genua.

Eine industrielle Datendiode für besonders kritische Anlagen und Prozesse

Für Monitoring oder zur Prozessoptimierung müssten auch gut abgeschottete Produktionsanlagen digital vernetzt werden. Für besonders kritische Anlagen ist eine direkte Kopplung allerdings höchst problematisch. Häufig überwiegen deshalb die Sicherheitsbedenken die Automatisierungsvorteile. Mit cyber-diode von genua liegt eine hochsichere und geeignete Technologie für aktuelle Automatisierungsanforderungen vor.

SecurITy made in Germany

Inhalt.

1. Alte und neue Anlagen sollen überwacht und die Prozesse optimiert werden 3

2. Ein wirksamer Cyber-Schutz für gut abgeschottete Anlagen 4

3. Sichere industrietaugliche Datendiode mit gehärteten Schutzfunktionen 5

4. Eine Datendiode mit Zustellungsgarantie 7

5. Unterstützung des Industrie-4.0-Protokolls OPC UA 8

6. Einsatz für aktuelle Automatisierungs-anforderungen 9

1. Alte und neue Anlagen sollen überwacht und die Prozesse optimiert werden

Betreiber von Maschinen und Anlagen erwarten höchstmögliche Produktivität und Verfügbarkeit. Die Prozessüberwachung ist daher ein sehr effektives Instrument für die Anlageneffizienz. Sie erfordert allerdings einen Online-Zugang der Anlagen, dadurch steigen die Sicherheitsrisiken erheblich.

Maschinen und Anlagen, die via Internet Daten senden, sind über diesen Weg prinzipiell auch angreifbar. Sollen Systeme digital vernetzt werden, müssen sie deshalb vor eindringender Malware und unbefugten Zugriffen geschützt werden.

Besonders hohen Sicherheitsbedarf haben Systeme, die kritische Infrastrukturen (KRITIS) oder andere Anlagen steuern, von deren fehlerfreier Funktion hohe Sachwerte oder gar Leben abhängen: z. B. Turbinen in Kraftwerken, chemische Fertigungsanlagen oder Industrieroboter in Produktionsstraßen.

Klassische IT-Sicherheitslösungen sind für Produktionsumgebungen (Operational Technology, OT) meistens nicht anwendbar. Viele Anlagen laufen auf veralteten Betriebssystemen. Sicherheits-Updates oder nachträgliche Härtungsmaßnahmen können häufig nicht umgesetzt werden. Zudem haben die Anlagen mit Lebenszyklen von 30 und mehr Jahren meist nur ein geringes Sicherheitsniveau.

Deshalb hat sich u. a. die Interessengemeinschaft Automatisierungstechnik der Prozessindustrie (NAMUR) mit der NAMUR Open Architecture (NOA) zum Ziel gesetzt, Produktionsdaten einfach und sicher für eine Anlagen- und Geräteüberwachung (Monitoring) und für Optimierungen nutzbar zu machen – und das auch für bestehende Anlagen (Brownfield).

2. Ein wirksamer Cyber-Schutz für gut abgeschottete Anlagen

Eine der Kernfragen aktueller Automatisierungsstrategien ist, wie gut abgeschottete Anlagen vor ungewünschten Zugriffen geschützt werden können. Die NAMUR-Initiative schlägt zur direkten Ausleitung von Prozessdaten einen sicheren One-Way-Kanal vor, zusätzlich zu den vorhandenen Automatisierungsstrukturen. Auf diesem zweiten Kanal können die Daten rückwirkungsfrei übertragen werden.

„Es muss sichergestellt sein, dass es keinerlei ungewollte und unkontrollierte Rückmeldungen aus dem zweiten Kommunikationskanal gibt, die die primäre Kommunikation oder die primären Systeme in irgendeiner Weise verändern“, so die NAMUR-Vorgabe. Für die Sicherheit des Datentransfers soll eine Diode sorgen, die ungewollte und unkontrollierte Rückmeldungen verhindert.

Für die Datenanbindung abgeschotteter Anlagen werden bisher Glasfaserdioden eingesetzt. Glasfaserdioden haben allerdings Nachteile: Es gibt selbst bei mehrfacher Übertragung keine Garantie für den fehlerfreien und vollständigen Empfang der gesendeten Daten. Außerdem ist der Datendurchsatz sehr gering, da es keine Informationen des Empfängers über die mögliche Bandbreite der Datenverbindung gibt. Schließlich ist der Einsatz von Glasfaserdioden oft mit hohen Kosten verbunden.

3. Sichere industrietaugliche Datendiode mit gehärteten Schutzfunktionen

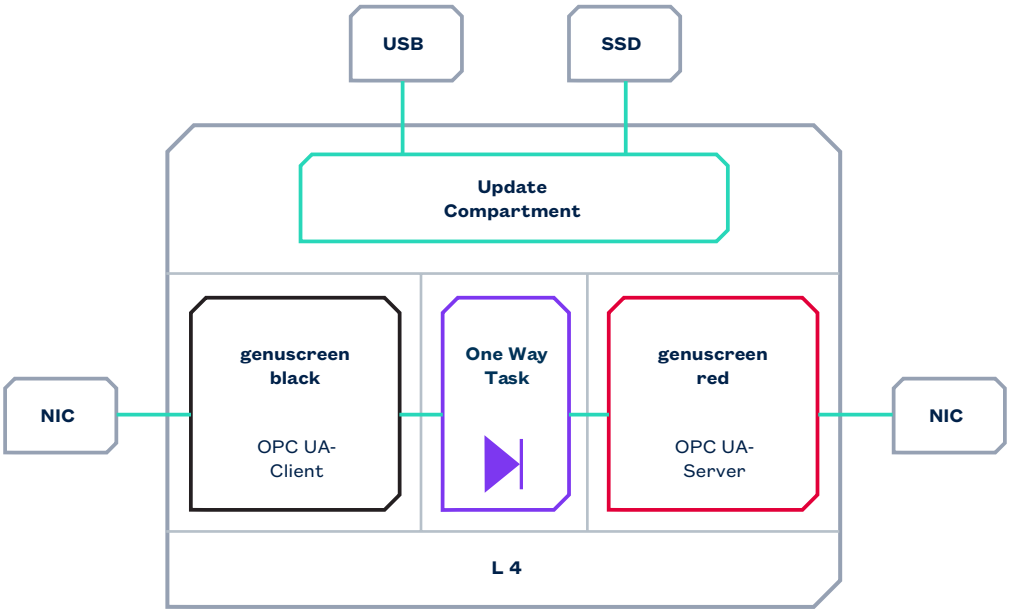
Die Datendiode cyber-diode ermöglicht einen sicheren Einbahn-Datentransfer, indem sie mehrere, sich ergänzende Sicherheitsmaßnahmen einsetzt (Defense in Depth). Die industrietaugliche Sicherheits-Hardware wird durch eine gehärtete Software (Security Appliance) ergänzt. Durch einfach gehaltene Komponenten und eine möglichst einfache und leicht überprüfbare Funktionalität bietet cyber-diode eine geringstmögliche Angriffsfläche.

Kernkomponente L4-Mikrokernel

Der L4-Mikrokernel unterteilt die Hardware in verschiedene abgeschottete Bereiche: die schwarze Seite (genuscreen black) zur Datenextraktion, die rote Seite (genuscreen red) zur Datenbereitstellung sowie den „One Way Task“ zur Weiterleitung der Daten von Schwarz nach Rot. Die schwarze und die rote Seite der Diode sind zwei virtualisierte, getrennte Komponenten mit einem eigenen, speziell gehärteten OpenBSD-Betriebssystem. Beide genuscreen-Komponenten basieren auf zertifizierten und zugelassenen Produkten.

Gehärtetes Betriebssystem

Das minimalistische und gehärtete OpenBSD-Betriebssystem der genuscreen-Komponenten und der minimalistische Mikrokernel sind mit wenigen Zeilen Code im Vergleich zu Millionen Zeilen Code eines Standard-Betriebssystems auf das Allernotwendigste reduziert. Der Code kann Zeile für Zeile überprüft werden, um Fehler auszuschließen.



Schematische Darstellung von cyber-diode

Hochsicherer Boot-Vorgang

Das System kann nur über eine signierte Software mit nicht veränderbarem Code gebootet werden (Secure Boot). Die Signatur des Kernels und der Software wird beim Bootvorgang überprüft.

Einbahn-Datentransfer

Der „One Way Task“ hat nur eine Aufgabe. Durch einen abgesicherten Kommunikationsmechanismus des Mikrokernels überträgt er die Daten in nur einer Richtung an die rote Seite.

Mikrokernel und genuscreen-Komponenten auf Basis zertifizierterProdukte

Die sichere Diodenfunktion wird auf der schwarzen und auf der roten Seite zusätzlich durch eine Firewall geschützt. Über die VPN-Funktionen der genuscreen-Komponenten erfolgt die Verschlüsselung des Datentransfers. Die Komponenten der cyber-diode erfüllen höchste Sicherheitsanforderungen und basieren auf Kernfähigkeiten von Schwesterprodukten, die nach Common Criteria (CC) EAL 4+ zertifiziert sind.

Gehärtete Schutzfunktion

Das Systemdesign sorgt durch die gestaffelten Sicherheitsmaßnahmen dafür, dass die Schutzfunktionen weder ausgeschaltet noch durch Konfigurationsfehler verändert werden können (Security by Design). Dadurch werden Sicherheitslücken durch Fremd-Software oder ein verändertes Betriebssystem unterbunden. So finden auch komplexe Cyber-Attacken keine Angriffspunkte.

State of the Art

cyber-diode entspricht dem aktuellen Entwicklungsstand der Sicherheitstechnologie (State of the Art). Die technisch ähnliche Datendiode vs-diode ist vom BSI für den Einsatz bis zur hohen Geheimhaltungsstufe „GEHEIM“ zugelassen.

> Cyberangriffe können den Produktionsablauf kritischer Unternehmen empfindlich stören und sogar deren Existenz bedrohen. cyber-diode schützt vernetzte Industrieanlagen zuverlässig vor solchen Bedrohungen.
>
> **Dr. Alexander Horch, Vice President Research, Development & Product Management, HIMA Paul Hildebrandt GmbH**

4. Eine Datendiode mit Zustellungsgarantie

Bestätigungs-Bit

Am Ende des Datentransfers wird über einen limitierten Feedback-Kanal eine Statusmeldung übermittelt. Der Empfänger meldet an den Sender zurück, ob alle Daten korrekt und komplett angekommen sind. Dieses Feedback besteht lediglich aus einem Status-Bit (o.k./nicht o.k.).

Zustellungsgarantie

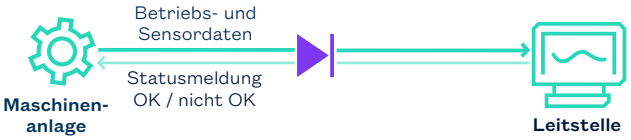
Mit dem Status-Bit wird bestätigt, dass der Empfänger bzw. die rote Seite der Diode die Daten erhalten hat (garantierte Zustellung).

Maximale Übertragungsgeschwindigkeit

Durch die Zustellungsgarantie wird eine maximale Übertragungsgeschwindigkeit bzw. ein technisch maximaler Durchsatz ermöglicht. cyber-diode lässt eine Übertragungsrate von bis zu 1 Gbit/s zu, für TCP sind bis zu 400 Mbit/s möglich.

Unterstützte Protokolle

cyber-diode unterstützt die Protokolle OPC UA, FTP, FTPS, SMTP, TCP, UDP und Syslog.



Logging-Informationen

Die Syslog-Daten zum Verbindungsaufbau und zum Datenfluss können durch ein übergeordnetes Monitoring oder durch ein SIEM-System zur Auswertung genutzt werden.

Central Management Station

Unternehmen, die bereits andere Lösungen von genua einsetzen, können diese zusammen mit cyber-diode zentral administrieren.

Im Unterschied zu Glasfaserdioden bietet cyber-diode eine Zustellungsgarantie.

5. Unterstützung des Industrie-4.0-Protokolls OPC UA

Die Datendiode cyber-diode unterstützt das Industrie-4.0-Protokoll Unified Architecture (OPC UA) zur Datenausleitung. Da OPC UA eine bidirektionale Kommunikation zwischen Client und Server erfordert, wurde in der Diode ein OPC UA-Client auf der schwarzen Seite und ein OPC UA-Server auf der roten Seite umgesetzt.

Offener Standard

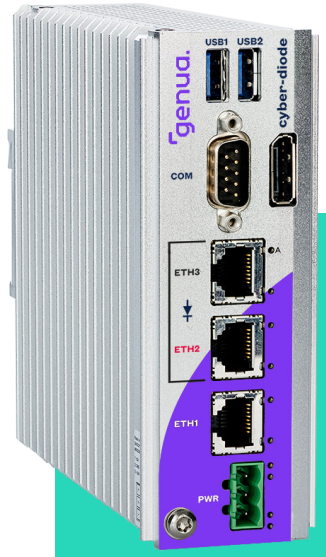
OPC UA ist ein offener Standard für den Austausch von Maschinendaten. Er unterstützt z. B. in Anlagen der Fertigungs- und Prozessindustrie eine sichere, zuverlässige, hersteller- und plattformunabhängige Kommunikation.

Feldebene bis in die Cloud

OPC UA kann für die Datenanbindung von Sensorik und Aktorik von der Feldebene bis in die Cloud eingesetzt werden, unabhängig von den bisherigen Einschränkungen der klassischen Automationspyramide.

VPN-verschlüsselt

Mit der VPN-Appliance genuscreen unterstützt cyber-diode den verschlüsselten Versand der Maschinendaten auch über ein eigenes Virtual Private Network (VPN) per Internet Protocol Security (IPSec). Damit wird jede Kommunikation gegen unbefugte Zugriffe geschützt. Dies gilt auch für die interne Kommunikation bspw. zwischen unterschiedlichen Sicherheitszonen des Netzwerkes. Zudem kann niemand den Datenverkehr abhören, modifizieren oder nochmals einspielen.



cyber-diode von genua unterstützt OPC Unified Architecture (OPC UA)- einen offenen Standard für den Austausch von Maschinendaten.

6. Einsatz für aktuelle Automatisierungsanforderungen

Mit cyber-diode als industrieller Datendiode werden die Kommunikationsbeschränkungen der traditionellen Automatisierungsstrukturen überwunden. Maschinen, Anlagen und generell IT-Systeme können über unsichere Netze hinweg Daten nach außen versenden, ohne dass ihre Integrität gefährdet wird. Kritische Zonen- und Domänenübergänge werden rückkopplungsfrei geschützt. Auch für Einbahn-Datentransfers zwischen unterschiedlichen Sicherheitszonen innerhalb eines Produktionsnetzes ist cyber-diode geeignet.

Damit können die aktuellen Möglichkeiten genutzt werden, die sich durch das industrielle Internet der Dinge (IIoT), Industrie 4.0 und vielfältige Cloud-Anwendungen von Data Analytics bis zum digitalen Zwilling bieten.

Anwendungen zum Monitoring und für Prozessoptimierungen sind dank der OPC UA-Datenübertragung nicht mehr an proprietäre Protokolle gebunden. Sie werden einfacher und preiswerter. So kann gemäß der NAMUR-Initiative die Kern-Prozessautomatisierung (Core Process Control, CPC) in der Prozessindustrie weitgehend unbeeinflusst bleiben, um Industrie-4.0-Innovationen auch in Altanlagen verfügbar zu machen.

NAMUR Open Architecture: cyber-diode als NOA Security Gateway

Um die Entwicklung marktreifer Lösungen für die NAMUR Open Architecture (NOA) zu beschleunigen, haben NAMUR (Interessengemeinschaft Automatisierungstechnik der Prozessindustrie) und ZVEI (Verband der Elektro- und Digitalindustrie) das NOA Implementation Project 2025 initiiert.

genua ist Projektpartner und arbeitet mit weiteren Herstellern und Anwenderunternehmen unter anderem an der Ausgestaltung des Security Gateways der NAMUR Open Architecture. Das NOA Security Gateway ermöglicht Einbahn-Datentransfers von innen nach außen, ein Zugriff von außen auf die Automatisierungstechnik oder das Manipulieren von Daten ist nicht möglich. Diese wichtige Funktion übernimmt die Datendiode cyber-diode von genua.

Weitere Informationen:

www.genua.de/cyber-diode

0425-02-DE

Über genua

Die genua GmbH sichert sensitive IT-Netzwerke im Public- und im Enterprise-Sektor, bei KRITIS-Organisationen und in der geheimschutzbetreuten Industrie mit hochsicheren und skalierbaren Cyber-Security-Lösungen. Dabei fokussiert sich das Unternehmen auf den umfassenden Schutz von Netzwerken sowie auf die interne Netzwerksicherheit für IT und OT. Das Lösungsspektrum umfasst Firewalls und Gateways, VPNs, Fernwartungssysteme, interne Netzwerksicherheit und Cloud Security bis hin zu Remote-Access-Lösungen für mobiles Arbeiten.

Die genua GmbH ist ein Unternehmen der Bundesdruckerei-Gruppe. Mit mehr als 400 Mitarbeitenden entwickelt und produziert sie IT-Security-Lösungen ausschließlich in Deutschland. Seit der Unternehmensgründung in 1992 belegen regelmäßige Zertifizierungen und Zulassungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) den hohen Sicherheits- und Qualitätsanspruch der Produkte. Zu den Kunden zählen u. a. Arvato Systems, BMW, die Bundeswehr, das THW sowie die Würth-Gruppe.

genua GmbH
Domagkstraße 7 | 85551 Kirchheim bei München
+49 89 991950-0 | info@genua.de | www.genua.de