SPS MAGAZIN
SONDERAUSGABE 1/2020
www.sps-magazin.de

INDUSTRIAL COMMUNICATION JOURNAL

ETHERNET WIRELESS SECURITY

NAT-Gateway/Firewall-Kombination für die Anbindung von Maschinen in übergeordnete Produktionsnetze

Sicher vernetzt

Seite 6

Helmholz®
COMPATIBLE WITH YOU

Titelbild: Helmholz GmbH & Co. KG

WAS KANN SPE UND WIE SIEHT ES AUS?
Trendumfrage zu Single Pair Ethernet
Seite 13

5G – GRUNDLAGEN UND ERSTE ANWENDUNGEN
Mehr Funk-Power für die Industrie
ab Seite 20

WENN DER HACKER DIE SPS ÜBERNIMMT
Produktionsanlagen richtig schützen
Seite 44

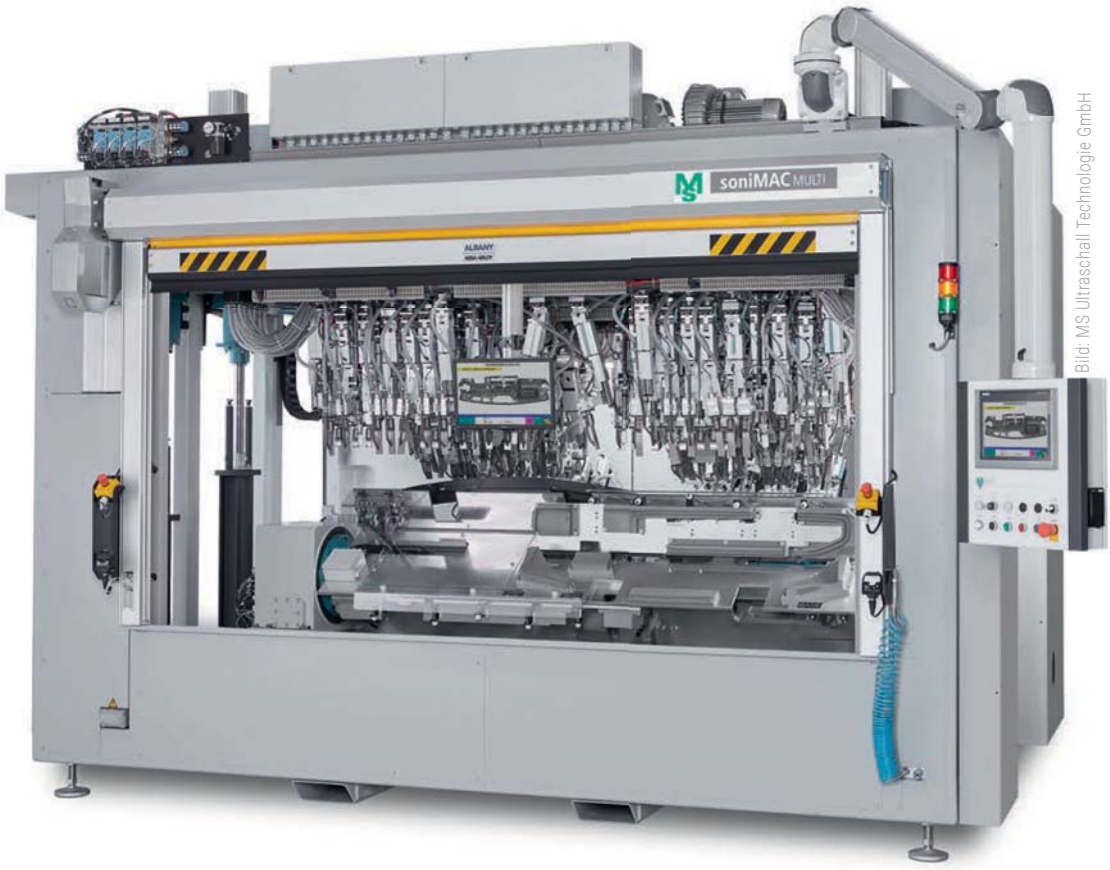


Bild: MS Ultraschall Technologie GmbH

Mit Wall IE von Helmholz lassen sich die Maschinen der Firma MS Ultraschall Technologie unkompliziert und sicher in Produktionsnetze integrieren.

NAT-Gateway/Firewall-Kombination für die Anbindung von Maschinen in übergeordnete Produktionsnetze

Sicher vernetzt

Als weltweit tätiger Maschinenbauer ist die Firma MS Ultraschall Technologie Tag für Tag mit der Anforderung konfrontiert, Maschinennetze sicher in übergeordnete Produktionsnetze zu integrieren. Mit einer Kombination aus Industrial NAT/Gateway und Firewall wurde eine ebenso zuverlässige wie praktikable Lösung für diese Aufgabenstellung gefunden. Trotz unkomplizierter Integration und Inbetriebnahme bieten sie bei der Vernetzung und Absicherung ein flexibel nutzbares Funktionsspektrum.

Ultraschall bringt thermoplastische Kunststoffe durch hochfrequente Schwingungen mühelos zum Schmelzen und sorgt damit in kurzer Zeit für eine sehr feste Verbindung der Fügepartner. Mit gutem Grund setzen deshalb viele Automobilzulieferer, aber auch andere Kunststoffverarbeiter weltweit auf dieses Verfahren. Ein Anbieter in diesem Bereich ist die Firma MS Ultraschall Technologie. Rund 350 Sonder- und Serienmaschinen verlassen deren Fertigung jährlich.

Industrial Ethernet und Cybersecurity

Der Siegeszug von Industrial Ethernet, konkret der Wandel von Profibus zu Profinet, macht dabei selbstverständlich auch vor diesem Maschinenbauer nicht halt. In den letzten Jahren hatten immer mehr Kunden die Anforderung gestellt, die Maschinen bzw. deren Kommunikationsnetze in ein übergeordnetes Produktionsnetzwerk zu integrieren. Technisch klingt das zunächst einmal machbar: Das Maschinennetz, also

Bilder der Doppelseite: Helmholz GmbH & Co. KG

das Netzwerk einer Automatisierungszelle mit einer oder mehreren Maschinen, ist dabei als Local Area Network (LAN) zu betrachten, das Produktions- bzw. Firmennetz als Wide Area Network (WAN). Aus Sicht der absolut notwendigen Cybersecurity stellt sich die Situation jedoch deutlich komplexer dar. Denn um Steuerungssysteme und Automatisierungsnetzwerke wirkungsvoll gegen Angriffe von außen zu schützen, muss das Maschinennetz sicher in das übergeordnete Produktionsnetz integriert bzw. von diesem abgegrenzt werden.

Praktikable Lösung

Die Realisierung einer solchen Schnittstelle war bis vor einigen Jahren nur über den Umweg komplexer Firewall-Lösungen möglich. Die sind allerdings für einen solchen Einsatzzweck überdimensioniert, und damit auch entsprechend teuer und kompliziert in der Handhabung. Für MS Ultraschall Technologie war deshalb klar, dass eine praktikable Lösung gebraucht wird. Fündig wurde der Maschinenbauer 2015 auf der SPS-Messe in Nürnberg. Dort stellte das Unternehmen Helmholz erstmals die NAT-Gateway/Firewall-Kombination Wall IE vorstellte.

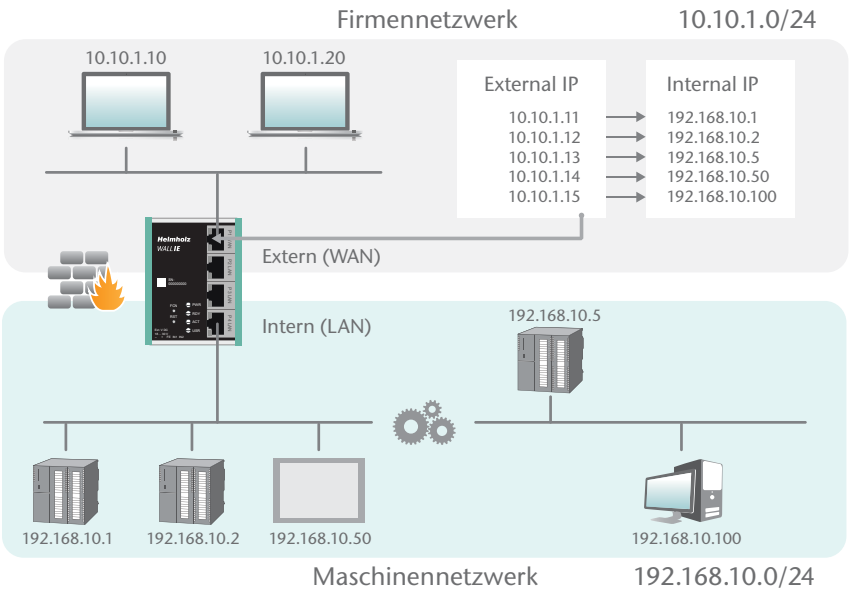
Leistungsstarker Helfer

Die robuste und unkomplizierte Ethernet-Komponente ermöglicht eine einfache Integration von Maschinennetzen in das übergeordnete Produktionsnetz. Konkret schützt Wall IE die Netze, indem genau geregelt wird, welcher Teilnehmer mit welchem Gerät kommunizieren und Daten austauschen darf. Wall IE passt sich durch eine individuelle Konfiguration über das Webinterface den jeweiligen Anforderungen des vorhandenen Maschinennetzwerks an. Die Beschränkung von Zugriffsrechten auf autorisierte Personen stellt dabei eine Grundvoraussetzung für den Schutz der Automatisierungsumgebung dar. Dabei bleiben die hinter Wall IE liegenden Netze bzw. IP-Adressen verborgen und sind von außen nicht sichtbar. Wird das Firmennetz nun durch einen Hackerangriff oder auch nur durch Unachtsamkeit eines Mitarbeiters von einer Schadsoftware oder einem Computervirus bedroht, bleibt das Automatisierungsnetz hinter Wall IE davon unberührt und dementsprechend sicher.

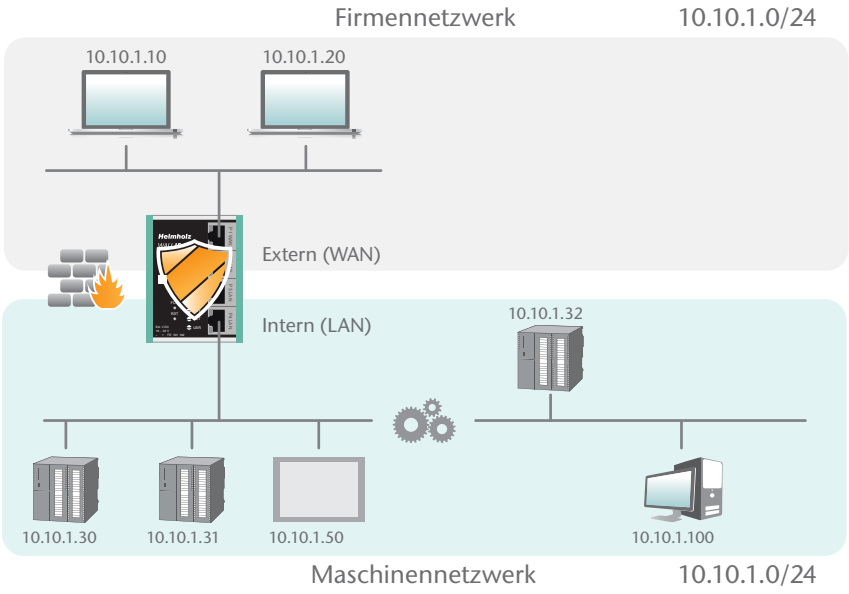
Paketfilter regelt Datenverkehr

Die Voraussetzung dafür schafft eine Paketfilterfunktion: Mit dieser Eigenschaft wird die Sicherheit dahingehend erhöht, dass nur erwünschte Kommunikation stattfindet. Ein unnötiger Datenaustausch wird blockiert. Folglich wird der Zugriff zwischen dem Fabriknetzwerk und dem Maschinennetzwerk passend ausgelegt.

Als Filterkriterien auf Layer 3 und 4 stehen bisher IPv4-Adressen, Protokoll (TCP/UDP), Ports und MAC-Adressen zur Verfügung. Als weitere Besonderheit kann Wall IE im NAT-Betriebsmodus und gleichermaßen auch als Bridge eingesetzt werden. Im Bridge-Betriebsmodus agiert das Gerät als Layer 2 Switch. Im Gegensatz zu marktüblichen Switches ist jedoch auch in dieser Betriebsart eine Paketfilterung möglich. Dadurch kann die Einschränkung des Zugriffs zu einzelnen Bereichen eines Netzwerks erreicht werden, ohne dass hierfür unterschiedliche Netzwerke verwendet werden müssen.



Basic NAT ist die Übersetzung von einzelnen IP-Adressen und auch ganzer Adressbereiche.



Im Bridge-Betriebsmodus agiert Wall IE als Switch mit Paketfilter zwischen der Automatisierungszelle und dem Produktionsnetz.

Nicht nur die zuverlässige Hardware von Wall IE konnte überzeugen, sondern auch die Software und die Philosophie dahinter.

Industrietaugliche Hardware

Wall IE unterstützt Industrial Ethernet mit einer Übertragungsrate bis 100Mbit/s. Die zugrundeliegende Software ist Linux-basiert und wurde komplett von Helmholz selbst entwickelt. Die Hardware ist industrietauglich robust und geeignet für die Montage auf der Hutschiene. Die Konfiguration erfolgt unkompliziert und schnell über ein responsives Webinterface. In die übersichtliche Benutzerführung hat Helmholz die langjährigen Erfahrungen aus der Toolbox TB20 einfließen lassen. Der Online-Zugang ist streng passwortgeschützt und läuft über eine verschlüsselte HTTPS-Verbindung.

NAT-Betriebsmodus

Bei der Verwendung von NAT (Network Address Translation) erlaubt es Wall IE, die IP-Adressen der vorhandenen Maschinen zu belassen, aber die Kommunikation zum Maschinennetz mit eigenen IP-Adressen aus dem Produktionsnetz zu ermöglichen. Im NAT-Betriebsmodus leitet Wall IE den Datenverkehr zwischen verschiedenen IPv4-Netzwerken (Layer3) weiter und nutzt Paketfilter für die Zugriffsbeschränkung auf das dahinterliegende Automatisierungsnetzwerk. Dabei wird die Adressübersetzung mittels NAT unterstützt. Kollisionen, die andernfalls durch die nicht eindeutigen Adressen im Gesamtnetz entstehen würden, sind damit ausgeschlossen. Für die Kommunikation mit anderen Automatisierungszellen kommen statische Routen zum Einsatz. Hierfür muss das Netzwerk sowie die Adresse des dafür zuständigen Routers (Next Hop) konfiguriert werden.

Router-Betriebsmodus

Im Router-Betriebsmodus unterstützt Wall IE zwei NAT-Funktionen: BasicNAT und NAPT. BasicNAT (auch 1:1NAT oder StaticNAT genannt) ist die Übersetzung von einzelnen IP-Adressen und auch ganzer Adressbereiche. Die Übersetzung geschieht ausschließlich auf IP-Ebene, wodurch alle Ports ohne explizite Weiterleitungen angesprochen werden können. Bei NAPT (Network Address and Port Translation, auch 1:NNAT oder Masquerading genannt) hingegen werden nicht nur die IP-Adressen, sondern auch Port-Nummern umgeschrieben. Alle Adressen der Automatisierungszelle werden in eine einzige Adresse des Produktionsnetzwerks übersetzt. Die Absenderadressen von Paketen aus der Automatisierungszelle werden durch diese ersetzt. Das DHCP-Protokoll (Dynamic Host Configuration Protocol) ermöglicht per DHCP-Server auf der LAN- sowie DHCP-Client auf der WAN-Seite eine automatische Vergabe von Adressen und DNS-Namen. Zudem ist nun nicht mehr für jeden einzelnen Port eine eigene Regel erforderlich, denn über Wildcards können ganze Port-Ranges gebündelt werden.

Einfache Integration mit SNAT

Mit der Funktion SNAT (SourceNAT) gibt Wall IE den eingehenden Datenverkehr WAN-seitig transparent an das LAN-Netzwerk weiter. Dabei werden alle ausgehenden Datenpakete mit der Absender-IP-Adresse der Komponente versehen. Somit bleiben die festgelegten Parameter aller LAN-Teilnehmer unverändert und die Eintragung eines Gateways entfällt. Dies ist ein erheblicher Vorteil bei der Integration in bestehende Netzwerkstrukturen. Alle Vorgaben können bei Wall IE anwenderspezifisch definiert und konfiguriert werden. Diesen Mehrwert durch Individualisierung bietet Helmholz seinen Kunden auch als Serviceleistung an. Die bereits anwendungsspezifisch konfigurierte Firewall wird dann einsatzbereit geliefert und muss nur noch mit Spannung versorgt werden.

Positive Praxiserfahrungen

MS Ultraschall Technologie liefert inzwischen rund die Hälfte der Sondermaschinen standardmäßig mit der NAT-Gateway/Firewall-Kombination aus, also im Durchschnitt eine Maschine pro Woche. Die Entscheidung für die Lösung von Helmholz hat sich aus Sicht des Maschinenbauers damit längst bestätigt. Nicht nur das Produkt selbst und die zuverlässige Hardware konnte überzeugen, sondern auch die einfache Menüführung der Software und die Philosophie dahinter. Der Anwender sieht anstelle der Ports, die hinter Wall IE verschaltet werden, nur eine einzige IP-Adresse. Damit kommt der Maschinenbauer nach eigenen Angaben gut klar. ■

Vertrieb Schweiz:
Amriswilerstrasse 155
8570 Weinfelden
+41 (0)71 626 58 80
WITO AUTOMATION AG www.wito-ag.ch

Lucia Zimmermann,
Head of Marketing,
Helmholz GmbH & Co. KG
www.helmholz.de

Produktdetails online ansehen

Bild: MS Ultraschall Technologie GmbH