Secure Network Segmentation for AdBlue Production

A high-performance industrial firewall helps companies in the chemical industry to securely segment their IT/OT networks – and to meet the requirements of the NIS-2 Directive.

PROTECTION FOR THE PLANT CONTROL SYSTEM IN CHEMICAL PARK

Dr. Wilhelm Greiner, journalist

In Geleen, Netherlands, lies one of Europe's largest chemical parks. On the 880-hectare site of the "Chemelot" chemical park – an allusion to Camelot, the legendary castle of King Arthur and his Knights of the Round Table – some 8,500 employees from over 200 companies work on chemical products and their further development. In 60 factories, they produce around 7.5 million tons of chemical products annually. Chemelot is not only an industrial area but also a research hub: round about 3,000 specialists and 1,200 students are conducting research here on the future of chemical products.

Project Description

The Customer:
Companies and plant operators in the Chemelot chemical park in Geleen, Netherlands.

The Task:
Chemical production facilities must be consistently protected against operational disruptions and cyberattacks. This requires the establishment of network segments for highly critical production systems and strict control of data traffic.

The Solution:
genuwall stands for "Security Made in Germany" and utilizes expertise from the classified industry sector. The industrial firewall segments production networks and reliably protects industrial facilities from unauthorized access.

To ensure that “the chemistry is always right” in everyday industrial and research operations, two things are needed: facilities for the reliable operation of production and a highly secure network to control the machines and systems. After all, according to the new EU directive NIS 2 (Network and Information Security Directive 2), the chemical industry is considered a “critical sector”. This means that chemical production facilities must be consistently protected against unauthorized access; otherwise, the operator faces heavy fines – and in a worst-case scenario, management is liable for inadequate or omitted measures.

The Challenge: Protecting Critical Facilities

The looming threat of the NIS-2 Directive exacerbates a dilemma facing virtually all manufacturing companies: On the one hand, modern production requires networked industrial plants. This is the only way for OT (Operational Technology) personnel to remotely monitor and control the equipment – via a network, potentially even the internet. And it’s the only way for operators to collect sensor data for AI analysis in the context of a “smart factory.” On the other hand, every network also carries risks, as attacks on corporate infrastructure typically originate from the internet. Here, dangers such as ransomware attacks, industrial espionage, and – particularly in the industrial sector – sabotage lurk.

The European Union introduced the NIS-2 Directive to improve the protection of critical infrastructures against cyberattacks and disruptions.

The NIS-2 Directive requires organizations to implement appropriate measures to ensure the security and resilience of their networks and information systems. These requirements include risk management, technical and organizational measures, incident reporting, as well as compliance and enforcement.

Therefore, it is essential to strictly isolate systems of high to highest criticality (levels 0 to 3 in the Purdue reference model) from less critical systems – for example, from ERP software (level 4) or the office LAN (level 5). Industrial firewalls provide the highest possible level of protection in this regard.

Industrial Firewalls for the AdBlue Production

In Geleen, nitrogen is produced, which is needed, for example, for fertilizers, as well as melamine, a basic material for resins, adhesives, and coatings. At the end of 2022, the site was expanded to include a plant for the production of the fuel additive AdBlue. One requirement was that the AdBlue tanks be protected according to state-of-the-art technology and remotely controllable. This was because the distance between the production facility and the AdBlue tanks on the expansive Chemelot site was approximately one kilometer, and various customers also had to be connected along this route.

This required connecting the plant controllers (Programmable Logic Controllers, PLCs) – HIMA HIMatrix Safety PLCs are used for this purpose – to the backbone network, and also to the SCADA PCS (Process Control System). These components operate at different Purdue levels. Therefore, a firewall must always be in place to ensure compliant data traffic.

Previous Solution: Too Complex, Too Few Ports

For years, the firewall technology of an international provider was relied upon for this purpose. However, their industrial firewalls have two major drawbacks: the firewall configuration is complex, and the devices only have two ports. Therefore, a separate firewall must be implemented and configured for each network connection between the PLC and the backbone, as well as between the PLC and the PCS.

For this reason, in the spring of 2023, the operators began searching for an easily configurable industrial firewall that could handle both tasks simultaneously. They consulted HIMA Paul Hildebrandt GmbH, with whom they had already enjoyed a very successful collaboration on automation projects more than 25 years.

AdBlue reduces emissions from diesel vehicles. At the end of 2022, the Chemelot chemical park was expanded to include a plant for the production of this fuel additive. Industrial firewalls from genua ensure protection in accordance with the NIS-2 Directive.

During the research, the Industrial Firewall genuwall from the German IT and OT security specialist genua, based near Munich, also came across and is recommended by Erik van Wouwe, Sales Manager Benelux at HIMA. Van Wouwe is well aware of the quality of German security technology, as HIMA operates a security lab in Bruehl together with genua.

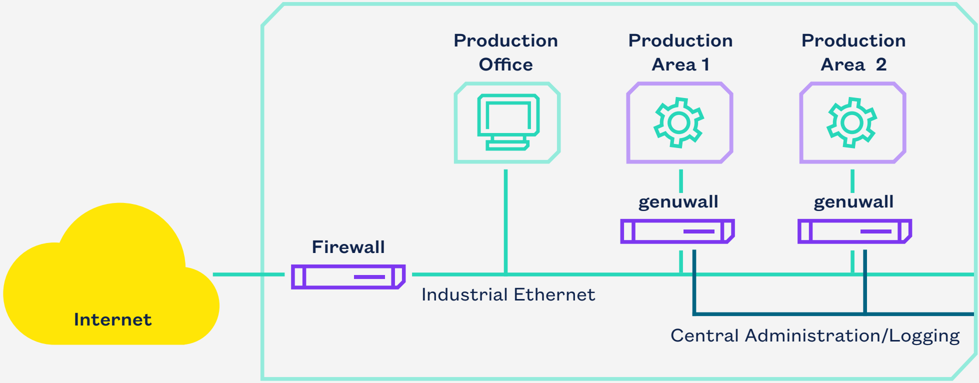
genuwall Offers a Very High Level of Protection

The Industrial Firewall genuwall offers “Security Made in Germany” and utilizes expertise from the classified information protection sector: It is based on the proven genua firewall genuscreen, which is certified as “EAL 4+” by the German Federal Office for Information Security (BSI) according to the international Common Criteria (CC) standard. The firewall is therefore demonstrably suitable for use in public sector networks as well as in critical infrastructure (KRITIS) environments – or, in NIS-2 terminology, for essential and important facilities.

For highly secure segmentation of industrial networks, genuwall detects and rejects unauthorized data packets from OT protocols (OPC UA, Modbus TCP, IEC 60870-5-104) down to the application level. This provides reliable protection against unauthorized access. The firewall can be quickly installed via USB boot and easily integrates into existing network environments. Management is possible both locally and – with the same high level of security – via a central management solution.

One Firewall, Up to Four Purdue Levels

In addition to the aforementioned advantages of genuwall, the responsible engineer noticed a seemingly trivial, yet crucial point: the firewall has four ports instead of just two. “genuwall allows us to set up zones, meaning we can implement the separation between the PLC and SCADA system, as well as between the PLC and the network backbone, with a single device,” he explains. “With four firewall ports, I can securely connect equipment with up to four



Network segmentation: Secure production areas through zoning with the Industrial Firewall genuwall.

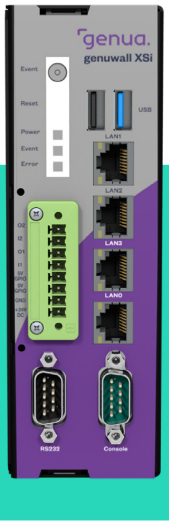
different Purdue levels. This means that a separate firewall is no longer needed for each data stream, as was previously the case." For the AdBlue project, this allowed the HIMA PLCs to be securely networked via HIMA's SafeEthernet protocol using genuwall, while communication between the PLC and SCADA system also runs securely via Modbus TCP.

This consolidation simplifies firewall management and device maintenance. genuwall proves its worth through its ease of use. Equally important in a chemical plant: with fewer devices to manage, faults can be isolated more easily and devices shut down more quickly – potentially providing a crucial time advantage in an emergency.

Fewer Devices, Less Effort, Lower Costs

Switching to genuwall devices from the German security specialist genua enables the consolidation of firewall operations at the Chemelot chemical park, significantly reducing both effort and costs. In the current AdBlue production plant project, a single genuwall replaces the two previously required industrial firewalls per PLC. Its intuitive operation simplifies both commissioning and maintenance.

Five genuwall devices are already in use on the Chemelot campus, and five more are to be added. This has brought together a new group of experts at Chemelot – not to search for the Holy Grail like its historical counterpart, but to reliably protect one of Europe's largest chemical parks from operational disruptions and cyberattacks.



The Industrial Firewall genuwall from the German manufacturer genua offers four firewall ports to enable zone creation.

Further Information:

genua.eu/genuwall

About genua

With its IT security solutions developed and produced in Germany, genua GmbH is a pioneering force in digital sovereignty. Government agencies, organizations subject to secrecy protection, and operators of critical infrastructures rely on genua to protect their critical and highly sensitive digital infrastructures.

genua's portfolio includes highly secure, backdoor-free, and scalable IT security products such as firewalls, gateways, quantum-resilient VPNs, remote maintenance systems, and complete solutions for mobile working with approval for processing classified information. Many products are also available as virtualised versions for flexible cloud integration. Regular certifications and approvals by the German Federal Office for Information Security (BSI) attest to the high level of security and quality.

With around 500 employees, genua GmbH is part of the Bundesdruckerei Group. The company is classified as a 'qualified manufacturer' by the BSI and its products are listed on the central purchasing platform for German federal authorities (Kaufhaus des Bundes). Its customers include BMW, the German Armed Forces, the THW, and the Würth Group.

Part of the Bundesdruckerei Group

bdr.

genua GmbH

Domagkstrasse 7 | 85551 Kirchheim, Germany
+49 89 991950-0 | info@genua.eu | www.genua.eu