

# Umstellung notwendig

## Migration von serieller zur Ethernet-Übertragung

Theo Bongartz

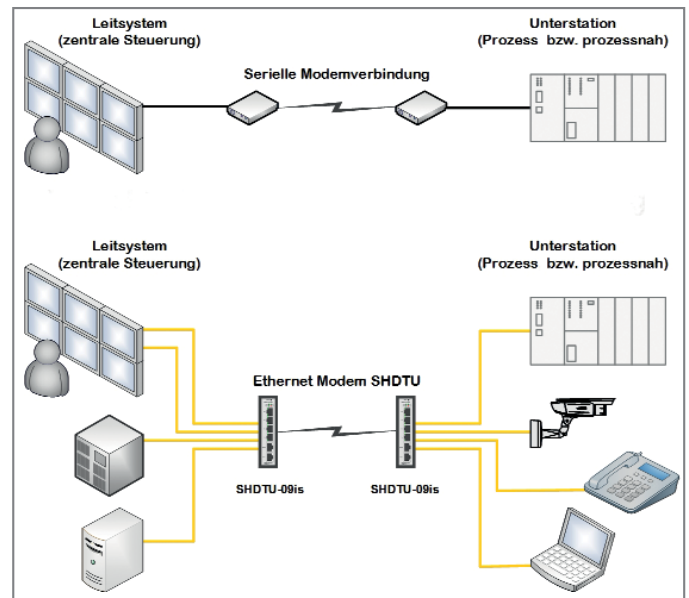
Migration ist nicht nur ein Modewort, sondern eine tatsächliche Herausforderung für viele Anwender im Bereich der industriellen Datenübertragung. Die bisherigen Verbindungen zwischen dezentralen Automatisierungsanlagen bei Versorgern, in der Industrie oder im Verkehrswesen und der zentralen Leittechnik werden vielfach noch über proprietäre oder genormte serielle Protokolle und Schnittstellen abgewickelt. Hierzu werden häufig analoge Stand- oder Wählverbindungen über öffentliche und/oder eigene Netze genutzt. Anders ausgedrückt: Zehn bis zwanzig Jahre alte serielle Infrastruktur muss auf ein modernes Ethernet-basiertes Netz umgestellt werden.

In der Regel besteht ein serielles Fernwirk- oder Automatisierungsnetz aus einer Vielzahl von Einzelverbindungen in einer Stern- oder Linienstruktur mit langsamer Datenübertragung (600/1.200 bit/s), großer Reichweite (bis zu 20 km) und einer stabilen und zuverlässigen Übertragung. Dazu wurden betriebseigene Kupferleitungen, pri-

### Übertragung über öffentliche Netze

Die Übertragung über öffentliche Netze hat sich im Laufe der letzten Jahre entscheidend verändert. Im Jahr 2010 wurden die analogen Standardfestverbindungen abgekündigt, über die ein erheblicher Anteil der Außenstationen angebunden war. Zudem werden die Datendienste im GSM-Netz

Bild 1: Im Gegensatz zum seriellen Fernwirk- oder Automatisierungsnetz (oben) erlaubt eine Ethernet-basierte Infrastruktur (unten) das Übertragen verschiedener Dienste über eine Verbindung



vate Datenfunkverbindungen, gemietete analoge Standleitungen oder Wählverbindungen im Fest- oder im GSM-Netz verwendet. Über diese konnte das zentrale Leitsystem ständig (bei Standleitungen) oder im Aufrufbetrieb (Wählverbindungen) mit den Außenstationen kommunizieren. Über die dazu genutzten Verbindungswege ist nur diese und keine weitere Anwendung möglich.

### Wechsel zu Ethernet

Der Wechsel zu Ethernet als Infrastruktur für die Datenübertragung hat vielfache Gründe. Sie können in drei Kategorien gegliedert werden:

- Übertragung über öffentliche Netze;
- erhöhtes Datenvolumen;
- technische Anforderungen.

und aktuell auch im Sprachnetz von Leitungsvermittlung auf paketorientierte Übertragung umgestellt (All-IP). Das hat für die Nutzer der Datendienste den Nachteil, dass die Laufzeiten der Datenpakete erheblich verlängert werden und eine serielle Übertragung dadurch mit sehr großen Time-out-Zeiten arbeiten muss, falls die Kommunikation überhaupt noch möglich ist.

### Erhöhtes Datenvolumen

Durch technische und gesetzliche Vorgaben im Bereich der Abfragezyklen und Datenpunkte werden immer größer werdende Datenmengen benötigt. Ferner kommen neue Dienste wie IP-Telefonie oder Kameraanwendungen hinzu, die über serielle Verbindungen nicht zu realisieren sind. Letztendlich muss das ganze Netz

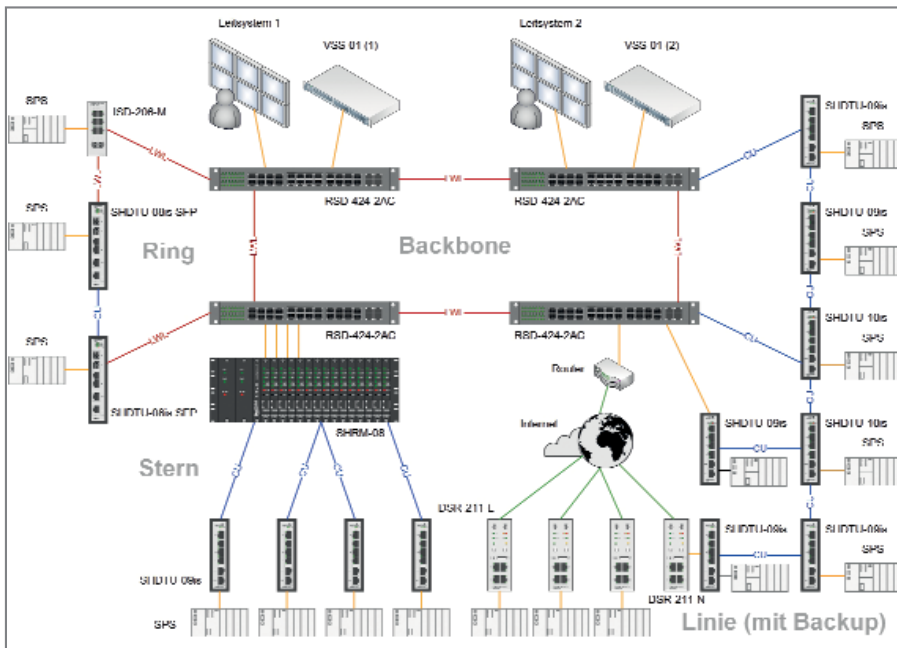


Bild 2: Im Backbone des Ethernet-basierten Netzes laufen alle Datenverbindungen zusammen

überwacht werden, d.h., auch hier kommt es wieder zu einem höheren Datenaufkommen.

#### Technische Anforderungen

Die technischen Anforderungen an die Fernwirkübertragungsnetze steigen weiter. Längst ist nicht mehr nur der Datendienst gefordert, über die Verbindungen soll telefoniert und Bild-daten sollen übertragen werden, der Zugriff auf zentrale Daten muss gewährleistet sein und das ganze Netz muss überwacht werden können (Bild 1). Ferner müssen neue Techniken wie Glasfaser und UMTS/LTE-Netze integriert werden. Nicht zuletzt verfügen viele Endgeräte nicht mehr über serielle Schnittstellen.

### Lösung: Ethernet-Infrastruktur

Der Wechsel zur Dateninfrastruktur Ethernet bringt deutliche Vorteile mit sich: Es können viele Dienste parallel und mit sehr hoher Übertragungsgeschwindigkeit übertragen und redundante Verbindungen aufgebaut werden, ein Fernzugriff auf die Stationen und Geräte ist von überall möglich und die Integration öffentlicher Netze (UMTS/LTE oder IP-Festanschlüsse) ist problemlos umsetzbar.

Der Wechsel von serieller zu IP-basierter Übertragung birgt aber auch Nachteile, denn bisher abgesicherte Pro-

duktionsprozesse werden von außen und innen angreifbar. Vor allem bei älteren Fernwirkanlagen ist damit zu rechnen, dass das Thema Sicherheit bisher nachrangig behandelt wurde.

### Netzaufbau

Ethernet kann im Prinzip über alle vorhandenen Medien wie Glasfaser, Kupfer, Datenfunk oder öffentliche Netze/Mobilfunk übertragen werden. An die Übertragungsnetze werden in der Regel folgende Anforderungen gestellt:

- hohe Verfügbarkeit: Netze und Übertragungssysteme sind jederzeit nutzbar;
- zuverlässige Übertragung: Daten treffen mit größter Sicherheit beim Empfänger ein;
- unverfälschte Übertragung: Daten kommen ohne ungewollte Veränderung beim Empfänger an;
- schnelle Übertragung: Daten kommen mit möglichst geringer Verzögerung beim Empfänger an;
- effiziente Übertragung: die Auslastung des Übertragungskanal für Nutzdaten ist möglichst hoch.

Dazu wird im Kernbereich des Netzes zwischen wichtigen Knotenpunkten der sog. Backbone (Rückgrat) aufgebaut (Bild 2). Da hier alle Datenverbindungen zusammenlaufen, werden hohe Datenraten und ein redundanter Aufbau (Ring) benötigt. Der Backbone

wird in den meisten Fällen über Glasfaserverbindungen realisiert. Daran werden alle weiteren Stationen ring- oder sternförmig angebunden. Ebenso werden hier Netzübergänge zu öffentlichen Netzen oder Büronetzen bewerkstelligt.

Zur Überwachung und zum Management der Übertragungskomponenten und der Infrastruktur können Standardsysteme auf SNMP-Basis (Simple Network Management Protocol) eingesetzt werden. Allerdings muss hier zwingend die SNMP-Version 3 genutzt werden, da alle Vorgängerversionen Passwörter unverschlüsselt übertragen.

### Sicherheit

Durch den Wechsel von serieller zu IP-basierter Übertragung muss auch der Punkt Datensicherheit näher betrachtet werden. Mit seiner Veröffentlichung am 24. Juli 2015 trat das IT-Sicherheitsgesetz in Kraft und brachte spezielle Anforderungen für Betreiber kritischer Infrastrukturen mit sich. Betroffen sind vor allem die Sektoren Energie, Wasser, Transport und Verkehr sowie Informationstechnik und Telekommunikation, die die Mindeststandards zur IT-Sicherheit aus dem am 12. August 2015 veröffentlichten IT-Sicherheitskatalog umsetzen, einhalten und zertifizieren müssen. Die Zertifizierung muss der Bundesnetzagentur bis zum 31. Januar 2018 nachgewiesen werden. Ausschlaggebend dazu ist der ISO-Standard 27001 inklusive der ergänzenden Standards mit den fortlaufenden Nummern 270xx.

Für das Datennetz müssen die eingesetzten Komponenten im Minimum folgende Standards einhalten:

- Trennung der Anwendungen durch VLAN;
- eigenes VLAN für das Management der Geräte;
- HTTPS, SSH: Zugriff mit eigenen Zertifikaten;
- SNMPv3 für die Überwachung;
- passwortgeschützter Zugriff mit unterschiedlichen Administrationsebenen;
- Abschalten nicht genutzter Ports;
- MAC- und IP-Authentifizierung je Port.

## Nutzung der vorhandenen Kabelinfrastrukturen und der öffentlichen Netze

Glasfaserverbindungen sind mit Sicherheit die beste Wahl für schnelle Datenverbindungen, doch in vielen Fällen sind diese Netze bei den Versorgern, in der Industrie oder im Verkehrswesen noch im Ausbau oder noch gar nicht vorhanden. Hier können die vorhandenen Kupferleitungen in Telefonqualität und/oder öffentliche Netze zur Übertragung genutzt werden.

Für die IP-basierte Übertragung über eigene Kupferleitungen werden Ethernet-Modems verwendet, die in Linien-, Stern- oder Ringstrukturen eingesetzt werden können. Je nach Hersteller können Entfernungen bis 25 km ohne Repeater bei Geschwindigkeiten bis zu 15,3 Mbit/s je Kupferdoppelader überbrückt werden. Werden höhere Geschwindigkeiten benötigt, können mehrere physische zu einer logischen Leitung zusammengeschaltet werden (Bonding).

Die eingesetzten Modems sollten den Sicherheitsanforderungen nach DIN 27001 entsprechen und im Layer-2 (Bridge) oder Layer-3-Betrieb (Router) eingesetzt werden können. Für sicherheitskritische Anwendungen empfiehlt sich zudem eine Verschlüsselung der Daten per VPN, wenn keine Ende-zu-Ende-Verschlüsselung von der Fernwirkanlage zum Leitsystem möglich ist.

Ebenfalls vorteilhaft ist eine Kombination aus Kupfer- und Glasfaserports, so dass Netze mit unterschiedlichen Medien einfach – ohne zusätzliche Geräte – miteinander gekoppelt werden können.

Bei der Datenübertragung über öffentliche Netze sollten grundsätzlich Router mit VPN-Verschlüsselung zur Anbindung der Außenstationen eingesetzt werden, damit ihre Daten entsprechend geschützt werden. Auf der zentralen Seite können Router oder Firewalls zur Verwaltung und Rechtevergabe der einzelnen Verbindungen verwendet werden. Die Einrichtung dieser Verbindungen ist in vielen Fällen nicht ganz einfach und erfordert

ein tiefes IT-Know-how. Daher werden häufig VPN-Security-Server (VSS-01) eingesetzt, die auf feste Router-Typen abgestimmt sind und eine automatische Einrichtung über die Weboberfläche erlauben. Damit ist es auch dem Nicht-IT-Fachmann möglich, hochsichere und zertifikatsbasierte VPN-Verbindungen zu etablieren.

## Migration seriell zu Ethernet

Es ist nicht in allen Fällen möglich, die Infrastruktur und die Fernwirkstationen gleichzeitig zu tauschen. Zumeist erfolgt ein fließender Übergang durch den Wechsel des Leitsystems, das Einrichten der Infrastruktur und den schrittweisen Austausch der Fernwirkstationen. Für die Übergangszeit ist es erforderlich, dass die seriellen Verbindungen über die Ethernet-Infrastruktur weiterbetrieben werden können. Dazu werden Ethernet-Seriell-Konverter verwendet, die im einfachsten Fall ein Standleitungsmodem simulieren (Bild 3). Diese Konverter können als separate Geräte eingesetzt oder in die Übertragungstechnik integriert werden. Sie bieten eine serielle Schnittstelle zum Endgerät und eine Schnittstelle zur Einbindung in die IP-Welt. Einfach formuliert: An beiden Enden der Übertragungsstrecke steht eine serielle Schnittstelle zur Verfügung, wie bei den bisher eingesetzten Modems, mit dem Unterschied, dass nicht mehr über die Kupferleitung, sondern über die Ethernet-Infrastruktur übertragen wird.

Interessanter wird es bei dem Aufrufbetrieb, bei dem – von zentraler Stelle – die Außenstationen über analoge oder GSM-Wählverbindungen angerufen und die Datenübertragung etabliert wird. Auch hier können entspre-

chende Router in der Zentrale und den Außenstationen eingesetzt werden, die zusätzlich über den AT-Befehlsatz verfügen und sich wie ein Wählmodem verhalten. Anstatt der Telefonnummer wird nun die IP-Adresse des Ziels eingegeben, und die Anwendung kann wie bisher weiter betrieben werden.

## Fazit

Durch den Wegfall bzw. die Änderung der Dienste in öffentlichen Netzen und die immer größer werdenden Anforderungen und Datenmengen ist

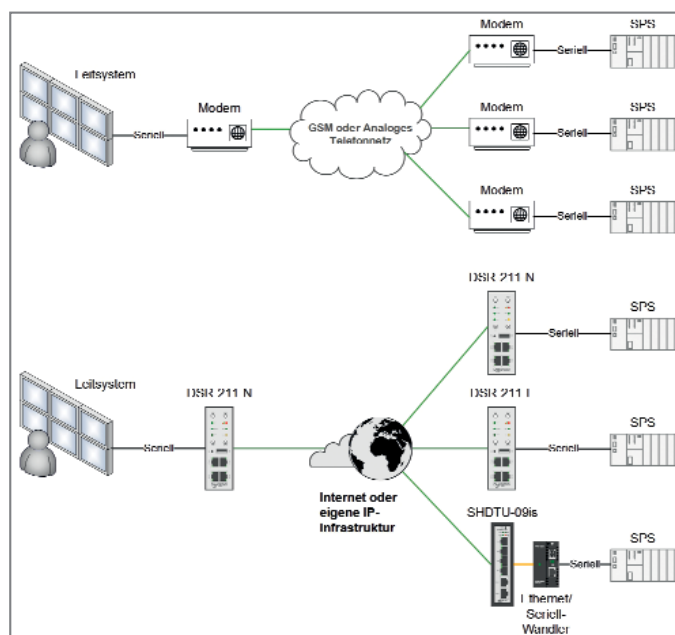


Bild 3: Für den fließenden Übergang von der seriellen zur Ethernet-basierenden Infrastruktur kommen Ethernet-Seriell-Konverter zum Einsatz

der Umstieg von der seriellen auf die IP-basierte Übertragung in den meisten Fällen unausweichlich. Es muss rechtzeitig mit der Planung begonnen werden, unter Einbeziehung aller möglichen bzw. vorhandenen Infrastrukturen wie Glasfaser, Kupfer, Datenfunk und/oder öffentliche Netze. Zumindest die Betreiber kritischer Infrastrukturen müssen dabei die erforderlichen Sicherheitsbestimmungen in der Datenübertragung einhalten und zertifizieren lassen.

Für den fließenden Übergang von einer seriellen Datenübertragung zu Ethernet stehen entsprechende Lösungen zur Verfügung, die es erlauben, serielle Verbindungen über eine IP-Infrastruktur weiter zu betreiben. (bk)