genua.

# An Industrial Data Diode for Especially Critical Plants and Processes

For monitoring or for process optimization, well-isolated production plants also need to be digitally networked. For especially critical plants, a direct connection is, however, extremely problematic. Security concerns therefore frequently outweigh the automation advantages. cyber-diode from genua represents a highly secure and suitable technology for current automation requirements.

SecurITy made in Germany

# Content.

# 1. Old and New Plants are to be Monitored and the Processes Optimized

Operators of plants and machinery expect the highest possible productivity and availability. Process monitoring is, therefore, a very effective instrument for plant efficiency. It does, however, require online access to the plants. This significantly increases security risks.

All plants and machinery that send data over the Internet are, in principle, vulnerable via this path. If systems are to be digitally networked, they must therefore be protected from infection by malicious software and other forms of unauthorized access. Subject to a particularly high protection requirement are systems that control critical infrastructure or other plants where incorrect functioning could lead to extensive damage or loss of life, e.g., power station turbines, chemical production plants and industrial robots on production lines.

Classic IT security solutions cannot usually be used in production environments (operational technology, OT). Many plants run on outdated operating systems. It is often not possible to implement security updates or retrofitted hardening measures. Moreover, the plants – with life cycles of 30 or more years – usually have a low security level. Among others, the User Association of Automation Technology in Process Industries (NAMUR) therefore set the goal with the NAMUR Open Architecture (NOA) of making production data easily and securely usable for plant and device monitoring and for optimizations – even for existing plants (Brownfield).

**Highly secure monitoring – also for older industrial plants.**

# 2. Effective Cyber Protection for Well-Isolated Plants

One of the key questions of current automation strategies is how well can isolated plants be protected against unauthorized access. For the direct extraction of process data, the NANUR initiative proposes a secure one-way channel in addition to the existing automation structures. On this second channel, the data can be transferred non-reactively.

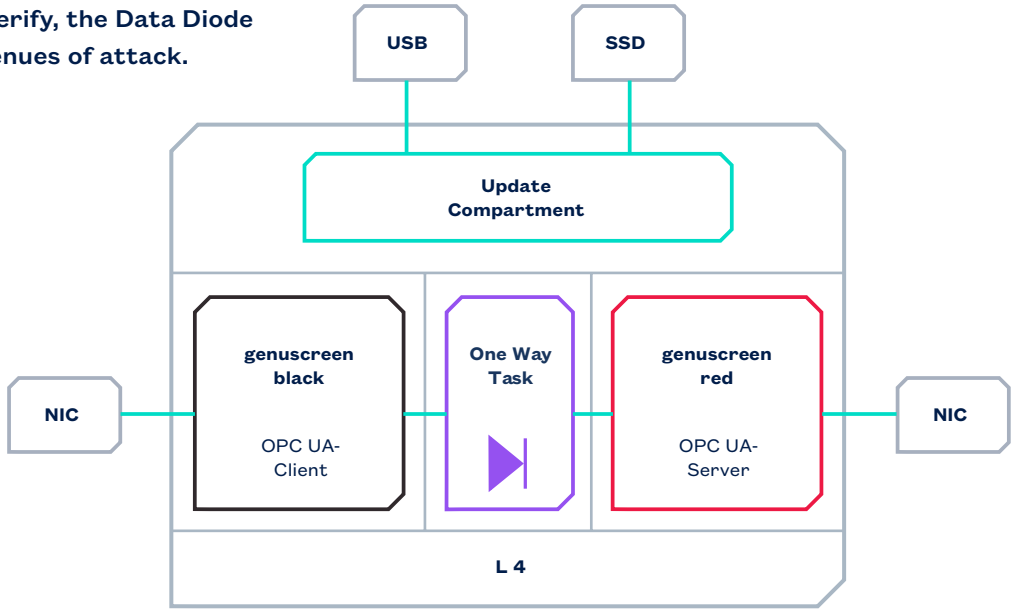
„It must be ensured that there is absolutely no undesired and uncontrolled feedback from the second communication channel that changes the primary communication or the primary systems in any way," according to the NAMUR specification. Security of the data transfer is to be ensured by a diode that prevents undesired and uncontrolled feedback.

Up until now, fiber optic diodes have been used for the data connection of isolated plants. Fiber optic diodes are not without disadvantages, however. Even if transferred multiple times, there is no guarantee that the sent data is received error-free and in full. Moreover, the data throughput is very low, as the receiver provides no information about the possible bandwidth of the data connection. Lastly, the use of fiber optic diodes is often associated with high costs.

**The data diode cyber-diode from genua is an alternative to the fiber optic diode. It combines high security standards with current automation requirements at a relatively low cost.**

# 3. Secure, Industry-Grade Data Diode with Hardened Protective Functions

**The Data Diode cyber-diode enables a secure, one-way data transfer through the use of multiple, complementary security measures (Defense in Depth). The industry-grade security hardware is complemented by hardened software (Security Appliance). Though components that are kept simple and functionality that is as straightforward as possible and easy to verify, the Data Diode cyber-diode offers minimal avenues of attack.**




### Core component – L4 microkernel

The L4 microkernel divides the hardware into various isolated areas: the black side (genuscreen black) for data extraction, the red side (genuscreen red) for data provision as well as the „one way task“ for passing the data from black to red. The black and red sides of the diode are two virtually separated devices with their own, specially hardened OpenBSD operating system. Both genuscreens are based on certified and approved products.

### Hardened operating system

The minimalistic and hardened OpenBSD operating system of the genuscreen devices and the minimalistic microkernel are, with a very small number of lines of code compared to the millions of lines in a standard operating system, reduced to the bare essentials and thereby offer minimal avenues of attack.

### Highly secure boot process

The system can only be booted using a signed software application with unalterable code (secure boot). The signature of the kernel and of the software is verified during the boot process.

### One-way data transfer

The „one-way task“ has just one job. Through a secured communication mechanism of the microkernel, it transfers the data in only one direction to the red side.

**Microkernel and genuscreen components based on BSI-approved products**
The secure diode function is also protected on the black side and on the red side by a firewall. Encryption of the data transfer takes place via the VPN functions of the genuscreen technology. The components of the cyber-diode satisfy the highest security requirements and are based on the core capabilities of sister products that are certified according to Common Criteria (CC) EAL 4+.

**Hardened protective function**
Through the tiered security measures, the system design ensures that the protective functions can be neither switched off nor changed as a result of configuration errors (Security by Design). Security gaps caused by external software or a changed operating system are thereby prevented. As a result, even complex cyber attacks are unable to gain a foothold.

**State of the art**
cyber-diode corresponds to the current state of the art of security technology and is approved in a technically similar version as the vs-diode by the BSI for use up to the high classification level „SECRET."

# 4. A Data Diode with Delivery Guarantee

**Unlike fiber optic diodes, cyber-diode makes a delivery guarantee possible.**

**Confirmation bit**
At the end of the data transfer, a status message is transmitted via a limited feedback channel. This allows the receiver to send back a signal to the sender to confirm that all data has been completely and correctly received. This feedback consists of only a status bit (OK/not OK).

**Delivery guarantee**
The status bit serves to confirm that the receiver, or the red side of the diode, has received the data (guaranteed delivery).

**Maximum transmission speed**
The delivery guarantee enables a maximum transmission speed or a maximum technical throughput. The cyber-diode permits a transfer rate of up to 1 Gbit/s; for TCP up to 400 Mbit/s is possible.

**Supported protocols**
cyber-diode supports protocols OPC UA, FTP, SMTP, TCP, UDP as well as Syslog.

**Logging information**
The Syslog data for connection establishment and for the data flow can be used by a higher-level monitoring system or by a SIEM system for evaluation purposes.

**Central Management Station**
Companies that already use other components from genua can administer these together with the cyber-diode from a single location.

# 5. Support of Industry 4.0 Protocol OPC UA

**The Data Diode cyber-diode supports the Industry 4.0 protocol Unified Architecture (OPC UA) for data extraction. Because OPC UA requires a bi-directional communication between client and server, an OPC-UA client was implemented in the diode on the black side and an OPC-UA server was implemented on the red side.**

### Open standard

OPC UA is an open standard for the exchange of machine data. In plants in the manufacturing and process industry, for example, it supports secure, reliable and manufacturer- and platform-independent communication.

### From the field level to the cloud:

OPC UA can be used for the data connection of sensors and actuators from the field level to the cloud, independent of the previous restrictions of the classic automation pyramid.

### Encrypted VPN

With the VPN Appliance genuscreen, the cyber-diode also supports the encrypted transfer of machine data via its own virtual private network (VPN) using Internet Protocol Security (IPSec). All communication is thereby protected against unauthorized access. This applies as well for internal communication, such as between various security zones of the network. In addition, no one can intercept, modify or again transfer the data traffic.


**cyber-diode supports the Industry 4.0 protocol Unified Architecture (OPC UA). This is an open standard to exchange machine data.**

# 6. Use for Current Automation Requirements

With the cyber-diode as an industrial data diode, the communication restrictions of the traditional automation structures can be overcome. Plants, machinery, and general IT systems can send data to the outside via non-secure networks without risking their integrity. Critical zone and domain interfaces are protected feedback-free. cyber-diode is also suitable for one-way data transfer between different security zones within a production network.

The current possibilities afforded by the Industrial Internet of Things (IIoT), Industry 4.0 and various cloud applications from data analytics to the digital twin can thereby be used.

Thanks to OPC-UA data transfer, monitoring and process optimization applications are no longer tied to proprietary protocols. They become simpler and more economical. As a result, the core process automation (Core Process Control, CPC) in the process industry can, according to the NAMUR initiative, remain largely unaffected in order to make Industry 4.0 innovations available even in old plants.

**cyber-diode allows only one-way data transfer between different security zones within a production network.**

## Further information:

www.genua.eu/cyber-diode

## About genua

genua GmbH is a proponent of the digital transformation. We secure sensitive IT networks in the public and enterprise sectors, for critical infrastructure organizations, and in industries with an obligation to maintain secrecy with highly secure and scalable cyber security solutions.

In doing so, genua GmbH focuses on the comprehensive protection of networks, communication and internal network security for IT and OT. The range of solutions spans from firewalls & gateways, VPNs, remote maintenance systems, internal network security and cloud security to remote access solutions for mobile employees and remote workers.

genua GmbH is a subsidiary of the Bundesdruckerei Group. With more than 300 employees, it develops and produces IT security solutions exclusively in Germany. Since the founding of the company in 1992, regular certifications and approvals from the German Federal Office for Information Security (BSI) provide proof of the high security and quality standards of the products. Customers include, among others, Arvato Systems, BMW, the German Armed Services, Federal Agency for Technical Relief (THW) as well as the Würth Group.

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