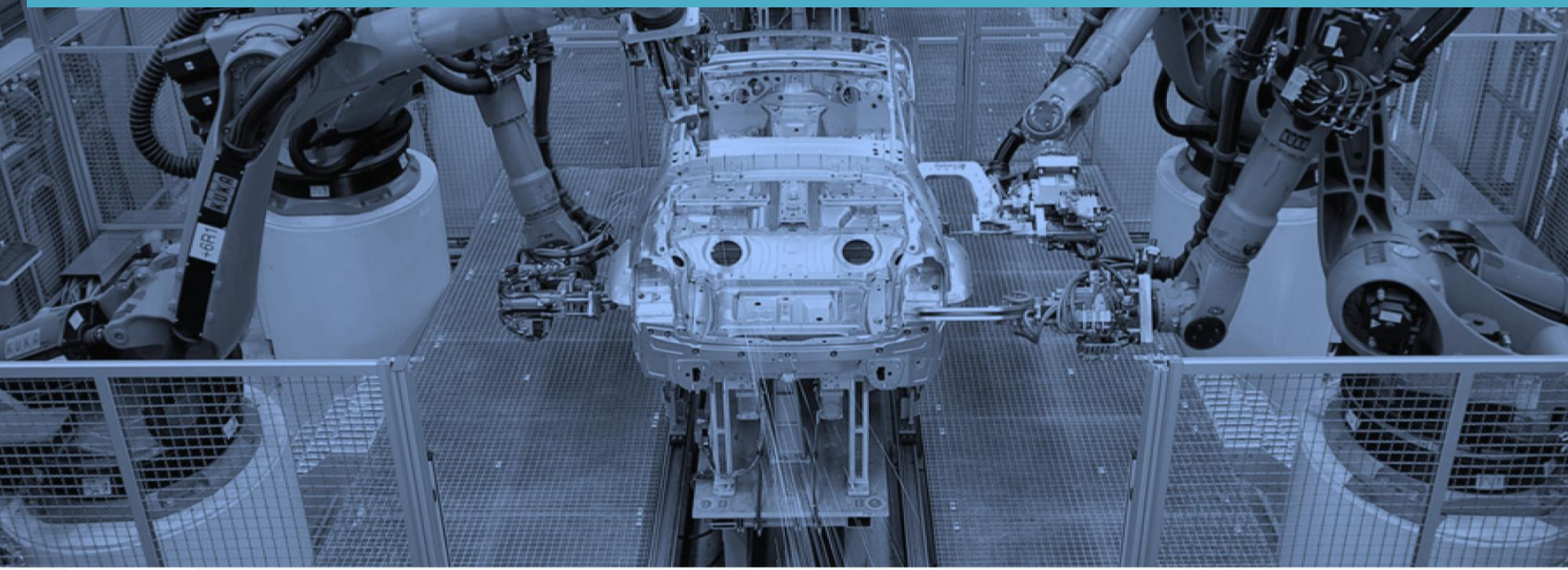
Stuxnet zum Frühstück
Industrielle Netzwerksicherheit 2.0

Stuttgart und München



TÜV SÜD

HIRSCHMANN
A BELDEN BRAND

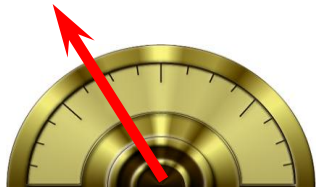
secXTREME
Information Security

YELLO NETCOM

Gefahrenpotentiale

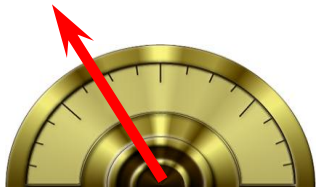
Gefahrenbereich	Bedeutung heute Rang	Prognose Rang	Schäden Rang	Schäden ja, bei
Irrtum und Nachlässigkeit eigener Mitarbeiter	1	2	1	49%
Malware (Viren, Würmer, Trojanische Pferde)	2	1	4	35%
Software-Mängel/-Defekte	3	5	2	46%
Hardware-Mängel/-Defekte	4	6	3	45%
unbefugte Kenntnissnahme, Informations-diebstahl, Wirtschaftsspionage	5	3	7	12%
unbeabsichtigte Fehler von Externen	6	7	5	30%
Hacking (Vandalismus, Probing, Missbrauch, ...)	7	4	8	12%
höhere Gewalt (Feuer, Wasser, ...)	10	11	9	12%
Sabotage (inkl. DoS)	11	10	11	10%

Ist die totale IT-Sicherheit möglich ?

Verfügbarkeit		Sicherheit
Erreichbarkeit		Authentifizierung
Performance		Authorisierung
Einfachheit		Accounting
Managebarkeit		Integrität
Vielfältigkeit		Vertraulichkeit

Ist IT-Sicherheit ohne technische Massnahmen möglich ?

Menschen	Maschinen
Weisungen	Firewall
Checklisten	IPS/IDS
Richtlinien	NAC
Standards	SecureMail
Vorschriften	AntiVirus/SPAM
Ausführungsbestimmungen	VPN



Achtung !

Bezüglich Sicherheit gibt es grundsätzlich keine Unterschiede zwischen «grossen» und «kleinen» Netzwerken !

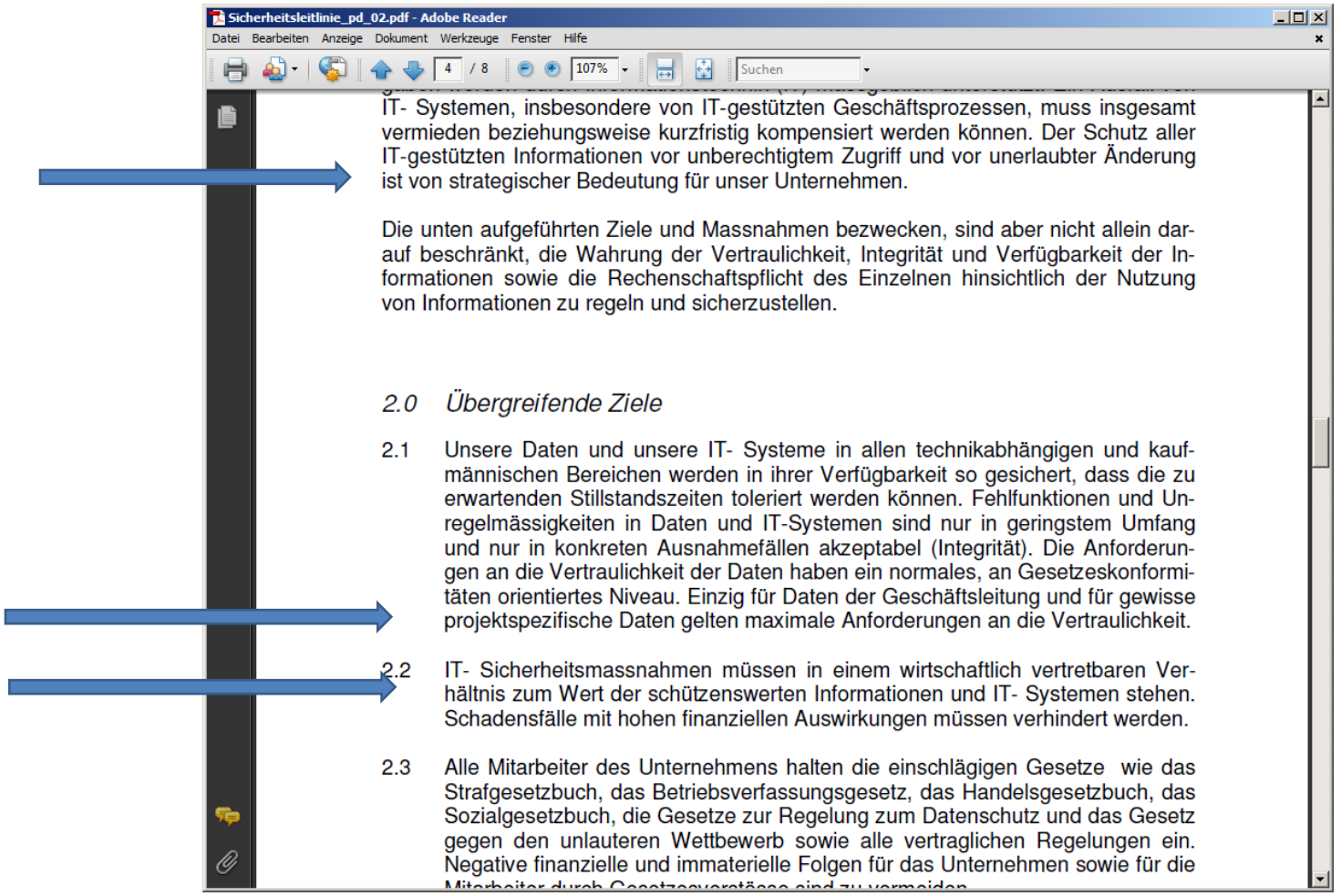
Das generelle Sicherheitsbedürfnis und somit die Komplexität der gewählten Massnahmen ist von Netzwerk zu Netzwerk unterschiedlich.

Sicherheits- Strategie

Die Strategie legt zukünftige Ziele der IT sowie die lang- und mittelfristigen Handlungsvorgaben zu ihrer Erreichung innerhalb einer Planungsperiode fest

- Risikoanalyse, Risikokategorien bilden, geeignete & zweckmässige Massnahmen treffen
- Sicherheitsleitlinie (Security Police) erstellen

Sicherheitsrichtlinie (Security Policy)



Risikopotential Mensch

Das schwächste Glied in der Kette: Risikofaktor Mensch !

- Social Engineering
- Human Firewall

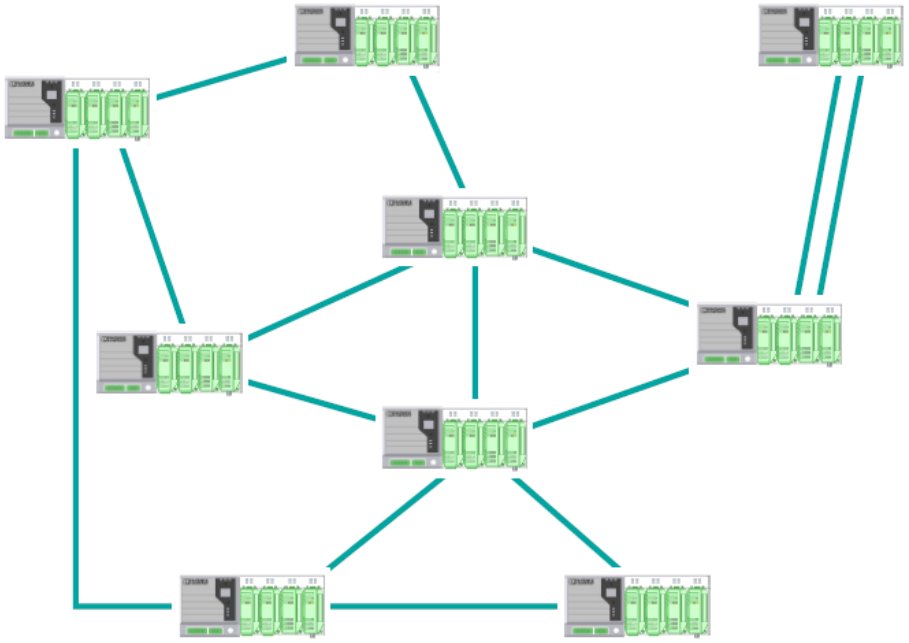
Materialwahl

Sicherheitsrelevante Planung, Konzeption, Realisierung & Unterhalt
Nur den Anforderungen entsprechende aktive und passive Komponenten einsetzen !

Wieso Industriekomponenten ?

	Büro- Netzwerk	Industrie- Netzwerk
Installation	• Feste Grund-installation im Gebäude (UKV) • Variabler Geräteanschluss an Standardarbeitsplätzen • Überwiegend sternförmige Verkabelung	• Anlageabhängige Verkabelung und Kabelführung • Feldkonfektionierbare Steckverbinder bis IP 67 • Redundante Verkabelung, häufig Ringstrukturen
Daten	• Grosse Datenpakete • Mittlere Netzverfügbarkeit (STP/RSTP) • Haupsächlich azyklische Datenübertragung • Kein Echtzeitverhalten notwendig	• Kleine Datenpakete • Sehr hohe Netzwerkverfügbarkeit (MRP) • Hauptsächlich zyklische Datenübertragung • Echtzeitverhalten z.T. notwendig
Umwelt	• Normaler Temperaturbereich • Wenig Staub, Feuchtigkeit und Erschütterungen • Kaum mechanische und chemische Belastungen • Geringe EMV-Belastung	• Erweiterter Temperaturbereich • Staub, Feuchtigkeit und Erschütterungen möglich • Gefahr durch mechanische Beschädigung oder chemische Belastung • Hohe EMV-Belastung

Topologie: Spanning Tree Protokoll



Medienredundanz

Auflösung von Schleifen im Netzwerk

Beliebig vermaschte Netzwerkstrukturen möglich

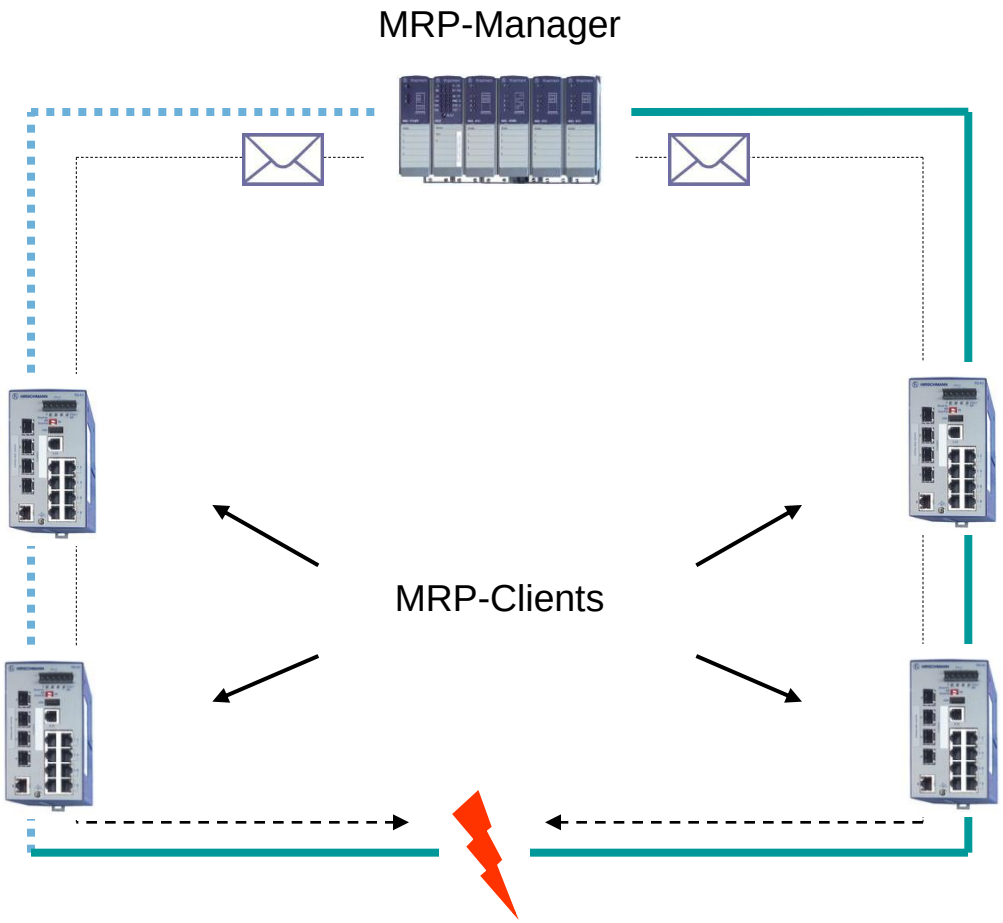
Erzeugung einer logischen Baumstruktur

Reduzierung der Umschaltzeit durch RSTP

Umschaltzeiten (abhängig von der Netzwerkgrösse, STP: 30 - 90 s, RSTP: < 2 s bis max. 7s)

Standards: IEEE 802.1D (STP); IEEE 802.1W (RSTP)

Topologie: Media Redundanz Protokoll



Standardisiertes Medienredundanzprotokoll

Hochverfügbare Netzwerke

geeignet für kritische Automatisierungsanwendungen

Keine vermaschten Topologien

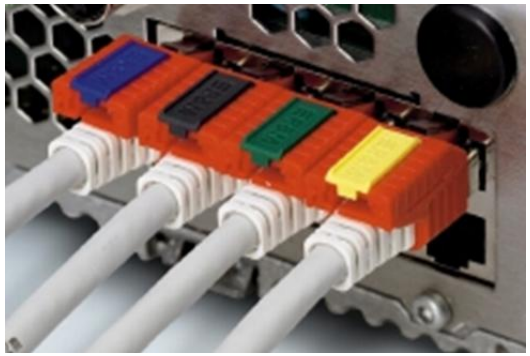
Weniger komplex als RSTP

Reine Ringstrukturen

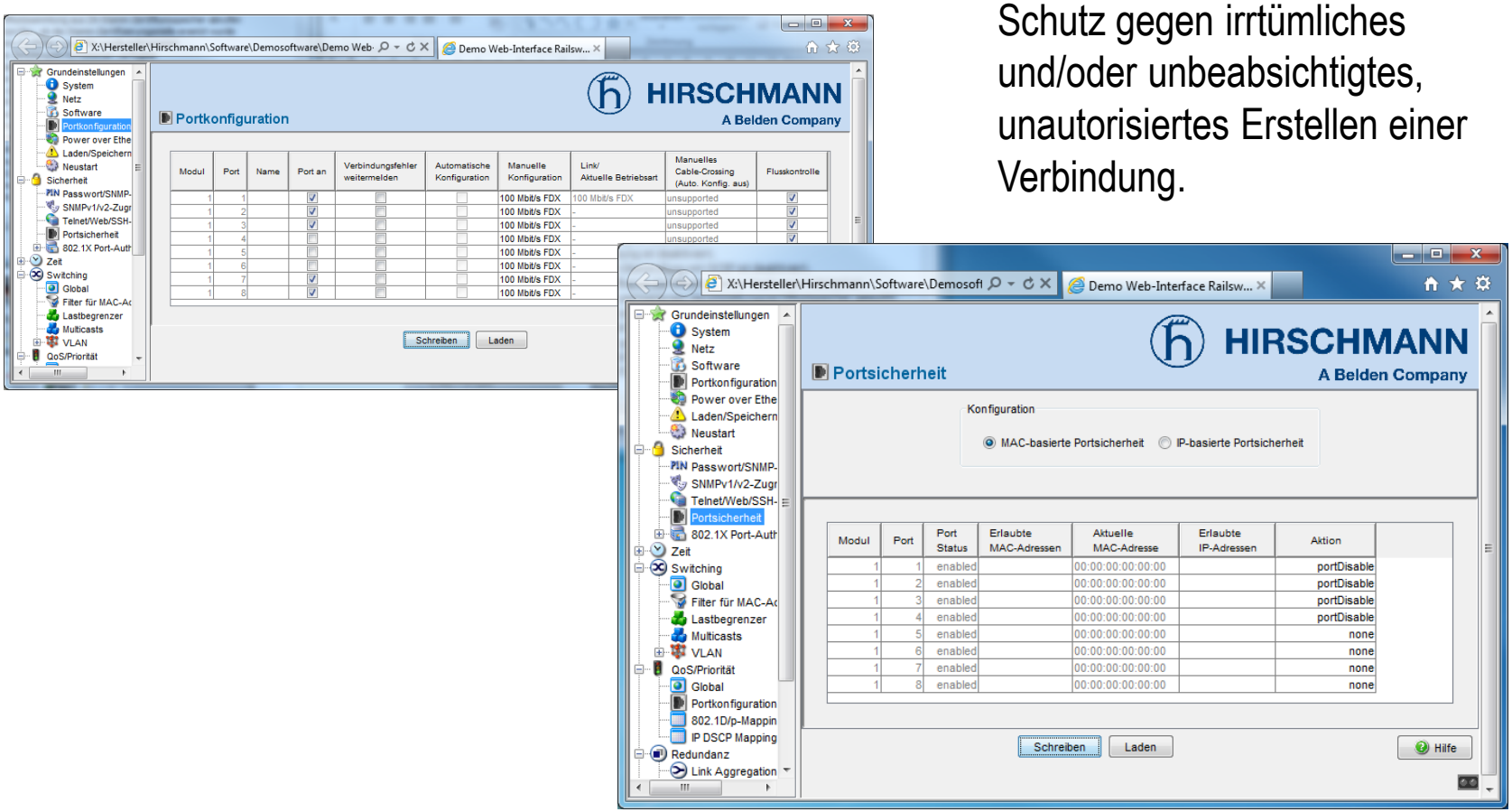
Umschaltzeiten: < 200 ms

Layer 1: Bitübertragungsschicht

Schutz gegen irrtümiches, unbeabsichtigtes und/oder unautorisiertes Lösen einer Verbindung



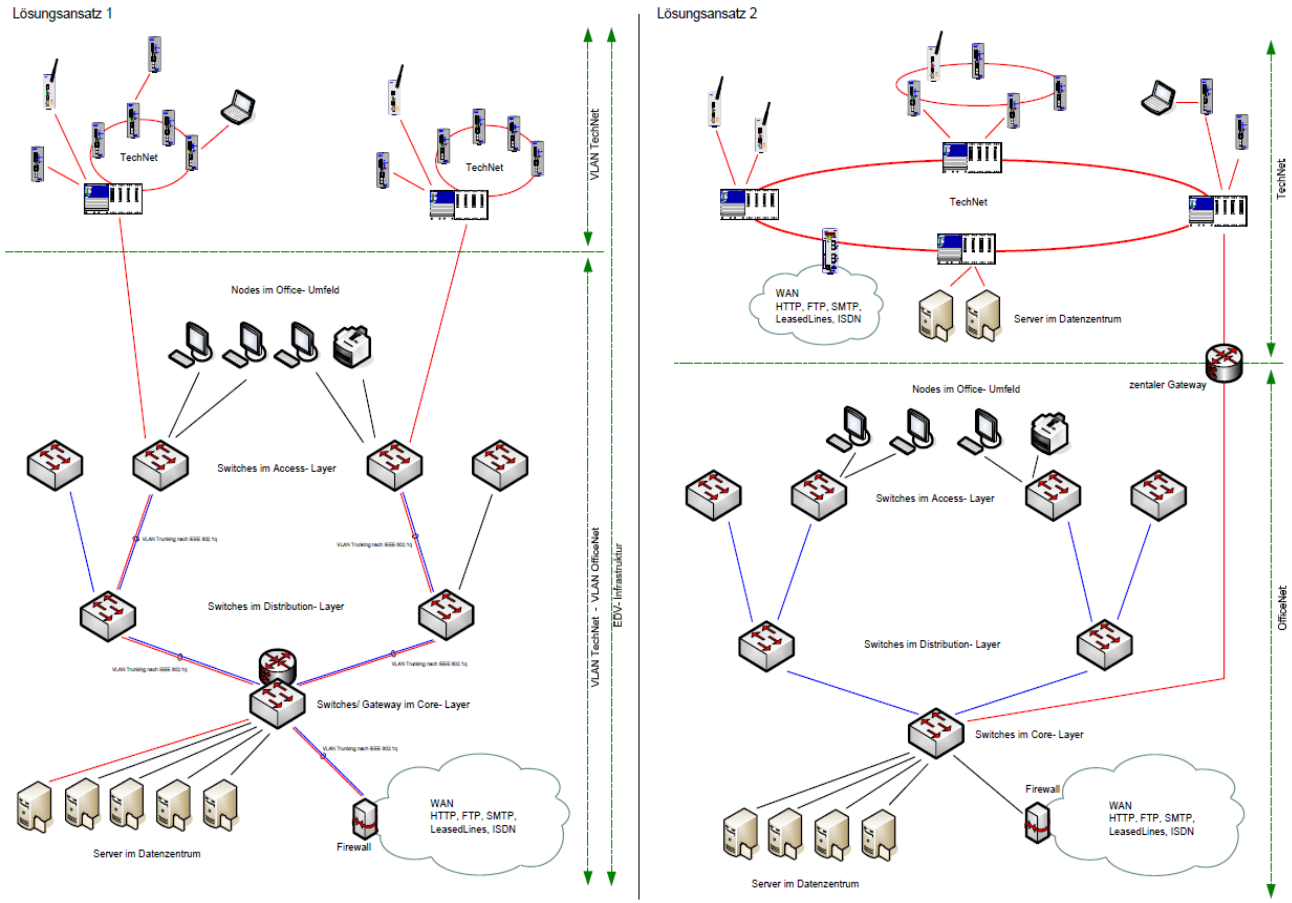
Layer 1: Bitübertragungsschicht



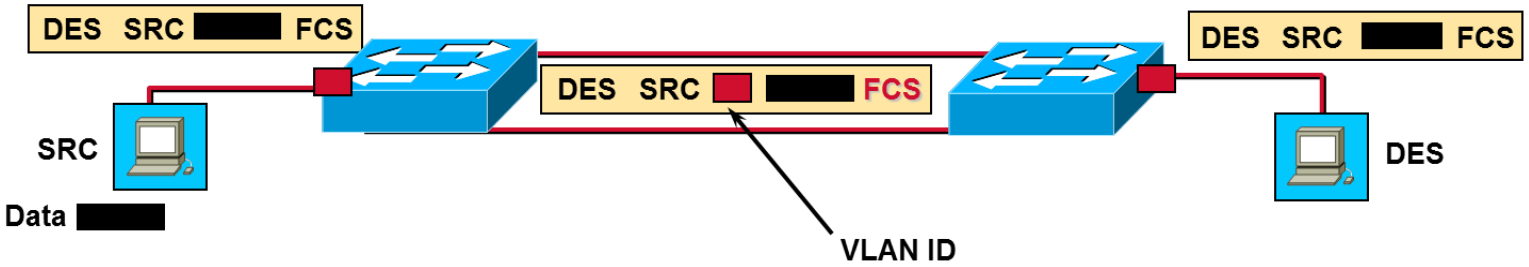
Schutz gegen irrtümliches und/oder unbeabsichtigtes, unautorisiertes Erstellen einer Verbindung.

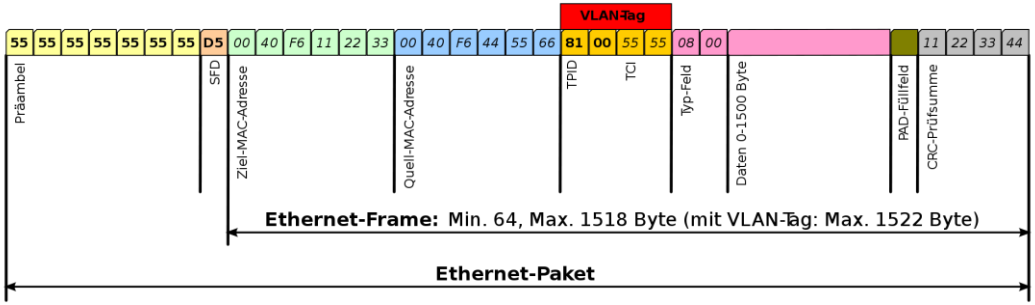
Layer 2: Sicherungsschicht

Logische Gruppierung von Netzwerkgeräten oder Benutzer, die nicht auf ein physikalisches Segment beschränkt ist.



Layer 2: Sicherungsschicht





Technische Umsetzung eines VLAN-Konzepts

Layer 3: Vermittlungsschicht

Router transportiert Datenpakete aufgrund von eindeutigen Anweisungen von einem Netzwerk zum andern (Layer 3, bzw. IP-Adressen) und blockiert Broadcasts.

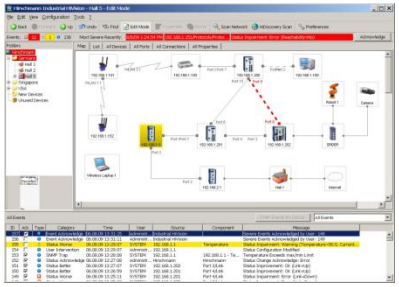
Layer 4/5: Transportschicht

Alle Daten von internen Netzwerk nach aussen und umgekehrt müssen durch die Firewall (keine Hintertüren).

Es werden ausschliesslich autorisierte (Auf der Grundlage eines Sicherheitskonzepts) festgelegte Verbindungen zugelassen.

Die Firewall selbst ist immun gegen Angriffe (ist unsichtbar).

Layer 7: Anwendungsschicht



VLAN
Voice

VLAN
Daten

VLAN
Video

TÜV SÜD

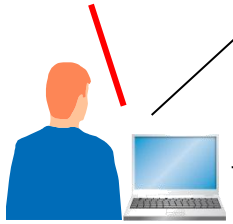
HIRSCHMANN
A BELDEN BRAND

secXTREME
Information Security

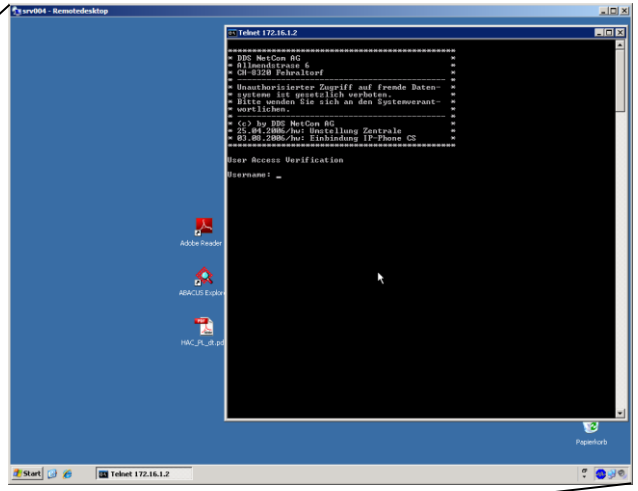
YELLO NETCOM

Layer 7: Anwendungsschicht

LAN



Zugriff für Wartung und Unterhalt erfolgt nur über TerminalService, das löst Sicherheitsprobleme bei den Service-PC‘s.



Zusammenfassung

Layer 1

Netzwerktopologie bestimmen

Netzwerk physikalisch gegen Nachlässigkeit und Irrtum schützen

Layer 2

Netzwerk durch virtuelle Netzwerke VLAN segmentieren (1 VLAN pro Risikogruppe)

Layer 3

Segmentierte Netzwerke verbinden, Broadcast‘s verhindern, Netzwerkadressen verbergen

Zusammenfassung

Layer 4 / Layer 5

Datenverbindungen zwischen verschiedenen Netzwerken zentral definieren, authentifizieren und autorisieren.

Layer 7

Netzwerke passiv schützen, indem schlecht gesicherte Systeme simuliert werden, die Angriffe melden.

Wartungsverbindungen immer über TerminalServices realisieren.

Besten Dank.

Besten Dank für ihre Aufmerksamkeit.

YELLO NetCom GmbH & Co. KG
Birkenallee 115-117
48432 Rheine
Telefon 05971 / 961 76-0
Telefax 05971 / 961 76-25
rheine@yello-net.de
hanspeter.weingartner@dds.ch

TÜV SÜD HIRSCHMANN A BELDEN BRAND secXTREME Information Security YELLO NETCOM