



Zehn Jahre Secure OT für cybersichere Maschinen

## INDUSTRIAL NAT-GATEWAY UND FIREWALL WALL IE VON HELMHOLZ FEIERT JUBILÄUM

Cybersichere Maschinennetzwerke werden mit den aktuellen Vorgaben der Europäischen Maschinenverordnung und der IEC 62443 für jeden Pflicht, der Maschinen in Verkehr bringt. Helmholtz hat diese Herausforderung schon viel früher erkannt und eine ebenso wirkungsvolle wie einfach konfigurierbare Lösung für vernetzte Maschinen und Produktionsanlagen entwickelt: Vor genau zehn Jahren kam das erste Security Gateway – Industrial NAT-Gateway/Firwall WALL IE auf den Markt.

Mit dem Siegeszug der Ethernet-Vernetzung in Maschinen und Produktionsanlagen muss dort auch die Cybersecurity eine ganz zentrale Rolle spielen. Diese Notwendigkeit schlägt sich dementsprechend in der aktuellen Normen- und Richtlinien-Situation nieder: Die 2023 zuletzt überarbeitete internationale Normenreihe IEC 62443 zum Beispiel befasst sich mit der Cybersecurity von „Industrial Automation and Control Systems“ (IACS) und verfolgt dabei einen ganzheitlichen Ansatz für Betreiber, Integratoren und Hersteller. Auch die Europäische Union hat den Ernst der Lage erkannt und reagiert darauf etwa mit der NIS-2-Richtlinie (Network and Information Security Directive, seit 2023 in Kraft), dem Cyber Resilience Act (CRA) und der neuen Europäischen Maschinenverord-

nung 2023/1230. Letztere ist ab dem 20. Januar 2027 für das Inverkehrbringen von Maschinen anzuwenden.

### MASCHINENNETZE SICHER INTEGRIEREN

Nicht nur diese aktuellen Vorgaben zeigen: Das Thema Maschinensicherheit geht inzwischen jeden an. Dabei geht es im Kern darum, Maschinennetze sicher in das übergeordnete Produktionsnetzwerk zu integrieren. Das Stichwort ist hier „Secure OT“ – also sichere operative Technologie aus Software und Hardware zur Steuerung, Absicherung und Kontrolle von industriellen Steuerungssystemen, Geräten und Prozessen.

Angesichts wachsender Datenkommunikation führt vor diesem Hintergrund

kein Weg an der Trennung bzw. Segmentierung von Netzwerken vorbei. Konzepte mit Vertrauens-Zonen und sicheren Zonenübergängen (Zones & Conduits) haben sich hierfür als besonders wirksam erwiesen. Deshalb schreibt auch die IEC 62443 ein entsprechendes Schutzkonzept vor: Demnach ist es für große oder komplexe Systeme oft nicht angebracht, den gleichen Schutzbedarf für alle Komponenten zu verwenden, da diese unterschiedliche Bedrohungen und Risiken aufweisen. Unterschiede können durch das Konzept der „Sicherheitszone“ dargestellt werden.

### ROBUSTE UND KOSTENGÜNSTIGE ABSICHERUNG MIT WALL IE

An diesem Punkt stellt sich die Frage, wie ein solches Zones & Conduits-Schutz-

# Ihr Netzwerk Coach – Die Helmholz Industrial Security Gateways

**Hohe Sicherheit**  
durch Zugriffsbeschränkung  
mittels Paketfilter (IPv4-Adressen,  
Protokoll (TCP/UDP), Ports,  
MAC-Adressen).

**Zeitersparnis**  
durch Übersetzung  
IP Integration ohne Änderung  
der bestehenden Netzwerkkonfiguration  
der Maschine (NAT).



© Helmholz GmbH & Co. KG

**Reibungsloser  
Produktionsablauf**  
durch Netzwerksegmentierung  
für mehr Performance im Netzwerk.  
Durch Filterung von Broadcasts und  
Multicasts.



konzept für vernetzte Maschinen konkret umgesetzt werden kann. Der Markt hält dafür zahlreiche Highend-Lösungen bereit, die allerdings für die Absicherung einer einzelnen Maschine meist überdimensioniert sind. Das heißt in aller Regel auch: überkomplex und nicht zuletzt unnötig teuer. Vor allem der mittelständische Maschinenbau und seine Kunden suchen daher nach praktikableren Lösungen, die nicht nur sicher und zuverlässig sein sollen, sondern auch schlank, effizient und einfach ohne weiteren externen Support einsetzbar.

Eine solche Lösung ist seit 2015 das Industrial Security Gateway WALL IE von Helmholz: Einmalig und dauerhaft zwischen der Maschine und dem Produktionsnetzwerk installiert, verbindet die

robuste und besonders kompakte Ethernet-Komponente Bridge- und Firewall-Funktionen im tatsächlich notwendigen Umfang.

Konkret schützt die Komponente die Netze, indem sie genau regelt, welcher Teilnehmer mit welchem Gerät Daten austauschen darf. Die Voraussetzung dafür schafft eine Paketfilter-Funktionalität: Damit lässt sich der Zugriff zwischen dem Produktionsnetzwerk und der Automatisierungszelle einschränken. Mit dem WALL IE können dann IP-Adressen, Ports, MAC-Adressen und die Telegrammart in beide Richtungen gefiltert werden.

Gleichzeitig ermöglicht der WALL IE auch eine Anpassung der vorhandenen IP-Ad-

ressen der Maschine an die IP-Adressen im Fabriknetzwerk durch NAT (Network Address Translation). Dabei wird jedem Gerät in der Maschine – welches nach außen sichtbar sein soll - eine IP-Adresse im Adressraum der Fabrik zugeordnet. Geräte in der Maschine, die nicht mit der Außenwelt kommunizieren sollen, werden hierbei einfach ausgenommen. Die Verwendung von NAT ermöglicht es darüber hinaus auch, mehrere gleichartige Automatisierungszellen mit gleichem Adressbereich in das Produktionsnetz einzubinden, ohne die Maschinen umzukonfigurieren zu müssen.

Für den Fall, dass im Fabriknetzwerk nicht genug IP-Adressen zur Verfügung stehen, kann der WALL IE auch mit einer einzigen IP-Adresse im Fertigungsnetzwerk eingebunden werden. Der Zugriff auf die Geräte in der Maschine erfolgt dann über Portforwarding. Die Filterung und der Schutz funktionieren immer in beide Richtungen. Somit kann auch ein Fabriknetzwerk vor kompromittierten Geräten in der Maschine geschützt werden.

Als weitere Besonderheit kann der WALL IE neben dem NAT-Betriebsmodus auch als Bridge eingesetzt werden. Im Bridge Mode haben die Netzwerkteilnehmer der Maschine bereits IP-Adressen im gleichen Bereich wie das Fabriknetzwerk. Alle Filterfunktionen sind aktiv, nur NAT ist hierbei abgeschaltet.



Das Helmholz Portfolio für Security Gateways in den Bauformen: Plus, Standard, Compact. Variantenabhängig auch für Gigabit Ethernet-Netzwerke.

© Helmholz GmbH & Co. KG

## NOCH MEHR MÖGLICHKEITEN IM JUBILÄUMSJAHR

Seit der Markteinführung des Industrial Security Gateway WALL IE vor genau zehn Jahren hat sich dieser inzwischen in über 15.000 Anwendungen bewährt. Größtenteils auf konkrete Kunden-Anfragen hin wächst der Funktionsumfang seitdem ständig, auch im Jubiläumsjahr: Zu den jüngsten Neuerungen zählt die Implementierung von 802.1X zur Authentifizierung. Über diese neue Funktion lässt sich vom Endkunden im Fabriknetzwerk sicherstellen, dass keine unerlaubten Geräte im Netzwerk aktiv werden.

Zusätzlich wurden Funktionen wie erweitertes Logging und ein verbessertes Benutzermanagement implementiert. Weitere Features wie z. B. Ping und Traceroute werden in Zukunft im Webinterface integriert. Darüber hinaus passt Helmholz die Firmware des WALL IE permanent an die spezifischen Anforderungen der IEC 62443-4-2 an.

Die Konfiguration des WALL IE kann jederzeit heruntergeladen, gesichert und bei Bedarf editiert werden.

Auch mit diesen Erweiterungen bleibt Helmholz dem Anspruch treu, dass für die Inbetriebnahme des WALL IE Netzwerk-Basiswissen ausreicht. So ist beispielsweise keine Anpassung der Netzkonfiguration im LAN-Netz notwendig. Zudem lassen sich Serienmaschinen mit gleichen IP-Adressen einfach in ein großes Fabriknetzwerk integrieren.

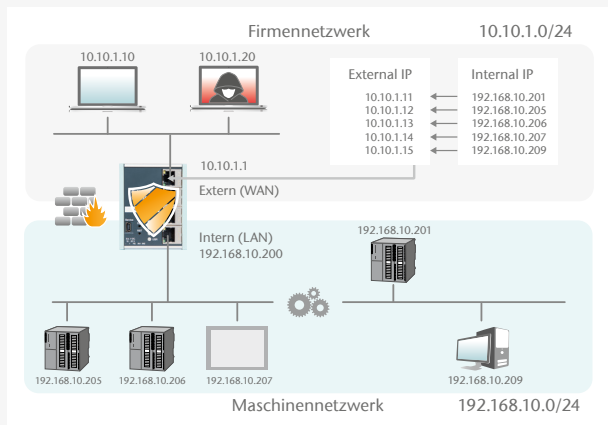
### FAZIT

**Seit inzwischen zehn Jahren schützen die leicht zu konfigurierende Industrial Security Gateway, NAT-Gateways bzw. Maschinenfirewalls der WALL IE Serie von Helmholz ohne großen Aufwand sensible Daten und kritische Systeme vor Cyber-Bedrohungen. Und die Zukunft hat bereits begonnen: Anfang 2026 wird die Zertifizierung gemäß IEC 62443 durch das Prüfunternehmen TÜV Süd abgeschlossen sein.**

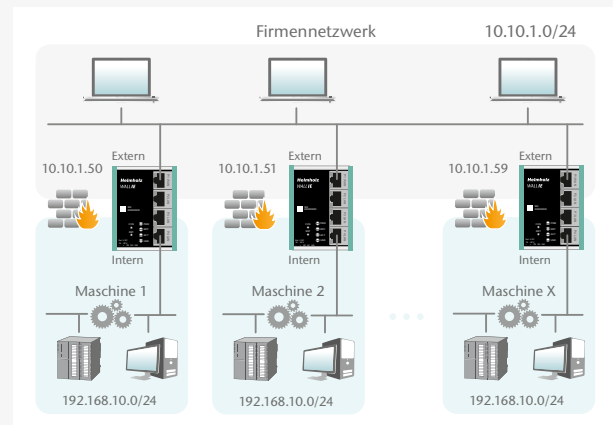
Autor: Karsten Eichmüller  
Managing Director

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

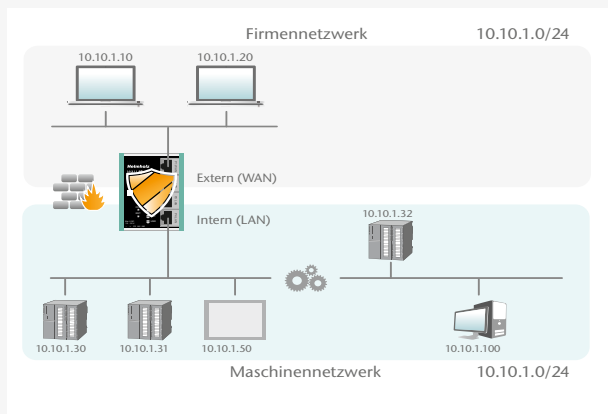
NAT-Betriebsmodus (Basic NAT)



NAT-Anwendung



Bridge-Betriebsmodus



NAPT: Network Address and Port Translation

