SIEMENS

Reference

Production Network: Transparent and Safe

Scalable Network Technology for transparent, access-protected, and failsafe production of aluminum profiles

With industrially certified, scalable network technology from a single source, a manufacturer of aluminum profiles has realized a high-performance, horizontally and vertically integrated data flow – and thus a high degree of transparency in its production. Matched IT security components provide effective protection against unauthorized access from inside and outside. The easy, flexible integration of the most varied communication levels and media is very important – in the past and today.

Since 1958, extruded sections (semi-finished products) out of aluminum are produced, refined, and post-processed in Rackwitz near Leipzig, Germany. The press plant steeped in tradition is now one of the most efficient of the globally operating Sapa Group, a joint venture of the market leaders Sapa and Hydro Extruded Products. At the Rackwitz site, the Sapa Extrusion Deutschland GmbH produces high-grade aluminum profiles for a wide range of application on two fully automated press lines (8 inch and 10 inch).

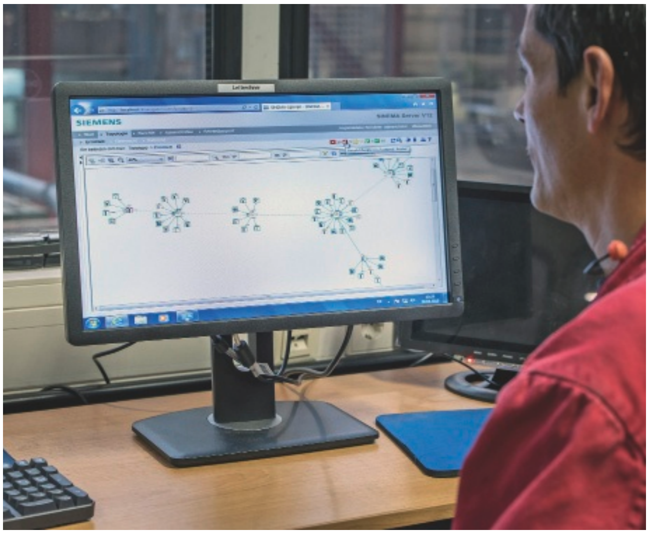
Sapa relied on technology from Siemens from the beginning: The SCALANCE Industrial Wireless LAN (IWLAN) devices ensure that the previously error-prone optical communication in the plant along the profile extrusion routes in the aluminum processing are now highly available and failsafe. New requirements concerning real-time communication and PROFINET connection in the production environment – to further increase productivity – necessitated the renewal of the network infrastructure.

On two extrusion presses in the Rackwitz plant, Sapa Extrusion Deutschland produces high-grade aluminum profiles for a wide range of applications, and refines and postprocesses them.

Within the framework of the CE certification of its products, Sapa reviewed certain production conditions in the plant. In the process, a so-called security quick check was performed together with consultants from Siemens, Sapa's long-time supplier for electrical and automation technology. In general, the availability of the entire network was to be examined to assess the risks of system failures, e.g., caused by cyber-attacks, and their impact on production systems. The security analysis then revealed that the industrial suitability of individual network components as well as the access protection to switches, PCs, controllers, and communication processors in the field could be optimized. The same applies to the failsafe communication during the operation of the three trolleys for the transport of press tools and scrap. As a result, specific measures were derived and practical solutions developed together with the supplier – some of which are already implemented.

Security becomes transparent – Security Quick Check reveals vulnerabilities

The result of the security quick check from Siemens includes an appraisal of the essential availability and security requirements, which provides a quick overview of how things stand in various security-relevant areas and points out potential risks. These can be evaluated and specific solution possibilities be developed.



With the network management and diagnostics software SINEMA Server, the profile manufacturer now always keeps track of the production network.

Systematic Network Management

One of the first measures was the use of the network management and diagnostics system SINEMA Server from Siemens. With this software, the operator could quickly and conveniently get an overview of the "evolved" production network and continuously monitor it. The system – easily usable via a web browser – automatically recognizes conventional and industrial network components and automatically visualizes doubly assigned IP addresses in the network (in the latest V13 edition). It thus reliably prevents conflicts. The system clearly depicts the current states of network devices that can be sorted according to different criteria and allows for individual reports and analyses. The results can be visualized on HMI systems via web mechanisms, reports be automatically sent by e-mail to selected recipients, and malfunctions be reported by SMS.

Once the infrastructure has been captured, the program monitors it and reports any change. With these means, the network could be appropriately redesigned to meet the needs of both the production and IT specialists in the company.

Nine fully modular managed Industrial Ethernet switches SCALANCE XR324-12M from Siemens form a high-performance and reliable backbone in the profile production.

A number of network devices are connected to the backbone via subordinated managed switches of the type SCALANCE X-200 in control cabinets.

Reliable Production Backbone with SCALANCE X-300

As a result of the network monitoring with SINEMA Server, an industrial-grade – i.e., a high-performance, rugged, and reliable – production backbone based on the fully modular, managed Industrial Ethernet switches SCALANCE XR324-12M was set up. Expanded IT functions are provided by the rugged Industrial Ethernet switches SCALANCE XR-300 from Siemens. Following a brief test operation with one of these switches, the existing devices by other manufacturers not explicitly designed for industrial use were replaced: Nine XR-300 switches now make up a stable, easily expandable production backbone. At present, this backbone is not closed to form a redundant ring, which however can be done later at any time. With it, the availability can be further increased. The connection to higher-level systems on the enterprise level is also possible.

“We chose the rack switches because they fit into the existing 19” cabinets and because devices can be easily integrated into the network using a wide range of optical and electrical media types,” says Andreas Steinberg, who is responsible for the maintenance and automation technology of the production environment at Sapa. The devices are equipped with twelve ports (at the front in this case) for plug-in media modules with two ports each. Future expansions can thus be easily carried out, since the existing infrastructure can simply be supplemented.

Some of the currently approximately 200 relevant participants in the field are connected to the backbone directly and some via subordinated managed Industrial Ethernet switches SCALANCE X-200 in decentralized control cabinets. As a result, a horizontally and vertically integrated, rugged, and reliable communication can be ensured production-wide.

In addition, the switches from Siemens utilized feature a slot for a so-called C-PLUG, a storage medium on which the current device configuration is saved. This device configuration can be quickly transferred to a replacement device through simple re-plugging. According to the persons in charge of the press plant, Siemens could be ensure that spare parts for all components would be available even after many years.

Access Protection from inside and outside

At the interfaces to the office world, special security modules from the product family SCALANCE S with integrated firewall provide a separation of the production systems, in particular from the World Wide Web. Thus only authorized internal and external users have access to the network components in the production. This ensures secure, but also convenient business operations. The remote maintenance of systems by external suppliers is also possible, which can be decisive for the availability. Standard as well is a protected remote access for the maintenance personnel via VPN (Virtual Private Network) tunnel – enabling them to quickly intervene in the case of malfunctions.

Without this separation of the corporate and production networks, it is entirely conceivable that the failure of one participant in the corporate network causes the RST (Rapid Spanning Tree) protocol to automatically route through the production network, which under unfavorable conditions can increase the production network load to such a degree that its functionality can no longer be guaranteed. The risk of misuse is higher without this separation, too. “That’s why only certain communication protocols and participants are allowed. The access rights are reduced to a necessary, safe level, which could be implemented with the Siemens network technology,” explains Karsten Konschak, the head of IT at the Sapa site. In addition, the real-time capability of the network, among other things, provides for a failsafe communication.

The RCoax cable from Siemens is a radiating antenna cable routed along the railway that ensures a WLAN field over the travel path.

RCoax as simple solution

Also easy to integrate into the whole ensemble are previously or in parallel modernized partial solutions to the mechanical backbone of the production – the overhead monorail system for transporting press tools (from the centralized high-bay warehouse to the preheating furnaces and presses) as well as scrap. The original optical communication system became more and more error-prone and also no longer met the requirements concerning functional safety when moving three trolleys in specific, worker-accessible zones. The solution – realized with Siemens assistance and SCALANCE IWLAN components – enables an interference-free failsafe, prioritized communication via PROFINET/PROFIsafe and thus a safe operation under all circumstances.

To this end, up to 130 m long, so-called RCoax cables (radiating cables) from Siemens are installed along the railway. These RCoax cables are IWLAN antennas, which were routed along the travel path – thus ensuring a homogenous WLAN field over the entire railway. They transmit the signals of the IWLAN clients in the network of the trolley-installed SIMATIC controllers to the associated IWLAN access points and vice versa – failsafe via an exactly defined radio field.

Powerful Network Technology is indispensable

Compared to the office world, network technology for the production demands considerably more with regard to performance, reliability, and availability. “The reliability of the communication is now more important than ever, since the strictly order-oriented production in smaller lot sizes results in more frequent production changeovers and thus a far greater exchange of data. This also applies to the following shopping cart transport system and the higher-level host computer,” states Steinberg. The progressing replacement of PROFIBUS components with PROFINET components will inevitable increase the number of network devices in the plant even more. A powerful network management thus becomes indispensable to keep track with reasonable effort.

With the steps implemented so far and the components from Siemens, the persons in charge at Sapa in Rackwitz consider themselves on the right path. The added value of this total package – consisting of network technology ranging from IWLAN devices to switches to the monitoring system SINEMA Server, and the new network infrastructure based on the results of the security check – stands out: The production network has become high-performing, highly available, and transparent. Additional modernization and integration projects have already been initiated.

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 only form one element of such a concept. For more information about industrial security, please visit **www.siemens.com/industrialsecurity**

Siemens AG
Process Industries and Drives
Process Automation
Postfach 48 48
90026 Nürnberg
Germany

© Siemens AG 2016
Subject to change without prior notice
PDF
Reference
FAV-193-2016-PD-PA
BR 082016 En
Produced in Germany

The information provided in this brochure 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.
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.

siemens.com/scalance