Security-Gateway mit Firewall

Artikel vom **5. Mai 2026**
Security: Systeme und Komponenten

Für vernetzte Maschinen und Anlagen hat Helmholz »Wall IE« entwickelt, ein industrielles NAT-Gateway mit integrierter Maschinen-Firewall.



Das Security-Gateway ist in drei Bauformen verfügbar (Bild: Helmholz).

Im Sinne von Secure OT, also sicherer operativer Technologie aus Software und Hardware zur Steuerung, Absicherung und Kontrolle von industriellen Systemen, führt kein Weg an der Trennung bzw. Segmentierung von Netzwerken vorbei. Konzepte mit Vertrauenszonen und sicheren Zonenübergängen (Zones & Conduits) haben sich hierfür als besonders wirksam erwiesen, weshalb die IEC 62443 (Cybersecurity in der Industrieautomatisierung) ein entsprechendes Schutzkonzept vorsieht.

NAT-Gateway »Wall IE«

Hier suchen vor allem der mittelständische Maschinenbau und seine Kunden praktikable Lösungen, die nicht nur sicher und zuverlässig, sondern auch schlank, effizient und einfach ohne weiteren externen Support einsetzbar sein sollen. Eine solche Lösung ist das NAT-Gateway »Wall IE« von Helmholz. Einfach und dauerhaft zwischen der

Maschine und dem Produktionsnetzwerk installiert, verbindet das robuste und kompakte Security-Gateway Bridge- und Firewall-Funktionen im benötigten Umfang. Laut Hersteller schützt es die Netze, indem genau geregelt wird, welcher Teilnehmer mit welchem Gerät Daten austauschen darf. Die Voraussetzung dafür schafft eine Paketfilterfunktion zur Einschränkung des Zugriffs zwischen dem Produktionsnetzwerk und der Automatisierungszelle. Mit dem Gateway können IP-Adressen, Ports, MAC-Adressen und die Telegrammart in beide Richtungen gefiltert werden. Gleichzeitig ermöglicht das Gerät auch eine Anpassung der vorhandenen IP-Adressen der Maschine an die IP-Adressen im Fabriknetzwerk durch NAT (Network Address Translation). Dabei wird jedem Gerät in der Maschine, das 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 hiervon ausgenommen. Die Verwendung von NAT ermöglicht es auch, mehrere gleichartige Automatisierungszellen mit gleichem Adressbereich in das Produktionsnetz einzubinden, ohne die Maschinen umkonfigurieren zu müssen. Neben dem NAT-Betriebsmodus ist auch die Verwendung als Bridge möglich. Im Bridge-Modus haben die Netzwerkteilnehmer der Maschine bereits IP-Adressen im gleichen Bereich wie das Fabriknetzwerk. Alle Filterfunktionen sind aktiv, nur NAT ist abgeschaltet. Eine Neuerung des Geräts ist die Implementierung von 802.1X zur Authentifizierung. Darüber lässt sich vom Endkunden im Fabriknetzwerk sicherstellen, dass keine unerlaubten Geräte im Netzwerk aktiv werden. Der Anbieter passt zudem die Firmware permanent an die spezifischen Anforderungen der IEC 62443-4-2 an.

Hersteller aus dieser Kategorie

© 2025 Kuhn Fachverlag