

Success Story

Augmented security in the production network of ZF Sachs

ZF Sachs, an international automotive supplier for drive and chassis components headquartered in Schweinfurt / Germany, has permanently improved the security of its industrial networks. The starting point: a decentralized security architecture with industrial firewalls.



All photos: ZF Sachs AG / Germany

The reasons for stronger security in the production plants included virus problems in the office network. Compared to the manageable risk of an office computer infection, the risk potential for production facilities was considered to be significantly higher. In order to minimize the risk of possible disturbances or even production downtimes through faulty accesses or malware, ZF Sachs decided to implement additional security precautions.

Decentralized security philosophy

The task of the new security architecture was to protect the production plants from both undesirable external and internal accesses and limit the spread of infiltrating virus attacks.

Sealing off the office network from the production network was considered to be the most suitable strategy; this was carried out with a large firewall and structured security architecture (defense in depth), with which critical individual systems could also be safeguarded. The control and filtering of network traffic through firewalls took on a key role. More perfectly organized and distributed protection, along with the greater degree of flexibility for a typical industry network design and lower investment/operating costs: all these factors argued in favor of a decentralized architecture with firewalls. The segmentation through VLAN-compatible switches into logically separated segments was evaluated and

rejected, as virtual LANs were considered to be too difficult to control from a security point of view.

The automation technology and machine maintenance departments were responsible for the implementation, in coordination with the IT department. Along with the use of virus scanners in the production area, the most important measure became the segmentation of the production network into small and manageable machine networks. The assignment was conducted spatially based on building zones with additional Profinet components for individual installations. A total of 40 decentralized machine networks were implemented and each of these subnetworks was secured by an mGuard firewall from Phoenix Contact and Innominate.

“We evaluated different firewall security products under two main criteria. Industrial suitability with, e.g., an extended temperature range was particularly important to us. We also needed a solution that could be integrated as flexibly as possible and with a low level of complexity into our automation component environment,” says Asmund Hey, head of automation technology for ZF Sachs technical services, in explaining the decision for the mGuard security solution.



“A total of 40 decentralized machine networks were set up at ZF Sachs. Each of these subnetworks is protected by an mGuard firewall from Phoenix Contact and Innominate.”

Setting up decentralized firewalls

The implementation of the decentralized security architecture was based on the network structure plan. This describes the individual network segments and contains specifications concerning which device is attached to which port, as well as which IP addresses, MAC addresses, firmware version and product designations are given.

“To ensure that the decentralized architecture with 40 individual machine networks did not lead to greater configuration and operative effort, we first developed a basic set of common firewall rules for all subnetworks as an overriding control. The implementation was relatively simple,” reports Asmund Hey. For the rollout, the master parameters were read out from a memory chip upon start-up and applied to the subnetwork. This meant that most of the requirements were already covered. Only individual rules had to be added for special cases, e.g. for controller access to office server shares.

A three-month introductory and learning phase followed start-up, allowing any missing accesses or ports to be included. “During this phase, we realized how important a careful network architecture plan is. The more time invested here, the smaller the correction effort will be later. We also discovered the advantages of central device management,” says Asmund Hey, listing the most important experiences gained during the start-up.

Automation technology requirements

Various requirements need to be taken into account when setting up the decentralized security architecture. The production facility with Profinet components needed to be sealed off from disturbances from the network. The “8HP” (a torque converter for 8-gear automatic transmissions) requires TCP/IP communication on the level of Profinet protocols. In the process, a good deal of IP addresses had to be managed and a clear segmentation and sealing-off were necessary for the field bus components. As a jitter period of less than a microsecond is given for the response time behavior of the components in real time, they had to be consistently sealed off in a network to prevent disturbances like the typical broadcast. Therefore a dedicated network segment was reserved for the 8HP. A further requirement was 1:1 NAT (network address translation) for DNC (distributed numerical control) machines. This concerned the software for the distribution of the DNC programs running in the office network. Since the mGuard components support 1:1 NAT, no adjustments to the internal address space of the machines were necessary for the software.

Setting up port forwarding was a further important requirement, as central databases had to be accessed from the outside in the plant stations. Strict outgoing rules were also necessary. The spatial separation of plants leads to a distribution of the software and process data, which must then be centrally merged again on a server. Access to the central server is enabled through rules in the central firewalls, but any other uncontrolled access is prevented.

Decentralized firewalls have increased security

The mGuard security solution has been used at ZF Sachs for two years now. The decentralized firewalls in new plants or in plants with Profinet components are now equipped to protect against disturbances. “The decentralized networks run smoothly. There is nothing that halts the automation technology and operation continues largely without maintenance. We also successfully protected several older machines without virus protection from disturbances and attacks. Thanks to the segmentation, any virus brought in by a technician has not been able to spread into the network,” says Asmund Hey in summing up his experiences. And he has a good comparison, as the virus problem continues to be present in the office area or in old machines without firewall protection. Asmund Hey emphasizes that a secure production flow is also guaranteed when other network components fail. If this is the case, the firewall protects the plants from disruptive broadcasts or defective packages.

“The experiences we’ve had with the launch, operation and the security standard attained through the decentralized firewalls have all been very good. This is probably also due to the excellent support provided by Innominate. The response times are short, and if we have ideas or improvement suggestions, these are normally included in one of the next versions,” says Asmund Hey in describing the collaboration.

Further improvements are planned

One of the extensions under way now is setting up a central administration for the decentralized machine networks. Goals include standardization to the largest extent possible, uniform configuration and an easier administration of the networks. To this end, the Innominate Device Manager (IDM) is being introduced, which provides the status information of all administered components for a central monitoring. Finished configurations or updates can be transferred from the IDM to the decentralized firewalls. And a high degree of automation for the configuration of individual devices can be obtained through its template and inheritance technology.

Another project is related to the use of mGuards for remote maintenance. The plant manufacturer, but also the internal test equipment design, requires remote maintenance access. The employees at ZF Sachs have longstanding experience with remote maintenance. Through the new security architecture with the machines behind the firewall, however, a new solution needs to be found that is aligned with the altered security rules. The secure remote access via VPNs is therefore a highly interesting additional benefit provided by the mGuard protection.



About ZF Sachs / Germany

As the driveline and chassis components division of ZF Friedrichshafen AG, ZF Sachs AG is headquartered in Schweinfurt / Germany and employs a staff of 16,500 workers around the world. For more than 100 years, ZF Sachs has been a renowned partner of the automotive industry. Its products are not only used with traditional applications in cars, commercial vehicles, rail, construction and agricultural technology, but also in motorsports.

About Innominate Security Technologies AG

Innominate, a Phoenix Contact Company, is a leading supplier of components and solutions for controlled and secured communication in industrial networks. The German company specializes in the protection of networked industrial systems and the secure remote diagnosis and maintenance of machinery and equipment over the Internet. Its mGuard product line of network security appliances provides router, firewall, virtual private network (VPN), as well as quality of service (QoS) functionalities and helps with intrusion detection and antivirus protection. The mGuard portfolio is complemented by a highly scalable device management software. Innominate products are marketed worldwide under the mGuard brand through system integrators and OEM partners. Further information can be found at www.innominate.com.

Contact

Innominate Security Technologies AG
protecting industrial networks
Rudower Chaussee 13
12489 Berlin / Germany
Tel.: +49.30.921028-0
Fax: +49.30.921028-020
contact@innominate.com
www.innominate.com