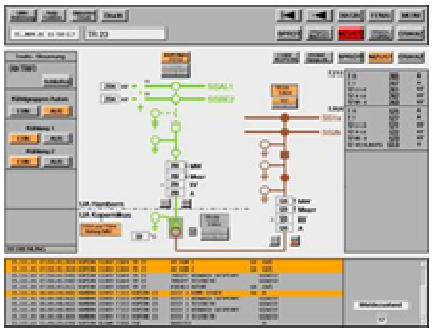




Rolf-Dieter Kasper
RWE Deutschland AG

Management der Informationssicherheit in Energienetzen

SECMGT-Workshop zum Management
von Informationssicherheit kritischer Infrastrukturen
10. Juni 2011 in Frankfurt/Main

VORRWEG GEHEN

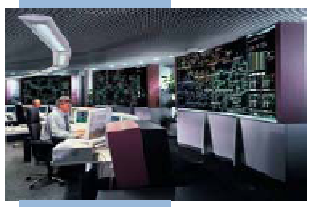
Agenda

- Intelligente Energienetze
- Entwurf DIN 270xx: Informationssicherheit in der Energieversorgung
- Anforderungen an Produkte: BDEW Whitepaper und Ausführungshinweise

Intelligente Netze („Smart Grids“)

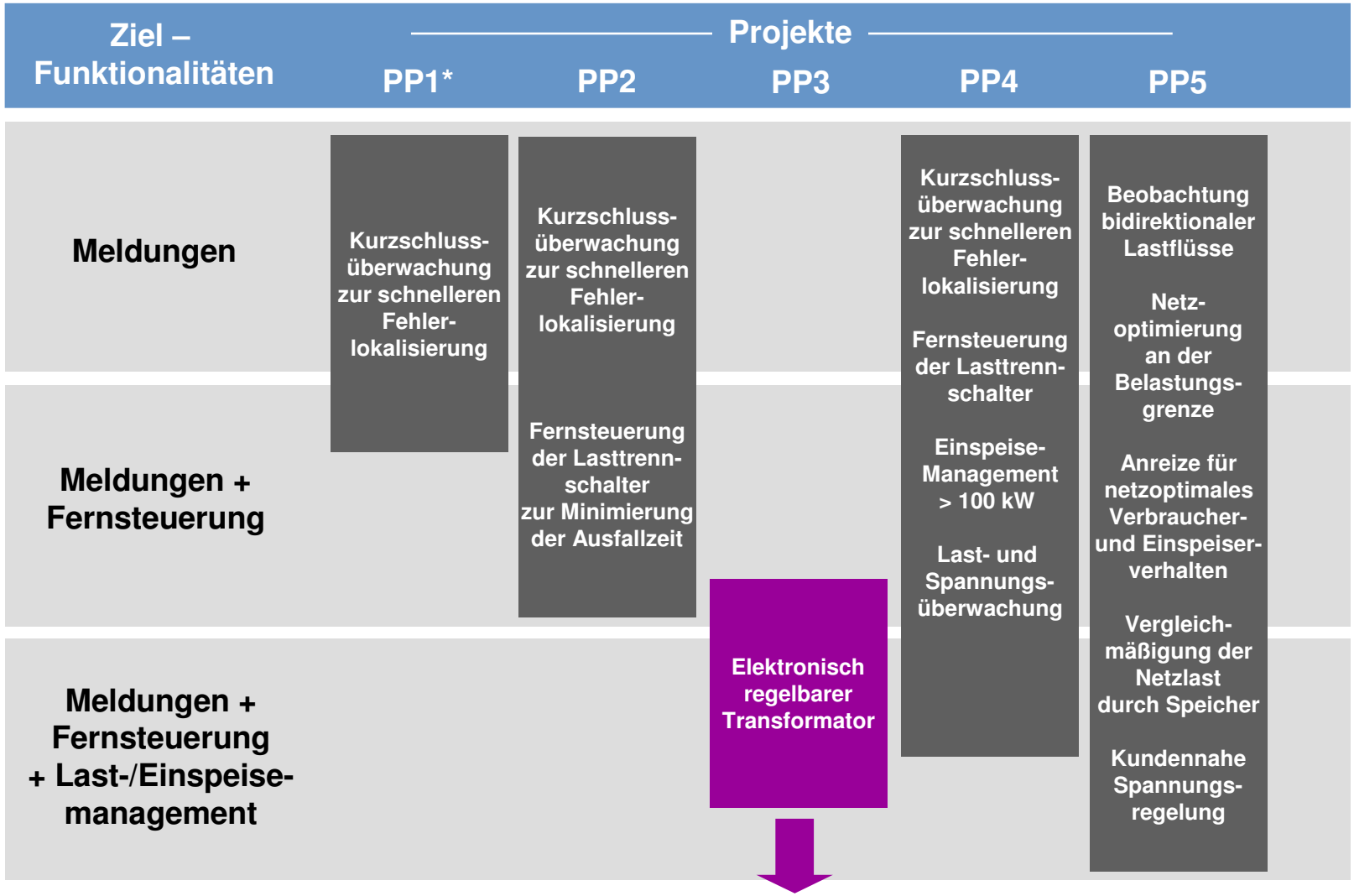
- Begriff „Smart Grid“
  Zukünftige Steuerung von Stromerzeuger, Speicher, Verbraucher und das Stromnetz mit moderner Informationstechnik.
- Deutschland – September 2010
  Die **Bundesregierung** wird für den Aufbau intelligenter Stromnetze die **rechtlichen Grundlagen** zur Einführung von intelligenten Zählern (Smart Metern) sowie für die kommunikative Vernetzung und Steuerung von Stromerzeugern, Speichern, Verbrauchern und Netzbetriebsmitteln schaffen. (Energiekonzept, 26.09.2010)
- Europa März 2011
  Veröffentlichung des **Mandats M/490 EU**
  „Auftrag an die Europäischen Normungsorganisationen zur Erstellung von Normen zur Unterstützung der Einführung intelligenter Stromnetze in Europa“

Ziel Netzstrategie: Statt einer maximalen, eine optimale Netzkapazität zur Verfügung zu stellen



- Der erhebliche Ausbau dezentraler Erzeugung konfrontiert einzelne Stromverteilnetzbetreiber bereits heute mit zusätzlichen Herausforderungen
- Mittelfristig werden diese auch durch neue volatile Lasten noch erheblich ansteigen
- Eine uneingeschränkte Bereitstellung der erforderlichen Netzkapazität führt zu sehr hohen Netzkosten, insbesondere in ländlichen Netzen
- In klar definiertem Umfang sollte die Möglichkeit bestehen, dezentrale Erzeugung und bestimmte Lasten (z.B. e-mobility, Wärme, Kälte, Speicher) zu steuern

Übersicht der Pilotprojekte in der RWE-Gruppe



* PPx – Pilotprojekte 1 - 5

PP3: Einspeise- und Lastmanagement mit einem regelbaren 10-kV-Transformator (1)

Ausgewählt wurde ein ländliches Netz bestehend aus Kabel und Freileitung

- NS-seitig mehrere Stromkreise (max. Netzlast 74 kW; angeschlossene Einspeiseleistung (Photovoltaik) 75 kWp; 14 Haushalte)
- MS-seitig WKA* mit 2 MW und ein großer Industriekunde; beide verursachen starke Spannungsschwankungen

Netztechnische Anforderungen

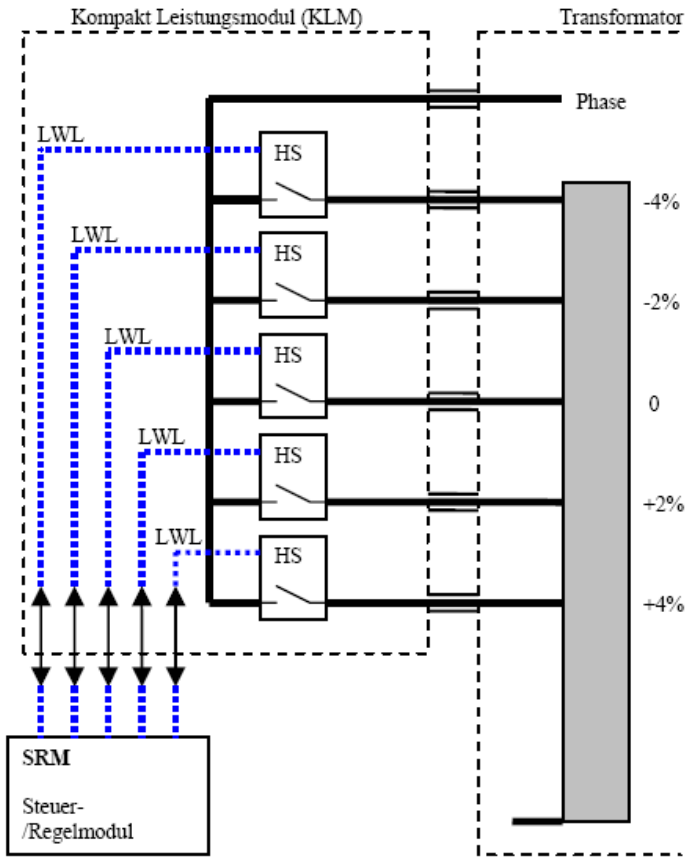
- Betriebsübliche Forderungen an Verfügbarkeit, Personenschutz, Bediensicherheit und Umweltschutz
- Automatische Regelung ohne manuellen Eingriff (erfolgt durch Umschaltung des Transformatorübersetzungsverhältnisses in Abhängigkeit von Netzlast und Spannungsniveau im Niederspannungsnetz)
- Für Kunden am angeschlossenen Niederspannungsnetz dürfen durch die Schaltvorgänge des Reglers keine Beeinträchtigungen der Spannungsqualität durch Netzrückwirkungen entstehen
- Dezentrale, eigenständig regelnde Einheit ohne leittechnische Anbindung

*) WKA - Windkraftanlage

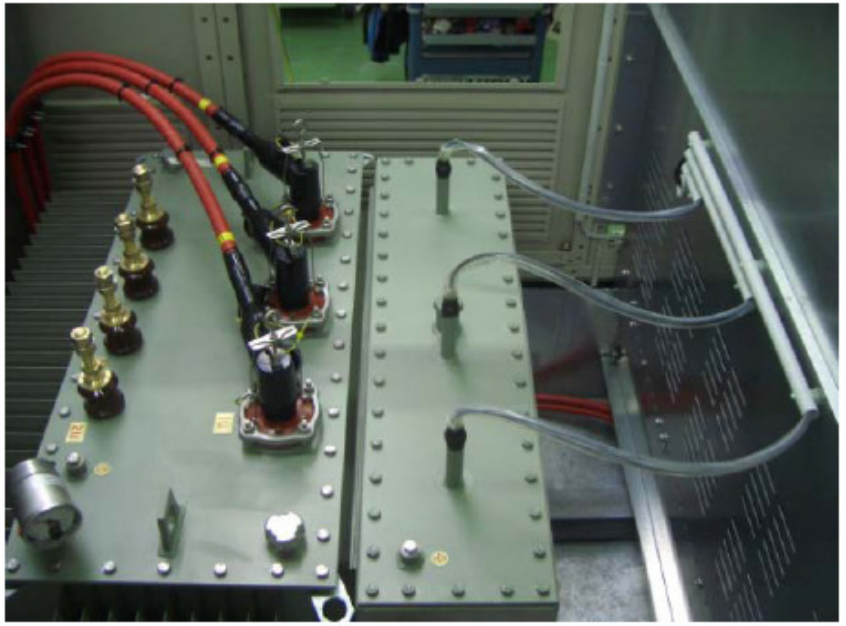
PP3: Einspeise- und Lastmanagement mit einem regelbaren 10-kV-Transformator (2)

Realisierung des Prototypen

- Prototyptransformator mit kurzschluss-festen Wicklungsanzapfungen der Stufen +4 /+2/ 0 /-2/-4%
- Anschlusskasten mit zugehöriger Leistungselektronik auf 10 kV Potenzial
- Umschaltung zwischen den Anzapfungen ohne Unterbrechung der Energiever-sorgung
- Verbindung zwischen dem Kompakt-leistungsmodul und dem Steuer- und Regelmodul über Lichtwellenleiter



PP3: Einspeise- und Lastmanagement mit einem regelbaren 10-kV-Transformator (4)



DIESES VORHABEN IST VOM EUROPÄISCHEN FONDS FÜR REGIONALE ENTWICKLUNG KOFINANZIERT WORDEN

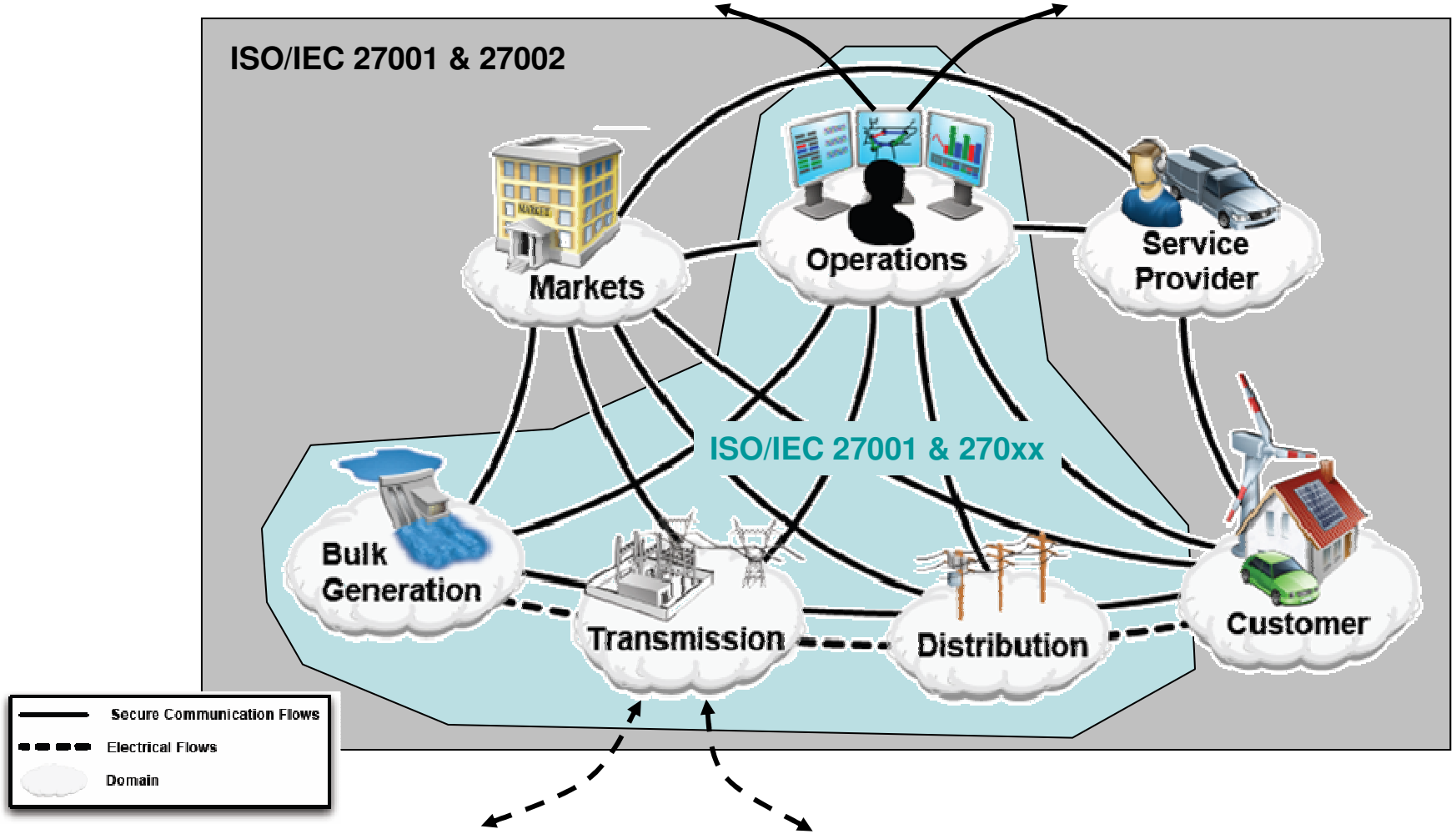
DIN 270xx: Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung
(Standardisierung nach ISO/IEC 27000)

Erweiterung der ISO 27000 Normenreihe um den PDV-Bereich der EVUs

- Ausgehend von den grundlegenden Standards der Normenreihe ISO 27000 soll eine Erweiterung deren konkrete Anwendung im EVU-Umfeld spezifizieren:
  - ISO 27001 definiert Anforderungen an das Informationssicherheits-Managementsystem (ISMS) und die umzusetzenden Kontrollziele.
  - ISO 27002 definiert Maßnahmen zur Umsetzung der Kontrollziele in den Bereichen Organisation, Prozesse, Betrieb und (indirekt) Technik.
  - ISO 270xx konkretisiert und ergänzt dann die ISO 27002-Anforderungen für den PDV-Bereich im EVU-Umfeld

- Vorgehen analog zur ISO 27011 für den Bereich Telekommunikation
- Berücksichtigung aller relevanten Bereiche, insbesondere auch der Organisation und des sicheren Betriebs

IT-Security Management nach ISO/IEC 27000 im EVU-Umfeld



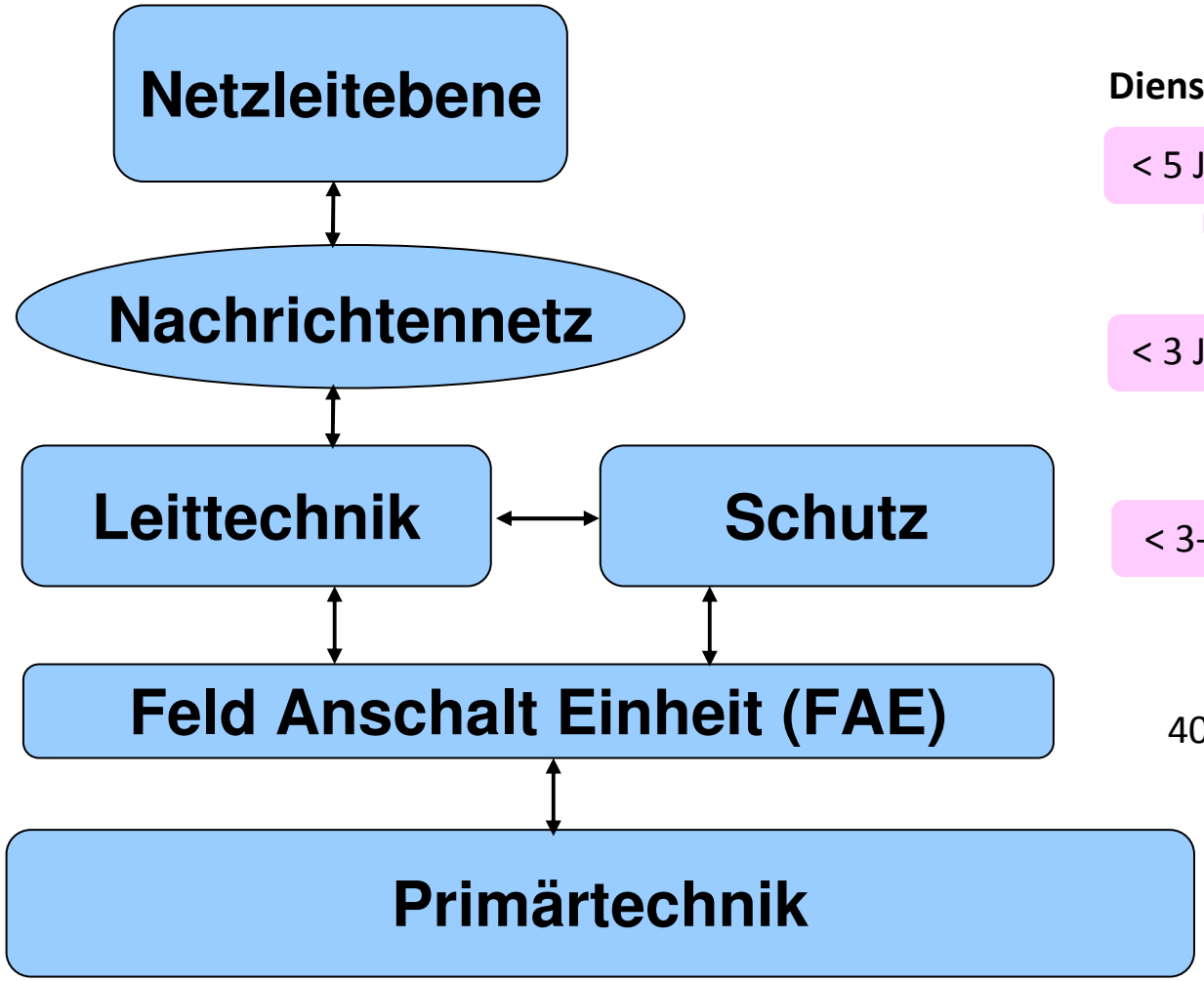
Notwendigkeit einer eigenen Norm für den PDV-Bereich der EVUs

- Ähnlich den Systemen der TK weisen PDV-Systeme in Ergänzung zu den in der ISO 27002 formulierten Sicherheitszielen und Maßnahmen zusätzliche Anforderungen auf
- Unterschiede zu herkömmlichen IT-Umgebungen in den Bereichen:
  - Entwicklung
  - Betrieb
  - Wartung
  - Einsatzumfeld
- Desweiteren bestehen relevante Unterschiede zu anderen PDV-Umgebungen, z.B. im industriellen Umfeld
- PDV ist integraler KRITIS-Bestandteil und für deren sicheren und störungsfreien Betrieb und zu Aufrechterhaltung der Energieversorgung zwingend notwendig

Charakteristika der PDV-Systeme im EVU-Umfeld Unterschiede zu herkömmlichen IT-Umgebungen

- Sicherheitsmerkmale
  - Verfügbarkeit und Integrität: fehlerhafte bzw. fehlende Daten führen zu
    - Fehlsteuerungen
    - Versagen von Schutz- und Safetysystemen
    - gefährlichen Fehlentscheidungen des Bedienpersonals
  - Berücksichtigung im Systemdesign, aber auch in Betriebsprozessen
- Systemarchitektur
  - Zentrale und dezentrale Systeme
  - Physikalischen Schutzniveau für dezentrale und zentrale Standorte nicht gleichwertig realisierbar
  - Schwierige Betriebs- und Managementprozesse für verteilte Systeme
  - Sicherstellung Systemwiederanlauf („Schwarzstartfähigkeit“)

Wesentliche Teilsysteme und typische Lebensdauern



Typische Lebensdauern

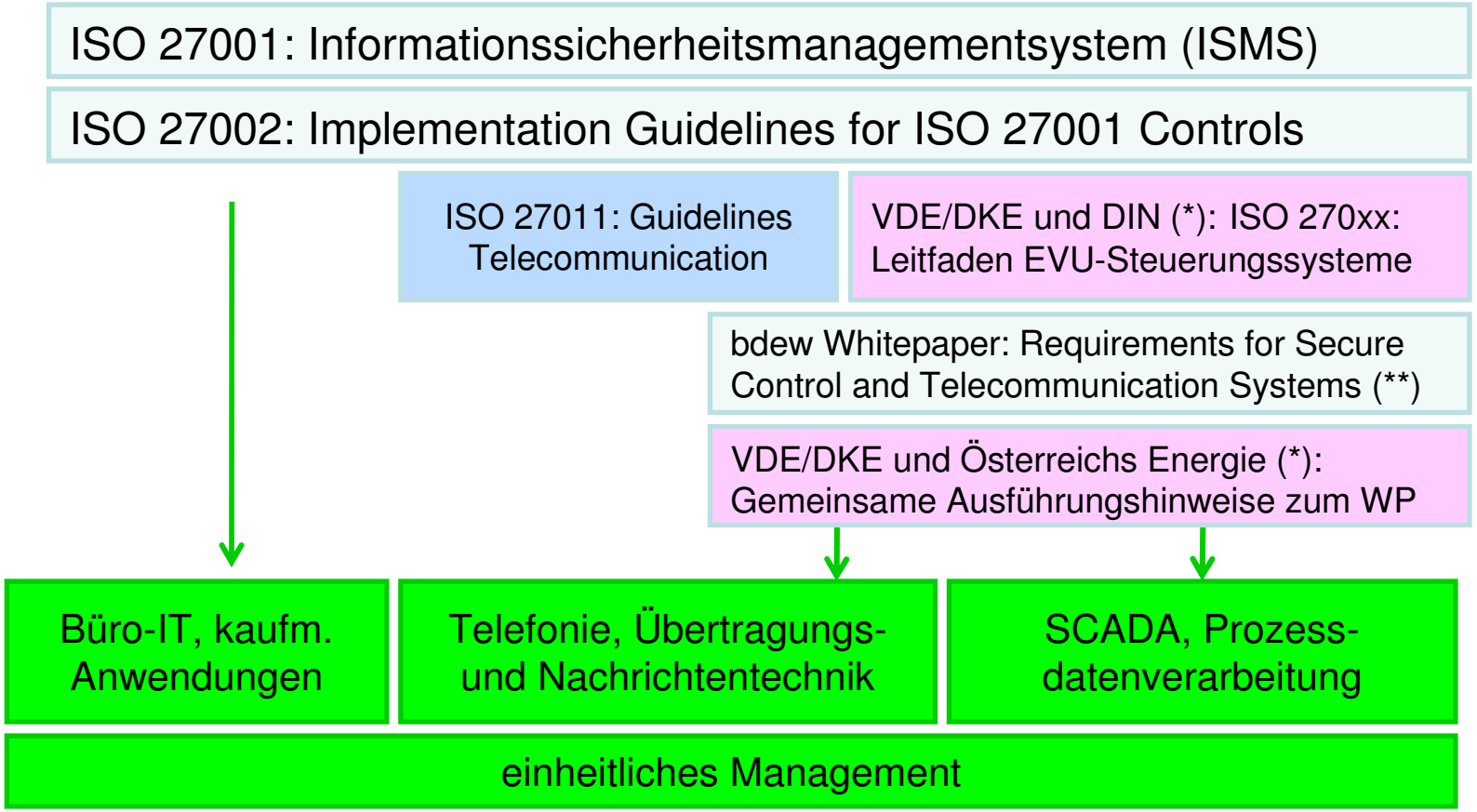
	Dienste und SW	Hardware
Netzleitebene	< 5 Jahre	<= 10 Jahre
	Einschätzung 2000: 15 Jahre insgesamt	
Nachrichtennetz	< 3 Jahre	10 - 15 Jahre
	Einschätzung 2000: 20 Jahre insgesamt	
Leittechnik / Schutz	< 3-5 Jahre	15 - 25 Jahre
	Einschätzung 2000: 25 Jahre insgesamt	
Feld Anschalt Einheit (FAE)	40 Jahre	40 Jahre
Primärtechnik		>40 Jahre

VORWEG GEHEN

Charakteristika der PDV-Systeme im EVU-Umfeld Unterschiede zu herkömmlichen IT-Umgebungen

- Wartung
  - Laufzeit Steuerungssysteme bis zu 25 Jahren
  - Spezielle Maßnahmen zum Umgang mit Standardsoftware notwendig
  - Häufige Außerbetriebnahmen von Steuerungskomponenten nicht realisierbar, insbesondere nicht in dezentralen Umgebungen
  - Wartungsfenster müssen langfristig geplant werden
  - Äußerst aufwendige Installations- und Funktionstests
- Geräteressourcen
  - Prozessnahe Komponenten verfügen häufig nicht über ausreichend Systemressourcen
  - Sicherheitsfunktionen schwierig realisierbar

Standardisierung nach ISO/IEC 27000 in Zusammenarbeit mit weiteren Verbänden



* Aktuell im Arbeit

** Das bdew Whitepaper befasst sich nur mit der typischen Anwendung der Telekommunikation im Rahmen der PDV, nicht aber umfassend mit allen von der ISO 27001 erfassten Systemen.

Inhaltsüberblick des Normentwurfs

- Berücksichtigung von EVU-typischen Organisationsstrukturen
  - Erzeugung und Netzbetrieb, Asset-Owner ggf. ungleich Betreiber
- Berücksichtigung von Anforderungen aufgrund von Regulierung
- Konkretisierung von Anforderungen und Maßnahmen, z.B.
  - Berücksichtigung weitreichender Netzausfälle und Telekommunikation, insb. im Krisenfall (Notfallmanagement, ISO 27002 14.1.1 bis 14.1.5)
  - Besonderheiten der Protokolle Prozessdatenkommunikation (Netzwerksicherheit, ISO 27002 10.6)
  - Berücksichtigung der verteilten Infrastruktur und kritischer Standorte wie z.B. Netzleitstellen (Sicherheit der Betriebsmittel, ISO 27002 9.2.1 bis 9.2.7)
  - Schnittstellensysteme zu anderen Netzbetreibern, z.B. TASE.2

Entwurfsinhalte Teil 1: Ergänzungen der DIN ISO/IEC 27002

- Umsetzungsempfehlungen und Informationen für die Energieversorgung wurden in den folgenden Kapiteln ergänzt:
  - Organisation der Informationssicherheit (Kapitel 6)
  - Management von organisationseigenen Werten (Kapitel 7)
  - Personalsicherheit (Kapitel 8)
  - Physische und umgebungsbezogene Sicherheit (Kapitel 9)
  - Betriebs- und Kommunikationsmanagement (Kapitel 10)
  - Zugangskontrolle (Kapitel 11)
  - Beschaffung, Entwicklung und Wartung von Informationssystemen (Kapitel 12)
  - Sicherstellung des Geschäftsbetriebs (Kapitel 14)
  - Einhaltung von Vorgaben (Kapitel 15)

Entwurfsinhalte Anhang A - „Erweiterter Maßnahmenkatalog für die Energieversorgung“

- A.9 Physische und umgebungsbezogene Sicherheit
  - A.9.1 Sicherheitsbereiche
    - A.9.1.7 Sicherung von Leitstellen
    - A.9.1.8 Sicherung von Technikräumen
    - A.9.1.9 Sicherung von Außenstandorten
  - A.9.3 Sicherheit in Räumlichkeiten Dritter
    - A.9.3.1 Betriebseinrichtung in Bereichen anderer Energieversorger
    - A.9.3.2 Betriebseinrichtung beim Kunden vor Ort
    - A.9.3.3 Gekoppelte Steuerungs- und Kommunikationssysteme

Entwurfsinhalte Anhang A - „Erweiterter Maßnahmenkatalog für die Energieversorgung“

- A.10 Betriebs- und Kommunikationsmanagement
  - A.10.6 Management der Netzsicherheit
    - A.10.6.3 Sicherung der Prozessdatenkommunikation
  - A.10.11 Altsysteme
    - A.10.11.1 Behandlung von Altsystemen
  - A.10.12 Betriebssicherheit
    - A.10.12.1 Integrität und Verfügbarkeit von Funktionen der Betriebssicherheit

Entwurfsinhalte Anhang A - „Erweiterter Maßnahmenkatalog für die Energieversorgung“

- A.11 Zugangskontrolle
  - A.11.4 Zugangskontrolle für Netze
    - A.11.4.1 Kopplung von Steuerungssystemen

- A.14 Sicherstellung des Geschäftsbetriebs
  - A.14.2 Wesentliche Notfalldienste
    - A.14.2.1 Notfall-Kommunikation

BDEW Whitepaper und Ausführungshinweise

(Anforderungen und Ausführungshinweise für die Informationssicherheit in der Energieversorgung nach ISO/IEC 27000)

bdew

Energie. Wasser. Leben.

BDEW Bundesverband
der Energie- und
Wasserwirtschaft e.V.

Reinhardtstraße 32
10117 Berlin

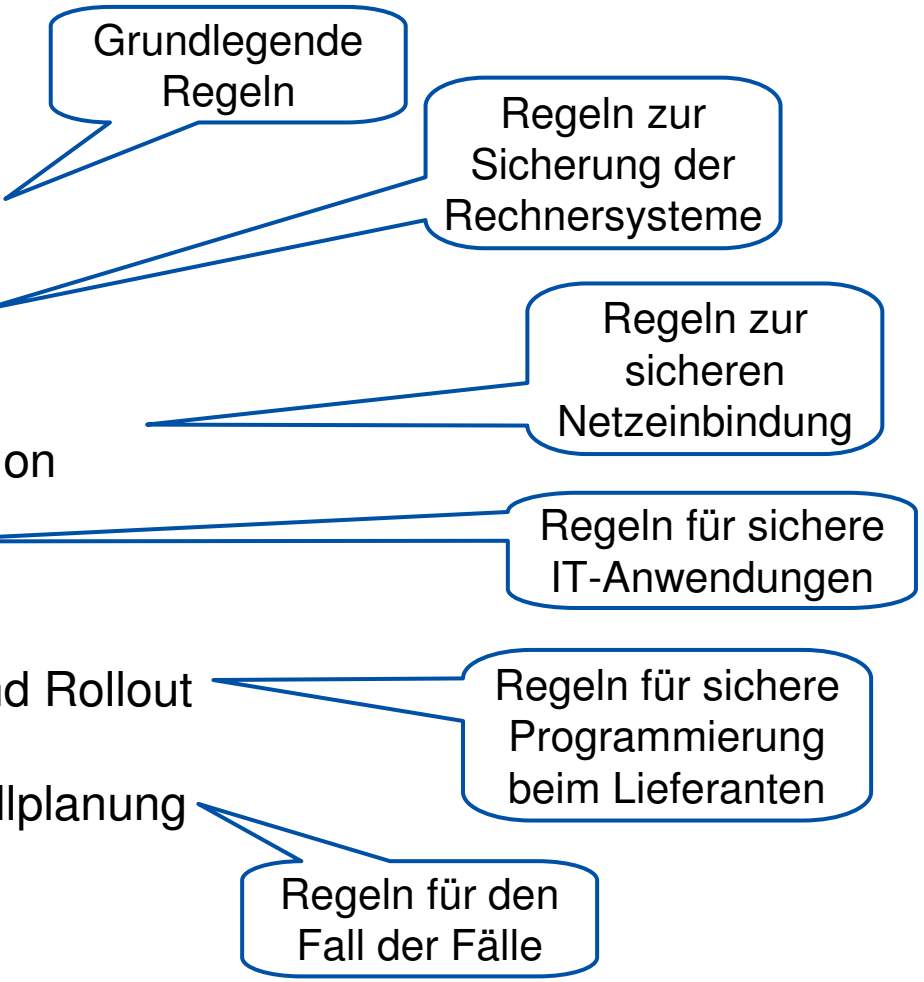
Whitepaper
Anforderungen an sichere Steuerungs- und Telekommunikationssysteme

White Paper
Requirements for Secure Control and Telecommunication Systems

Version 1.0
Berlin, 10. Juni 2008

Was regelt das BDEW Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ ?

- Abgedeckte Bereiche:
  - Allgemeines/Organisation
  - Bereich Basissysteme
  - Bereich Netze / Kommunikation
  - Bereich Anwendung
  - Bereich Entwicklung, Test und Rollout
  - Backup, Recovery und Notfallplanung



Aufbau der Ausführungshinweise zum BDEW WP

- Grundstruktur wie das BDEW Whitepaper (WP)
- Beschreibung des Lifecycle eines Leitsystems inkl. der Subsysteme
- Berücksichtigung der Ausführungshinweise bei
  - Projektplanungen/-umsetzen (Ausschreibungen) und Produktentwicklung
  - Produktservice
  - Leitstellen-/Systembetrieb
- Detaillierung der Sicherheitsanforderungen aus dem BDEW WP nach
  - grundsätzlichen Ergänzungen und Anmerkungen
  - speziellen Anforderungen
    - beim Leitstellen-/Systembetrieb
    - bei der Übertragungstechnik
    - bei der Sekundär-/Automatisierungstechnik
    - bei Organisation und Prozessen

Aktuelle Diskussionsthemen mit den Herstellern der Energieleittechnik

- Für typische Produkte wie
  - Zentrale Netzleitsysteme und Stationsleitsysteme (z.B. Ranger, NetworkManager, MicroSCADA)
  - Schutz und Stationsleittechnik (z.B. SAS 6x0, Relion)
  - Zugehörige Parametrierumgebungen
- Umsetzung der WP Anforderungen beim
  - Patchmanagement
  - Schadsoftwareschutz
  - Härtung der Systeme
  - Netzwerkstruktur und Kommunikation
  - Fernwartung
  - Sichere Entwicklungsprozesse
  - Datensicherung und Notfallkonzeption

Fazit:

- Grundverständnis Intelligente Energienetze
  - Smart Grid in der Perspektive 2020 ist realistisch
  - Smart Grid Realisierungen heute durch bekannte Steuerungstechnik
- Entwurf DIN 270xx: Informationssicherheit in der Energieversorgung
  - Grundsätzlich Umsetzung auf Basis heutiger Normen möglich
  - Es sind jedoch brachenspezifische Anpassungen erforderlich
  - Statt firmenspezifischer Anpassungen abgestimmte Vorgehensweise durch Normungsinitiative
- BDEW Whitepaper und Ausführungshinweise
  - Anforderungen an Hersteller werden verbindlich !