Konzept INAT

Werner Krings, INAT GmbH, Nürnberg

Entflechtung von Kommunikationsbeziehungen – Administration mit parametrierbaren Modulen

Die heutigen industriellen Ethernet Netzwerke unterscheiden sich nicht nur durch ihre Komplexität gegenüber den Büronetzen.
Seit zwei Jahrzehnten wächst das Anlagennetz mit herstellerspezifischen Protokollen wie Modbus on TCP, ISO on TCP (RFC1006), EtherNet/IP, Sinec H1 oder S7/S5.
Der Umgang mit solchen Anlagennetzwerken gehört "vom Tagesgeschäft" am allerwenigsten in die Hand des Maschinenbauers. Nur steht er seinem Kunden gegenüber in der Pflicht und Verantwortung.

Anlagennetzwerke können in viele, kleine Netzwerke unterteilt werden. Das vereinfacht den strukturellen Aufbau und dessen Pflege durch die IT-Abteilung, aber nicht die betriebstechnische Administration durch die Betriebstechnik bzw. durch die Instandhaltung.

Netzwerkwissen der IT-Profis und Anlagenwissen der Instandhalter müssen sich in intuitiv bedienbaren Werkzeugen wiederfinden - einfaches parametrieren von Beziehungen (Tabellen) statt komplexer Programmierung. Damit lässt sich nicht nur der Ist-Zustand der Kommunikationsbeziehungen erfassen und analysieren, sondern es ist auch eine Aufrechterhaltung der Kommunikation (Bypass) während der Umbauphase möglich.

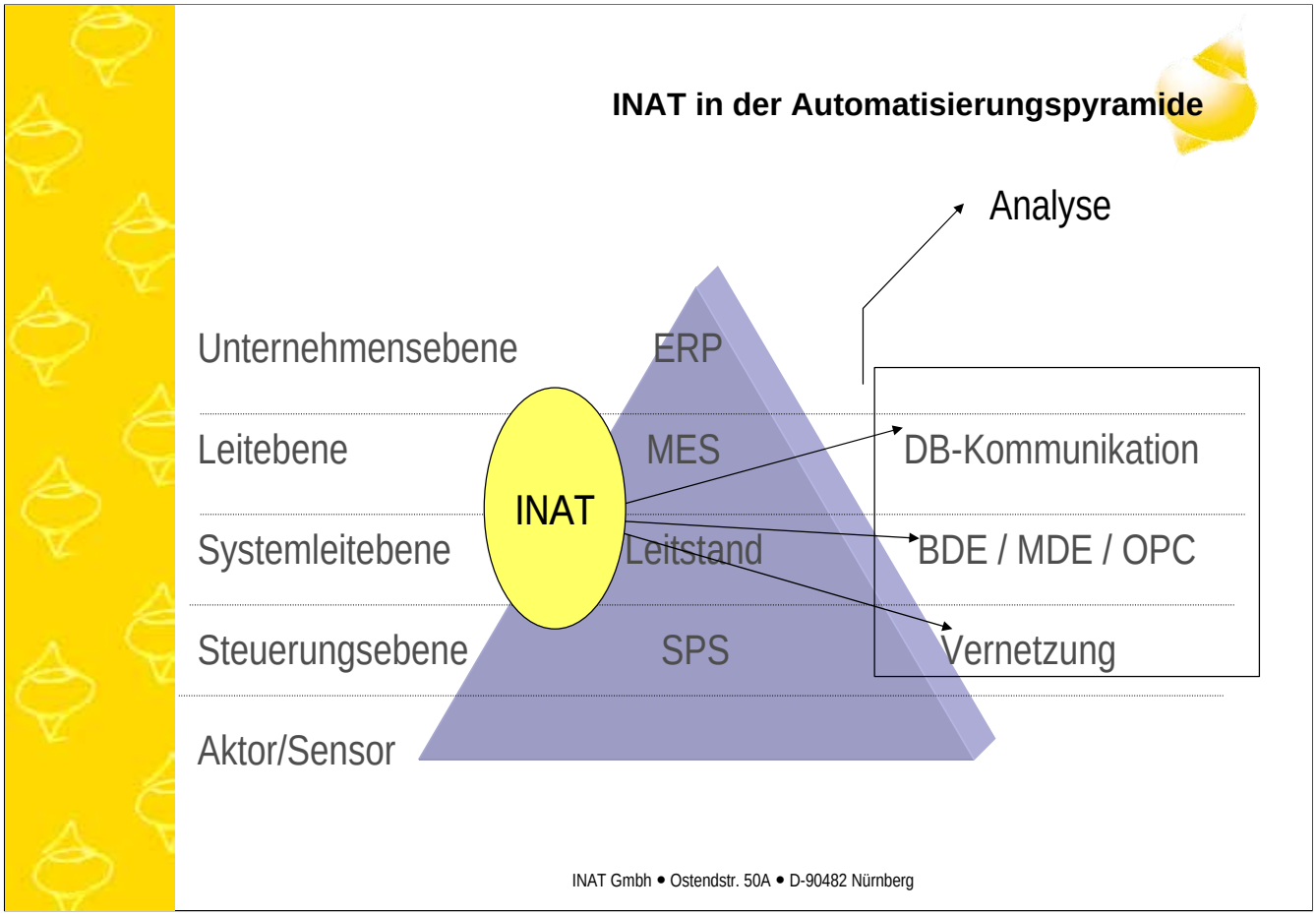
Prozessdaten können im Anschluss direkt, ohne das Steuerungsprogramm zu verändern, in eine Datenbankstruktur übertragen werden. Die sich daraus ergebenen Fortschritte der einzelnen Produktions- bzw. Montageanlagen stehen als Verbesserung zur Verfügung. Mit solch einer Vorgehensweise ist die Administration des Anlagennetzes, über einen logischen und organisatorischen Zugriffsschutz durch den Betriebstechniker möglich.

Werner Krings ist seit 11 Jahren geschäftsführender Gesellschafter der INAT GmbH.
Vorher war er 8 Jahre bei Honeywell-IPC und hat zusammen mit der Automobilindustrie Konzepte für die Anlagen- und Fertigungsvernetzung entwickelt und diese auch in Betrieb genommen. Zusammenfassend sind dies fast 20 Jahre Automatisierungsnetzwerke.
werner.krings@inat.de

Entflechtung von Kommunikationsbeziehungen

Administration mit parametrierbaren Modulen

Referent: Werner Krings
Geschäftsführer, INAT GmbH

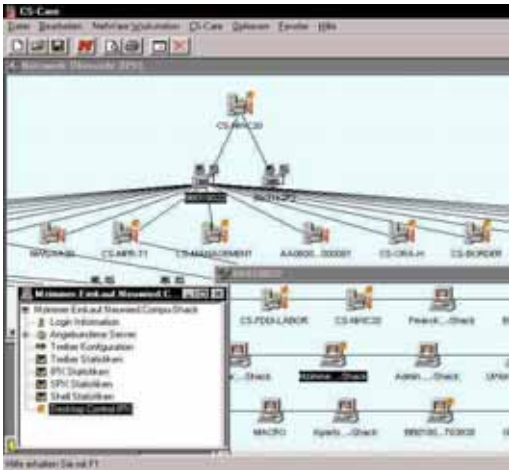

INAT in der Automatisierungspyramide
Analyse
Unternehmensebene
ERP
Leitebene
MES
DB-Kommunikation
INAT
Systemleitebene
Leitstand
BDE / MDE / OPC
Steuerungsebene
SPS
Vernetzung
Aktor/Sensor
INAT Gmbh • Ostendstr. 50A • D-90482 Nürnberg

Agenda

1. Engineering / Netzwerk-Infrastruktur
2. Umbau vs. Beeinträchtigungen der Produktion
3. Administration durch den Betriebselektriker
4. Organisation, unabsichtliche Störung vermeiden
5. Risiken im Netzwerk

1. Engineering / Netzwerk-Infrastruktur

- Erfassung des Ist-Zustandes – Teilnehmer im Netz
- 1. Möglichkeit - Aktive Diagnose



Vorteil:
- Netzwerkweiter Scan durch alle Topologien
- preiswert
- Tools frei verfügbar

Nachteil:
- Hohe störende Netzwerklast
- zeigt Aktivität aber nicht welche

Bei Anlagenerweiterungen ist es unabhängig, ob es sich um eine Alt- oder Neuanlage handelt. Unabdingbar ist die Erfassung des Ist-Zustandes. Erst wenn sämtliche Anlagenmodule in ihrer Funktion und in der Beziehung untereinander bekannt sind, wird üblicherweise ein neues Modul mechanisch wie auch elektrisch integriert.

Was an dieser Stelle für mechatronische Komponenten gilt, muss natürlich auch für Netzwerkkomponenten selbstverständlich sein. D.h. welche Netzwerkteilnehmer befinden sich in meinem Netzwerk?

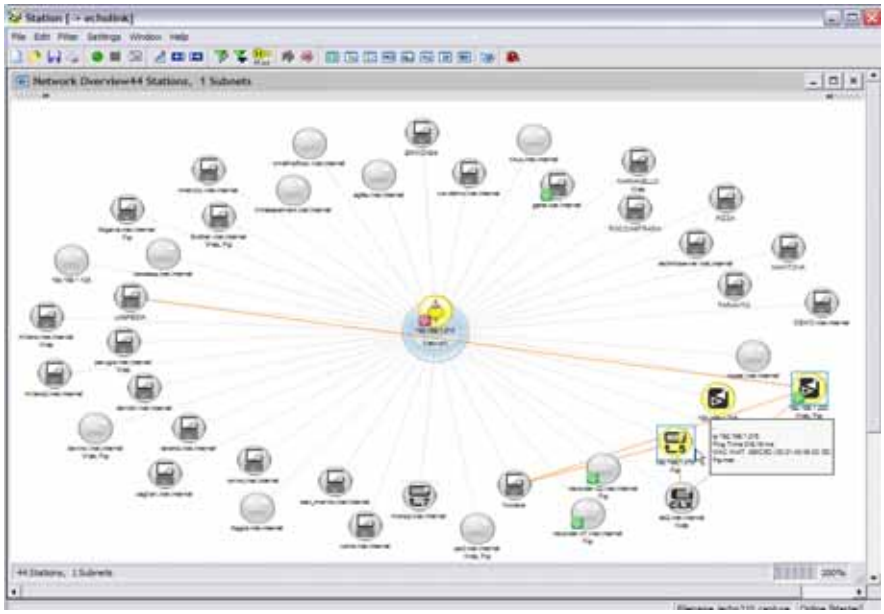
Um dies herauszufinden besteht die Möglichkeit einer aktiven Diagnose. Dabei wird ein aktiver Scan, also eine gezielte Suche durch alle Topologien des Netzwerkes geführt. Jede in diesem Netzwerk mögliche IP-Adresse wird gerufen – daher auch die Bezeichnung Brülltool. Sie sind am Markt freiverfügbar und verursachen keine hohe Investition.

Der Nachteil dieser Tools ist zweifellos die hohe Netzwerklast, die durch die Brüllerei im Netzwerk verursacht wird. Darüber hinaus wird zwar eine Aktivität angezeigt, aber nicht welche. Vergleichbar ist dies mit einer Anzeige an einer Telefonanlage. Es wird angezeigt welche Leitungen belegt sind, aber ob und welche Informationen ausgetauscht werden, ist nicht festzustellen.

……
……
……
……
……
……

1. Engineering / Netzwerk-Infrastruktur

- Auffindung der Kommunikationsbeziehung
- 2. Möglichkeit - Passive Diagnose (Mithören)



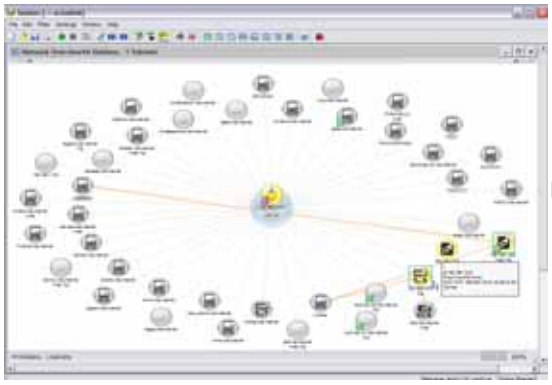
Um festzustellen welche Information im Netzwerk ausgetauscht werden, ist es notwendig die Kommunikationsteilnehmer zu kennen.

Ein passives Diagnosetool verhält sich wie ein Gerichtschreiber während einer Verhandlung - es werden Kommunikationsteilnehmer und Kommunikationsinhalt aufgezeichnet. Darüber hinaus wird ein graphischer Überblick des Netzwerkes erstellt. Spezifische Netzwerkteilnehmer wie SPS, PC, Konverter, Switche und Router können einer eindeutigen Symbolik zugeordnet werden. Kommunikationslinien zwischen den symbolischen Teilnehmern weisen auf eine Beziehung hin.

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

1. Engineering / Netzwerk-Infrastruktur

- Erfassung des Ist-Zustandes – Teilnehmer im Netz
- 2. Möglichkeit - Passive Diagnose (Mithören)



Vorteil:
- Auffindung der Kommunikationsbeziehung
- zeigt welche Aktivität
- zeigt Störung der Aktivität

⇨ somit geeignet für Fernwartung

⇨ „Agenten tauglich“

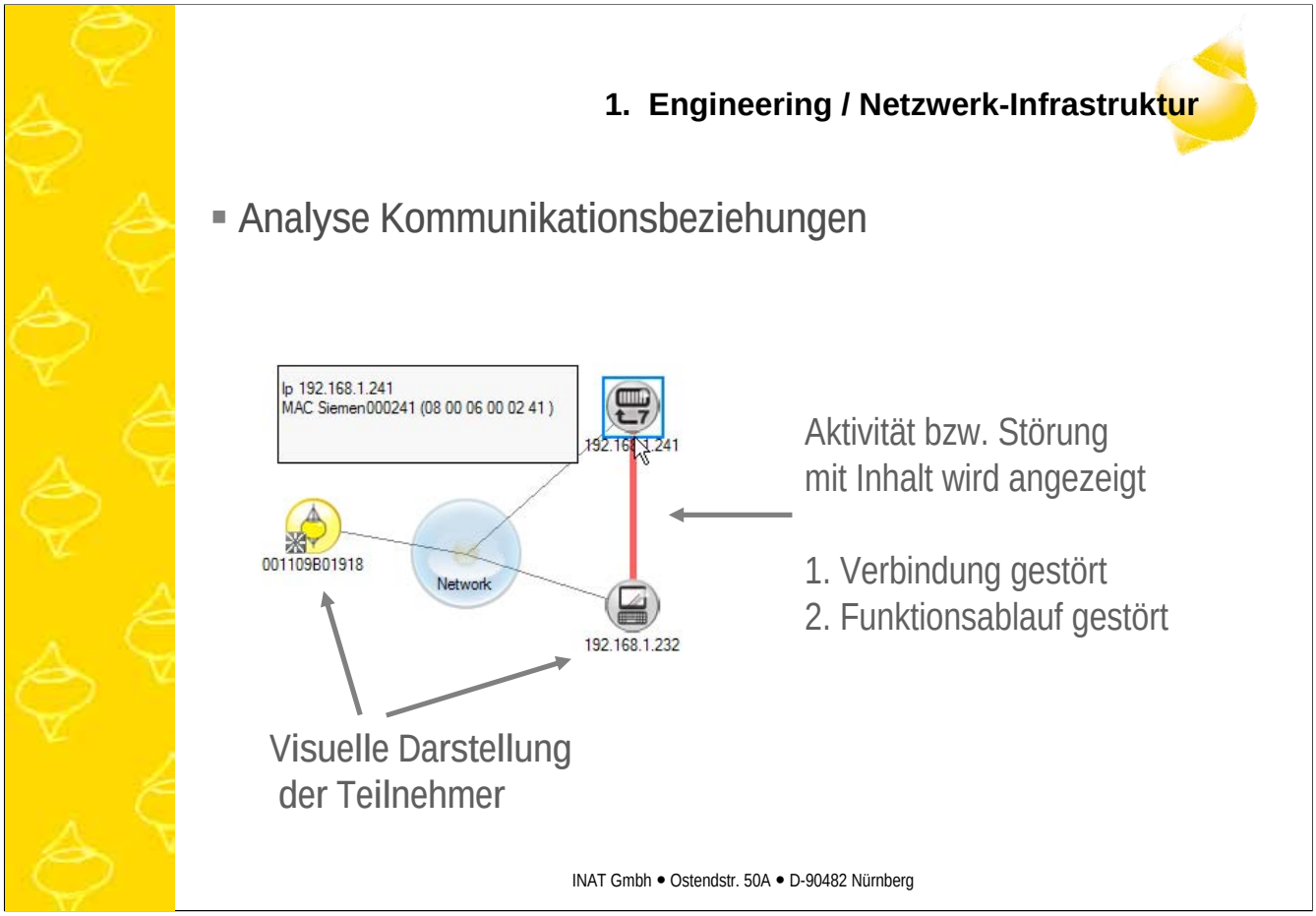
Nachteil:
- limitierte Anbieter

INAT Gmbh • Ostendstr. 50A • D-90482 Nürnberg

Nachdem öffnen der Kommunikationslinie wird der Inhalt der Beziehung sichtbar. Damit ist nicht nur der vom Leitrechner angeforderte Prozesswert, sondern auch der dazugehörende Inhalt von der SPS bereits während der Kommunikation nachweisbar.

Mit Hilfe von Hardwareagenten in Form von Seriell-Ethernet-Konvertern ist diese Diagnosefunktionalität auch in älteren gewachsenen Netzen integrierbar. Durch Analog- oder ISDN-Router ist die passive Diagnose auch für die Fernwartung geeignet.

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……



Störungen, wie nicht gewollte oder einseitige Kommunikationsbeziehungen, lassen sich somit sowohl in lokalen (LAN) wie auch in weit entfernten (WAN) Netzen schnell erkennen.

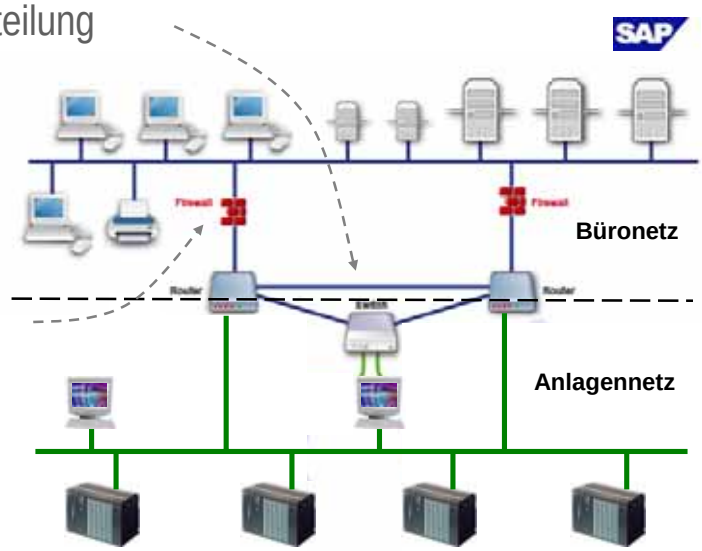
Durch die Analyse der Kommunikationsbeziehungen lässt sich nicht nur die Verbindung, sondern auch der komplette funktionale Ablauf des Montage- oder Produktionsschrittes dokumentieren.

Zusammen bildet das die Grundlage für ein Engineeringtool, das nicht nur in den Inbetriebnahmephasen, sondern auch während des kontinuierlichen Produktionsbetriebs wichtige Kenngrößen liefert.

……
……
……
……
……
……
……
……
……
……
……
……
……
……

2. Umbau vs. Produktionsbeeinträchtigung

- Aufrechterhaltung der Kommunikation
- Bypass zur Anlagenaufteilung
- Netzwerkaufteilung
- Prozessabsicherung
- Vermeidung von Stillstandszeiten
- sicherer Abschottung
- Aufrechterhaltung und Sicherung des Produktionsablaufes



INAT Gmbh • Ostendstr. 50A • D-90482 Nürnberg

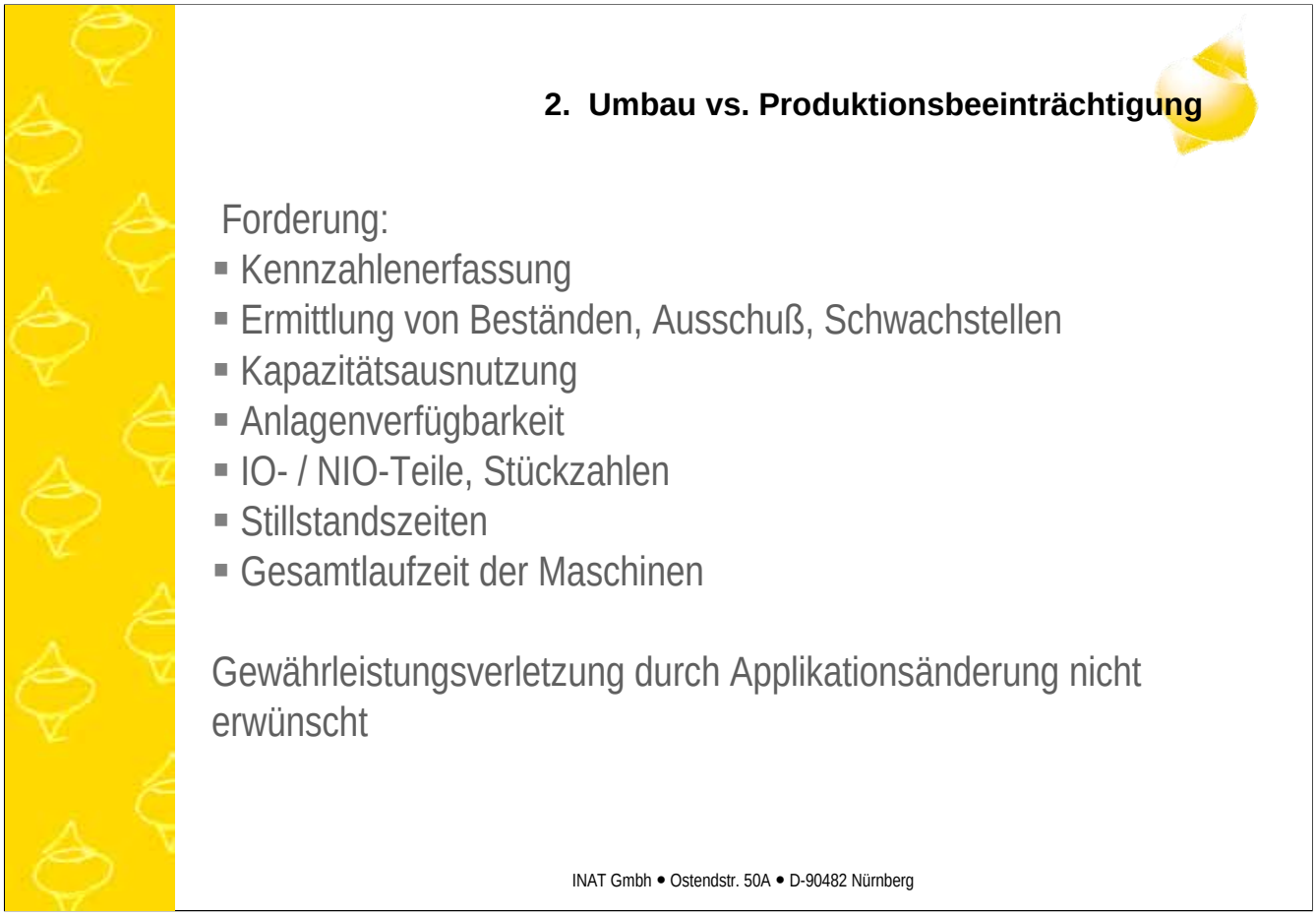
Nach der Auffindung, Erfassung und Analyse der Kommunikationsbeziehungen gilt es jetzt, die notwendigen Beziehungen während der Umbauphase aufrechtzuerhalten.

Das Anlagennetz, durch Firewall vom Büronetz getrennt, wird weiter in kleinere Netzwerksegmente aufgeteilt.

Der Übergang zwischen zwei getrennten Netzsegmenten wird durch die Zwischenschaltung einer Hard- oder Software geschützt. Somit wird das Eindringen in das jeweilige Anlagensegment verhindert.

Gezielte und bewusste Bypässe ermöglichen die Aufrechterhaltung und die Sicherung des Produktionsablaufes während des Umbaus.

……
……
……
……
……
……
……
……
……
……
……
……

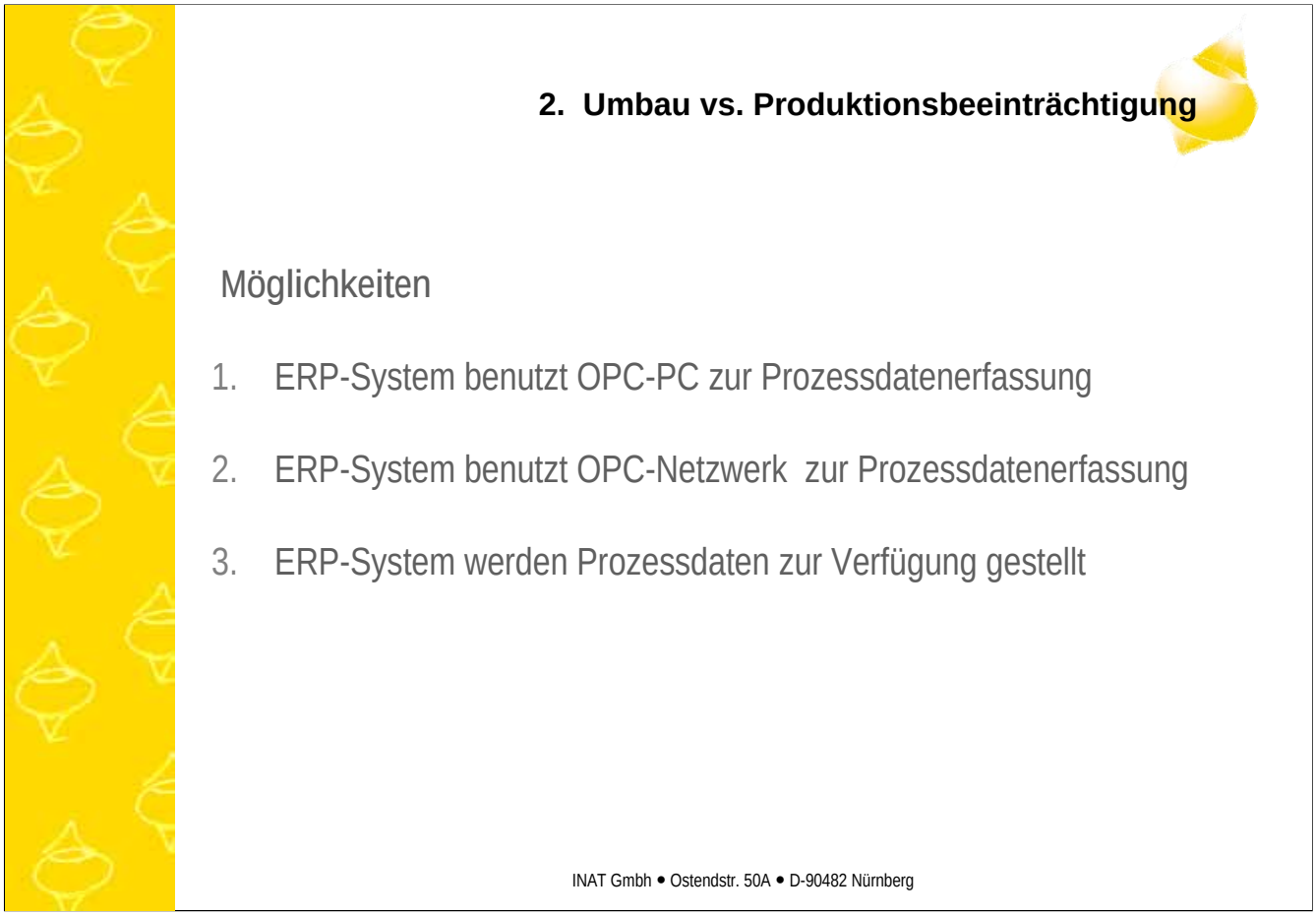


Meist ist der Auslöser der Umbaumaßnahme die Forderung einer Prozessdatenerfassung zur Bestimmung von Kennzahlen.

Die umbaubedingte Beeinträchtigung der Produktion wird u.a. durch den Einbau der Vernetzungskomponenten bestimmt. Hier hängt es im Wesentlichen von der Erweiterung des SPS-Programms und von der anschließenden Inbetriebnahme ab.

Bei Neuanlagen kommt durch die Programmänderung ggf. noch eine nicht erwünschte Gewährleistungsverletzung hinzu. Somit fällt auch die Fertigungs-IT und Anlagensicherheit beim Ausbau der Steuerungstechnik in der Verantwortung der IT-Abteilung. Damit hier das Risiko möglichst gering gehalten wird kommen immer häufiger Produkte zum Einsatz, die die Prozessdaten ohne Erweiterung des SPS-Programms erfassen.

……
……
……
……
……
……
……
……
……
……
……
……



Die von den Prozessdaten abgeleiteten Kennzahlen, wie z. B. die Stückzahlerfassung werden immer häufiger an ERP-Systemen (Enterprise Resource Planning – Planung der Unternehmensressourcen) zur weiteren Auswertung übergeben. Diese Übergabe erfolgt in der Regel über OPC-Mechamismen. Meist greift hier das ERP-System auf unterlagerte Visualisierungs-PCs oder einer OPC-Netzwerkstruktur zurück.

Es kommt aber immer häufiger die Anforderung, die Prozessdaten direkt von den Steuerungen in die Datenbankstruktur des ERP-Systems zu schreiben. Damit würden die Kennzahlen, also die ermittelte Stückzahl direkt in die Datenbanktabelle oder auch SAP übergeben.

……
……
……
……
……
……
……
……
……
……
……
……
……
……

2. Umbau vs. Produktionsbeeinträchtigung

2.1 ERP-System benutzt OPC-PC zur Prozessdatenerfassung

OPC

- heute der Standard zur herstellerunabhängigen Kommunikation in der Automatisierungstechnik
- OPC Foundation - seit 1996 zuständig für Pflege und Verbreitung des Standards
- basiert derzeit auf Microsoft DCOM-Technologie (Distributed Component Object Model)
- Üblicherweise innerhalb eines PCs

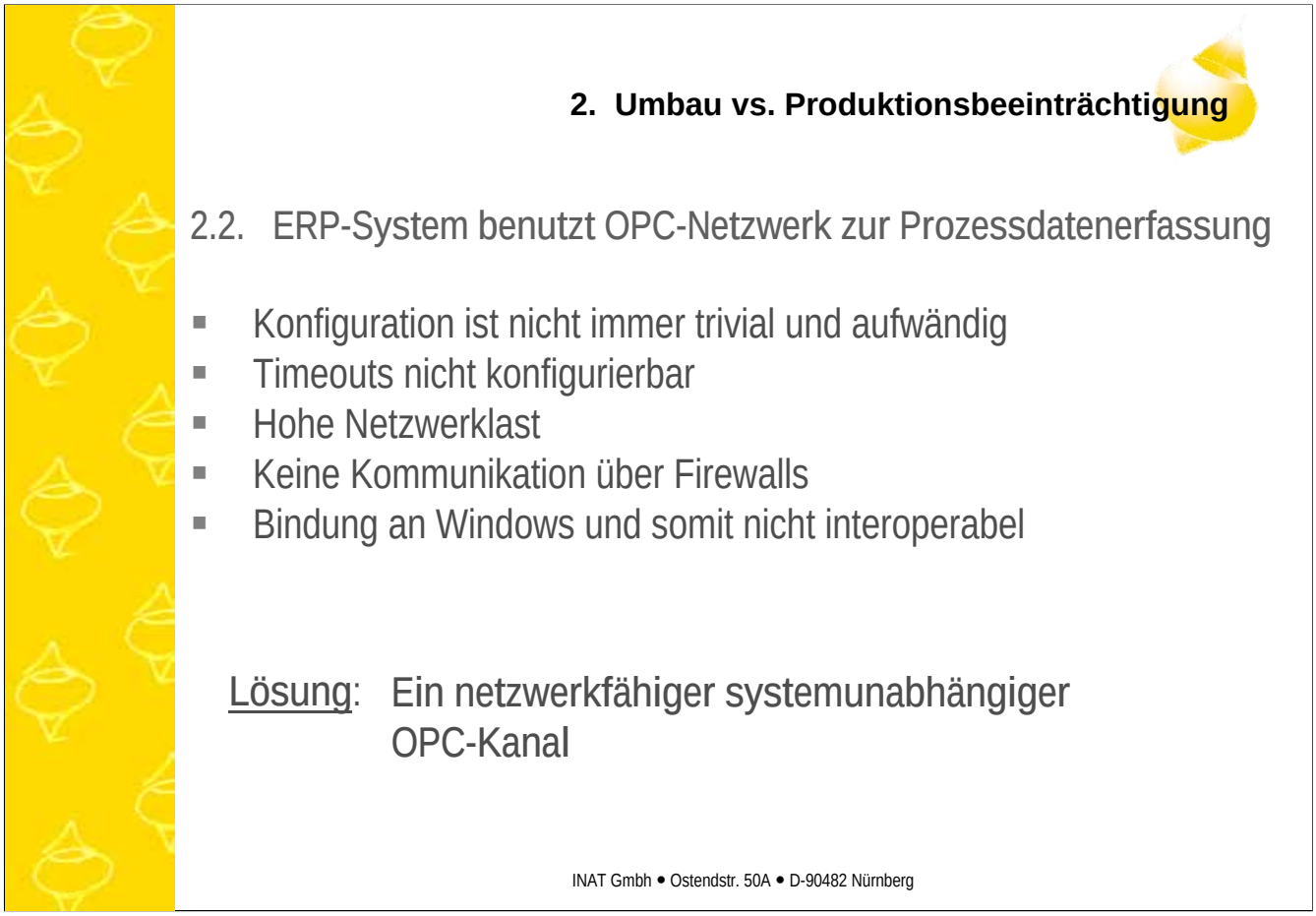
INAT Gmbh • Ostendstr. 50A • D-90482 Nürnberg

Über die OPC-Schnittstelle ist der Datenaustausch zwischen Automatisierungshardware und Anwendungssoftware auf einfachste Weise möglich. Der OPC-Server greift in einem vorgegebenen Intervall auf die Betriebs- oder Prozessdaten der Hardware zu und stellt diese dem OPC-Client zur Verfügung. Der OPC-Client liest die „durchgereichten“ Daten oder schreibt Befehle an den OPC-Server, die der Server dann als Steuerdaten an die Hardware weitergibt. Der Vorteil der OPC-Technologie besteht darin, dass die Dienste des Servers von den unterschiedlichsten Clients parallel genutzt werden können, ohne dass spezielle Treibersoftware nötig ist.

Befinden sich Client und Server auf einem Rechner, dann verwenden Sie die von Microsoft entwickelte Technologie COM – das Component Object Model - um Daten auszutauschen.

Dank der DCOM-Technologie (Distributed COM), ist OPC auch netzwerkfähig. DCOM ermöglicht COM-Aufrufe zwischen verteilten Rechnern innerhalb eines Netzwerkes.

……
……
……
……
……
……
……
……
……
……

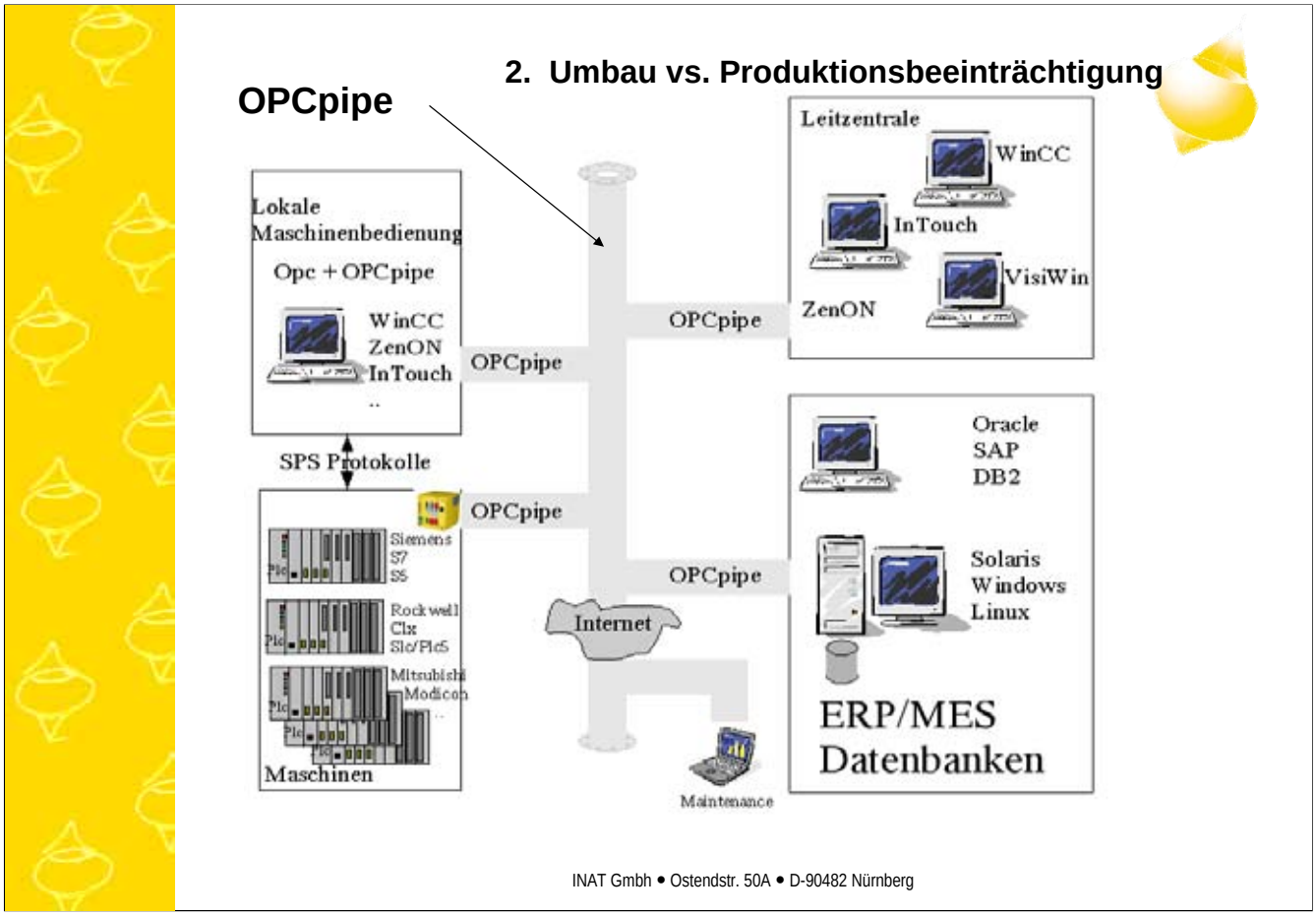


Um von einem OPC-Client auf einen entfernten OPC-Server zugreifen zu können, sind sowohl auf Client-Seite als auch auf Server-Seite Einstellungen nötig. Die Konfiguration ist jedoch alles andere als trivial und kann sehr komplex und aufwändig werden. Nicht umsonst ist DCOM das Problem Nummer 1, mit dem Anwender der netzwerkübergreifenden OPC-Kommunikation konfrontiert werden.

Ein weiteres Problem, das DCOM mit sich bringt ist die Tatsache, dass das Verbindungs-Timeout nicht konfigurierbar ist: Angenommen ein OPC-Client auf dem lokalen Rechner fordert von einem OPC-Server auf einem entfernten Rechner einen Wert an. Kommt es zu einer Unterbrechung der Netzwerkverbindung noch bevor der Client vom Server eine Antwort erhalten hat, kann der Client mehrere Minuten gezwungen werden, auf eine Antwort zu warten – auch dann, wenn die Verbindung sofort wieder hergestellt wird.

Des Weiteren funktioniert DCOM nicht mehr, wenn Firewalls zwischengeschaltet sind. Das neuste BS aus dem Hause Windows – Vista – unterstützt DCOM überhaupt nicht mehr.

……
……
……
……
……
……
……
……
……



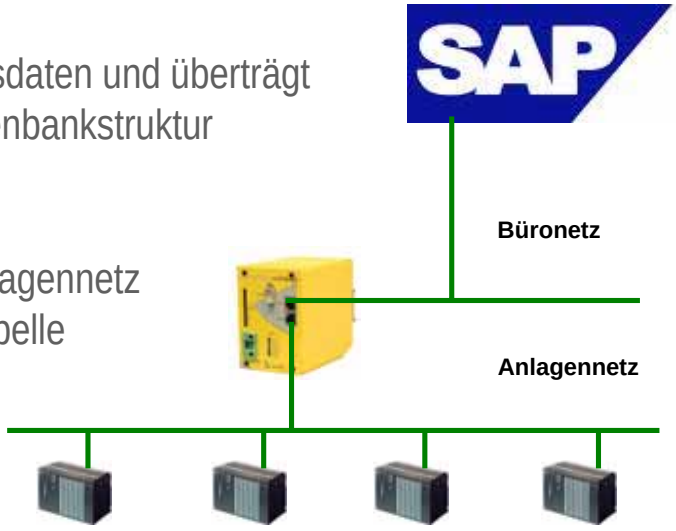
Die Lösung ist ein netzwerkfähiger, systemunabhängiger OPC-Kanal. Diese OPC-Pipe „tunnelt“ die Daten, die bei der OPC-Kommunikation zwischen Client und Server ausgetauscht werden. Die Client-Seite der OPC-Pipe, die auf demselben Rechner wie der OPC-Client installiert ist, nimmt die Anfrage des OPC-Clients entgegen und wandelt die OPC-Kommunikation in eine „normale“ TCP/IP-Kommunikation. So getunnelt werden die Daten über eine Standard TCP/IP-Verbindung über das Netzwerk zum Zielrechner übertragen. Dort angekommen, nimmt die serverseitige OPCpipe die Daten entgegen, „entschlüsselt“ sie wieder in eine OPC-Kommunikation und reicht die Daten an den OPCServer weiter. Der Server führt die Anfrage aus und schickt seinerseits die Daten zurück an den OPC-Client. Der Tunnel-Mechanismus ist in beide Richtungen identisch.

……
……
……
……
……
……
……
……
……
……
……

2. Umbau vs. Produktionsbeeinträchtigung

2.3. ERP-System werden Prozessdaten zur Verfügung gestellt

- … sammelt Prozessdaten und überträgt diese in eine Datenbankstruktur (SQL bzw. SAP)
- Trennung Büro-/Anlagennetz
- Zuordnung über Tabelle
- OPC unabhängig

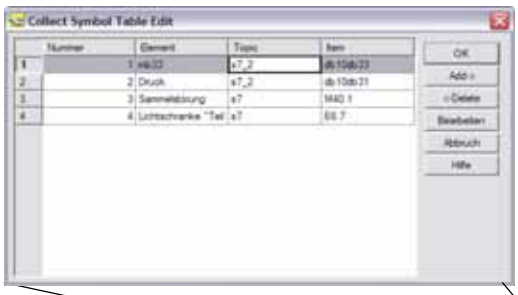


INAT Gmbh • Ostendstr. 50A • D-90482 Nürnberg

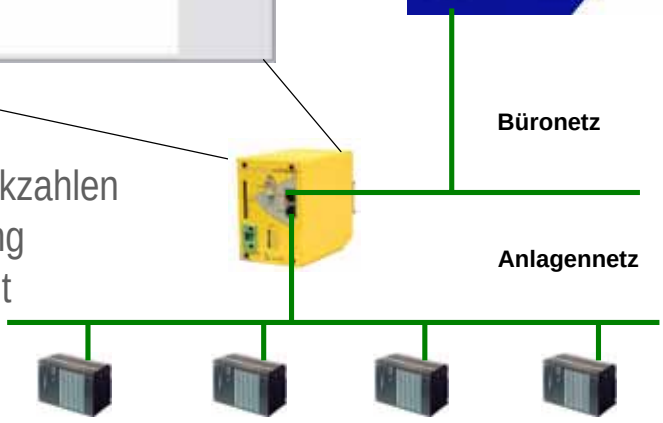
Noch einfacher ist es, wenn dem ERP-System die Prozessdaten zur Verfügung gestellt werden und nicht das ERP-System das OPC-Netzwerk nutzen muss. Echocollect sammelt Prozessdaten und überträgt diese in eine Datenbankstruktur (SQL bzw. SAP). Das Gerät mit 2 Ethernet-Schnittstellen fungiert zudem als Gateway und macht so die Trennung zwischen dem Büro- und dem Anlagennetz möglich. Die Zuordnung erfolgt über Tabellen, so dass es OPC-unabhängig arbeiten kann.

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

3. Administration durch den Betriebselektriker



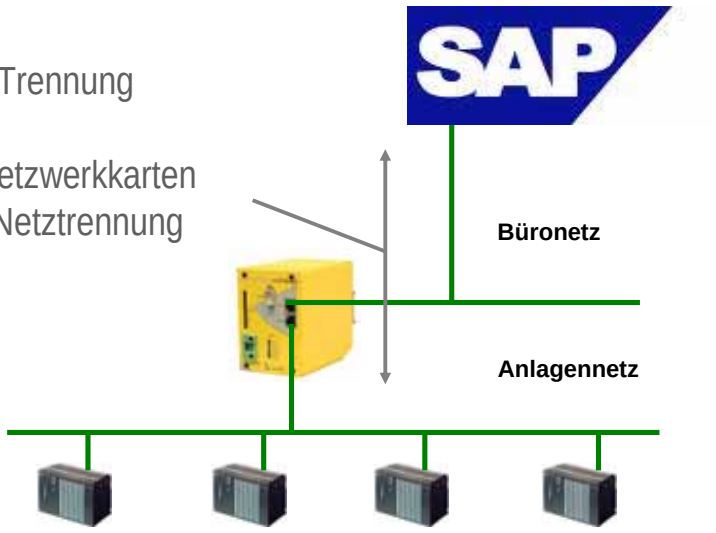
- Maschinenlaufzeit
- IO- / NIO-Teile, Stückzahlen
- Kapazitätsausnutzung
- Anlagenverfügbarkeit
- Stillstandszeiten



INAT Gmbh • Ostendstr. 50A • D-90482 Nürnberg

4. Organisation, unabsichtliche Störung vermeiden

- Zugriffsschutz
  - logische und organisatorische Trennung
  - 2 unabhängige Netzwerkkarten als Gateway zur Netztrennung

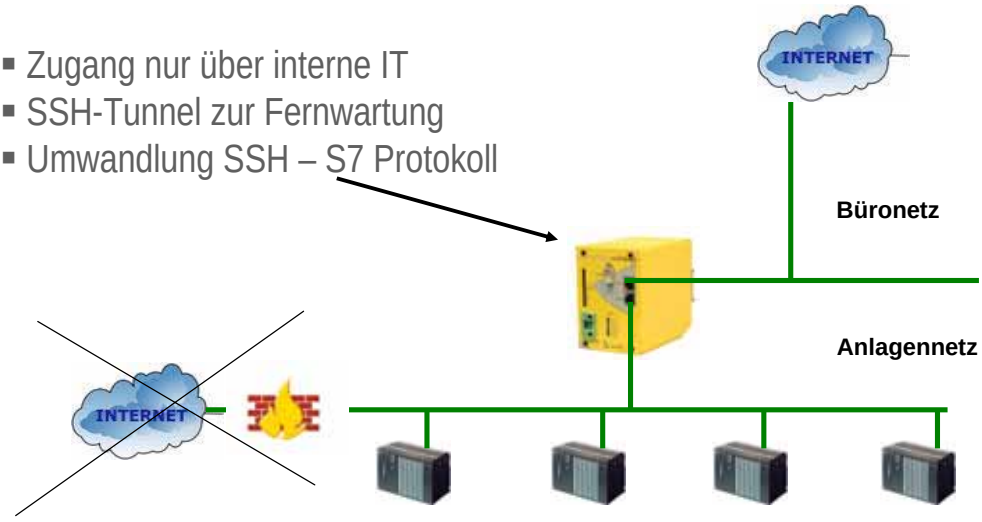


INAT Gmbh • Ostendstr. 50A • D-90482 Nürnberg

5. Risiken im Netzwerk - SPS mit sicherem Internetzugang

- Trennung von Büro- und Anlagennetz
- Technische Trennung an den Übergängen

- Zugang nur über interne IT
- SSH-Tunnel zur Fernwartung
- Umwandlung SSH – S7 Protokoll



INAT Gmbh • Ostendstr. 50A • D-90482 Nürnberg

Symmetrische Verschlüsselungsverfahren - Sender benutzt gleichen Schlüssel zum Verschlüsseln wie Empfänger zum Entschlüsseln. Je 2 Teilnehmer in einem Netzwerk benötigen einen geheimen Schlüssel.

Asymmetrische Verschlüsselungsverfahren – Ein Schlüsselpaar: Was mit dem einen verschlüsselt wurde, kann nur mit dem anderen entschlüsselt werden. Durch digitale Unterschriften wird eine Nichtabstreitbarkeit des Absenders erreicht.

IT-Sicherheit ist eine Managementaufgabe. Welchen Sicherheitsgrad man anstrebt, hängt von der Situation und dem potentiellen Schaden ab (Risikoanalyse). Je höher der Grad an Sicherheit, desto unbequemer und teurer wird Sicherheit, 100% Sicherheit gibt es nicht.

Schwachstellen sind Zugriffe über Mobile Geräte, wie Laptops oder USB-Sticks, die in das interne Netz gelangen.

SSH (Secure Shell)

……
……
……
……
……
……
……
……
……
……

Über INAT

Dienstleister mit Produkten zur Prozessabsicherung via Ethernet

- Seriell-Ethernet und Ethernet-Ethernet-Konverter
- Software OPC Server (1.000 Bytes in 40ms)
- Netzwerk Analyse (Siemens, Allen Bradley, Modicon)
- Entwicklungstools für Windows und Linux
- Schulungen und Workshops: Ethernet / Retrofit

INAT Gmbh • Ostendstr. 50A • D-90482 Nürnberg

Produktionsbereiche

INAT ist überall dort im Einsatz, wo Ware produziert und verteilt wird:

Automobilindustrie,
Lebensmittelindustrie,
Stahlindustrie,
Logistik,
Fördertechnik,
Chemie- und Pharmaindustrie,
Anlagen- und Maschinenbau usw.

Kontakt über Key Account Manager: JoergKubas@inat.de

INAT Gmbh • Ostendstr. 50A • D-90482 Nürnberg