


Secure OT mit Industrial NAT-Gateway und Firewall ***WALL IE*** von Helmholz

# SCHLANKE, KOMPAKTE UND EINFACHE LÖSUNGEN FÜR CYBERSICHERE MASCHINEN

**Keine neue Maschine kommt mehr ohne eigenes Maschinennetzwerk aus. Ebenso selbstverständlich sollte schon heute die Absicherung dieses Netzwerks gegen unerwünschte Zugriffe von außen sein. Spätestens mit neuen Vorgaben wie der IEC 62443 und der Europäischen Maschinenverordnung werden entsprechende Cybersecurity-Maßnahmen nun für jeden Pflicht, der Maschinen in Verkehr bringt. Mehr denn je sind damit praktikable Lösungen für cybersichere Maschinen gefragt – so wie das Industrial NAT-Gateway WALL IE von Helmholz.**

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 überabeitete 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. Sie betrifft also alle, die an Herstellung und Betrieb von Maschinen beteiligt sind, und definiert entsprechende Verantwortlichkeiten für Maschinenbauer, Zulieferer und Endkunden.

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) und dem Cyber Resilience Act (CRA).

Zudem hat die Europäische Kommission die Maschinenrichtlinie 2006/42/EG überarbeitet. Dabei ist die Richtlinie an den New Legislative Framework (NLF) angepasst worden. Außerdem haben neue technologische Entwicklungen wie z. B. Künstliche Intelligenz, Autonomie und Vernetzung bei der Anpassung der grundlegenden Sicherheits- und Gesundheitsschutzanforderungen der Richtlinie Berücksichtigung gefunden. Die entsprechende neue Europäische Maschinenverordnung 2023/1230 ist ab dem 20. Januar 2027 für das Inverkehrbringen von Maschinen anzuwenden.

## MASCHINENNETZE SICHER INTEGRIEREN

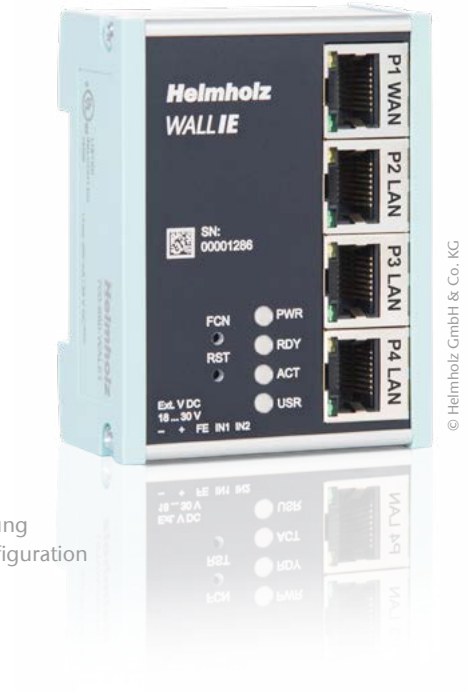
Nicht nur diese aktuellen Vorgaben zeigen: Das Thema Maschinensicherheit geht inzwischen jeden an. Dabei geht es im Kern darum, Maschinennetze sicher in das übergeordnete Produktionsnetzwerk zu integrieren.

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.

## **IHR NETZWERK COACH** – MEHR ALS NUR EINE FIREWALL!

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

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






**Reibungsloser Produktionsablauf**
**durch Netzwerksegmentierung**
für mehr Performance im Netzwerk. Durch Vermeidung von großen Broadcasts.

Video ansehen

Angesichts wachsender Datenmengen führt vor diesem Hintergrund kein Weg an der Trennung bzw. Segmentierung von Netzwerken vorbei. Konzepte mit 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. Eine Sicherheitszone ist eine logische Gruppierung von physikalischen Betrachtungsgegenständen, die den gleichen Schutzbedarf haben. Die Grenze der Sicherheitszone definiert, welche Komponenten innerhalb und welche außerhalb der Zone liegen. Um den benötigten Informationsfluss in eine und aus einer Sicherheitszone zu gewährleisten, werden sogenannte Kommunikationsleitungen (Conduits) definiert. Eine Kommunikation außerhalb von Conduits ist dabei nicht zulässig.

### ROBUSTE UND KOSTENGÜNSTIGE ABSICHERUNG MIT WALL IE

An diesem Punkt stellt sich die Frage, wie ein solches Zones & Conduits-Schutzkonzept für vernetzte Maschinen konkret umgesetzt werden kann. Der Markt hält dafür zahlreiche Highend-Lösungen bereit, die allerdings für die Absicherung eines einzelnen Maschinennetzwerks 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 umsetzbar. Eine solche Lösung ist das NAT-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. Zur Einfachheit und Sicherheit der Lösung trägt bei, dass die WALL IE mitsamt dem dahinter liegenden Maschinennetzwerk im Produktionsnetzwerk nur als eine einzige IP-Adresse angezeigt werden kann. Als weitere Besonderheit kann die WALL IE sowohl im NAT-Betriebsmodus als auch als Bridge eingesetzt werden. Im Bridge-Betriebsmodus agiert sie wie ein Switch. Im Gegensatz zu normalen Switches ist jedoch auch in dieser Betriebsart die Paketfilterung möglich. Dadurch kann die Einschränkung des Zugriffs zu einzelnen Bereichen des jeweiligen Netzwerks erreicht werden, ohne dass hierfür unterschiedliche Netzwerke verwendet werden müssen.

Im NAT-Betriebsmodus, den die meisten Anwender nutzen, leitet die WALL IE den Datenverkehr zwischen verschiedenen IPv4-Netzwerken (Layer 3) weiter und nutzt Paketfilter für die Zugriffsbeschränkung auf das dahinterliegende Automatisierungsnetzwerk. Dabei wird die Adressübersetzung mittels Network Adress Translation (NAT) unterstützt. Die Verwendung von NAT ermöglicht es darüber hinaus, mehrere gleichartige Automatisierungszellen mit dem gleichen Adressbereich in das Produktionsnetz einzubinden. Im NAT-Betriebsmodus unterstützt die WALL IE zwei NAT-Funktionalitäten: Basic NAT (auch „1:1 NAT“ oder „Static NAT“ genannt) und NAPT (Network Address and Port Translation, auch „1:N NAT“ oder „Masquerading“ genannt).

## NOCH MEHR MÖGLICHKEITEN DURCH NEUE VARIANTEN

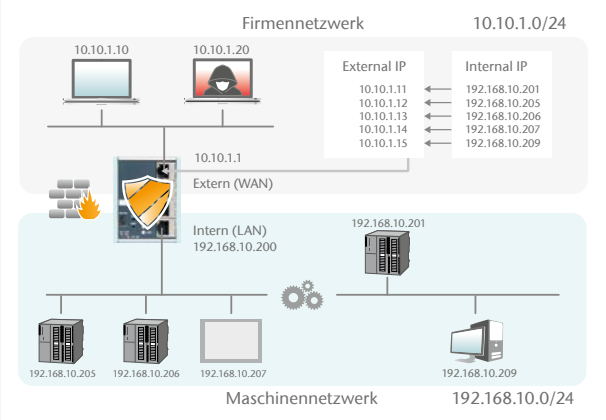
Seit der Markteinführung der WALL IE im Jahr 2015 hat sich diese inzwischen tausendfach bewährt. Der Funktionsumfang ist seitdem ständig gewachsen, größtenteils als Reaktion auf konkrete Kunden-Anfragen. Seit 2024 ergänzen nun zwei neue Varianten die bisherige „Standard“-Version (mit vier Ports und einer Übertragungsrate von 100 Mbit/s). Beide verfügen über einen schnelleren Prozessor mit Ethernet bis 1 GBit/s und erschließen damit neue Einsatzbereiche. Die neue „Compact“-Version beschränkt sich dabei auf zwei Ports - einer für das Firmennetzwerk (WAN), einer für das Maschinennetzwerk (LAN). Die „Plus“-Version bietet hingegen acht Ports. Die Ports können frei konfigurierbar als Switche für LAN oder WAN genutzt werden. Der Vorteil: Kleinere Netzwerke können also ohne zusätzliche Switche bzw. mit einem einzigen Device umgesetzt werden.

Allen drei WALL IE-Varianten ist gemeinsam, dass für die Inbetriebnehmer Netzwerk-Basiswissen ausreicht. So ist beispielsweise keine Anpassung der Netzkonfiguration im LAN Netz notwendig. Zudem lassen sich Serienmaschinen mit gleichen IP-Adressen einfach integrieren.

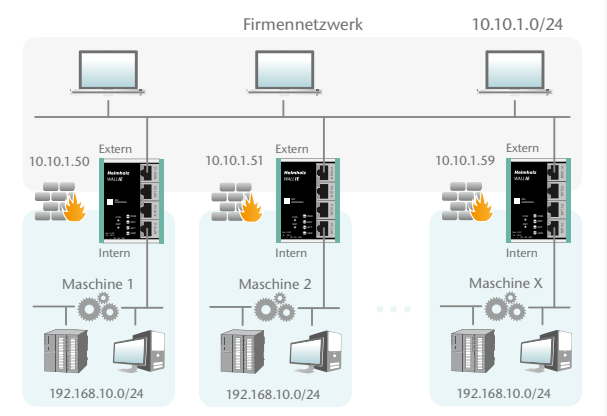
## FAZIT

**In der vernetzten Industrie der Zukunft ist die Sicherheit von Maschinen und Anlagen entscheidend für einen stabilen und ausfallsicheren Prozess. Durch Netzwerksegmentierung und sichere Zugriffe auf das Maschinennetzwerk lassen sich Abläufe einfach optimieren. Die leicht zu konfigurierenden NAT-Gateways bzw. Maschinenfirewalls der WALL IE Serie von Helmholz bieten mit wenig Aufwand maßgeschneiderten Schutz von sensiblen Daten und schützen kritische Systeme vor Cyber-Bedrohungen.**

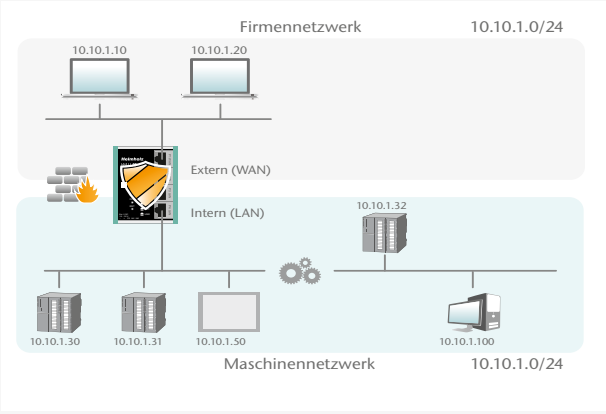
NAT-Betriebsmodus (Basic NAT)




NAT-Anwendung




Bridge-Betriebsmodus




NAPT: Network Address and Port Translation