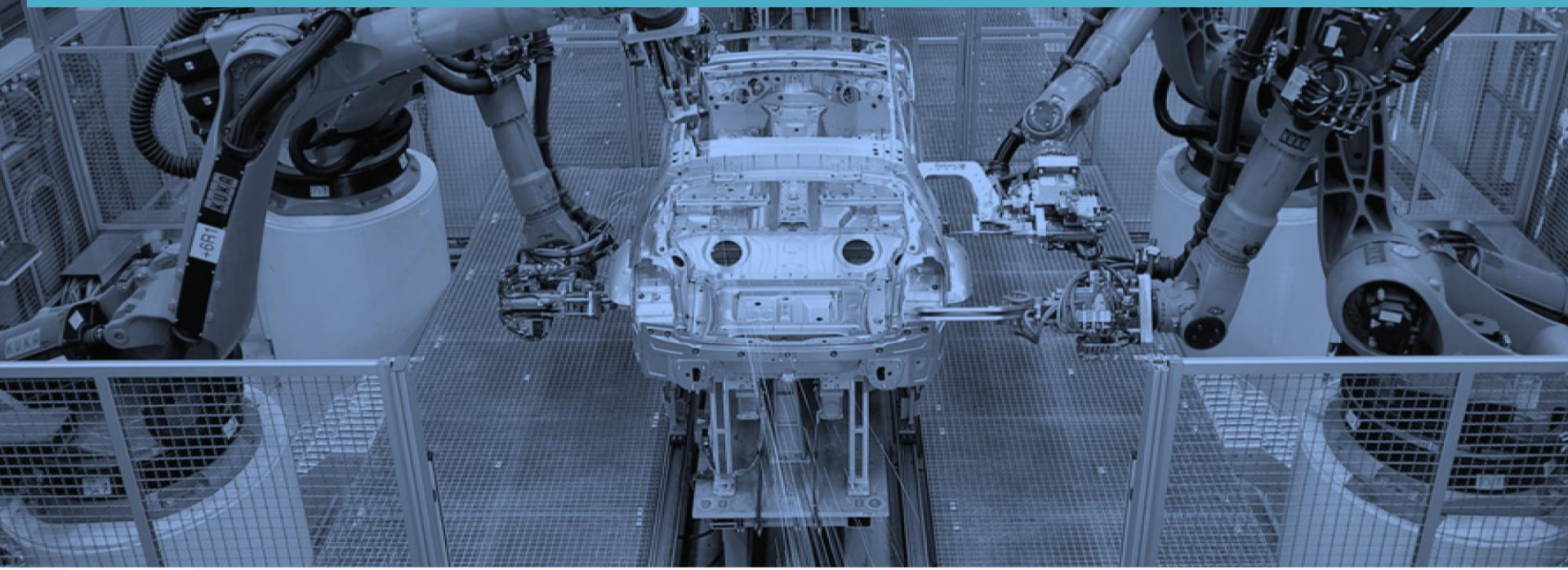
Stuxnet zum Frühstück
Industrielle Netzwerksicherheit 2.0

Stuttgart und München



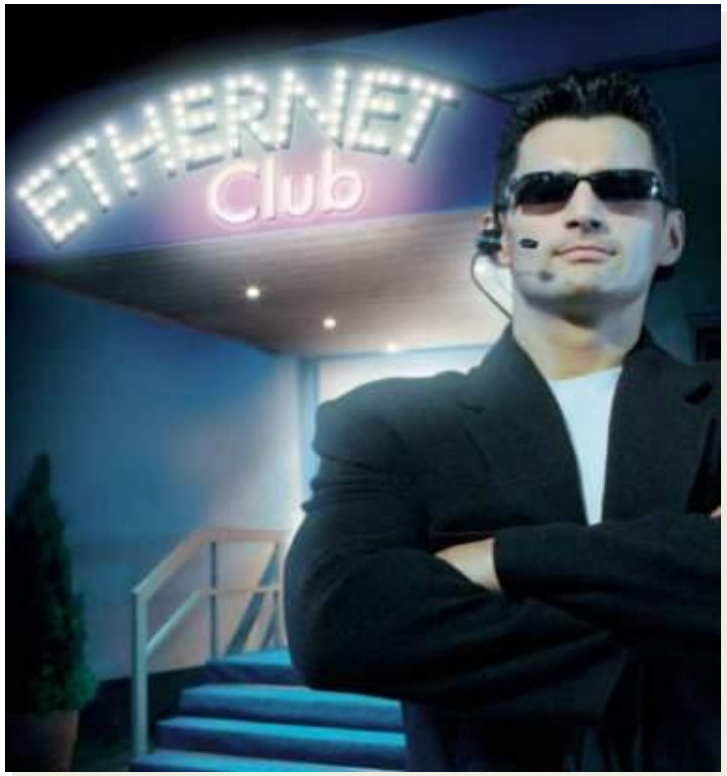
TÜV SÜD

HIRSCHMANN
A BELDEN BRAND

secXTREME
Information Security

YELLO NETCOM

Sicherheit durch Zugriffsschutz



Unternehmensdaten BELDEN 2010

- Konzernzentrale: St Louis, MO, USA
- Umsatz 2010: 1,62 Mrd. $
  - Gegenüber 2009 ca. 19% Wachstum
- 7200 Beschäftigte
- Über 16 Fertigungsstätten weltweit
- Über 20 Verkaufsniederlassungen weltweit
- Elektronik- und Kommunikationsmärkte
- Schlüsselmärkte:
  - Maschinenbau
  - Industrielle Automatisierung,
  - Broadcast, Audio/Video
  - Energiegewinnung und -verteilung,
  - Transport

Unternehmens Geschichte

BELDEN
SENDING ALL THE RIGHT SIGNALS

1902 gründet Joseph Belden die Firma Belden in Chicago, Illinois.

1993 expandiert Belden nach Europa.

2004 fusionieren Belden und Cable Design Technologies zu Belden CDT Inc.

2006 wird Belden CDT Inc. in Belden Inc. umbenannt

HIRSCHMANN
A BELDEN BRAND

1924 gründet Richard Hirschmann die Firma Hirschmann in Esslingen, Baden-Württemberg.

2005 wird die Hirschmann Automation and Control GmbH gegründet.

2007 erwirbt Belden Inc. Hirschmann Automation and Control.

lumbergautomation
A BELDEN BRAND

1933 gründen Karl und Erich Lumberg die Firma Lumberg in Schalksmühle, NRW.

2002 wird die Lumberg Automation Components GmbH gegründet.

2007 erwirbt Belden Inc. Lumberg Automation.

TÜV SÜD

HIRSCHMANN
A BELDEN BRAND

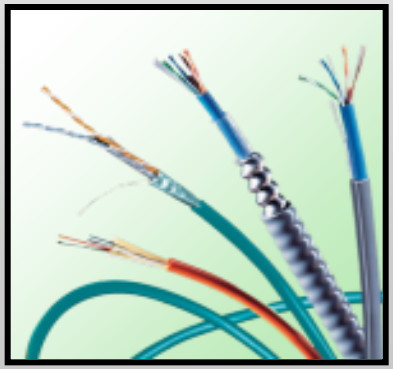
secXTREME
Information Security

YELLO NETCOM

Unsere Marken

BELDEN
SENDING ALL THE RIGHT SIGNALS

- Industriekabel
- Netzwerkkabel
- CATV-Kabel
- Rundfunkkabel
- Glasfaserkabel



HIRSCHMANN
A BELDEN BRAND

- Industrial Ethernet Switches
- FiberINTERFACES
- WLAN & Sicherheit
- Software-Management

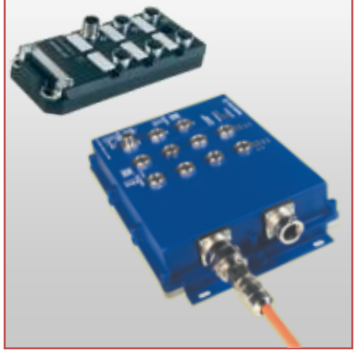
lumbergautomation
A BELDEN BRAND

- Industrielle Steckverbinder
- Aktorik-/Sensorik-Steckverbinder und Verteiler
- Feldbus-Module
- Verdrahtungslösungen

Industrial Ethernet Produkte

Switches für die Feldebene

IP67-Industrie-Switches



Control Level Switches

Security

FiberINTERFACES

Wireless LAN

Control Room Switches

Backbone-Switches

Ruggedized Switches

Netzwerk-Management

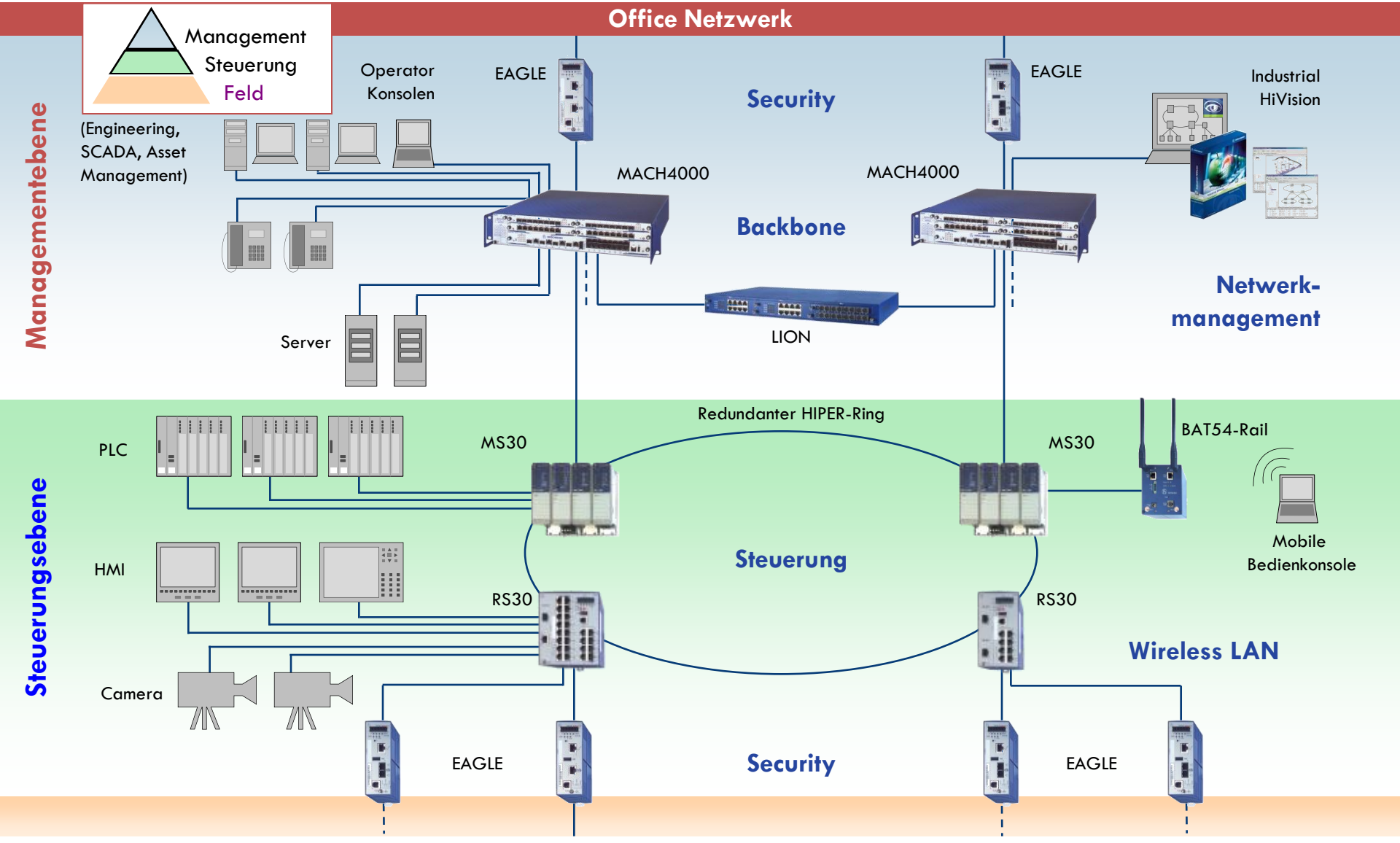
TÜV SÜD

HIRSCHMANN
A BELDEN BRAND

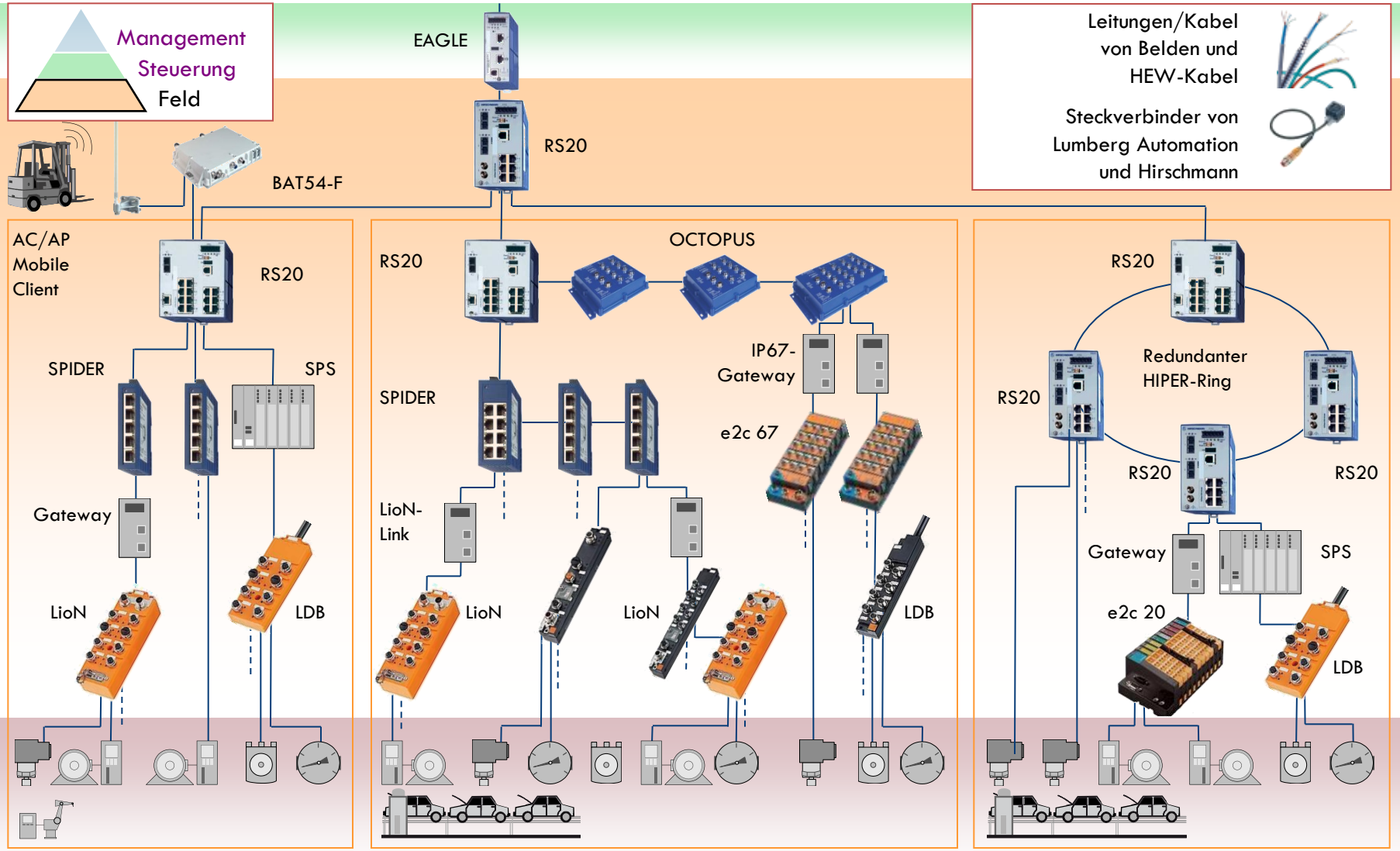
secXTREME
Information Security

YELLO NETCOM

Gesamtlösung BELDEN EMEA (I)



Gesamtlösung BELDEN EMEA (II)



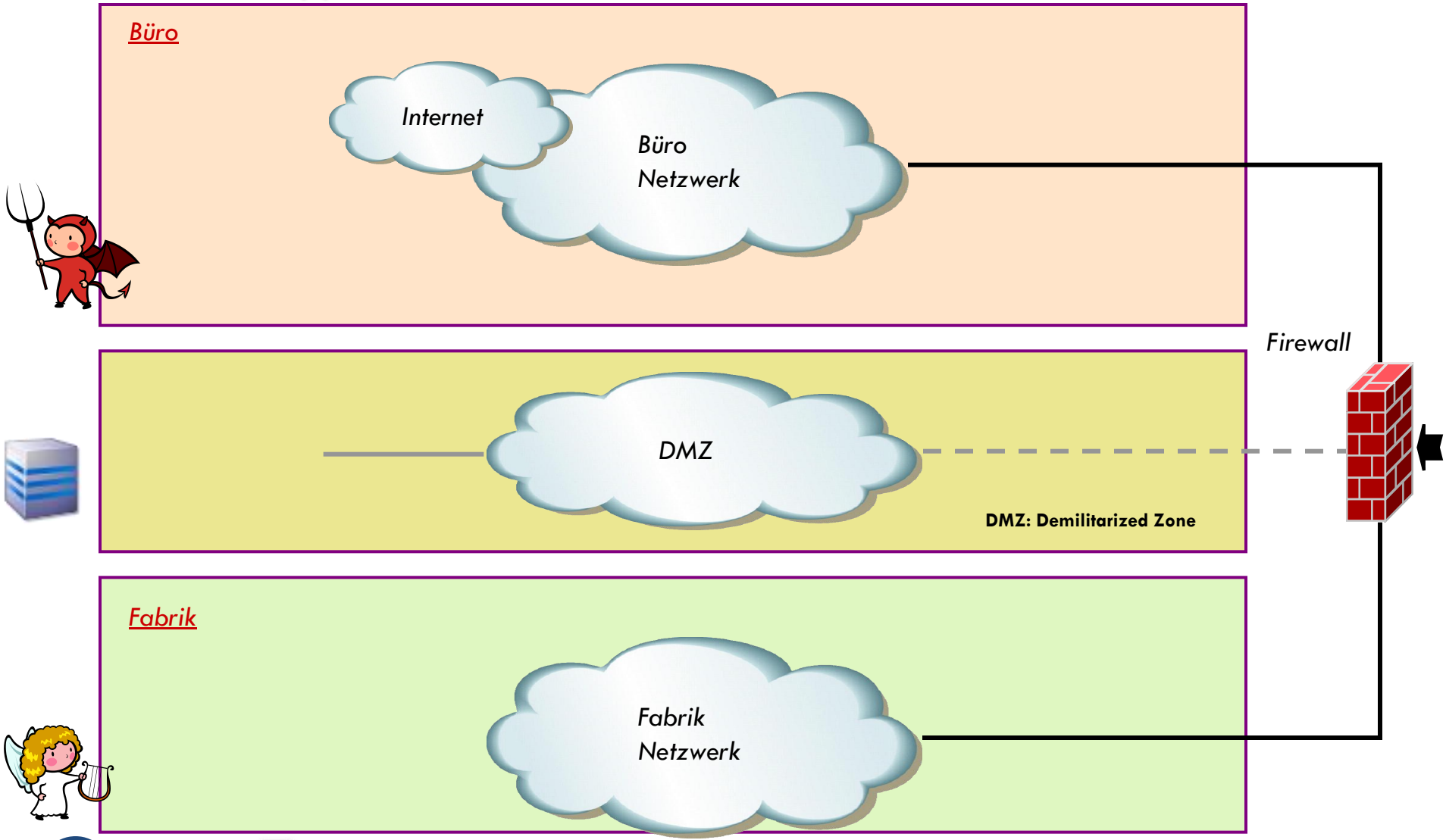
Situation Prozess- und Fabrikautomation

- Ehemals separierte Netze sollen in das Gesamtnetzwerk integriert werden um die Vernetzung von Planung und Produktion zu verbessern
- Wartungspersonal von Fremdfirmen "stöpselt sich" ungehindert auf die Maschinen bzw. in die Netze
- Es bestehen direkte Fernwartungszugänge zu Fremdfirmen
- Die Produktionsnetze sind flach aufgebaut oder die Subnetzadressen passen nicht ins IP-Konzept
- Es bestehen Garantie/Gewährleistungsansprüche bzgl. der Verfügbarkeit der Anlage, dass bedeutet, Eingriffe des Kunden in die Anlage sollten möglichst unterbunden werden

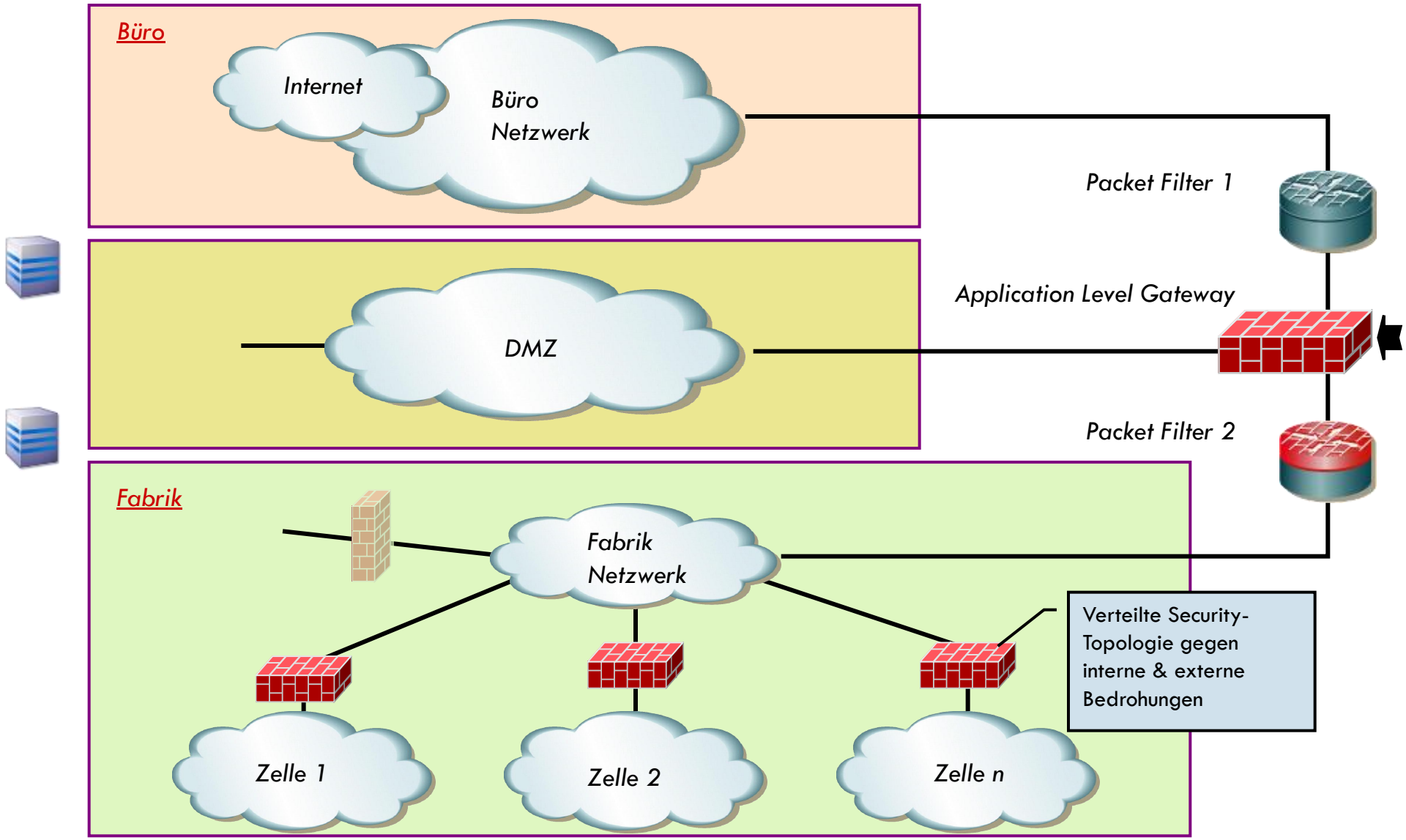
Vergleich: Büro - Produktion

	Office IT	Industrial IT
Topologie	hohe Anschlussdichte, strenge Sterntopologie	niedrige Anschlussdichte, oft Ringtopologie
Architektur	homogen, zentralisiert (Client/Server)	heterogen, lokal (autarke Zellen)
Expertenwissen und System-Know-how	zentral, hoch und spezifisch	lokal und eher breit
Wartungsfenster	periodisch, gleichzeitig (Nachtzeiten / Wochenenden)	prozessorientiert, kurz, zeitverschoben
Wichtigkeit für das Unternehmen	indirekter Einfluss auf den Unternehmenserfolg	direkte Auswirkung auf den Produktionsprozess
Anforderungen an die Ausfallsicherheit	Gelegentliche Netzwerkfehler tolerierbar	Netzunterbrechungen nicht akzeptabel
Anforderungen an die Störungsbeseitigung	Längere Zeiträume zur Fehlerbehebung werden akzeptiert	Sofortige Fehlerbeseitigung unumgänglich
Anforderungen an die Performance	Hoher Durchsatz gewünscht, Delay und Jitter unkritisch	Kritisch gegenüber Verzögerungen, moderater Durchsatz meist akzeptabel
Risikomanagement	reaktives Handeln, Funktionssicherheit (Safety) nicht betrachtet	Fehlertoleranz und Ausfallszenarien sind Planungsbestandteile

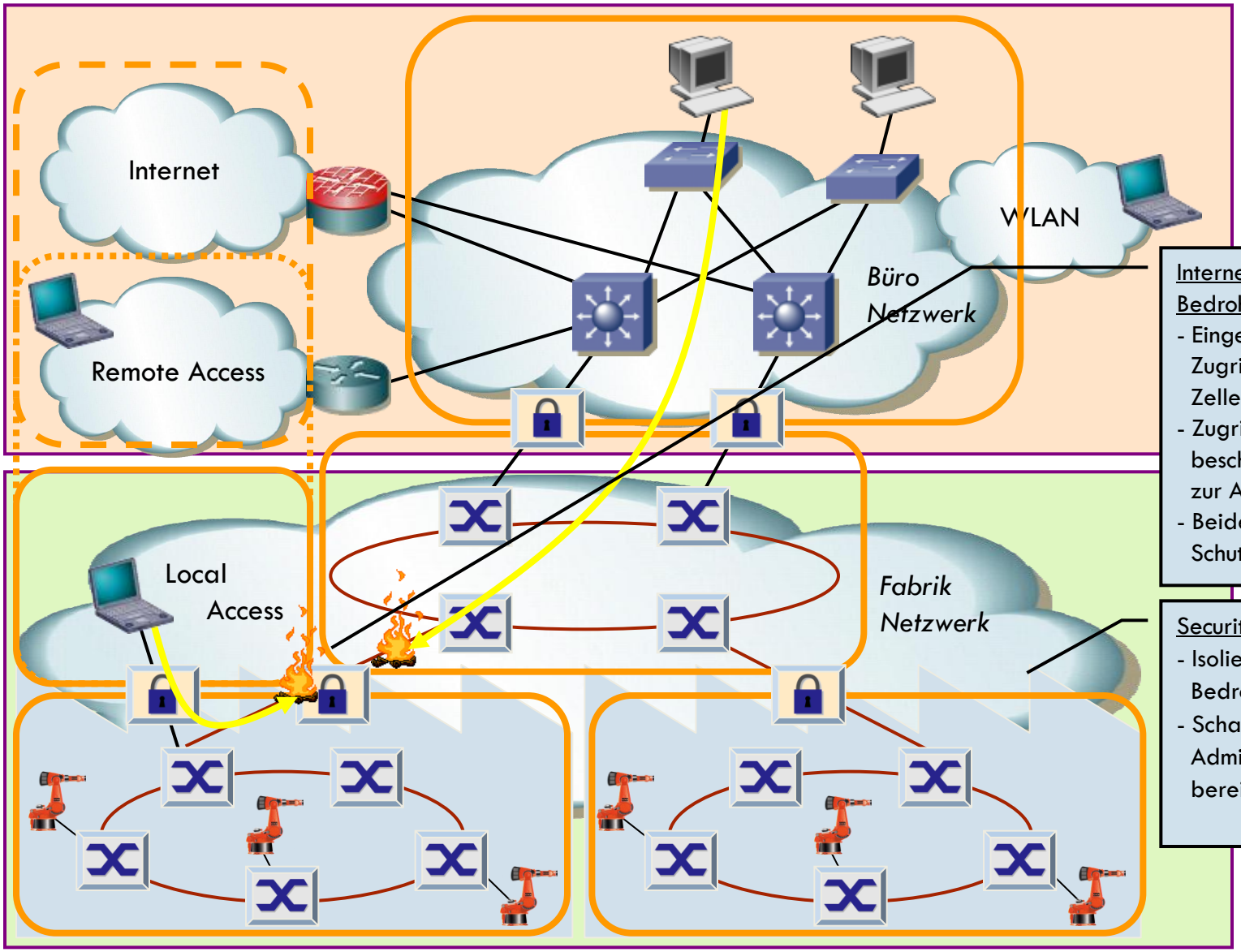
Der „Drinnen-Draußen-Ansatz“



Der „Verteilte-Security-Ansatz“



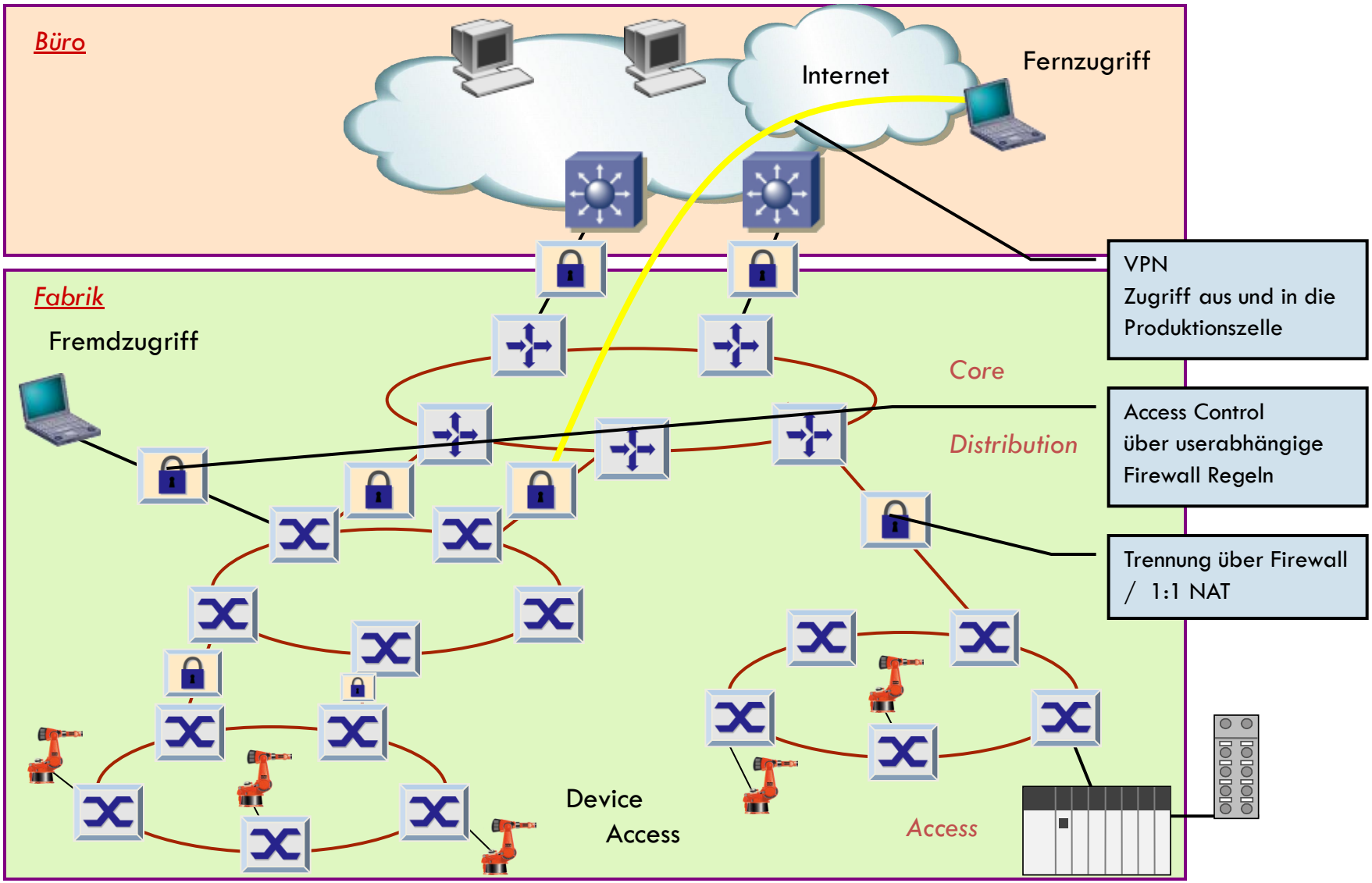
Security Zellen



Interne & externe Bedrohungen:
- Eingeschränkter Zugriff auf die Zelle
- Zugriffs-beschränkungen zur Außenwelt
- Beiderseitiger Schutz

Security Zellen:
- Isolierung von Bedrohungen
- Schaffung von Administrations-bereichen

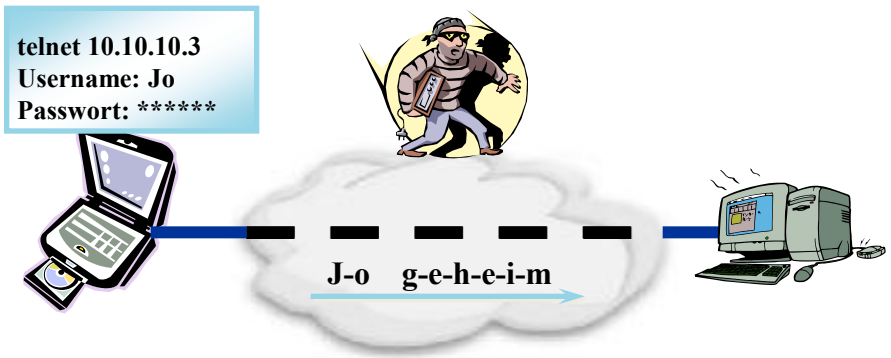
Topologie Fabrik-Netzwerk



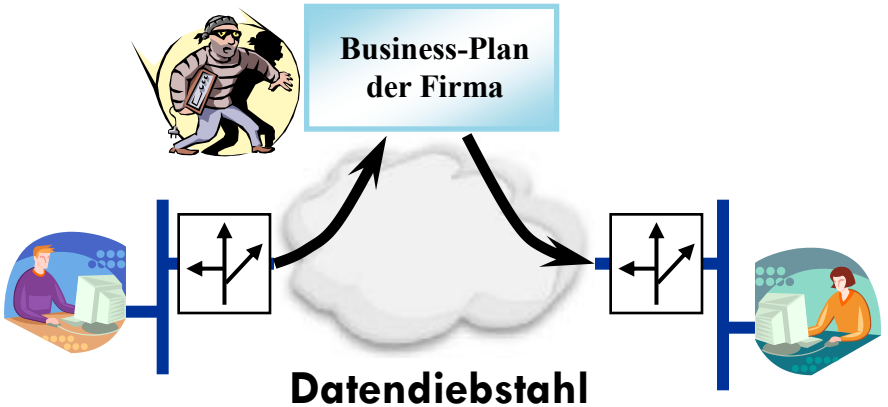
Was gilt es eigentlich zu schützen?

- **Daten**
  - Attacken durch Hacker (Viren, Würmer..) und Fehlbedienungen
- **Systeme und Ressourcen**
- **Image des Unternehmens**
  - Schutz der Produktion (Zelle) vor unberechtigtem Zugriff
  - Werksspionage nimmt noch nie dagewesene Formen an
- **Systemverfügbarkeit**
  - Verbindung zwischen höchster Sicherheit und leichter, webbasierter Administration

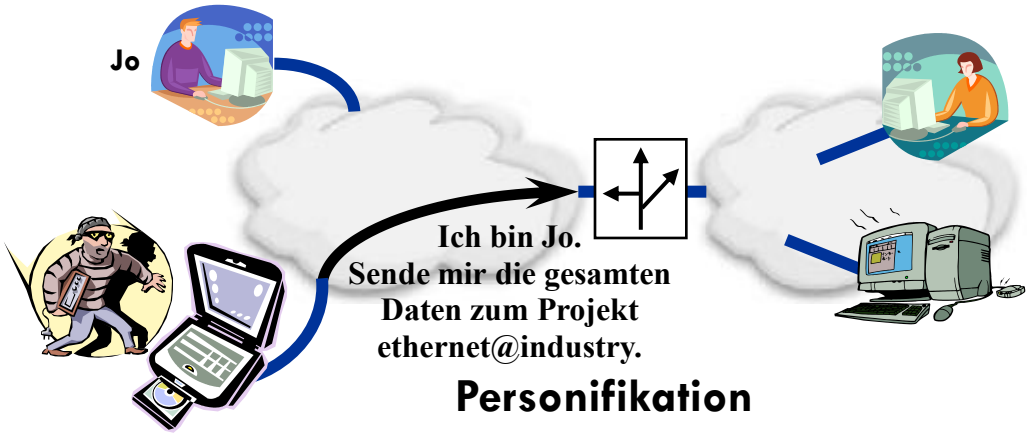
Typische Gefährdungen I



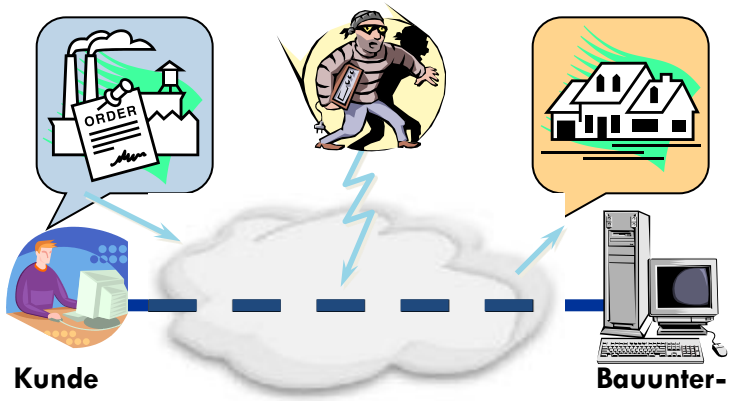
Verlust der Privatsphäre (Packet Sniffing)



Datendiebstahl (Data Theft)



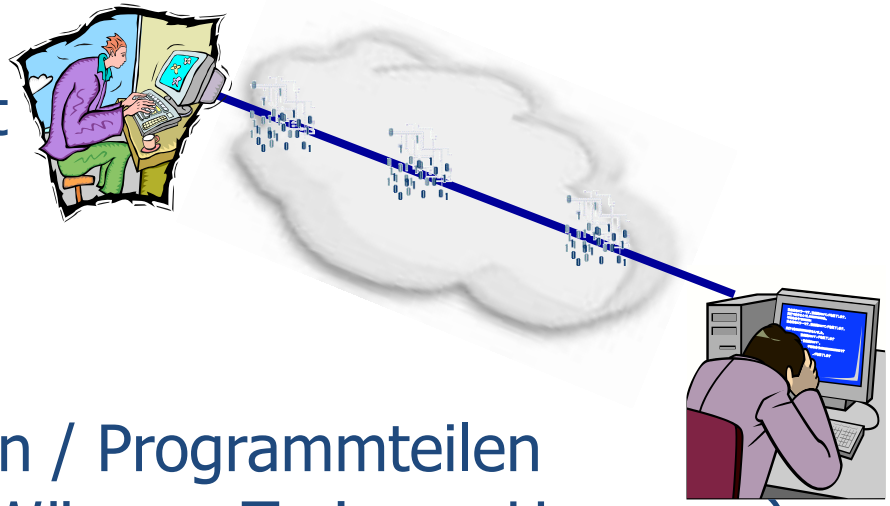
Personifikation (Identity Spoofing)



Verlust der Integrität (Data Alternation)

Typische Gefährdungen II

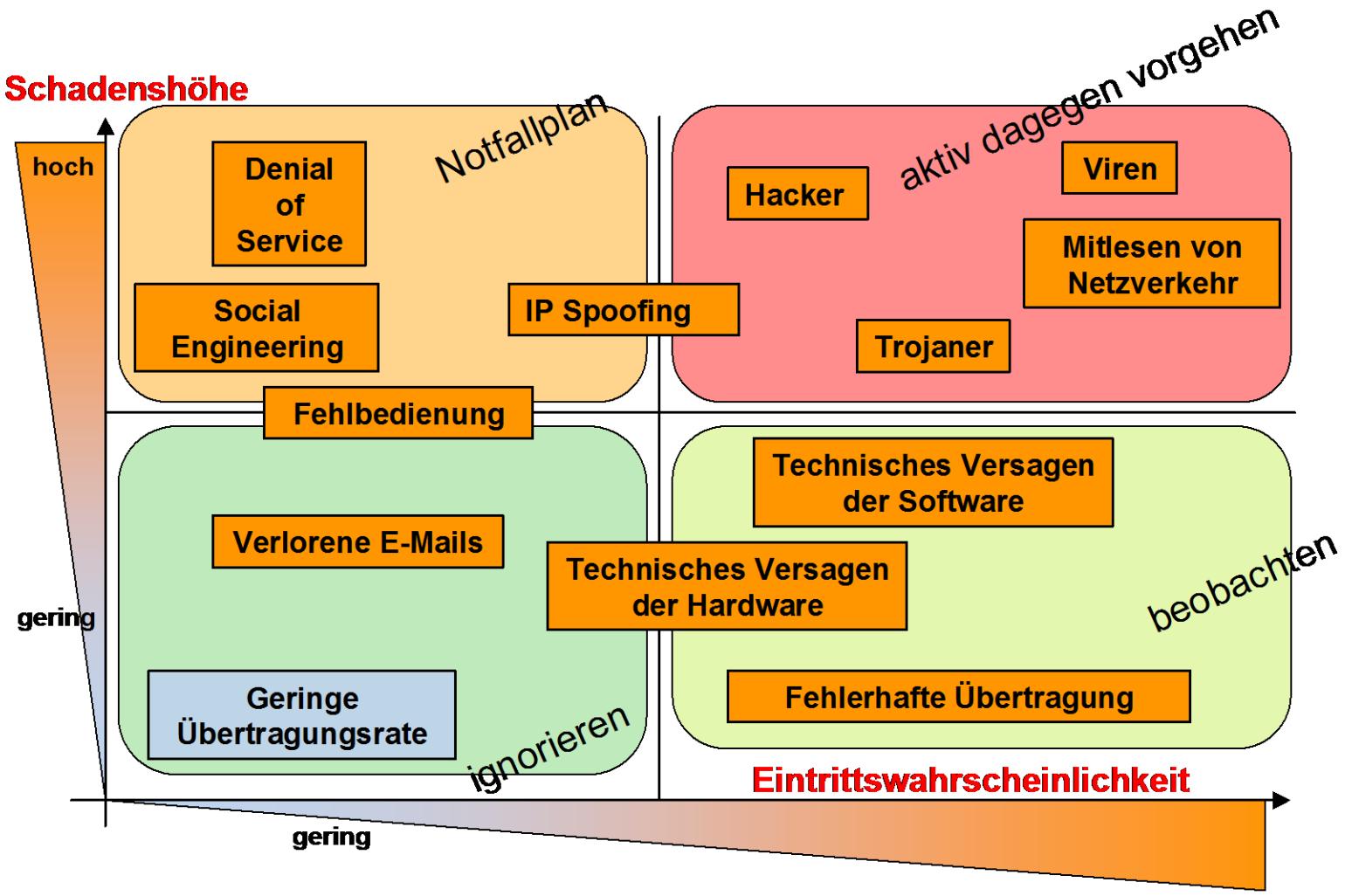
- Angriffe auf die Verfügbarkeit ("Denial-of-Service-Angriffe", ("Distributed-DoS-Angriffe")



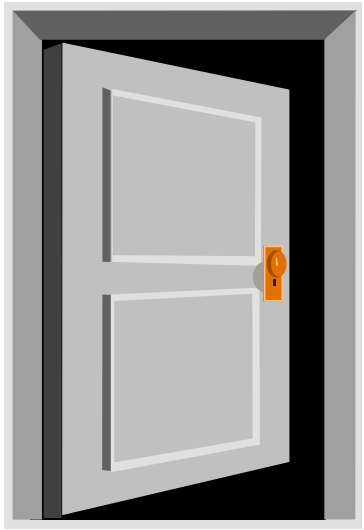
- Übertragung von Programmen / Programmteilen mit Schadfunktionen (Viren, Würmer, Trojaner, Hoaxes...)

- Menschliches Fehlverhalten (z.B. Preisgabe von Passwörtern)

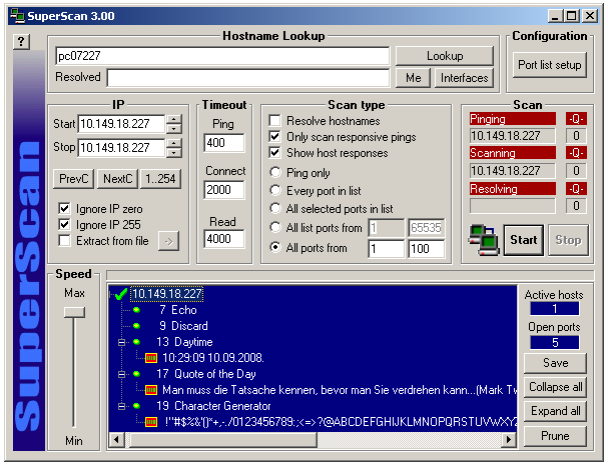
Bedrohungsszenarien



IT-Sicherheit - Schutzmaßnahmen



- **Minimieren der Angriffspunkte**
  - Nur absolut notwendige Ports öffnen
  - NAT 1:n (IP-Masquerading) / NAT 1:1
  - Sicherheitspatches bei Komponenten einspielen
  - Nur definierte IP- bzw. MAC-Adressen durchlassen
  - Anwender schulen
- **Schutz gegen Scanner**
  - Keine Reaktion (Rückmeldung) bei Scan eines gesperrten Ports
  - Firewall sperrt alle gefährdeten Ports
- **Schutz gegen Ausspähen**
  - Passwörter aus Kombination von Buchstaben und Zahlen
  - Mindestlänge von Passwörtern



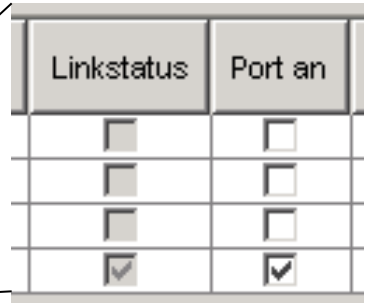
TÜV SÜD

HIRSCHMANN
A BELDEN BRAND

secXTREME
Information Security

IT-Sicherheit – kleine Schritte zu Beginn

- **Switches transportieren die Daten gezielt**
- **Zugang zu Netzkomponenten verhindern**
  - Abgeschlossene Racks
  - Zugang zum Management-Agenten sperren/limitieren auf wenige spezifizierte IP-Adressen
  - Telnet, Web.... Sperren
  - SNMPv3 einsetzen, wo vorhanden
- **Unbenutzte physikalische Ports sperren**



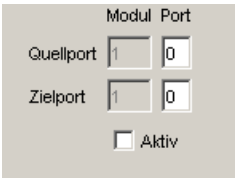
- **Access Control Liste ACL Prinzip:** Wer darf mit wem was?
- **Filter auf MAC- / IP-Adressen, Port-Nummern**

	Port	Erlaubte MAC-Adresse	Aktuelle MAC-Adresse	Aktion
	1	00 00 00 00 00 00	00 00 00 00 00 00	none
	2	00 00 00 00 00 00	00 00 00 00 00 00	none
	3	00 80 63 01 a4 2b	00 00 00 00 00 00	portDisable
	4	00 00 00 00 00 00	00 04 76 14 d9 6f	none

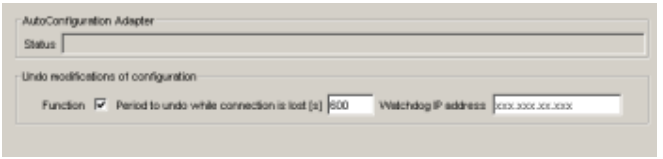
Integrierte Switch Security Features

Modul	Port	Port Status	Erlaubte MAC-Adressen	Aktuelle MAC-Adresse	Erlaubte IP-Adressen	Aktion
1	1	enabled		00:00:00:00:00:00		none
1	2	enabled		00:00:00:00:00:00		none
1	3	enabled		00:00:00:00:00:00		none
1	4	enabled		00:00:00:00:00:00		none
1	5	enabled		00:00:00:00:00:00		none
1	6	enabled		00:00:00:00:00:00		none
1	7	enabled		00:00:00:00:00:00		none
1	8	enabled		00:00:00:00:00:00		none
1	9	enabled		00:C0:EE:74:1C:29		none

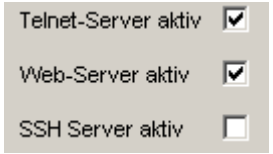
- **Access Control**
  - Bis zu 10 IP/MAC-Adr. Port Security
  - IEEE 802.1X
  - Unbenutzte Ports abschalten
  - Lese- und Schreib/Lese-Passwort für den Zugriff mit WEB/CLI/SNMP ändern
  - Konfigurationsänderung zu widerrufen (incl. Watchdog IP-Adresse)

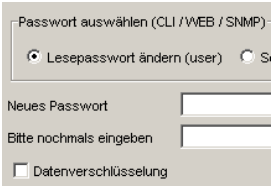


- **Monitoring (-> Intrusion Detection)**
  - Port Mirroring
  - Learning Mode
  - Doppelte IP-Adressen erkennen und beheben



- **Management Access**
  - SNMP V2, V3 (Passwort) Encryption
  - SSH (CLI)
  - Telnet-Server, Web-Server oder SSH-Server abschalten.





- **Protection**
  - IEEE 802.1Q (VLAN Tag)
  - ACLs (Layer 3 & 4)
  - Bandbreite Limitierung (Global & per Port)

Modul	Port	Eingangs Pakettypen	Eingangs-begrenzerrate (kbit/s)	Ausgangs-begrenzerrate (Pkt/s) Pakettyp: BC	Ausgangs-begrenzerrate (kbit/s) Pakettypen: alle
1	1	BC	0	0	0
1	2	BC	0	0	0
1	3	BC	0	0	0
1	4	BC	0	0	0
1	5	BC	0	0	0
1	6	BC	0	0	0
1	7	BC	0	0	0
1	8	BC	0	0	0
1	9	BC	0	0	0

TÜV SÜD

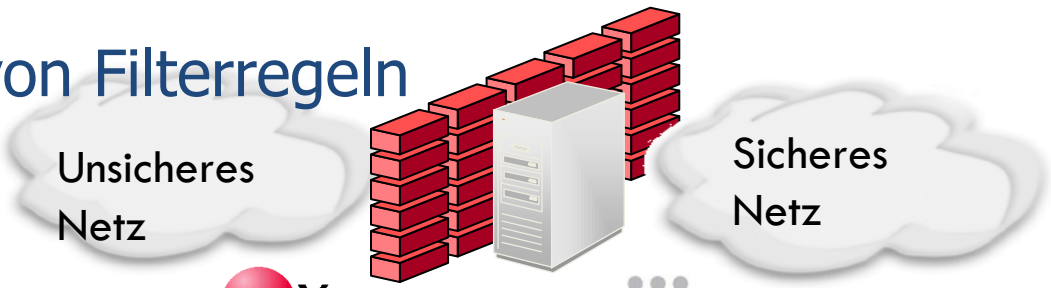
HIRSCHMANN
A BELDEN BRAND

secXTREME
Information Security

YELLO NETCOM

Firewall - Allgemein

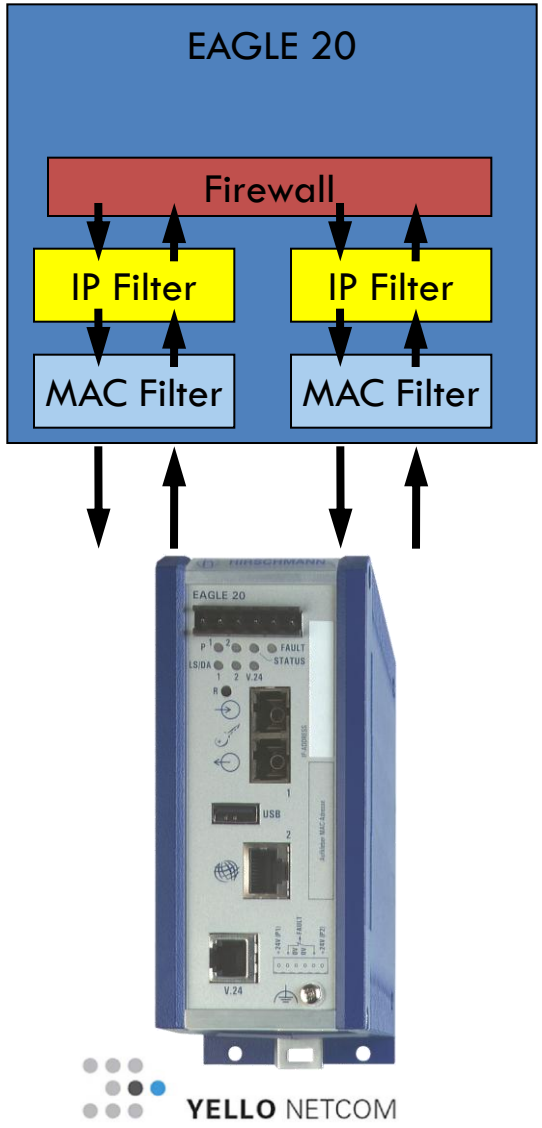
- Trennung von Netzen mit unterschiedlichem Schutzbedarf
- Zugangskontrolle gemäß Regelbasis für ein- und ausgehende Daten (getrennt definierbar)
- Access Control Listen ACLs
  - Kriterien: z.B. IP-Adresse und Port-Adresse
- NAT – Network Address Translation
- VPN – Funktionalität
- Erstellung von Logdateien und Statistiken über Nutzung und Angriffe
- Automatisches Lernen von Filterregeln



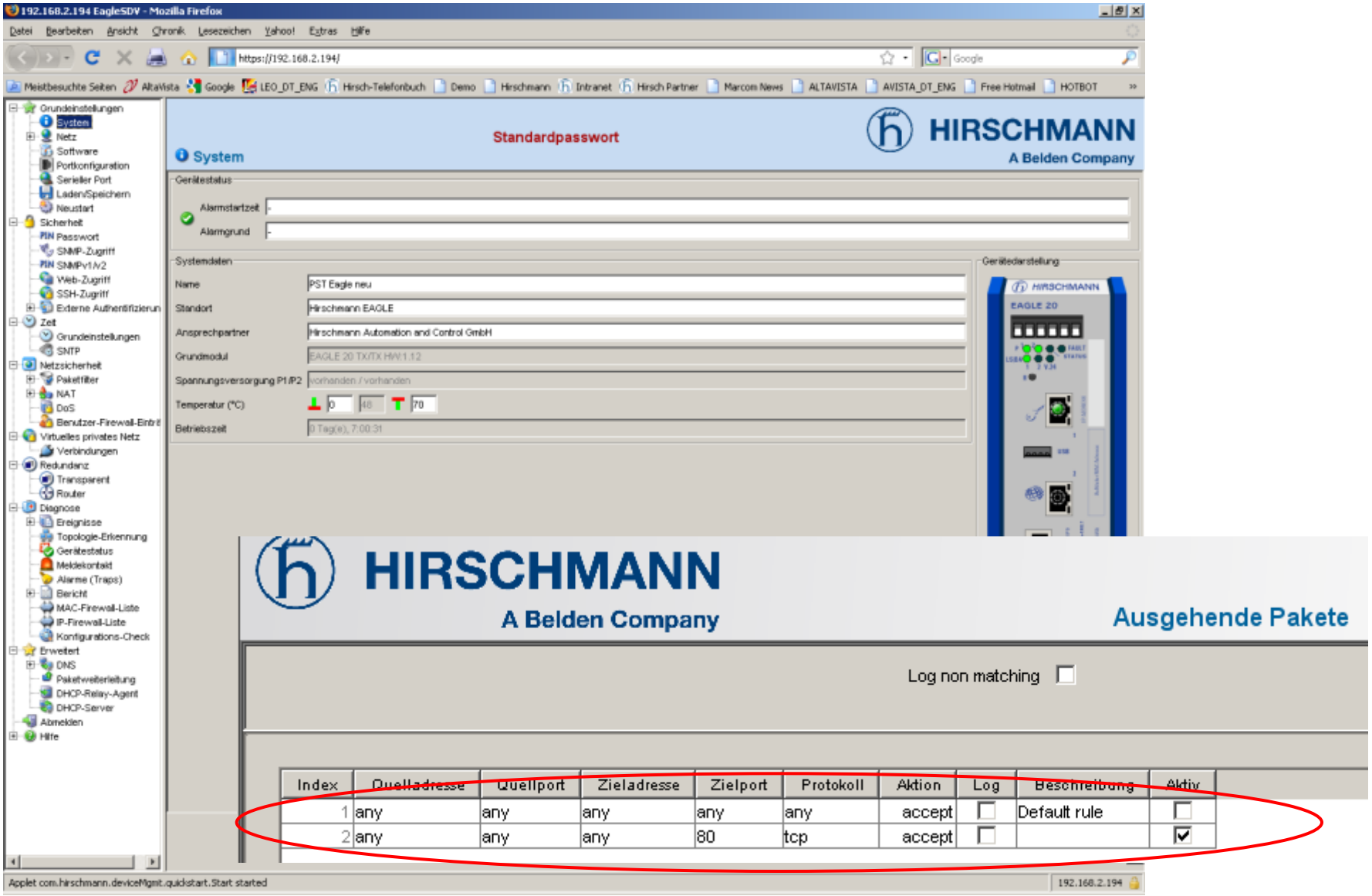
Firewall Funktionen - EAGLE 20

Was ist der EAGLE 20?

- Speziell für die industriellen Anforderungen
- Trennung von Netzen mit unterschiedlichem Schutzbedarf
- Zugangskontrolle gemäß Regelbasis (Filter) für ein- und ausgehende Daten (getrennt definierbar)
- Access Control Listen ACLs
- NAT – Network Address Translation
- VPN – Funktionalität
- Logdateien / Statistiken über Nutzung und Angriffe
- Automatische Lernen von Filterregeln
- DoS-Schutz Benutzer-Firewall
- Logfile, Eventlog, Meldekontakt, SMS…



Management - EAGLE 20



EAGLE Tofino™ System

Was ist der EAGLE Tofino?

- Netzwerk Security System speziell für industrielle Anwendungen
- Einfachere Konfiguration und Betrieb ..
- Oberfläche- / Management vergleichbar mit Industriesteuerungen
- Vordefinierte Templates verfügbar:
  - > 50 Industrielle Kommunikationsprotokolle
  - > 25 verschiede Steuerungen (Controllers)
- Beinhaltet: "Defence in Depth”
  - Tief gestaffelte Sicherheitsarchitektur
  - Bildung von Sicherheitszonen innerhalb des Netzwerkes

EAGLE Tofino™ Komponenten

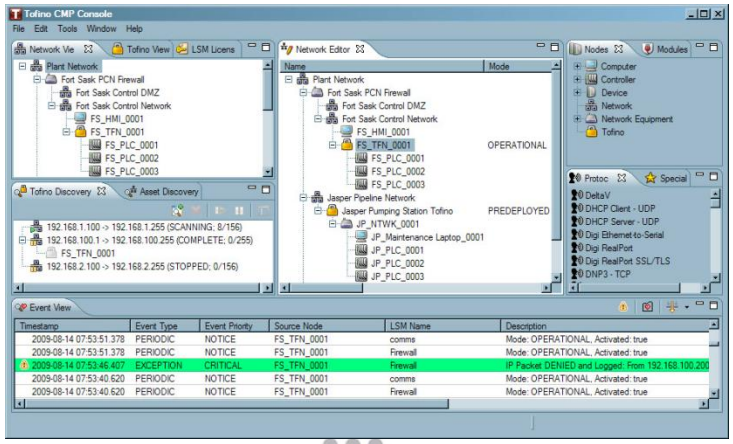
- **Tofino™ Central Management Platform (CMP)**
  - Zentrale Security Management Station

- **EAGLE02 Tofino™ Firewall Hardware**

- **Tofino™ Loadable Security Modules (LSM)**
  - Ladbare Tofino Sicherheitsmodule, um ihr industrielles Netzwerk optimal zu schützen

Tofino™ Central Management Platform

- Die Tofino™ Central Management Platform (CMP) als Software gestattet die Konfiguration, Verwaltung und Überwachung sämtlicher Tofino-Sicherheitsgeräte von einer einzigen Workstation aus
- Einfache Diagnose und Behebung von Sicherheitsprobleme
- Die CMP-Software erstellt ihnen ein Modell Ihres gesamten Steuerungsnetzwerks.
- Grafische Drag-and-Drop-Tools erleichtern Ihnen das Erstellen, Bearbeiten und Testen Ihrer Tofino-Konfiguration.
- Im Betrieb zeigt Ihnen die CMP-Software auf einen Blick den Status des gesamten Systems und ermöglicht Ihnen eine koordinierte Reaktion auf potenzielle Cyber-Gefahren



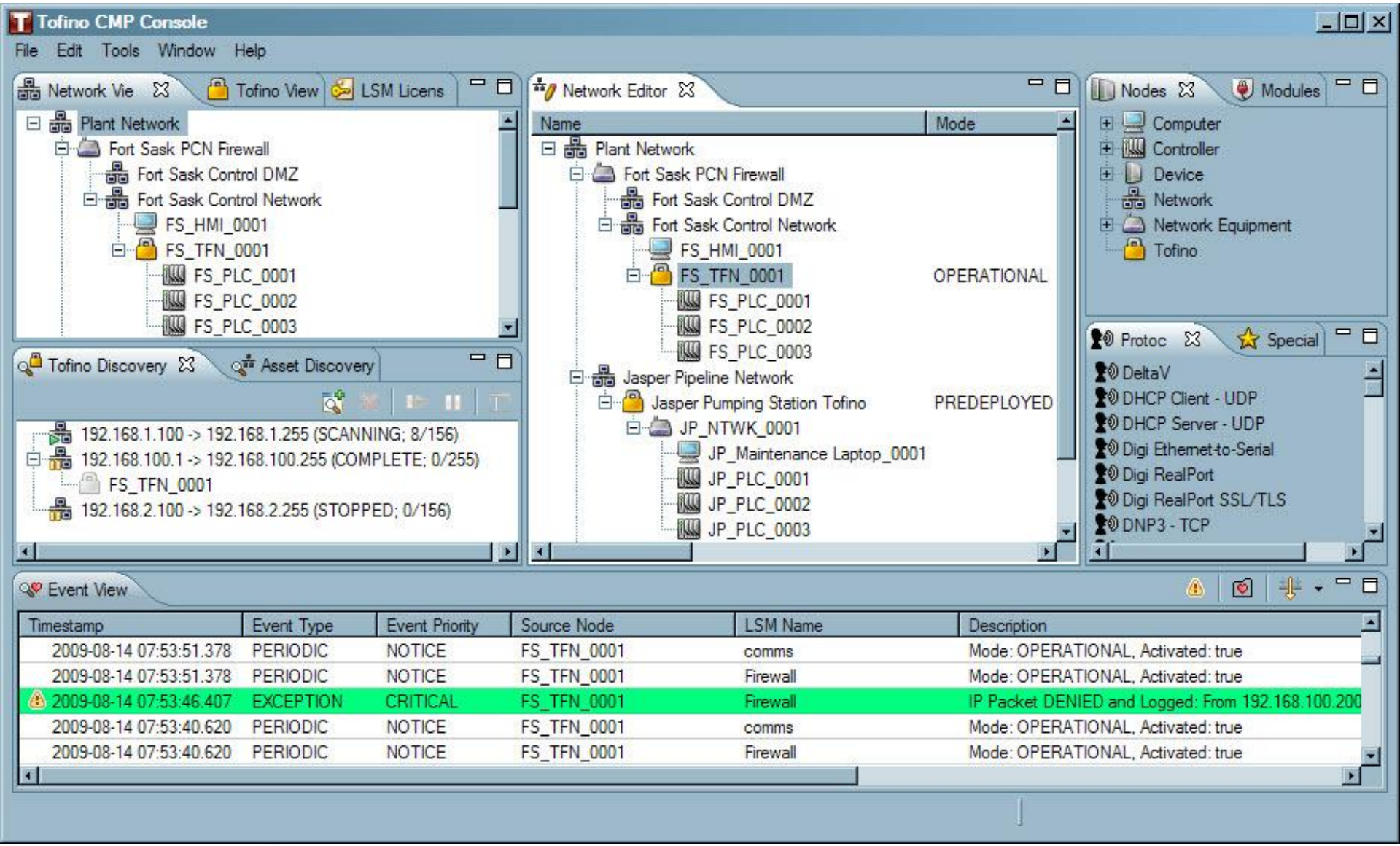
TÜV SÜD

HIRSCHMANN
A BELDEN BRAND

secXTREME
Information Security

YELLO NETCOM

Management Platform Oberfläche



EAGLE 20 vs. EAGLE Tofino™

	EAGLE 20	EAGLE 20 Tofino
Industrieller Einsatz	✓	✓
Konfiguration / Management Software	Industrial HiVision 4.0 incl. MultiConfig™	Central Management Platform
Konfiguration	Manual	Drag and Drop
Funktionalität	Integriert	Modular
Zielgruppe	IT Mitarbeiter	Automation Mitarbeiter
Preis	Niedriger Preis	Höherer Preis

Zusammenfassung

- Industrielle Netzwerke sind sehr anfällige gegenüber Angriffen
- Integration in bestehendes industrielles Netz
- Robustes, industrielles Design
- Preisoptimierter industrieller Router
- Benutzerfreundliche Konfiguration
- Schutz von Angriffen
- Schutz vor Kommunikationsüberlast
- Skalierbare Schutzfunktionalität
- Unterstützung bei der VPN Konfiguration
- Zwei unterschiedliche Lösungen
  - EAGLE 20: Ind. Layer 3 Firewall (Router) mit selbst zu erstellenden oder selbstlernenden Regeln
  - EAGLE Tofino: Ind. Layer 2 Firewall vorgegebenen oder selbst zu erstellenden Templates

TÜV SÜD HIRSCHMANN A BELDEN BRAND secXTREME Information Security YELLO NETCOM