



FCT-Anlagenbau GmbH setzt auf die WALL IE – Industrial Ethernet Bridge und Firewall

Echte Maschinensicherheit – statt Low-cost-Kompromisse

Mit dem Siegeszug der Ethernet-Vernetzung spielt auch die Cybersecurity eine ganz zentrale Rolle. Dabei geht es im Kern darum, Maschinennetze sicher in das übergeordnete Produktionsnetzwerk zu integrieren. Mit der Firewall WALL IE bietet Helmholtz seit rund zwei Jahren eine praktikable Lösung, die Bridge- und Firewall-Funktionen verbindet. Jetzt sind neue Funktionen verfügbar.

Auch in der digitalisierten Produktion gilt: Steuerungssysteme und Automatisierungsnetzwerke sind angreifbar, wenn keine angemessenen Sicherheitsmaßnahmen vorhanden sind. Cybersecurity bedeutet deshalb in Ethernet-vernetzten Produktionsumgebungen vor allem, Maschinennetze sicher in übergeordnete Produktionsnetze zu integrieren bzw. von diesen abzugrenzen. Das Maschinennetz, also das Netzwerk einer Automatisierungszelle mit einer oder mehreren Maschinen, ist dabei als LAN (Local Area Network) zu betrachten, das Produktions- bzw. Firmennetzwerk als WAN (Wide Area Network).

Um die Schnittstelle zwischen beiden sicher zu realisieren, war bisher nur der Umweg über komplexe Firewall-Lösungen möglich. Diese sind allerdings für diesen speziellen Einsatzzweck naturgemäß überdimensioniert. Und das bedeutet auch: dementsprechend teuer und kompliziert in der Handhabung. Noch weniger kommen allerdings sicherheitsgefährdende Low-cost-Kompromisse in Frage.

Leistungsfähige Alternative

Die Lösung bietet seit 2015 die ebenso leistungsfähige wie unkomplizierte Industrial Ethernet Bridge und Firewall WALL IE von Helmholtz. Die robuste

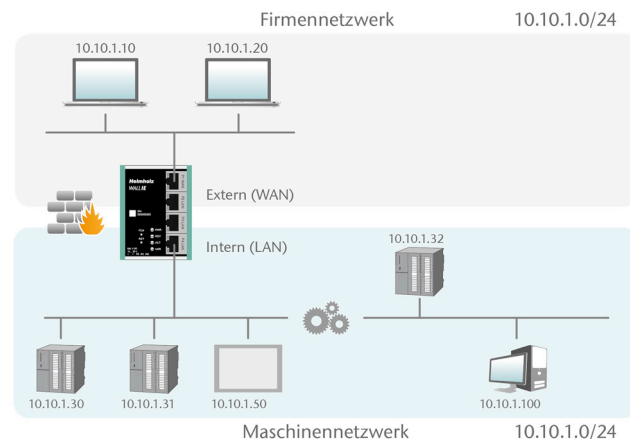
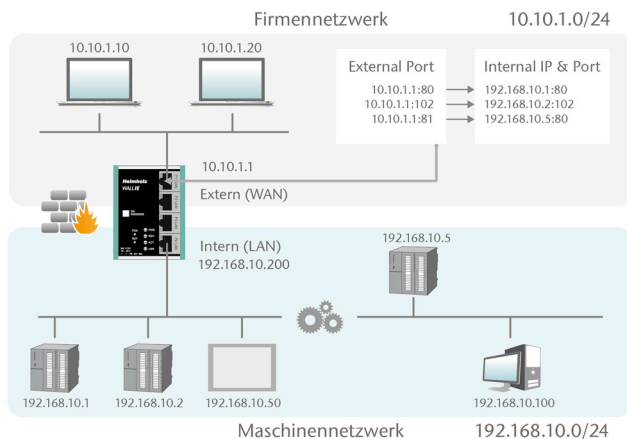
Ethernet-Komponente ermöglicht die einfache Integration von Maschinennetzen in das übergeordnete Produktionsnetz. Konkret schützt die Komponente die Netze, indem sie genau regelt, welcher Teilnehmer mit welchem Gerät Daten austauschen darf. In der Praxis nutzt ein Anwender die Komponente beispielsweise dazu, seine Logistikanlagen vollständig von anderen Netzwerken abzutrennen. Die Zugriffsrechte sind damit zuverlässig auf autorisierte Personen beschränkt. Das Automatisierungsnetzwerk ist entsprechend geschützt. Die hinter der WALL IE liegenden Netze bzw. IP-Adressen bleiben hingegen verborgen und sind von außen nicht sichtbar. Wird das Firmennetzwerk nun durch einen Hackerangriff oder auch durch Unachtsamkeit eines Mitarbeiters von einer Viren- bzw. Schadsoftware bedroht, bleibt das Automatisierungsnetz hinter der Wall IE davon auf jeden Fall unberührt und dementsprechend sicher.

Paketfilter regelt Datenaustausch

Die Voraussetzung dafür schafft eine Paketfilter-Funktionalität: Mit dem Paketfilter lässt sich der Zugriff zwischen dem Produktionsnetzwerk und der Automatisierungszelle einschränken. Beispielsweise kann konfiguriert

werden, dass nur bestimmte Teilnehmer aus dem Produktionsnetzwerk mit definierten Teilnehmern aus der Automatisierungszelle Daten austauschen dürfen. Andernfalls wird das Datenpaket zurückgewiesen bzw. verworfen. Als Filterkriterien auf Layer 3 und 4 sind bisher IPv4-Adressen, Protokoll (TCP/UDP) und Ports sowie MAC Adressen auf Layer 2 verfügbar. Als weitere Besonderheit kann die WALL IE sowohl im NAT-Betriebsmodus als auch als Bridge eingesetzt werden. Im Bridge-Betriebsmodus agiert WALL IE als Layer 2 Switch. Im Gegensatz zu normalen Switches ist jedoch auch in dieser Betriebsart die Paketfilterung möglich. Dadurch kann die Einschränkung des Zugriffs zu einzelnen Bereichen ihres Netzwerkes erreicht werden, ohne dass hierfür unterschiedliche Netzwerke verwendet werden müssen.

WALL IE ist konzipiert für 100 Mbit Industrial Ethernet. Die zugrundeliegende Software ist Linux-basiert und wurde von Helmholtz komplett selbst entwickelt. Die Hardware ist industrietauglich robust und geeignet für die Montage auf der Hutschiene. Die Konfiguration der WALL IE erfolgt schnell und einfach über ein responsives Webinterface. In die übersichtliche Benutzerführung haben die Helm-



Basic NAT (auch „1:1 NAT“ oder „Static NAT“ genannt) ist die Übersetzung von einzelnen IP-Adressen und auch ganzer Adressbereiche.

Im Bridge-Betriebsmodus agiert WALL IE als Layer 2 Switch zwischen der Automatisierungszelle und dem Produktionsnetzwerk.

holz-Entwickler ihre langjährigen Erfahrungen einfließen lassen. Der Online-Zugang ist streng passwortgeschützt und läuft über eine verschlüsselte HTTPS-Verbindung.

Router-Betriebsmodus und NAT-Funktionalität

Im Router-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 Address Translation (NAT) unterstützt. Die Verwendung von NAT ermöglicht es darüber hinaus, mehrere gleichartige Automatisierungszellen mit dem gleichen Adressbereich in das Produktionsnetz einzubinden. Kollisionen, die andernfalls durch die nicht eindeutigen Adressen im Gesamt-Netzwerk entstehen würden, sind damit ausgeschlossen. Als positiver Nebeneffekt können zudem im Produktionsnetz IP-Adressen eingespart werden. 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.

Im Router-Betriebsmodus unterstützt WALL IE zwei NAT-Funktionalitäten: Basic NAT und NAT. Basic NAT (auch „1:1 NAT“ oder „Static NAT“ 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 NAT (Network Address and Port Translation, auch „1:N NAT“ oder „Masquerading“ genannt) hingegen, werden nicht nur die IP-Adressen, sondern auch Port-Nummern umge-

schrieben. Alle Adressen der Automatisierungszelle werden in eine einzige Adresse des Produktionsnetzwerks übersetzt. Die Absender-Adressen von Paketen aus der Automatisierungszelle werden durch diese ersetzt.

Neue Funktionalitäten

Ab sofort ist für die WALL IE eine neue Firmware mit zusätzlichen Funktionalitäten verfügbar. So ermöglicht das DHCP-Protokoll (Dynamic Host Configuration Protocol) 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. Alle Vorgaben können bei der 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 dann nur noch mit Spannung versorgt werden.

FCT-Anlagenbau GmbH setzt auf die WALL IE

Überzeugt von den Vorteilen, setzt auch die Sonneberger FCT Anlagenbau GmbH bei der Realisierung von Bridge- und Firewall-Funktionen standardmäßig auf die WALL IE. „Immer mehr Kunden fordern für ihre Anlagen einen Netzzugang, zum Beispiel zur Archivierung der Daten“, beschreibt Jan Pommer aus der Abteilung Elektrokonstruktion den Weg dorthin. „Deshalb haben wir uns vor einiger Zeit systematisch auf die Suche nach einem geeigneten NAT-Übersetzer gemacht.“

Für die Helmholz-Lösung sprachen aus seiner Sicht insbesondere zwei Punkte: die kompakte Baugröße und der Funktionsumfang. „Die drei An-

schlüsse entsprechen genau unseren Anforderungen, mehr braucht es nicht“, so Pommers Einschätzung. Und noch etwas hat den Anlagenbauer überzeugt: „Für uns als Firma und auch für mich persönlich ist die IT-Security enorm wichtig. Und da zeigt die WALL IE beste Ergebnisse.“

Die Voraussetzung dafür ist, dass die Ethernet Bridge und Firewall richtig eingerichtet ist. Aber auch da gab es für Jan Pommer und seine Kollegen nie Schwierigkeiten: „Der Support von Helmholz hat uns von Anfang an sehr gut unterstützt und die Installation der WALL IE ist mit etwas Erfahrung wirklich kein Problem.“

Bis heute hat die FCT Anlagenbau GmbH bereits zahlreiche Kundenanwendungen mit der WALL IE erfolgreich umgesetzt.

Fazit

Die individuelle konfigurierbare WALL IE Industrial Ethernet Bridge und Firewall von Helmholz verbindet Bridge- und Firewall-Funktionalitäten. Sie gewährleistet damit echte Maschinensicherheit und hat dies inzwischen auch vielfach in der Praxis unter Beweis gestellt.

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