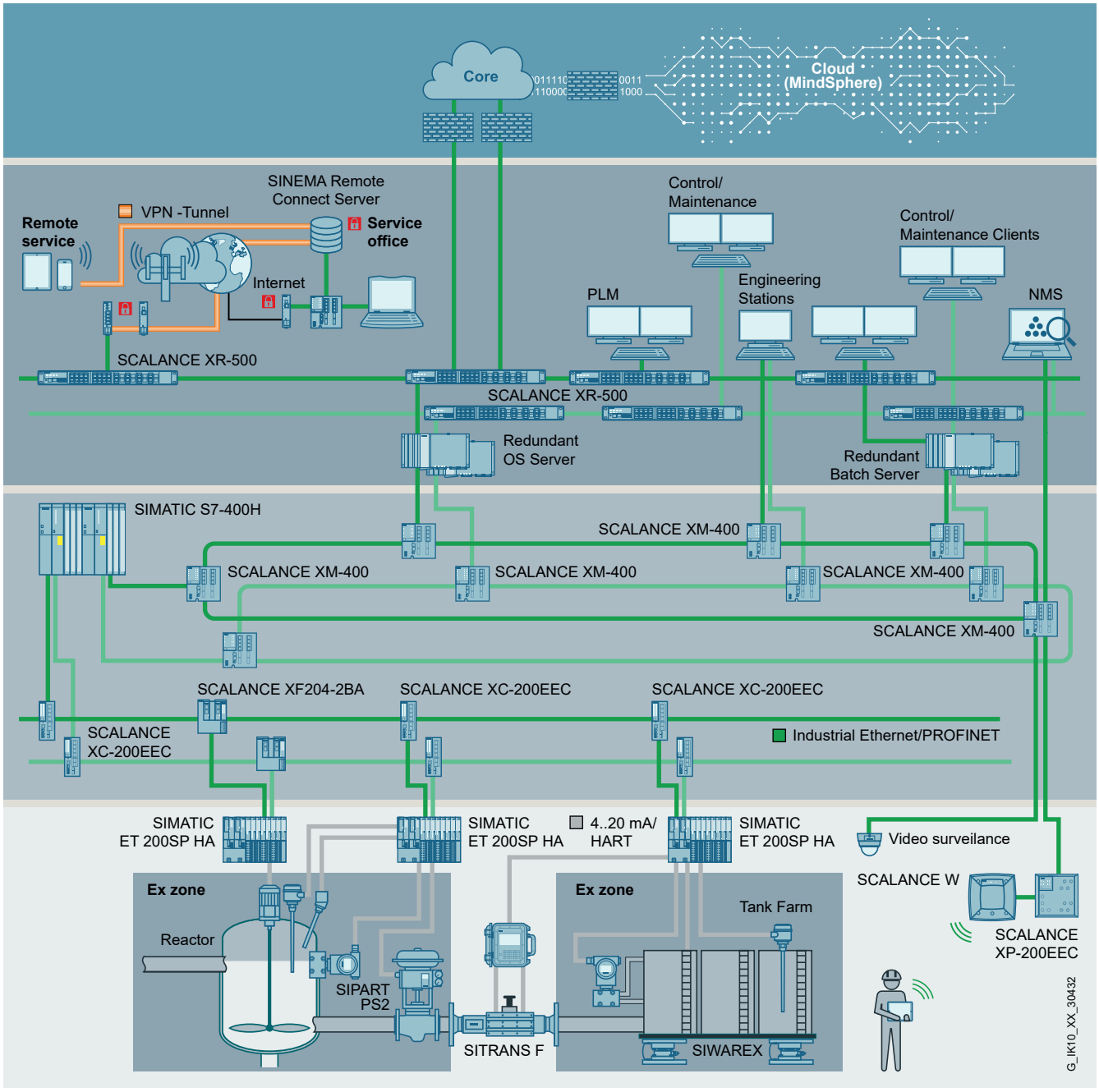
The APE operating system runs on its own hardware and is completely separated from the operating system of the RUGGEDCOM RX1500 router. This eliminates any negative impact on the functionality of the router.

Another possibility in the future is the decentralized installation of a network management agent on the APE. This allows individual cells to be diagnosed and up to 12,500 devices to be managed with a central instance on an industrial PC in a uniform user interface.

Network management made easy

Many network management systems on the market require in-depth knowledge and relatively extensive training. These systems are usually designed for the “IT specialist” and not for the “less experienced” user in the operational O&G environment. The operator can quickly lose the overview, especially with complex process plants with many network components and redundant PLC/PAC.

Reliable and robust Industrial Networks for the Oil&Gas Industry

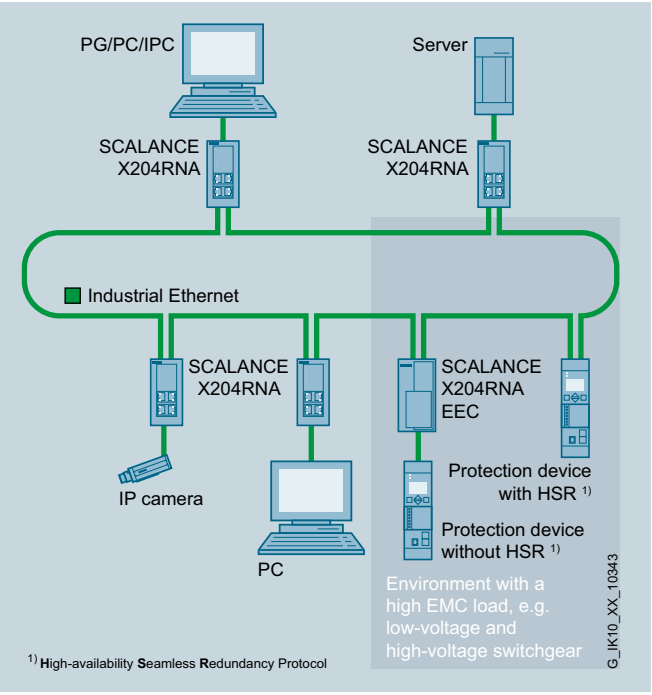


Diagnostics of complex networks with SINEC NMS

With SINEC NMS, new components can be easily integrated into the network and existing ones can be monitored and configured. The configuration is rule-based and can therefore be applied to several components. This provides significant time savings in configuring and troubleshooting, especially for large networks.

The advantages of this system include:

- Comprehensive monitoring of large, complex networks
- Rule-based configuration of the network infrastructure
- Central firmware management with topology-based rollout
- Cross-sector applications in all industries
- Fast response in the event of a fault
- Convenient remote network management

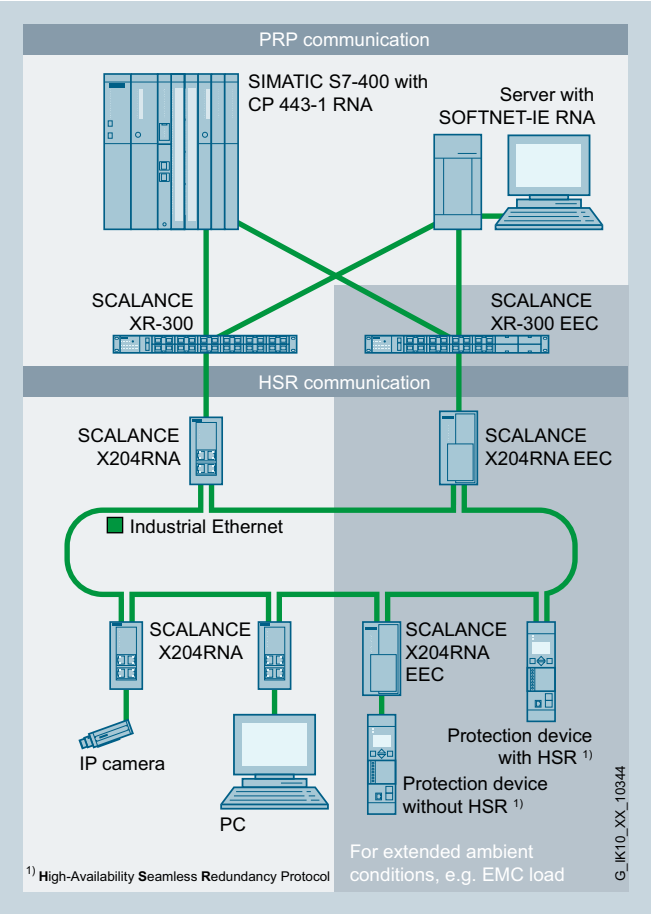


Redundant network with HSR

Redundant networks and coupling of network rings

Depending on the process or application, it may be necessary to set up a redundant network in different areas of the plant. This can take the form of a ring or two separate networks. A distinction is made here between networks which provide a short delay time for data transmission in the event of faults and "seamless switchover" which has no effect whatsoever on the time response of a data packet.

In the event that a ring-shaped network structure is to be set up for high availability plant components, it is best to use the HSR procedure (High Availability Seamless Redundancy Protocol) in accordance with the IEC 62439-3 standard. In this example's frames are sent to the ring-shaped network in both directions.



Redundant network with PRP

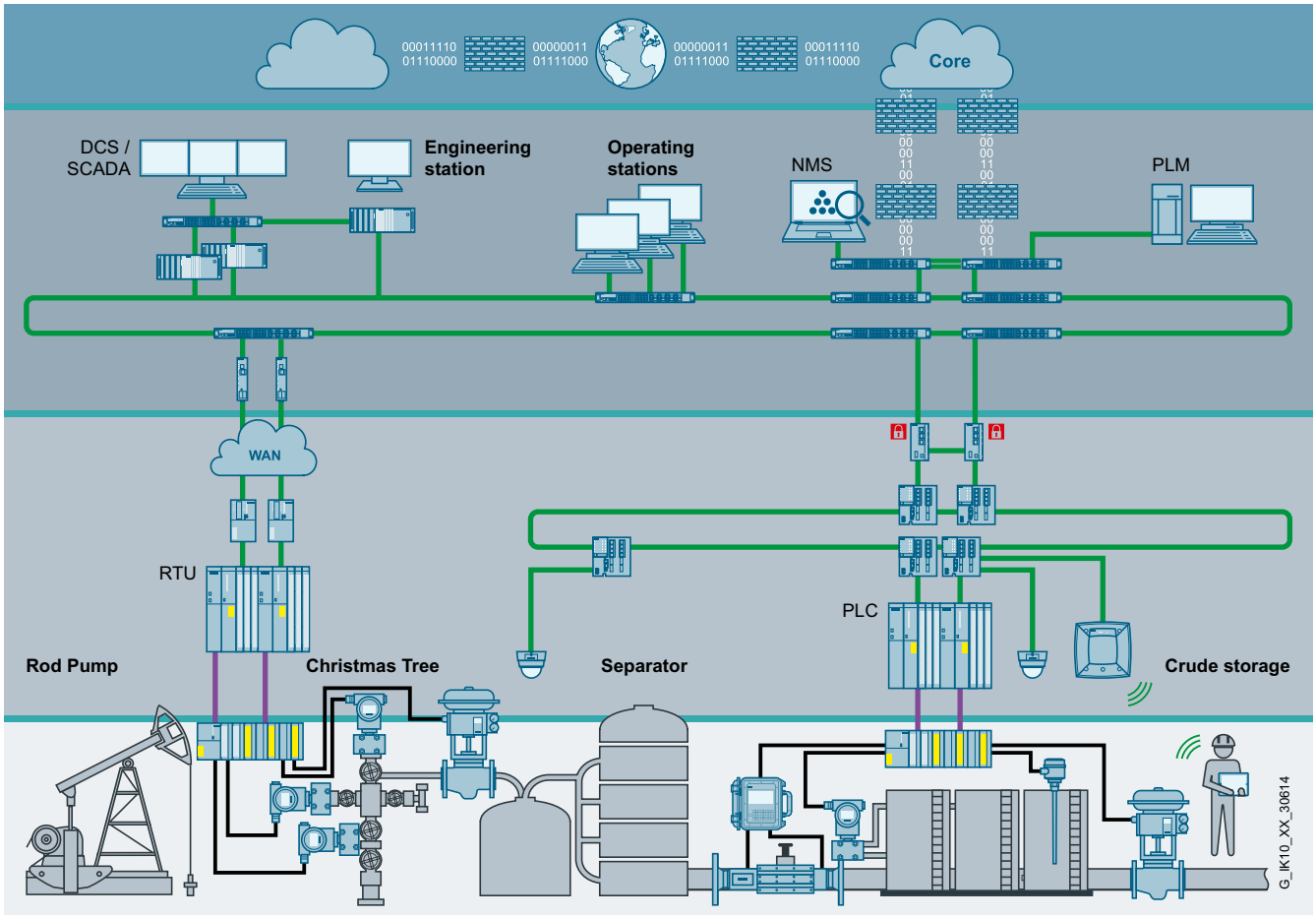
The transmission of a frame via two separate networks is also based on the same standard. With this PRP (Parallel Redundancy Protocol) network, all frames on the sender side are doubled and sent to the receiver via two separate networks

The SCALANCE X204RNA devices or the RUGGEDCOM RSG909R with HSR functionality can also be used for easy and redundant transition from HSR to PRP network structures.

The transmission of the frames is thus always ensured without delay even in the event of an error in both procedures. This means that relearning of the communication paths (reconfiguration time) is not necessary, unlike with most other redundancy protocols.

However, you can also use this solution in the system bus (i.e. when connecting DDC/PLC/PAC), or you can use simpler solutions such as MRP (Media Redundancy Protocol). MRP can compensate for individual failures in a PROFINET/ Industrial Ethernet in a simple ring topology. MRP does not support meshed networks and is both simple and deterministic. With MRP, reconfiguration times of 200 ms can be achieved in PROFINET networks. In future, faster switchover times of up to 30 ms are also being considered.

Reliable and robust Industrial Networks for the Oil&Gas Industry



Example configuration of redundant networks in O&G

If even greater demands are placed on availability, then the field devices (transducers, valves) and the digital I/O must also be doubled. However, this only makes sense if the higher-level automation is also redundant and connected to a redundant system bus.

Currently, there are still many field devices based on PROFIBUS. However, these are gradually being replaced by PROFINET devices. In addition, international standardization committees are working on an Ethernet-based solution for hazardous zones. With this solution, it would be possible to connect a cable directly from a device outside the hazardous zone to the corresponding terminal devices using an Ethernet cable in order to gain the benefit of greater bandwidth.

Protection of investment in Oil & Gas
Industrial communication differs significantly from the requirements of a normal IT infrastructure. In addition to the different requirements for redundancy, important points to consider when operating O&G systems include the wide temperature range in which the products are to work without any problems, the mechanical, electrical properties, fanless design and the certificates to be supplied, simple replacement without new configuration, long warranty periods for the products (up to 5 years) and extended product availability (>15 years).

All these advantages taken together and the possibility of integrating PROFIBUS devices and PROFIBUS PA devices for environments with particularly high explosion protection into automation today and in the future result in a high level of investment protection for the customer.

Equipped for the Internet of Things
The trend towards digitalization has by no means reached its peak. Quite the contrary! And that puts considerable pressure on the industry: Companies must be prepared for the Internet of Things (IoT) in order to remain successful in the long term in the face of global competition. However, one thing is often forgotten: There can be no digital transformation without an appropriate communication network.

For the digital factory, powerful and future-proof networks represent the core of this data communication. All assets involved in value creation can be seamlessly integrated using these networks. They enable seamless data exchange both horizontally and vertically. And they can grow with the increasing volume of data. This makes them an indispensable requirement for all companies that want to follow the path into a digital future.

Much greater numbers of sensors send their data to the customer-operated cloud for optimization of the systems. New protocols such as IPv6 (IP Next Generation Protocol, RFC 2460), standards such as IEC 62443 (Cybersecurity) and NOA (NAMUR open architecture) will have a major influence on the structure of communication networks. Will there eventually be a single converged network with low latency and high availability?

For these reasons, it would be a good idea to start planning the networks for tomorrow today.

More information and links
Industrial Communication for Oil&Gas
siemens.com/communications-for-oil-gas

References in Oil & Gas
https://sie.ag/2lOMmo1

Glossary

APE	Application Processing Engine, PC slide-in module for harsh environmental conditions in a RUGGEDCOM RX1500 router.	**NAT**	Network Address Translation, a method to rewrite IPv4 addresses into networks.
DCS	Distributed Control System, digital control system.	**NB-IoT**	Narrowband IoT.
DHCP	Dynamic Host Configuration Protocol, backward compatible with BOOTP and defined in RFC 2131. Using DHCP, the network setting of, for example, a computer (the DHCP client) is performed automatically at startup.	**NOA**	NAMUR open architecture, standardization efforts to forward the process data from the plant securely to other systems without influencing the process.
DHCPv6	DHCPv6 is the Dynamic Host Configuration Protocol for IPv6 in accordance with RFC 3315. In v6, unlike in DHCPv4, communication runs via the UDP ports 546 (client) and 547 (server).	**OPC UA**	OPC Unified Architecture, industrial M2M communication protocol that also describes the machine data semantically.
DNS	Domain Name Server: Server that resolves a symbolic Internet address as an IP address.	**OT**	Operational technology, network for production.
ERP	Enterprise Resource Planning, application software for planning resources in a company.	**PAT**	Port and Address Translation where, in contrast to NAT, not only the IP addresses, but also the port numbers are rewritten. PAT is used if multiple private IP addresses from a LAN must be translated into a public IP address.
FTP	File Transfer Protocol, definition according to RFC 959.	**PAC**	Process Automation Controller.
GSM	Global system for mobile communications; mobile wireless standard for fully digital mobile wireless networks.	**PLC**	Programmable Logic Controller, an umbrella term for a freely programmable controller.
HART	Highway Addressable Remote Transducer, widely used digital communication standard based on 4-20mA cabling to the sensors/actuators.	**PRP**	Parallel Redundancy Protocol.
HSR	High Availability Seamless Redundancy Protocol.	**RIR**	Regional Internet Registry, non-profit organization for the assignment of regional IP addresses.
IANA	Internet Assigned Numbers Authority, responsible for basic coordination on the Internet, such as the allocation of IP addresses and domain names.	**RFC**	Request for comments (RFC) to improve technical documents.
IDS	Intrusion Detection System, system for detecting attacks.	**RTU**	Remote Terminal Unit, remote control terminal, remote control unit.
IPv4 address	Unique numerical address for each IPv4 node on the Internet, e.g. 120.0.1.2.	**SCADA**	Supervisory Control and Data Acquisition, platform for data acquisition, evaluation and visualization.
IPv6 address	Unique hexadecimal address for each node on the Internet, e.g. 2001:000A:000B:000C:0000:0000:ABCD:0001	**SMPT**	Simple Mail Transfer Protocol, as per RFC 821, a simple and widely used e-mail transport protocol.
LoRaWAN	Long Range Wide Area Network is a network protocol designed for energy efficiency.		

Published by
Siemens AG

Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Germany

PDF
White Paper
6ZB5530-0DH02-0BA0
BR 0919 19 En
Produced in Germany

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

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.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit **https://www.siemens.com/industrialsecurity.**

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under **https://www.siemens.com/industrialsecurity.**