Technical article

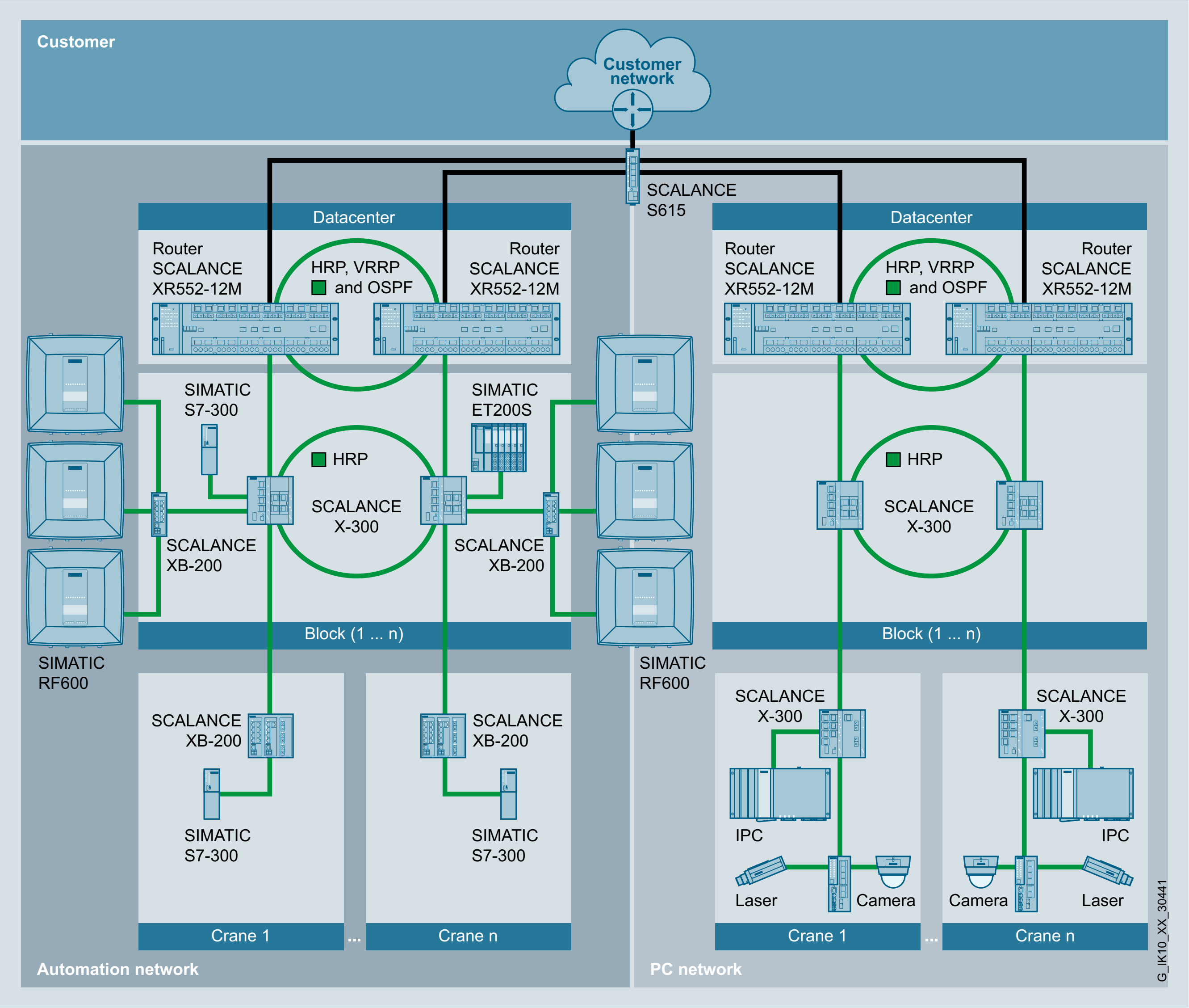
# Port crane network professionally planned and put into operation remotely

The network for a large number of automatic container stacking cranes has been planned in detail and secured by specialists from Siemens Professional Services. In doing so, devices were preconfigured, successively put into operation, and processes optimized. The largely redundant, routed network – with unique IP addressing of over 1,000 participants and strict separation of the automation and PC systems – is highly available. It thus contributes significantly to the performance of the container terminal.

More than 70 percent of the globally traded piece goods are currently transported in ISO containers by ship, rail, and truck. Centers for efficient cargo handling are container terminals, which are present in every major port. Essential for high-performance processes are stacking cranes, which bring the containers to the provided storage location and pick them up again from there for further transport. For cost and safety reasons, this is increasingly done fully automatic.

In addition to a high-performance warehouse management system and robust crane automation, a time- and route-optimized, collision-free operation also requires a reliable crane network tailored to the specific needs. One that transmits transport orders quickly, smoothly, and tamper-proof to the respective crane. The quality of automation and networking is crucial for the availability of the complete system. If only part of it fails, movement commands can no longer be transmitted and – in the worst case – no longer be executed.

To err on the side of caution, a renowned provider of container handling solutions relies on high-performance crane, automation, and network technology from Siemens in the building of a new port terminal. Divided into several storage segments with various storage blocks each, the final stage will have a large number of stacking cranes operating fully automatic. Linking the ship-to-shore cranes and warehouse are manned straddle carriers, which



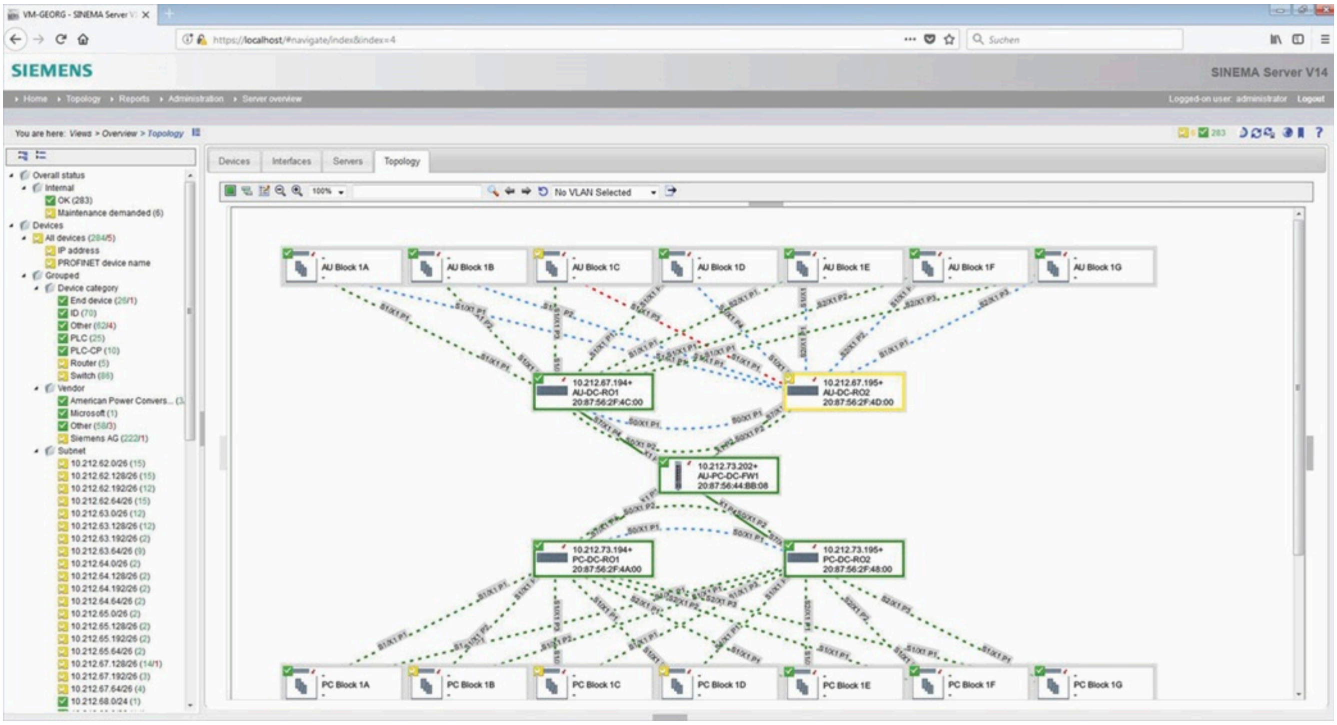
Core components of the network solution implemented with Siemens Professional Services include more than 300 switches of the SCALANCE X-500, X-300, and X-200 series for the structured, largely redundant communication among more than 1,000 participants.

accept the containers and transport them to the specified transfer point. RFID (radio frequency identification) technology from Siemens also plays an important role here.

### Combining competencies for a highly available solution

The automation and networking of the cranes and the connection to the warehouse management system were entrusted to the Siemens Expert House in Bremen (Germany), which also brought on board specialists from the Group's own Professional Services for Industrial Networks team to handle network technology. A tailor-made, individually structured and segmented, over long distances redundant solution with maximum availability and reliability was developed for the requirements of the application. Two separate networks were deliberately set up: physically separated networks from data center to crane level for automation applications and PC applications. For instance, data-intensive camera surveillance does not affect any of the other applications and subsections. A failure of a network component or line in a subnet also has only a limited effect on the associated block. Redundant ring structures and redundancy mechanisms, such as High Speed Redundancy Protocol (HRP) and Standby Coupling, Virtual Router Redundancy Protocol (VRRP), and the Open Shortest Path First (OSPF) routing protocol, achieve shortest reconfiguration times in the event of a fault – and thus the highest availability of the entire crane network.

The hub of the three-level network solution is formed by Layer 3 SCALANCE XR552-12M routers – two of each connected to a redundant ring in the operator's data center. One pair for the networking of automation components such as controllers, I/O modules, and drives, another one for PC-based applications such as server systems for crane control, and camera surveillance and laser sensor systems. All four routers are connected via a SCALANCE S615 Industrial Security Appliance to the higher-level backbone of the operator network. Thus, all subsections of the crane network are reliably protected against unauthorized access, even



The network devices were successively commissioned from afar via the SINEMA Remote Connect management platform for remote networks. The entire network solution can be conveniently monitored from afar via the SINEMA Server network monitoring and diagnostics software (pictured).

from the Internet. Via single-mode fiber-optic cables, the routers communicate with the subordinate, likewise ring-redundant block level – each made up of two Layer 2 switches of the SCALANCE X-300 series per block in separate VLAN segments. In these, only the logically related participants of a block interact, all others are not affected. With four additional switches of the X-300 and X-200 series for each crane, the number of installed SCALANCE devices increases to more than 300 and that of network participants to well over 1,000. In order to quickly identify and address all participants, a unique IP address was assigned to each of them.

### Delivered tested and preconfigured to the construction site

In order to achieve high functional reliability as early as possible, the Expert House set up the planned networking with all devices for the operation of a crane pair in Bremen and intensively tested all processes. The optimized configurations could be backed up and easily be transferred to other devices using adapted IP addresses. Already at this early stage, the Professional Services specialists utilized the SINEMA Remote Connect management platform for remote networks and the SINEMA Server network monitoring and diagnostics software, which should prove useful as the project progressed.

### Successive commissioning and optimization from remote location

Using the SCALANCE firewall and a secure VPN (virtual private network) connection, the devices could be commissioned on the building site via SINEMA Remote Connect – always exactly when another crane was assembled and ready for it. As a result, the originally planned on-site support that is dependent on the crane construction in terms of time, and thus is difficult to plan, became superfluous. Supported by SINEMA Server, Siemens network specialists were able to diagnose and detect errors and problems occurring during the step-by-step commissioning, which made a timely correction possible.

Ultimately, everyone involved benefits from the use of Siemens software. The Siemens Expert House can configure and program its automation systems from Bremen in the TIA Portal via SINEMA Remote Connect, and firmware as well can be easily updated in this way. SINEMA Server offers extensive network monitoring, diagnostics, and maintenance capabilities. The convenient handling is prompting the terminal operator to also consider using the Siemens solution in addition to already existing tools. Through the work with SINEMA Server, valuable insights for the further development of the software could be gained.

## Professional Services: Comprehensive support in all aspects of industrial communication networks

Together with industry- and IT-experienced Siemens Solution Partners, Siemens offers coordinated Professional Services for Industrial Networks for both existing and new industrial communication networks. The team was specifically established to support manufacturers and operators of machinery and equipment with network technology from Siemens and other suppliers in every life cycle phase – from design to service. On request, experienced specialists advise on the design of industrial-grade LAN and WLAN network infrastructures and mechanisms, and also take on the commissioning and optimization on-site. Furthermore, various standard and customized training courses impart sound product and network knowledge.

## 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, visit:
**https://www.siemens.com/industrialsecurity**

Published by
Siemens AG

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

PDF
Technical article
DI-PA-18/19-7
BR 0619 4 En
Produced in Germany
© Siemens 2019

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.

All product designations may be trademarks or product names of Siemens AG or supplier companies whose use by third parties for their own purposes could violate the rights of the owners.

**www.siemens.com/industrial-networks-services**