



Error proofing, increasing productivity and cost reduction

Industrial network infrastructure for secure and efficient automation solutions

Constantly growing quantities of data due to intelligent components, increasingly intense pressure for efficiency and not least, the necessity for the highest cybersecurity standards: With the increasing automation of industrial systems, the requirements of the corresponding network infrastructure are also increasing. Current solutions from Helmholtz show how these requirements can be realized both reliably and practice-oriented.

Whether Ethernet and PROFINET switches, fieldbus and NAT gateways, or secure online remote access: For the optimal realization of industrial network infrastructures in practice, the ideal and flexible solution with simple handling for each application is what counts. And this can, for example, consist of making the familiar better, solving tasks more elegantly, or designing components smaller to optimize them for the control cabinet. That these solutions also function without additional, complicated software tools, is an important argument for many Helmholtz customers.

Ethernet and PROFINET switches

The data transfer between controllers, PLCs and other network participants takes place via switches. They are thus among the most important network components – also in terms of numbers. Even the most minor optimizations therefore have a noticeable effect

on these components. This also applies to the design, because space in the control cabinet is of course limited.

The unmanaged Ethernet switches from Helmholtz set standards here with only 49 mm construction width in the 5 port version or 65 mm for 8 ports. Thanks to their highly compact design, they can be used for a variety of industrial applications. The light and yet robust industrial design is suitable for installation on the DIN rail and can be very easily integrated into the network. Once plugged in, they

are immediately ready for operation with the simple plug&play solution. The tool-free push-in terminal for the power supply thereby supports quick and uncomplicated installation.

However, the use of conventional Ethernet switches in connection with PROFINET networks should be viewed with caution due to the absence of frame prioritizing and the related data load in many machine networks. PROFINET switches are clearly the better alternative here.

One of the most important functions of a PROFINET switch is the prioritizing of the PROFINET frame traffic in the machine network. The managed switch can differentiate whether the frame is a web query, an FTP file transmission, a media stream, or a PROFINET frame. In the case of a high transmission load, the important frames can thus be prioritized in order to prevent frame losses or that the PROFINET network is no longer accessible. This also means the necessity for clear



Industrial Ethernet Switch, 5-port, unmanaged

and unambiguous segmentation between Ethernet and PROFINET. Without managed PROFINET switches, many profitable features of PROFINET are lost.



PROFINET Switch, 8-port, managed

Fieldbus and NAT gateways

Hardly less frequently used than switches are fieldbus gateways for the connection of individual automation networks. Regardless of the respective network bus (PROFINET, CANopen, DP), the smallest possible dimensions of the design are therefore also of decisive importance here. PROFINET-PROFINET gateways from Helmholz, for example, are only around a quarter of the size of comparable devices from other manufacturers. In addition to this, their installation, like that of the PROFINET switches, requires no additional software tool.

With the triumphal march of Ethernet networking, cybersecurity also plays a central role. Especially when considering the growing quantities of data, the separation or segmentation of networks is therefore urgently recommended. In the process, the central task is to securely integrate machine networks into the higher level production network. With the WALL IE NAT gateway, Helmholz offers a solution that concentrates on the central functions and a thus affordable solution: The robust and especially compact Ethernet components combine bridge and firewall functions. It therefore allows easy integration of machine networks into the higher level production network. Broadcast domains are thus reduced in size as a positive effect.

In concrete terms, the components protect the networks in that they precisely regulate which participants may exchange data with which device. The prerequisite for this is created by a packet filter functionality: This enables the limitation of access between the production network and the automation cell.

As a special feature, WALL IE can be used in both the NAT operating mode and as a bridge. In the bridge operating mode, WALL IE acts as a layer 2 switch. In contrast with normal switches, however, packet filtering is also possible in this operating mode. This means that the restriction of access to individual areas of your network can be achieved without having to use different networks for this purpose.

In the router operating mode, which is used by most users, the WALL IE forwards the data traffic between various IPv4 networks (Layer 3) and uses packet filters for limiting access to the automation network. In the process, address translation by way of Network Address Translation (NAT) is supported. The use of NAT also makes it possible to incorporate several automation cells of the same kind with the same address range into the production network. WALL IE supports two NAT functionalities in the router operating mode: Basic NAT (also referred to as "1:1 NAT" or "Static NAT") and NAPT (Network Address and Port Translation, also referred to as "1:N NAT" or "Masquerading").



WALL IE - Industrial NAT gateway / firewall

Secure online remote access

Not least, Helmholz also enables secure and simple online remote access: Especially mechanical engineers, but also production operations, use the REX industrial router to directly access the Ethernet networks of their machines and systems online, for example, for remote maintenance, for visualization, for gathering data, as well as for diagnostics and Web2Go (VNC and remote desktop) applications. The REX series, which covers a broad and application-specific range with the model series REX100 and REX200/250, offers various access possibilities for this via Ethernet, 3G, 4G, or WiFi.

The data transmission with all REX models generally takes place encoded via a VPN tunnel. The foundation for this is provided by the secure OpenVPN protocol. The Helmholz

myREX24 V2 IoT portal thereby serves as a mediation server for VPN communication between operators and their systems. This means that both sides can establish the VPN tunnel as an outgoing connection. Firewalls, as well as restrictions of services or cellular network operators are therefore no longer an issue. This is because they only affect data traffic into the network, but not out of the network. The outgoing connections are then briefly on hold until the VPN tunnel is established. The actual communication then takes place there via the IoT portal. The simple and intelligent user management and the quick configuration of the REX industrial routers has already convinced many customers when selecting among providers with similar systems. To this purpose, Helmholz offers a special test account that makes it possible for potential customers to thoroughly test the performance capability of the IoT portal in advance.

The Bottom Line

Whether Ethernet and PROFINET switches, NAT and fieldbus gateways, or secure IoT remote machine access: With current solutions from Helmholz, the high requirements of industrial networks in times of increasing automation can also be securely and efficiently fulfilled – including a high degree of operator comfort and optimal exploitation of the control cabinet width.

Helmholz GmbH & Co. KG
Hannberger Weg 2
91091 Großenseebach
Germany

Phone: +49 9135 7380-0
Fax: +49 9135 7380-110
info@helmholz.de
www.helmholz.de



IoT portal: myREX24 V2