# Sicherheitstor zwischen zwei Welten

## Schutz autarker Ethernet-Systeme vor unbefugter Nutzung

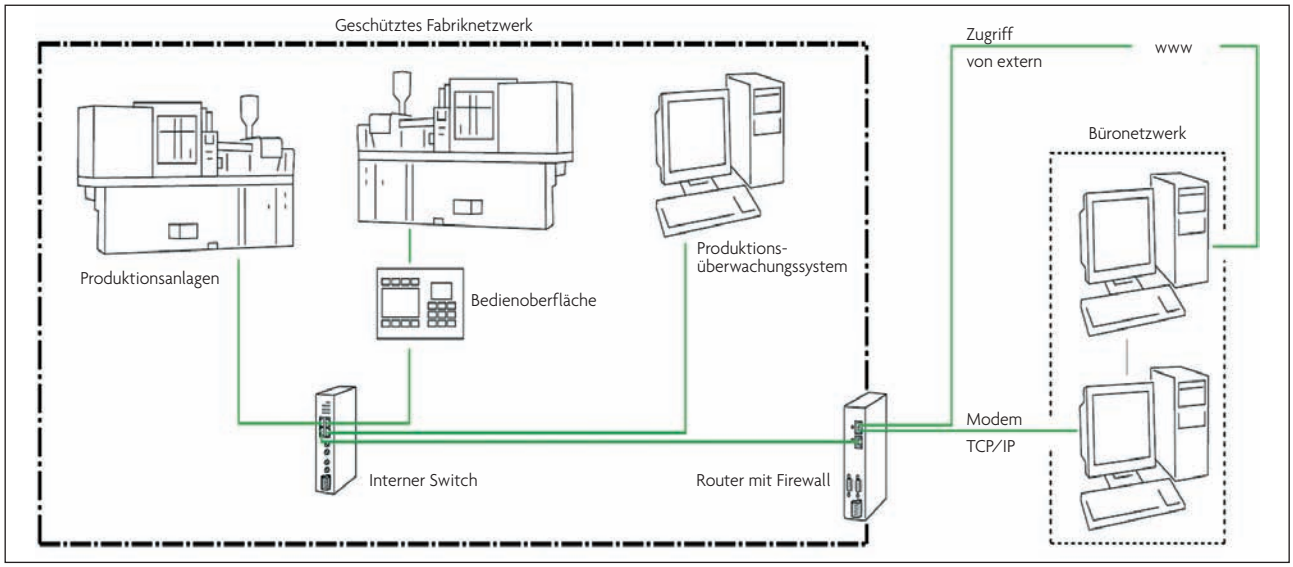


**Bild 1: Geschütztes Fabriknetzwerk**

Horst Kalla

**Industrial Access Router trennen zielgerichtet unterschiedliche Netzwerke. Sie stehen für zwei typische Anwendungsgebiete: Einerseits trennen sie Ethernet-Netzwerke aus Gründen der Datensicherheit oder wegen der einfacheren Konfiguration, andererseits eröffnen sie den Zugang ins Internet. Zugriffe auf das Fertigungsnetzwerk hinter einem Router sind nur autorisierten Benutzern erlaubt. So lässt sich eine angeschlossene Anlage hinter einer einzigen IP-Adresse verbergen.**

Die Zukunft der Kommunikation liegt in nur einem Netzwerk. Es entsteht eine durchgängige Kommunikation von der Office-Welt bis hinunter in die Maschine. Die durchgängige Ethernet-Kommunikation vereinfacht und beschleunigt Prozesse, schafft Transparenz und reduziert Kosten. Allerdings ist Industrial Ethernet als offenes System konzipiert und somit auch offen für ungebetene Gäste und Daten. Hier spielt das Thema Datentransfer und Datenschutz eine wichtige Rolle. Erst seit kurzem denken Anwender über Sicherheitsstrategien nach und setzen erste Konzepte auf. Weidmüller bietet als »Tor zwischen den Ethernetwelten« Security Router an. Sie schützen autarke Systeme im Industrial Ethernet Feld vor unnötigem Traffic (Datenaufkommen) und unbefugter Nutzung (**Bild 1**).

Industrial Access Router gestatten einfache, sichere Verbindungen zwischen Büro- und Fertigungsnetzwerken sowie Verbindungen über das Internet. Router trennen zielgerichtet unterschiedliche Netzwerke. Zugriffe auf das Fertigungsnetzwerk hinter dem Router sind nur autorisierten Benutzern erlaubt. So lässt sich eine angeschlossene Anlage mit eigenem IP-Subnetz hinter einer einzigen IP-Adresse verbergen. Das reduziert den Installationsaufwand erheblich. Ein integriertes Modem (analog oder ISDN) macht den Router weltweit verfügbar für Konfiguration, Verwaltung und Überwachung via Telefonnetz. Eine VPN-Verbindung (Virtual Private Network) lässt sich zwischen zwei Routern über den lokalen Internet-Provider herstellen. Zulässig sind nur autorisierte Anwendungen. Optional kann man ein externes Modem am Router anschließen, z. B. ein GSM-Modem für Funkverbindungen.

### Welche Sicherheits-Anforderungen muss Industrial Ethernet erfüllen?

Die Grundanforderungen an die Netzwerksicherheit des Industrial Ethernet entsprechen denen der Office-Welt – allerdings mit anderer Gewichtung:

- **Integrität**: Übertragene Daten werden auf dem Transportweg nicht modifiziert, sie sind vollständig und erreichen das Ziel in vorgegebener Reihenfolge.
- **Verbindlichkeit**: Es lässt sich jederzeit nachweisen, wer eine Verbindung initiiert und wer welche Daten zu welchem Zeitpunkt übertragen hat. In der Praxis bedeutet das: Daten von Log-Files sind eindeutig und nicht verfälschbar.
- **Vertraulichkeit**: Dritte können die Daten auf dem Transportweg nicht einsehen.
- **Verfügbarkeit**: Netzwerk und angeschlossene Geräte sollten Daten jederzeit und in definierten Zeiträumen versenden und bearbeiten können. Verfügbarkeit stellt einen sehr heiklen Punkt der Netzwerksicherheit in Automatisierungssystemen dar.
- **Identifizierung**: Bei der Identifizierung wird festgestellt, welche Identität der Kommunikationspartner hat und ob er berechtigt ist, auf den gewünschten Dienst zuzugreifen.
- **Prüfbarkeit**: Die Prüfbarkeit beschreibt, ob der Verlauf des Zustands

Dipl.-Ing. *Horst Kalla*,
Referent Fachpresse, Weidmüller Interface GmbH & Co. KG, Detmold

eines Systems rekonstruierbar ist. Ein Beispiel hierfür sind Log-Files eines Webservers. Anhand dieser Dateien lässt sich die Befehlsreihenfolge nachvollziehen, die der Server ausgeführt hat.

- **Schutz von Dritten:** Der Schutz von Dritten verhindert, dass eine Anlage als Ausgangsbasis für Angriffe auf Dritte, also z. B. ein anderes Unternehmensnetzwerk, missbraucht werden kann.

## Sicherheit durch IP-Adressen

Netzwerke, wie sie bei der industriellen Fertigung, bei industriellen Maschinen oder in Büros vorkommen, verwenden zwar den gleichen Ethernetstandard – sie haben aber trotzdem Unterschiede. Der Schutz der einzelnen Anlagenteile bzw. der gesamten Anlage kann durch Security Router erfolgen. Anwender können hinter einer IP-Adresse die gesamte Anlage oder Anlagenteile verbergen. Das reduziert den Aufwand bei der Installation und Verwaltung.

Statische Routing-Funktionalitäten, wie sie Industrial-Ethernet-Router heute bieten, erlauben komplexe Szenarien zur Anbindung von Maschinen- und Anlagenteilen an Netzwerke. Dabei erscheinen die IP-Adressen, die innerhalb der Maschine vergeben werden, nicht im

## GLOSSAR

**RSTP**: Der IEEE-Standard Rapid Spanning Tree Protokoll ist neben Rapid Ring eine andere Option, um Redundanz in einem Netzwerk herzustellen. RSTP ermöglicht eine netzähnliche Struktur des Netzwerkes. Eine mehrfache Redundanz wird erzielt. Die Verwendung des RSTP in einem Netzwerk ist nicht so einfach wie die Verwendung des Rapid Ring, dafür bietet der RSTP interessante Optionen.

**Rapid Ring**: Die Ring-Topologie ist der einfachste und effektivste Weg zum Erzielen einer Netzwerkredundanz. Die Rapid Ring Technologie wurde »aus der Not« entwickelt, denn ein Standard war nicht vorhanden. Rapid Ring bietet Redundanz gegen einzelne Fehler. Die zu einem Ring zusammengeschlossenen Geräte werden wie ein tatsächlicher logischer Ring verkabelt. Da die Ringstruktur im Netzwerk zu einer Schleife (Loop) führen würde wird ein Link logisch deaktiviert (Backup-Link).

**TCP-Flags**: TCP-Flags sind Sitzungs-Befehle (Kommandos), die den Aufbau, den Erhalt und den Abbau/Abbruch der Sitzung kontrollieren. Die verschiedenen TCP-Flags sind:

- **SYN** = Synchronize: Der TCP-SYN Befehl wird gesendet, um die Empfänger-Station zu veranlassen, in einen Sitzungs-Aufbau einzuwilligen. Die Einwilligung wird signalisiert mit TCP-SYN-ACK. Unter SYN Flooding wird folgender Vorgang verstanden: Ein Angreifer sendet ständig TCP-SYN-Pakete an den Empfänger. Da dieser für jeden TCP-SYN-Anruf Resourcen bindet, die erst nach einiger Zeit wieder frei gegeben werden, führt dies zu einer Beeinträchtigung in der Arbeitsfähigkeit des Empfängers. Es kann zu Systemabstürzen kommen. Um diese Folgen zu vermeiden, werden angegriffene TCP-Ports bei den meisten Systemen nach kurzer Zeit gesperrt. Der Angreifer erreicht indirekt sein Ziel, die Arbeitsfähigkeit des Angegriffenen zu beeinträchtigen. Diese Denial-of-Service-Attacks werden über das Internet von Computer-Viren angewendet, um Server angegriffener Unternehmen lahm zu legen.
- **ACK** = Acknowledge: Dieses Signal bestätigt den Erhalt von Daten der Gegenstelle. Außer dem TCP-ACK-Flag muss die sog. »Acknowledge Number« gegeben sein: dies ist ein numerischer DWORD-Ausdruck (32 bit), der den Offset anzeigt (die Sende-Position innerhalb des Datenstroms), bis zu dem Daten einwandfrei und unterbrechungsfrei empfangen wurden.
- **PSH** = Push: Hat der Sender alle Daten, die zu versenden waren, gesendet, oder hat der Sender den Rx-Buffer (Eingangs-Puffer ausweislich der angezeigten TCP Window Size) der Gegenstelle ausgeschöpft, signalisiert er mittels TCP-PSH, dass der TCP-Treiber die Daten der letzten Übertragung »nach oben« an die Applikation weiter leiten soll (engl. »push« = schieben).
- **URG** = Urgent: Dieses Signal weist darauf hin, dass im TCP-Hedaer ein »Urgent Pointer« gegeben ist: Dies ist ein Offset-Zeiger, der eine bestimmte Byte-Position in der Nutzdatenmenge (»user data«) markiert. Urgent Pointer wurden wesentlich für Telnet entwickelt und sind höchst selten in Gebrauch.
- **FIN** = Final: Kommt ein Dialog geordnet zu seinem Ende, sendet eine Seite TCP-FIN, die Gegenstelle antwortet mit TCP-FIN-ACK.
- **RST** = Reset: Abbruch-Signal, das entweder gesendet wird, um ein erhaltenes TCP-SYN abzulehnen (Session Denial), oder um eine laufende Sitzung abzubrechen (Session Abort).

**SSH**: SSH ermöglicht eine sichere, authentifizierte und verschlüsselte Verbindung zwischen zwei Rechnern über ein unsicheres Netzwerk. Secure Shell oder SSH ist sowohl ein Programm als auch ein Netzwerkprotokoll, mit dessen Hilfe man sich über eine verschlüsselte Netzwerkverbindung auf einem entfernten Computer einloggen und dort Programme ausführen kann. Die neuere Version SSH2 bietet weitere Funktionen wie Datenübertragung per SFTP. Die Iaona hat dem Protokoll den TCP-Port 22 zugeordnet.

**DynDNS**: Wer von außerhalb auf seinen Rechner zu Hause zugreifen möchte, hat ein Problem: Bei der meist obligatorischen Zwangstrennung bekommt der Rechner eine neue IP-Adresse. Und wer die nicht kennt, erreicht auch nicht den Rechner. Abhilfe schafft der **DynDNS-Dienst**: Er leitet Anfragen an eine Domain an einen dynamische IP-Adresse weiter. DynDNS steht für Dynamic Domain Name System. Bekanntester Anbieter ist dyndns.org, eine dynamische Domain gibt es hier kostenlos. Das Prinzip ist einfach: Ein kleines Programm im Router oder auf dem Rechner meldet die aktuelle IP-Adresse an DynDNS, dort werden dann die Domainanfragen einfach auf die entsprechende IP-Adresse umgeleitet. Viele Router haben bereits einen DynDNS-Client eingebaut, ansonsten muss man sich mit einem lokalen, also auf dem Rechner installierten Client begnügen. Ein Beispiel hierfür wäre der DynDNS Updater, den dyndns.org empfiehlt. Hierbei gilt: Läuft DynDNS auf dem Router, müssen von dort aus die Anfragen an den betreffenden Rechner weitergegeben werden. Dazu sollte man dann mit festen IPs arbeiten.

**Callback**: Callback ist der Versuch, über einen Umweg günstiger zu telefonieren als direkt. Das Verfahren funktioniert, indem man eine spezielle Rufnummer anruft, gleich wieder auflegt und wartet, bis der Telefoncomputer zurückruft. Mit dieser Leitung kann man dann seine Zielnummer wählen. Beim Callback werden, technisch gesehen, zwei Leitungen zu einer zusammengekoppelt. Das kann schon mal zu Störungen kommen, die dann auch beide Gesprächsteilnehmer im Ohr haben. Inzwischen gehen auch einige Anbieter von Internet-Telefonie dazu über, Callback anzubieten. Hier werden die beiden Gesprächskanäle dann über VoIP zusammengeschaltet. Doch wer braucht Callback? Grundsätzlich lassen sich vier Nutzergruppen definieren: Jene die mit ihrem Handy ins Ausland telefonieren und sparen wollen, jene die ein Mobilfunkprodukt mit Festnetzrufnummer haben und hierdurch sparen können sowie Kunden alternativer Festnetzanbieter, die kein Call by Call nutzen können. Last not least richtet sich Callback auch an jene, die abgehend keine Telefonate führen können oder dürfen - z.B. auf dem Bürotelefon.

**Dial on Demand**: Wenn in Weitverkehrsnetzen (WAN) Verbindungen zwischen Knoten immer nur nach Bedarf aufgebaut werden, spricht man von Dial-on-Demand-Routing. Diese Technik spart insbesondere in Netzen mit geringem Datenaufkommen Kosten, da keine festgeschalteten Verbindungen zwischen den Netzknoten benötigt werden

angebundenen Netz. Das bietet zwei Vorteile:

- **Reduzierter Konfigurationsaufwand:** Man muss lediglich eine IP-Adresse für die Ethernet-Schnittstelle vergeben. Der Anwender kann IP-Adressen in der Produktionszelle nach eigenem Schema zuteilen. Diese Vorgehensweise reduziert mögliche Fehlerquellen durch eine falsche Adressevergabe.

Die in der Grafik verwendeten Abkürzungen stehen für:

- **MD:** Machine Distributor, nimmt die direkte Anbindung einer Maschine an das Netz vor
- **FD:** Floor Distributor, verbindet mehrere zusammengehörige Maschinen
- **BD:** Building Distributor, verbindet verschiedene FD miteinander

Die Verbindung zwischen Bürowelt und Produktion übernimmt aus Sicherheitsgründen ein Packet Filter. Dieser kann auf Basis von IP-Adressen sowie Quell- und Zielports bestimmten Netzwerkverkehr ausfiltern.

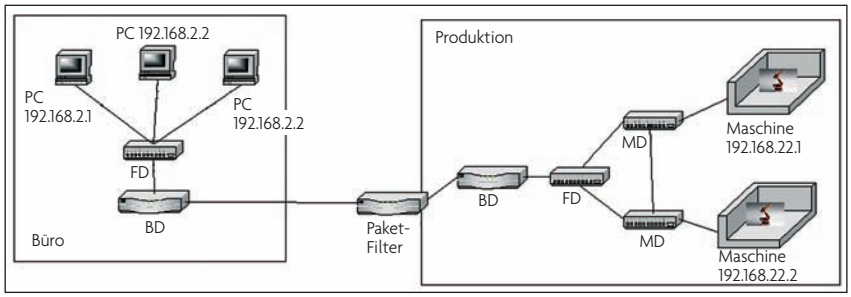


**Bild 2: Die Verbindung zwischen Bürowelt und Produktion übernimmt aus Sicherheitsgründen ein Paket-Filter**

- Da keine direkte Kommunikation zwischen Maschine, Anlage oder Anlagenteilen und angebundenem Netz mehr stattfindet – der Router wird als Instanz stets mit eingebunden – erhöht sich die Netzwerksicherheit. Ein Angreifer kann weder die IP-Adressen der Maschine ergründen noch komplexe Angriffsvorbereitungen wie Port-Scans durchführen.

Es stellt sich die Frage: Wie können Anlagen oder Maschinen hinter einem statischen Router mit der Außenwelt kommunizieren, wenn keine direkten Verbindungen möglich sind? Die Lösung: Zwei sehr leistungsfähige Verfahren aus der Welt der IP-Protokoll-Familien übernehmen die Kommunikation: Network Address Translation (NAT) und Destination NAT (DNAT).

## Network Address Translation

NAT ist ein Verfahren, um eine IP-Adresse in einem Datenpaket durch eine andere zu ersetzen. Das Verfahren dient dazu, interne IP-Adressen auf öffentliche IP-Adressen abzubilden.

**Bild 2** zeigt ein Produktionsnetzwerk, das mit dem Office-Netzwerk verbunden ist. In diesem Beispiel geht man davon aus, dass beide Maschinen im Produktionsnetz vom gleichen Maschinenhersteller stammen.

Die Architektur entspricht dabei dem von der Iaona im Industrial Ethernet Wiring and Installation Guide dargestellten Vorschlag (siehe **www.iaona.org**).

Das Produktionsnetz lässt sich folgendermaßen realisieren:

- FD und MD werden als Switche ausgeführt. Aufgrund der redundanten Auslegung müssen sie ein Redundanz-Protokoll (etwa RSTP oder Rapid Ring) unterstützen.
- Der BD wird durch einen Router mit statischem Routing realisiert. Weitere Sicherheitsmaßnahmen, wie ein zusätzlicher Packet Filter im BD, können die Netzwerksicherheit zusätzlich erhöhen.

Wie zuvor angedeutet, bekommt der BD nur eine Netzwerkadresse aus dem Produktionsnetz (192.168.2.X). Die Maschinen, Anlagen oder Anlagenteile können vorkonfiguriert nach dem Standardverfahren des Maschinenherstellers ausgeliefert werden. Die Umsetzung der Adressen obliegt dem Router. Zur Anwendung kommt dabei das NAT genannte Verfahren:

Angenommen, Maschine 1 aus dem Produktionsnetz muss mit einem Rechner aus dem Büronetz kommunizieren, z. B. zum Abruf neuer Produktionsdaten. Die Maschine weiß, dass der BD als Gateway für andere Netz konfiguriert ist, so sendet sie die Daten für das Office an den Router. Der Router empfängt das Paket von Maschine 1. Bevor er die Daten weiter versendet, ändert er die Quelladresse des Pakets von der IP-Adresse der Maschine 1 auf seine eigene. Der

## Destination NAT

| lokales Netz (LAN) | | | öffentliches Netz (WAN) | |
|---|---|---|---|---|
| **Quell-IP** | **Ziel-IP** | **Router** | **Quell-IP** | **Ziel-IP** |
| 170.0.0.1 | **192.168.0.2** | <========== | 170.0.0.1 | **205.0.0.2** |
| 170.0.0.1 | **192.168.0.3** | **NAT** | 170.0.0.1 | **205.0.0.4** |
| 170.0.0.1 | **192.168.0.4** | | 170.0.0.1 | **205.0.0.3** |

**Bei eingehenden Paketen lässt sich anhand der IP-Adresse und des Eintrags in der Tabelle feststellen, welcher Computer die Pakete angefordert hatte**

**Bild 3: Der Einsatz von Routern gestattet die Aufteilung in Subnetze mit unabhängigen IP-Adressen und die sichere Anbindung an das Internet**


Router vermerkt in einer internen Tabelle die Adresse des Originalpaketes und versendet das veränderte Paket weiter. Für den Zielrechner ist der Absender stets der Router. Maschine 1 taucht in der gesamten Kommunikation nicht auf. Der Zielrechner kann nun auf das empfangene Paket antworten und sendet Daten zurück an den Router. Kann der Router das Paket als Antwort auf ein Paket von Maschine 1 interpretieren (z.B. ein TCP-SYN ACK auf ein TCP-SYN), so wird er die Antwort an Maschine 1 weiterleiten.

Der gerade beschriebene Ablauf zeigt auch einen Nachteil von NAT auf: Die Kommunikation kann nur einseitig von Maschine 1 aufgebaut werden. Die Existenz von Maschine 1 ist dem Büronetz nicht bekannt. Als Lösung dieses Problems bieten Industrial Ethernet Router das so genannte Destination NAT an.

### Destination NAT

Beim Destination NAT wird ein Router so konfiguriert, dass er eine bestimme Kombination aus Zieladresse/Zielport auf eine neue Kombination aus Zieladresse/Zielport umsetzt.

Angenommen, von einem PC im Büronetz aus will ein Anwender per Webbrowser Produktionsdaten von Maschine 1 lesen. Dafür wird der Router so konfiguriert, dass er an ihn gerichtete IP-Pakete mit Zielport 8080 an Port 80 von Maschine 1 weiterleitet. Es wird die Zieladresse des Paketes umgeschrieben (DNAT). Antworten von Maschine 1 leitet der Router dann wieder mit veränderter Adresse an den Office-PC weiter.

Der Office-PC richtet seine Anfragen nun direkt an die Router-IP-Adresse und den Port 8080. Die Daten die er erhält, stammen in Wirklichkeit von Maschine 1. Auch hier bleibt dem Office-Netz die wirkliche Adresse von Maschine 1 verborgen. Dies erhöht die Sicherheit der im Produktionsnetz hinter dem Router angeordneten Geräte.

**Beispiel: Destination NAT**

Bei eingehenden Paketen lässt sich anhand der IP-Adresse (welche nun die Ziel-IP-Adresse ist) und des Eintrags in der **Tabelle** feststellen, welcher Computer die Pakete angefordert hatte (hier: 192.168.0.2, 192.168.0.3 und 192.168.0.4). Das NAT-Gerät kann dadurch die (öffentliche) Ziel-IP-Adresse durch die ursprüngliche Quell-IP-Adresse 192.168.0.2, 192.168.0.3 bzw. 192.168.0.4 austauschen.

Für die beteiligten Endgeräte (Maschinen, Anlagen oder Anlagenteile) im internen Netz (z.B. 192.168.0.2) oder externen Netz sind diese Vorgänge transparent, d.h. sie bekommen von der Adressumsetzung nichts mit.

### Tore zwischen Ethernetwelten – Anbindung an das Internet

Die beiden Industrial Access Router IE-AR-10T und IE-AR-10T ISDN von Weidmüller binden industrielle Ethernet-Netzwerke sicher und einfach ans Internet (**Bild 3**). Hierfür stehen das integrierte analoge oder ISDN-Modem mit globalen Einsatzmöglichkeiten. Externe Modems (ISDN, GSM, analog) lassen sich einfach über die Schnittstelle RS232 anschließen. Eine integrierte Firewall schützt die Systeme zuverlässig. Die Programmierung/Konfiguration erfolgt über Browser oder Textkonsole bzw. SSH. Auch Laptops oder Handhelds lassen sich verwenden. Dies benötigt keine separate Konfigurationssoftware, sie ist bereits im Gerät implementiert. Aktualisiert wird die Software via Fernzugriff – im Rahmen der Fernwartung. Als Standard enthalten sind Funktionen wie VPN, DynDNS und Call Back.

Eine ausführliche Übersicht zu den Eigenschaften der Router finden Sie in der Online-Version dieses Beitrags unter **www.de-online.info**.

### Zusammenfassung

Router sind höchst wirkungsvoll, um Netze zuverlässig zu trennen. Nur autorisierte Benutzer greifen von außen in das geschützte Netzwerk hinein, und nur freigeschaltete Geräte versenden Daten aus dem geschützten Netzwerk heraus. Das NAT-Verfahren verbirgt eine Maschine mit eigenem IP-Subnetz und mehreren Netzwerkteilnehmern hinter einer einzigen IP-Adresse. Externe Zugriffe auf diese IP-Adresse werden selbsttätig an eine vorbestimmte IP-Adresse im Netzwerk hinter den Router weitergeleitet. Bei Bedarf bleibt das Gerät somit von außen erreichbar. Das gewährleistet eine hohe Sicherheitsstufe.

### Quellenangaben

Bundesamt für Sicherheit in der Informationstechnik, www.bsi.bund.de/gshb/deutsch/m/m05070.htm
www.weidmueller.com
Industrial Ethernet, Weidmüller-Katalog 9-2007.