Erzeugeranlagen mit statischen Frequenzumrichtern – Kommunikation mit IEC 61850 und Maßnahmen der IT-Sicherheit

16. Symposium für Netzleittechnik, VDE

DB Energie – bringt voran.

DB Energie GmbH

Jan-Thomas Walther

I.EBZ 4

Meißen, 19.09.2013

Typische Anwendungen für Kommunikation im Bereich Energieerzeugung und Energieverteilung sind …

(1) Prozessdatenübertragung für operativen Netzbetrieb und Kraftwerksbetrieb,
(2) Notbedienung von Anlagen bei Ausfall der Datenwege und Nichtverfügbarkeit der Leitstellen

(3) Störungsdiagnose von Stationsleit- und Netzleittechnik, Übertragungstechnik
(4) Störschreiberauslesung von z.B. schutztechnischen Einrichtungen
(5) Monitoring und Überwachung von Großgeräten, Schaltmitteln etc.
(6) Fernservice und Parametrierung
(7) Datenadministration, Datenverteilung und Datenspeicherung

(8) Informationsaustausch zwischen operativem Betrieb (Leitstellen) und Unternehmens-IT
(9) Informationsaustausch zwischen operativen Betrieben
(10) Zählerfernauslesung

Typische Systeminfrastruktur in einem großflächigen Versorgungsunternehmen

Netzleitsystem

Prozessdatenverwaltung

Administration

Switch

Switch

Datenhaltung

Instandhaltungssysteme Büro

Intranet Firma

Service

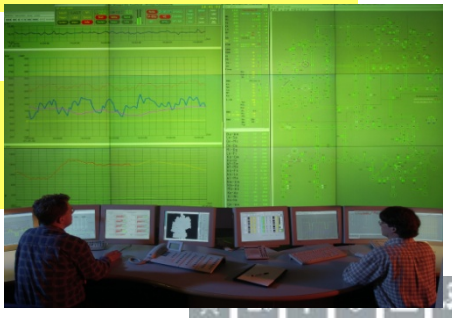
Internet, öffentliches Netz

VPN Firma

Datennetzübergänge

VPN 2 Firma

Externe Leitsysteme



unternehmensinterne Leitsysteme

Switch

Switch

Datenknoten

SLT

Großgeräte

SLT

Schutz

Zählung

Was kennzeichnet diese Infrastruktur ?

(besonders **aus Sicht der IT-Sicherheit)**

Die Kommunikationsteilnehmer:

… sind territorial verteilt mit automatisiertem, unbemanntem Betrieb in den Stationen und Werken, besetzte Leitstellen arbeiten im Verbund an mehreren Standorten,
… sind firmenspezifische Applikationen der NLT auf Basistechnologien,
… nutzen teilweise in IP-Netzen routbare Kommunikationsstandards,
… haben eigene Sicherheitsmechanismen besonders auf Applikationsebene,
… unterliegen einer gesonderten Verantwortlichkeit, Administration und Pflege,
… haben eine Nutzungsdauer von 10-20 Jahren

Die Kommunikationsinfrastruktur:

… erfolgt über geschlossene, private oder öffentliche Datennetze (und Datendirektverbindungen) leitungsgebunden/-ungebunden,
… besitzt Systeminfrastruktur mit eigenen Basistechnologien/Routingstandards,
… hat Sicherheitsmechanismen auf Netzebene,
… unterliegt oft einer eigenen Verantwortlichkeit und Administration,
… unterliegt teilweise kurzen Weiterentwicklungszyklen (< 10 Jahre)

Problemstellungen, die sich daraus ergeben …

(1) Systemtechniken der Datennetze und Netzleittechnikanwendungen (Teilnehmer) mit ihren entsprechenden Sicherheitsmechanismen unterliegen Unterschiedlichkeiten bei

→ **verwendeten Basistechnologien auf Anwendungs- und Netzebene,**

→ **Verantwortlichkeit in Betrieb, Administration und Datenpflege,**

→ **Innovationszyklen und Nutzungsdauer**

(2) Existenz einer Reihe firmenspezifischer Lösungen, bei der die Schutzmaßnahmen zur Übertragungssicherheit, Integrität und Authentizität durch die jeweilige Anlage mit ihrer Anwendung gewährleitstet wird und nachgewiesen werden muss. Das gilt sowohl bei den Netzleittechnikapplikationen, als auch bei den Verfahren der Datennetzbetreiber.

→ **aufwendige Schutzbedarfsfeststellung und Risikoanalyse,**

→ **aufwendige Implementierungen und Tests im laufenden Betrieb,**

→ **Aufwand in Systemführung, -überwachung und Administration**

(3) Akzeptanz und Kosten für Aufbau und Betrieb geschlossener Kommunikationsinfrastrukturen sind für Betreiber inzwischen inakzeptabel.

Normativen und Empfehlungen besonders für Versorgungsunternehmen

- ISO/IEC 27000, 27001 und 27002 – Management der Informationssicherheit – Überblick, Anforderungen und Leitfaden – Grundsätze für die Unternehmen,
- DIN SPEC 27009 – Management der Informationssicherheit im Prozessbereich eines EVU
- ISO/IEC 17799 - Code of Practice für Management der Informationssicherheit,
- IEC 62351, Teile 1-6 (7, 8) - Power systems management and associated information exchange - Data and Communication Security,
- IEC 62443-3 - Security for industrial process measurement and control,
- IEC 61850 – Communication network and systems in power utility automation,

- BDEW-Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“,
- Gemeinsame Ausführungshinweise zur Anwendung des Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“
- BSI-CS 054 – Grundregeln zur Absicherung von Fernwartungszugängen

Schutzbedarfsfeststellung und Risikoanalyse

Die wichtigsten Bewertungskriterien des Schutzbedarfes sind :

- finanzielle Auswirkungen,
- Verstoß gegen Gesetze, Vorschriften und Verträge,
- Beeinträchtigung des informationellen Selbstbestimmungsrechts (besonders bei personenbezogenen Daten),
- Beeinträchtigung Geschäftsabläufe, immatrielle Schäden (Schutzrechtsverletzungen)
- negative Außenwirkung (Imageverlust),

Ergebnis einer Schutzbedarfsfeststellung in Kategorien können sein : klein, mittel, hoch, sehr hoch

Risikoanalyse

Gemeinsame Ausführungshinweise zur Anwendung des Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“

Gefahren von außen und innen betrachten!

Restrisikodeklaration

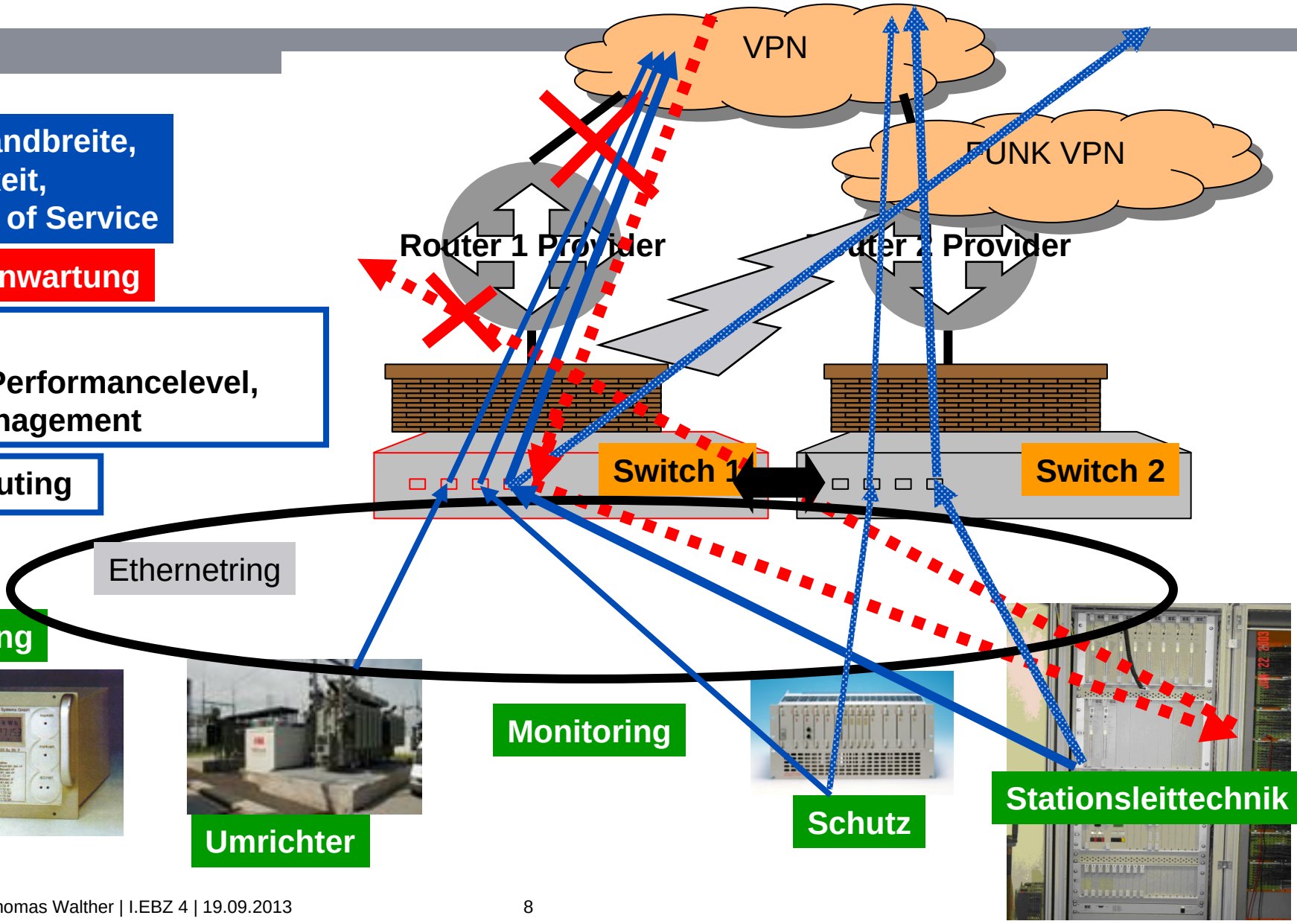
IT-security VPN-Prozessanschluß
Verantwortung beim Betreiber

**Verfügbare Bandbreite,
Geschwindigkeit,
Class-/Quality of Service**

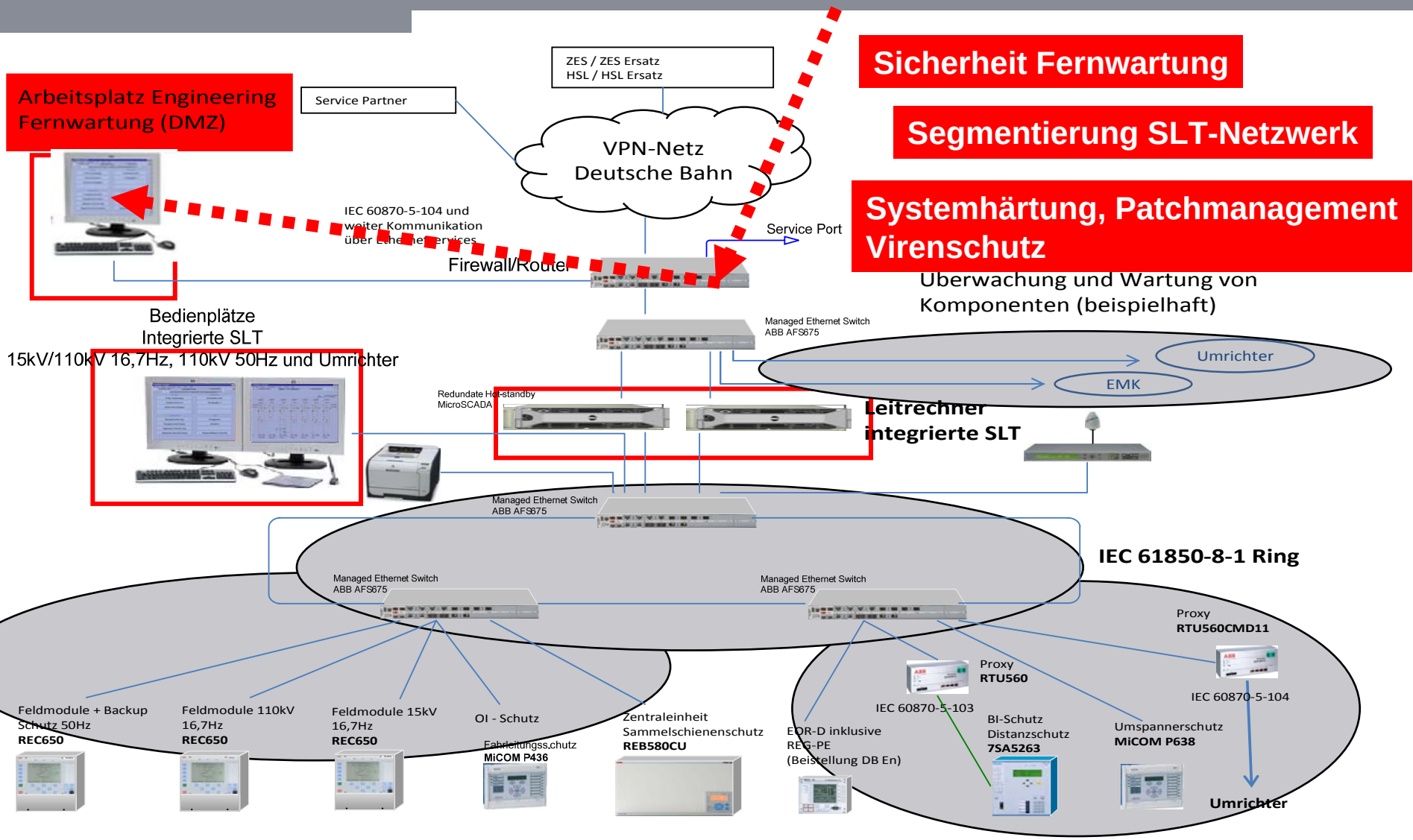
Sicherheit Fernwartung

**Verfügbarkeit,
Service- und Performancelevel,
Anschlussmanagement**

Ersatzwegerouting



Maßnahmen IT-security durch den Lieferanten der SLT



Typische Systeminfrastruktur in einem großflächigen Versorgungsunternehmen

FERNWARTUNGSZUGRIFF

Netzleitsystem

Prozessdatenverwaltung

Administration

Switch

Switch

Datenhaltung

Instandhaltungssysteme Büro

Service

Intranet Firma

Internet, öffentliches Netz

VPN Firma

Datennetzübergänge

VPN 2 Firma

Externe Leitsysteme

Switch

Switch

Datenknoten

SLT

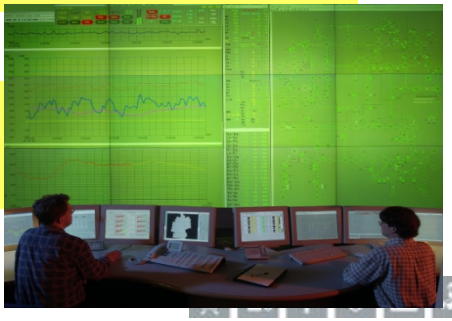
Großgeräte

SLT

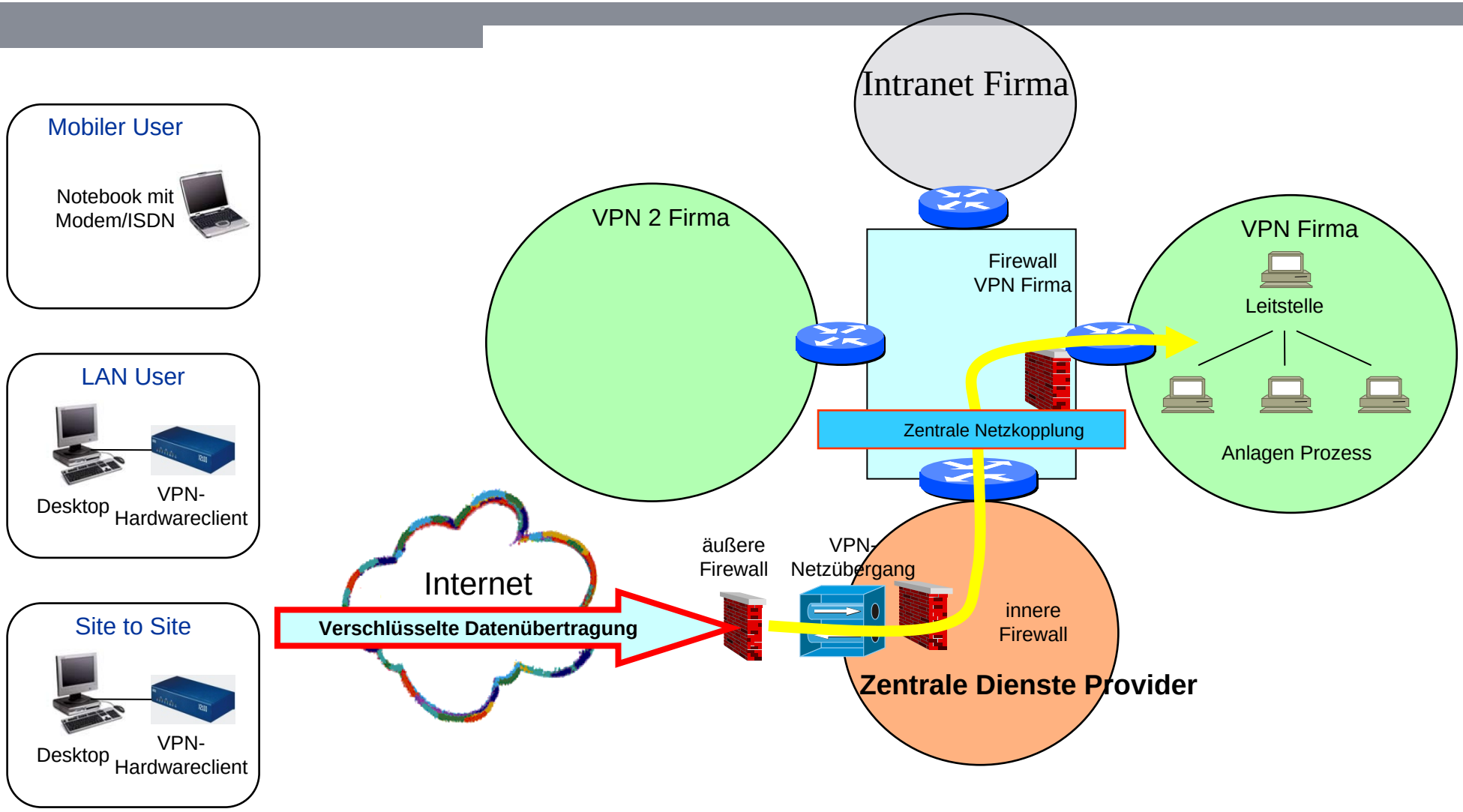
Schutz

Zählung

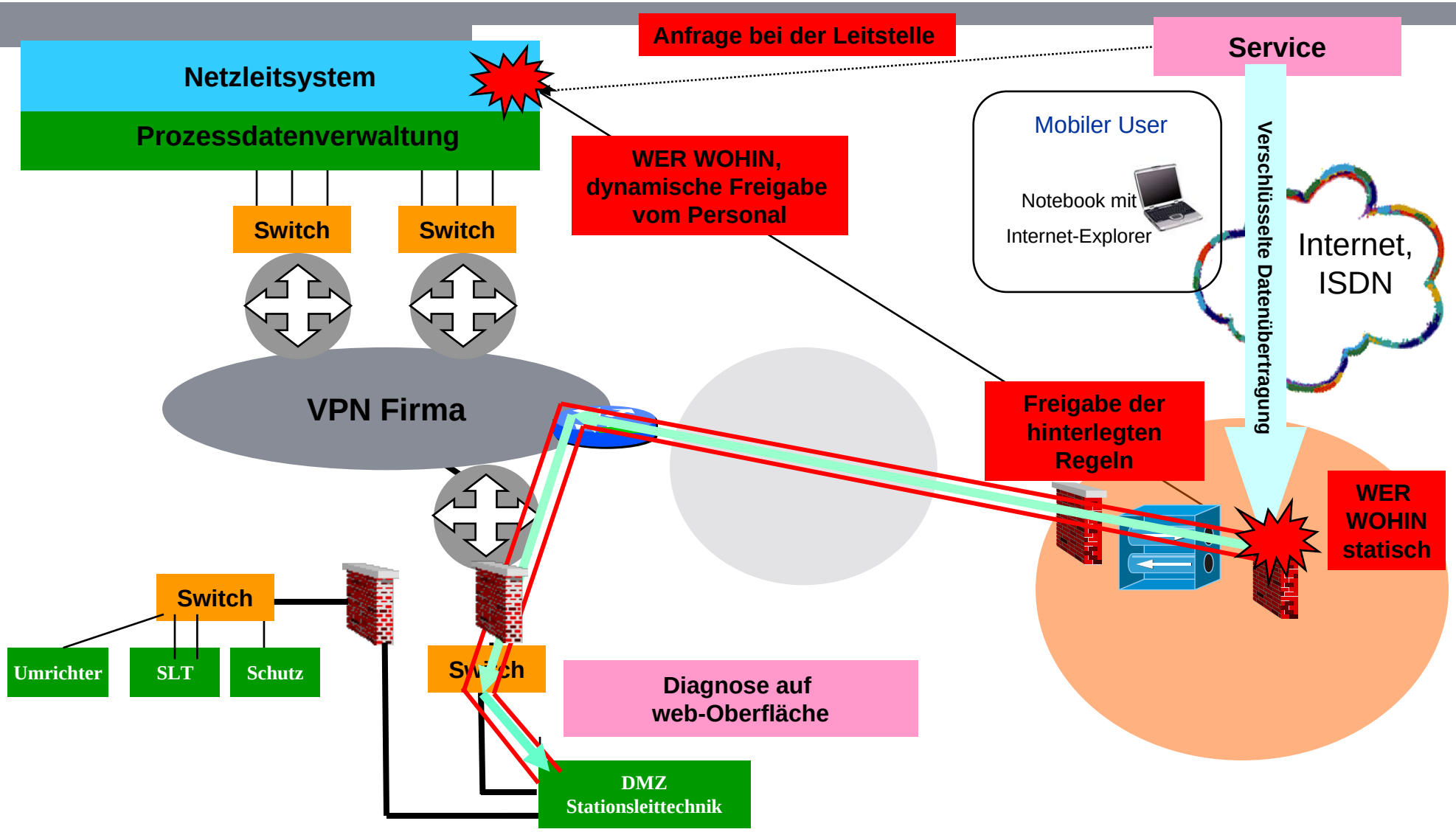
unternehmensinterne Leitsysteme



Sichere Fernwartung aus dem öffentlichen Datennetz an das VPN Firma



Ablauf eines sicheren Fernwartungszugriffes in das Prozessdatennetz



Kommunikation mit Schutzbedarf über IP VPN
Organisation und Maßnahmen (1)

Verantwortung des Provider / Netzanbieter

- **Netzverfügbarkeit / Bandbreite (besonders „Provinz“), vermaschter eigener Back-Bone, Anzahl Unterlieferanten, Back-Up/ Ersatzwegekonzept**
- **Endgerätetechnik (Router, Modem, Switch) - Einbaugrößen, Versorgungsspannung, Datenkabelverlegung usw.**
- **VPN-Netztyp, Kopplung zum öffentlichen Netz und zu anderen VPN / Intranet - Sicherheitskonzept, Risikoanalyse**
- **Remote Access / Fernwartung - Vorraussetzungen Hard-/Software und Autorisierungsverfahren**
- **Verfügbarkeit und Wiederherstellzeit (SLAs = Service Level Agreements), Einhaltung, Prüfbarkeit und Transparenz der SLAs, langfristige verfügbare Ansprechpartner, Eskalationsverfahren für Störungen**
- **Verkehrsprioritäten und Qualitätsmerkmale für den Datentransport (Quality of Service, Class of Service)**
- **frei skalierbares, erweiterbares IP-Adresskonzept im privaten Bereich, Routingverfahren**
- **Netz- und Geräteadministration, Monitoring (SNMP), Datenfluss- und Ereignisprotokollierung, Sicherheitsadministration, Pflege bestehender Anschlüsse**
- **Anschluss- und Betriebskosten**
- **Erweiterbarkeit des Netzes, Regularien für Netzausbau, Aufwand und Kosten**

Kommunikation mit Schutzbedarf über IP VPN
Organisation und Maßnahmen (2)

Verantwortung des Betreibers

- **Verfügbarkeitsanforderungen für Prozessankopplung in Leitstellen und Kommuniktionsschnittstellen der Stationsleittechnik aus Sicht eines vernünftigen Kosten / Nutzen-Verhältnisses**
- **Festlegung der Dienste und Teilnehmer VPN-intern und extern, Schutzbedarfsermittlung, Risikoanalyse**
- **Infrastrukturvorraussetzungen für Endgerätetechnik des Providers, wer bringt was wohin ?, Schnittstellen**
- **Schaffung routfähiger Fernwirktelegramm-strukturen für das VPN (z.Z. Standard: IEC 870-5-104), Anzahl und Routing IP-Datenströme und TCS 104-Datenströme, Subnet-IP-Adresskonzept, Merkmale QoS/CoS, Sicherheitsstammdatenpflege**
- **Remote Access / Fernwartung- dynamische Autorisierung beim Betreiber, wer darf was, wo und wann ?**
- **VPN-Monitoring, Protokollierung**
- **Bedarfsplanung der Anschlüsse für Zeitraum, Überwachung Rückbau Alt-Netz (parallele Kosten)**
- **Bestellung/Beschaffung von Netzanschlüssen und Einwahl-Zugängen**
- **Ansprechpartner, Eskalationsverfahren bei Störungen**