

Kommunikation mit 1:1 NAT-Router: Produktions- und Prozesszellen sicher vernetzen

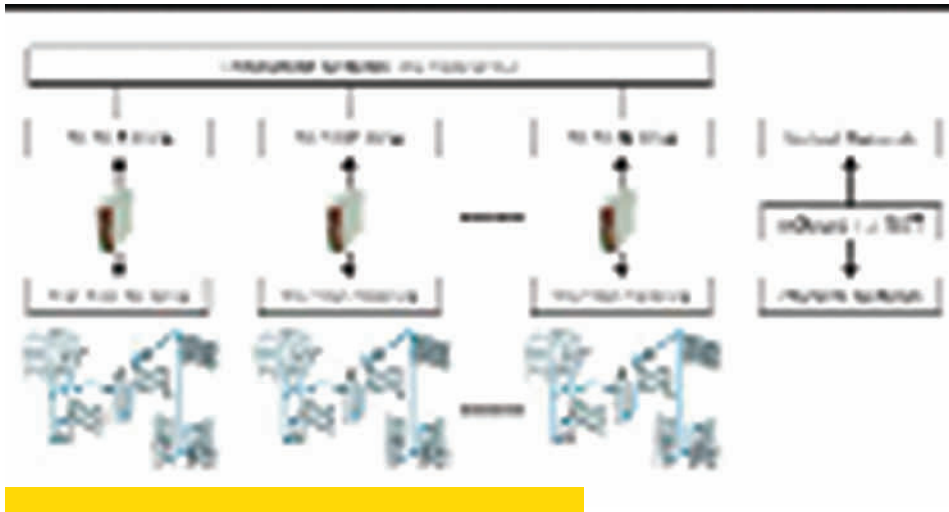


Bild 1: Funktionsweise von mGuard Appliances als 1:1 NAT-Router.

Soll eine neue Produktionsanlage mit bis zu 20.000 IP-Knoten mit einem bestehenden Werksnetz kommunizieren, ist die Einbindung in eine flache Netzwerkstruktur keine praktikable Lösung. Hierfür wird ein Router benötigt, der durch 1:1 Network Address Translation Subnetze auf virtuelle Netzwerke abbilden kann.

Das Konzept der Strukturierung komplexer Produktionsabläufe in vernetzte, weitgehend eigenständige und meist 'Zellen' genannte Steuerungsbereiche ist sowohl für Anlagen der Fertigungs- als auch der Prozessindustrie weithin geläufig. Erfolgt die Vernetzung der zellinternen Ein/Ausgabe- und Sensor/Aktor-Komponenten auf Basis traditioneller Feldbusse wie Profibus oder Interbus, bleibt die Zahl per Ethernet- und TCP/IP-verbundener Knoten (Steuerungen, Bedienrechner usw.) vergleichsweise überschaubar. Deren Kommunikation mit dem übergeordneten Werksnetz ist dann – zumindest theoretisch – noch in einer flachen Netzstruktur organisierbar. So umfasst etwa eine komplette Rohbaulinie für die Fertigung eines Pkw-Modells ca. 80-100 solcher Steuerungsbereiche und zwischen 1.000 und 2.000 IP-Knoten bei Nutzung von Feldbussen innerhalb der

Zellen. Auch in diesem Fall kann es bereits Vorteile haben, den Ethernet/IP-basierten Teil der Zellennetze gleichförmig zu gestalten, wie es für den Feldbus-basierten Teil möglich und üblich ist, da viele gleichartige Zellen ihren Dienst in der Fertigungslinie verrichten und/oder mehrere Anlagen des gleichen Typs für verschiedene Produkte, Standorte oder Betreiber gebaut werden. Zusätzlicher Aufwand, wie er bei Lieferanten und Betreibern für Engineering, Programmierung, Dokumentation und Inbetriebnahme individualisierter Zellennetze erforderlich wäre, werden durch dieses 'Klonen' der Zellen vermieden, indem diese intern ein immer gleiches Standard-Netz und die einzelnen Komponenten darin jeweils konstante Adressen verwenden. Auch das Risiko von Design-Fehlern wird durch die Vereinheitlichung reduziert. Diesem Bestreben steht allerdings häufig entgegen, dass es durchaus

möglich bleiben muss, aus dem übergeordneten Produktionsnetz heraus gezielt mit einzelnen Knoten in den Zellen zu kommunizieren. Ein einfacher NAT-Router am Übergang vom Zellennetz zum Produktionsnetz wird dieser Aufgabe nicht gerecht, da die Knoten im Zellennetz von außen dann nicht adressierbar sind. All dies gilt umso mehr beim Übergang zur zellinternen Vernetzung mit Industrial Ethernet und der damit verbundenen Explosion des IP Adressbedarfs. So wächst im Beispiel der oben genannten Pkw-Rohbaulinie die Anzahl der IP-Knoten bei diesem Übergang um das Zehn- bis Zwanzigfache auf ca. 15.000 bis 20.000 Knoten. Die Einbindung einer solchen Linie in eine flache Werksnetz-Struktur ist damit keine praktikable Option mehr, zumal der weit überwiegende Teil dieser Knoten nur zellintern und nicht über das Werksnetz mit anderen Zellen kommuniziert.

Sichere Automation

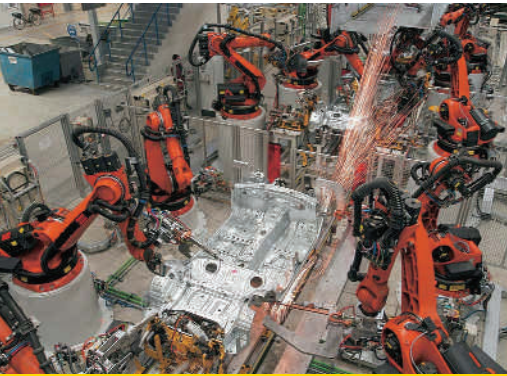


Bild 2: Typische Fertigungszelle im Automobil-Rohbau.



Bild 3: Der Innominate mGuard industrial RS im Einsatz als Security Router mit 1:1 NAT.

Sicherer 1:1 NAT-Router mit zentralem Management

Benötigt wird vielmehr ein Router mit der Fähigkeit, die internen Zellennetze bzw. Subnetze von diesen mit externem Kommunikationsbedarf durch so genannte 1:1 Network Address Translation (1:1 NAT) ganz oder teilweise auf jeweils eindeutige, virtuelle externe Netze (Subnetze des übergeordneten Werksnetzes) abzubilden. Die Innominate mGuard Security Appliances leisten diese 1:1 NAT Router-Funktionalität mit flexibler Konfiguration und voller 100MBits/s Wire-Speed Performance. Sie bilden in dieser Funktion typischerweise auch die Schnittstelle der Verantwortungen zwischen Werksnetz einerseits und Zellen-Automatisierung andererseits (vgl. Bild 1). Besonderen Charme für die Vernetzung einer größeren Zahl von Zellen erhält die Lösung durch den Innominate Device Manager (IDM) als zentraler Management-Komponente. Durch die im IDM verwendete Vorlagen-Technik muss die Konfiguration der mGuard Router- und Security-Einstellungen im Wesentlichen nur einmalig in einer Vorlage (Template) erstellt werden und kann über diese auf eine beliebige Zahl von Geräten (Devices) – sprich Zellen – ausgerollt werden.

Dabei kann der IDM durch sein Konzept der so genannten Adress-Pools sogar die Vergabe und Zuordnung eindeutiger virtueller externer Netze aus einem dafür definierten Gesamtadressraum zu den internen Netzen der Fertigungszellen automatisieren. Gleiches gilt für die Vergabe der Adressen an die externen Router-Interfaces. De facto können so dutzende oder gar hunderte von Zellen-Routern vollautomatisch aus einer einzigen Vorlage konfiguriert werden, ohne dass es dazu manueller Anpassungen für einzelne Geräte bedarf. Auch Konfigurationsänderungen im späteren Lebenszyklus der Zellen-Router können per IDM effizient zentral verwaltet und per Configuration Push oder Pull innerhalb weniger Minuten auf eine Vielzahl von Geräten ausgerollt werden.

Firewall, User Firewall und sichere Fernwartung über VPN

Innominate mGuard Security Appliances verbinden die Funktion als 1:1 NAT Router mit zahlreichen Mehrwerten im Bereich der Netzwerksicherheit. So gewährleistet die integrierte Stateful Packet Inspection Firewall eine gezielt konfigurierbare Beschränkung der zulässigen Kommunikation auf produktiv erforderliche Verbindungen. Besonders sensitive Zu-

griffe in die Zellen hinein, etwa zur Manipulation von Steuerungen mit einer SPS-Programmierungsumgebung, müssen nicht pauschal erlaubt sondern können durch die User-Firewall von einer vorherigen Authentisierung autorisierter Benutzer abhängig gemacht werden. Und auch für die sichere Anbindung zur Fernwartung der Zellen durch externe Lieferanten oder Service Provider kann die gleiche mGuard Infrastruktur dank optional integrierter VPN-Technologie (Virtual Private Networks) genutzt werden. Bei Investition in vergleichbarer Größenordnung zu einem einfachen Router kommt so ein Vielfaches an Funktionalität und Mehrwert als Return on Investment in die Anlage zurück.



Autor: Torsten Rössel ist Director Business Development bei der Innominate Security Technologies AG in Berlin.

www.innominate.com