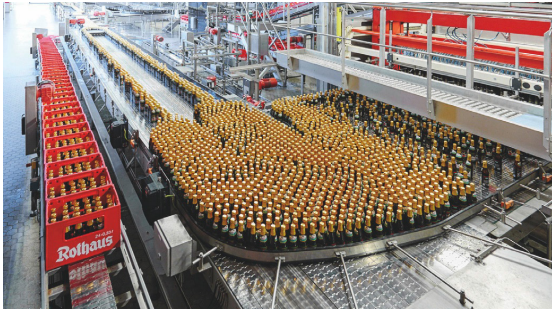


## Reference

## Network upgrade for fast, access-protected, and highly available processes in beer production

Using high-performance network technology from Siemens, the Badische Staatsbrauerei Rothaus AG has made its production network fit for the future. Redundant ring structures, high data transmission rates, cell protection with segmentation, and access via firewalls are essential for a fast, access-protected, failsafe, and highly available communication. Siemens, the Siemens partner HWI IT, and Rothaus have jointly developed and optimized the concept for this and implemented it during active operation.

Whether in classic discrete manufacturing or brewery operations – in the course of digitalization, automated processes require high-performance and secure communication from and with machine and plant control systems. With every modernization, the Badische Staatsbrauerei Rothaus AG is faced with the challenge of integrating machinery and equipment into the existing network and ensuring secure access to them. On the one hand, from Rothaus' own production and enterprise (MES and ERP) level, and on the other hand, equipment suppliers as well must be able to access their systems, whether on site or externally, in order to save time, travel, and costs.



Water, hops, malt, and a high-performance network are elementary “ingredients” at Rothaus for the efficient production of quality beers. Copyright: HWI IT GmbH

And with every innovation cycle, the amount of data grows with the possibilities. For these reasons, the traditional brewery from the Black Forest had to act.

The existing production network was already segmented and linearly followed the different areas of the brewery: from the malt intake, the brewhouse, to the fermenting, yeast and storage cellars, the filter and pressure tank cellar, the bottling, the sorting as well as the energy supply and the brewery's own wastewater treatment plant. With the risk that in case of failure of a network device or a transmission path, the communication to subsequent devices and for entire areas could fail.

In light of continuously increasing amounts of data and growing communication needs, the until now limited data rate of up to 100 Mbps was also deemed inadequate. Therefore, the network had to be modernized from the ground up and upgraded with the currently most powerful components according to the latest standards. The planning and implementation was entrusted to HWI IT GmbH, an engineering company based in Malterdingen, Germany, specialized in highly available network infrastructure solutions. The company has been working with SCALANCE network technology from Siemens for years, which is inherently tailored to the SIMATIC automation portfolio preferred by Rothaus. The competence of the HWI IT network experts is consolidated by their upcoming certification as Siemens Solution Partner for Industrial Communication. With the support and longtime

experience of the network specialists from Siemens in Stuttgart, all parties involved were able to collaborate in the development of a customized network concept for the brewery operations and implement it step-by-step.

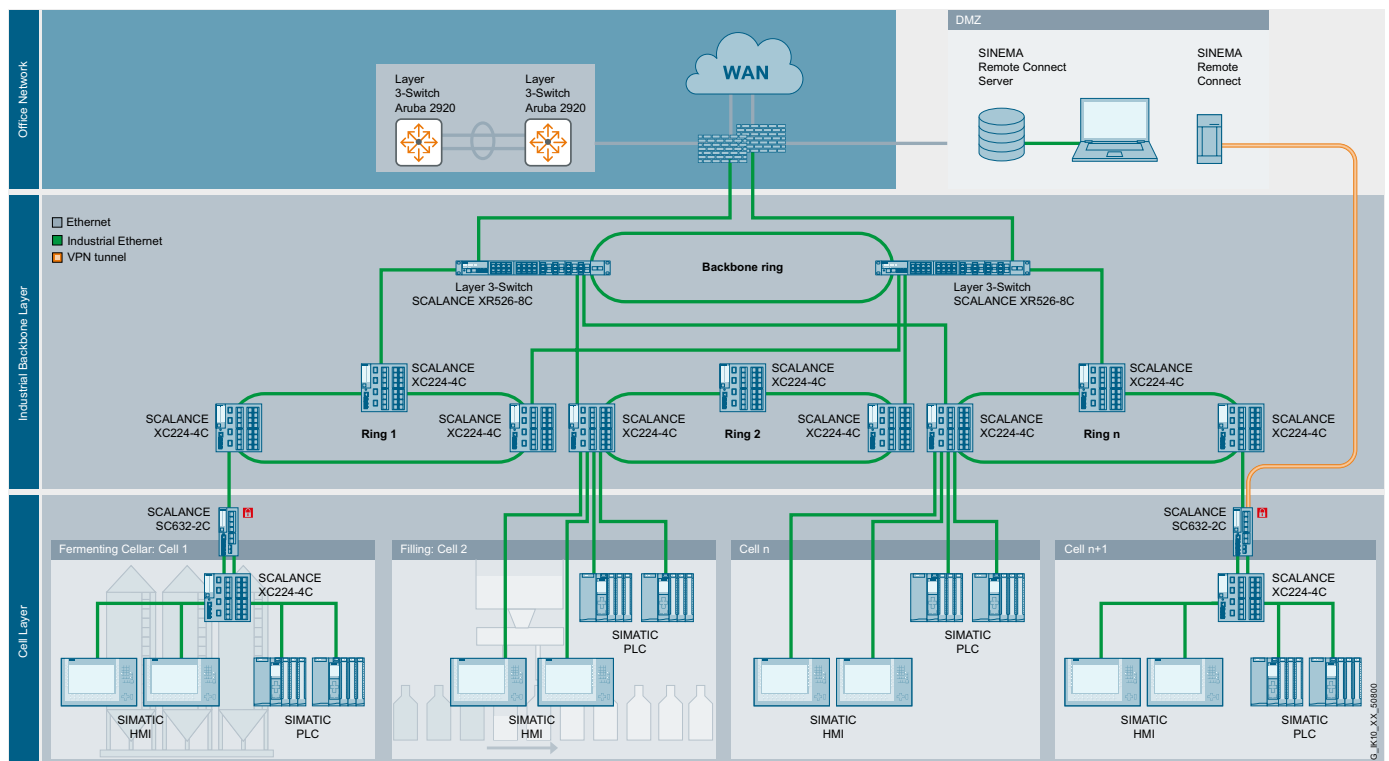
### **Secure (remote) access to machine and plant control systems**

End-to-end networking and communication via Industrial Ethernet and PROFINET are replacing traditional fieldbus systems such as PROFIBUS more and more often. This also enables commissioning, diagnostics, and maintenance of the systems over the network – and puts the focus on the topic of industrial security. It must be ensured that only authorized users have access to the plant sections that are relevant to them.

After a pilot project, the prerequisites for this were created throughout the production in the form of around 60 secure, standardized points of access to the automation level. Mainly to the SIMATIC PLCs S7-300, S7-400, and the latest generation – SIMATIC S7-1500. The access protection is realized by a SCALANCE S615 Industrial Security Appliance, which monitors network traffic as a firewall. An additional central security component for device



SCALANCE S615 Industrial Security Appliances and a higher-level SINEMA Remote Connect server ensure that only authorized users can access the control systems in the production.



Segmented and redundant – thus highly available – but at the same time offering high-performance and access protection: the production and enterprise system (MES and ERP) network developed and implemented by HWI IT GmbH and Siemens meets the high requirements for future-proof networking.

access was installed via a higher-level SINEMA Remote Connect server, the management platform for remote networks from Siemens. It grants access by means of a VPN tunnel and a SINEMA RC client exclusively to users authorized by certificates. Another barrier is the access control via an integrated key in the production cabinet. With them, the connection to each individual PLC can be enabled (as agreed upon). “It was important that the processes mentioned do not affect the regular operation and data traffic in the production environment,” says Adriano Pederiva, Head of Automation at Rothaus.

### Segmentation and ring redundancy for maximum reliability and availability

Due to increasing requirements, the network of the process control system was independently reorganized from scratch – with the existing line structure being converted into three ring segments with logically as well as spatially related devices. New network components of the SCALANCE X series networked via redundant fiber optic rings provide greater performance, access protection, and reliability – thus making the network highly

available. A central, redundant backbone ring will connect all devices in the future. At the heart of this backbone are two SCALANCE XR526-8C Industrial Ethernet managed switches with integrated layer 3 functionality (routing).

The two devices are linked via the Virtual Router Redundancy Protocol (VRRP) to a logical virtual router – of which one is active and the other one is operated in hot-standby mode. The data rate in this ring is 10 Gbps. If one device fails, the other assumes all tasks within milliseconds. The backbone ring is also the bridge between IT (Information Technology) and OT (Operation Technology) of the company. To this end, the central office firewall is connected, and virtual LANs (VLANs) logically separate IT and OT. “Especially the transitions between the two worlds require an exact knowledge of the processes on both sides,” emphasizes Holger Wiedel, Managing Director of HWI IT. “In addition to responsibility, every single connection also has to be precisely planned to avoid unnecessary communication and to be able to define clear rules. Only then will it be possible in the future to easily integrate and connect additional



## 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 [siemens.com/industrialsecurity](https://siemens.com/industrialsecurity)

Siemens AG  
Digital Industries  
Process Automation  
Östliche Rheinbrückenstr. 50  
76187 Karlsruhe, Deutschland

Reference  
DI-PA-18/19-10  
BR 1022 4 En  
Produced in Germany  
© Siemens 2022

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

devices. In manageable subnets, innovative functionalities such as anomaly detection can be used simply and efficiently for network monitoring.” In order to make the interaction between OT and IT even more efficient, Siemens works closely with Aruba, a Hewlett Packard Enterprise company. At Rothaus, too, the switches in IT come from Aruba and in OT from Siemens – both portfolios complement each other and the interoperability of the devices is also ensured.

The subordinate Gigabit ring segments are redundantly connected to the backbone via layer 2 switches of the SCALANCE X-300 and X-200 series – depending on the scope and required functionality. Here, as well, proven redundancy mechanisms reliably maintain the communication in the event of a network device failure. To protect against unauthorized access to cells in the process control system network, high-performance SCALANCE SC636-2C Industrial Security Appliances have been specified and in some cases are already in use. “Because we exactly know the processes, these cell firewalls can be easily retrofitted at any time,” states Michael Dufner, IT engineer at HWI IT responsible for the project.



SIMATIC HMI Panels integrated into the production network make the processes locally transparent and easy to operate.

## Fast, secure, available, and ready for the future

“With high-performance network technology and the bundled competence of all those involved, we have achieved our goals throughout and implemented a fast, access-protected, failsafe – and thus highly available production network,” says Adriano Pederiva. “Right from the start, we were keen to design structures and processes in a way that keeps open all paths for future developments.” Among other things, it is planned to virtualize parts of the production control system and to configure, monitor, and manage the production network effortlessly via the SINEC NMS Network Management System.