TeleTrusT
Pioneers in IT security.

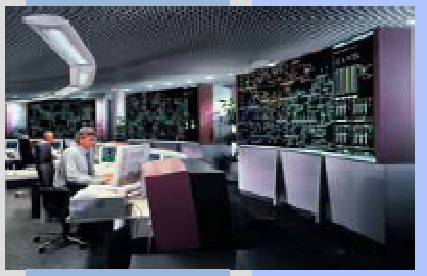
TeleTrusT-Informationstag "IT-Sicherheit im Smart Grid"

Berlin, 31.05.2011

Rolf-Dieter Kasper
RWE Deutschland AG
Sicherheit im Smart Grid

Agenda

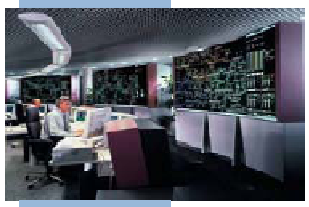
- Grundverständnis „Smart Grid“
- IT-Sicherheit in Energienetzen Beispiel RWE
- Entwurf DIN 270xx: Informationssicherheit in der Energieversorgung
- BDEW Whitepaper und Ausführungshinweise



Smart Grid – von der Innovation zur Realisierung
Bericht der EU-Kommission

- Die EU-Kommission sieht folgenden dringenden Handlungsbedarf:
  - Technische Standards entwickeln
  - Datenschutz für den Endkunden gewährleisten
  - Rechtliche Rahmenbedingungen für Anreize zum Ausbau von Smart Grids schaffen
  - Offenen und wettbewerbsfähigen Handelsmarkt für die Endkunden garantieren
  - Fortlaufende Unterstützung für technische Innovationen bereitstellen
- 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

IT-Sicherheit in Energienetzen
Beispiel RWE

Hauptaufgaben der Security Organisation für den gesicherten Betrieb bei RWE

Betrieb

Management / GF

initial:

- setzen der Vorgaben
- in Kraft setzen von Policy, Scope und Strategie

zyklisch:

- Review der Berichte und Ergebnisse
- Genehmigung von Maßnahmen und Veränderungen
- Bereitstellung der Ressourcen
- Akzeptanz von Restrisiken

ISMS Management

Management Framework:

- Policies
- Standards
- Prozesse

ISMS Operational Management

- Risiko-Management
- Sicherer Betrieb
- Business Continuity Mgmt.
- Ausbildung und Awareness
- Monitoring and Reporting
- Audit and Review

Sicherer Betrieb

Monitoring / Ereignisse

- reaktiv (nach Ereignissen)
- proaktiv (Audits und Tests)

Dokumentation

und Analysen

- revisionsfest

ISMS Forum

- Prüfung und
- Verbesserung des Sicherheitsmanagements
- Reporting an den LK

ISMS Security Organisation der RWE Deutschland AG

ISMS Lenkungskreis

Prämissen aus der **Geschäftsstrategie**

Einfluss auf das **Geschäftsergebnis**

Kreis der ISMS Delegierten
(Security Management Committee)

Formulierung Sicherheitsziele aus den Prämissen und dem in der **ISMS Policy** definierten Scope

Auswirkungen der Sicherheitsmaßnahmen auf die **Geschäftsrisiken**

ISMS Foren Prozess- & Büronetz

Umsetzung des Sicherheitsziele in IT-Technische Anforderungen und Formulieren der **Maßnahmenpakete**

Feststellung der Wirksamkeit der Maßnahmen und Umsetzungsgrad der Sicherheitsziele

Linienorganisation Abteilungsleiter Mitarbeiter

Umsetzen der Maßnahmenpakete in **IT-technische Lösungen**

Berichte zu definierten **ISMS-Controls** (Fehler, Verfügbarkeiten, Änderungen, Erweiterungen usw.)

Ebene der „Bits und Bytes“

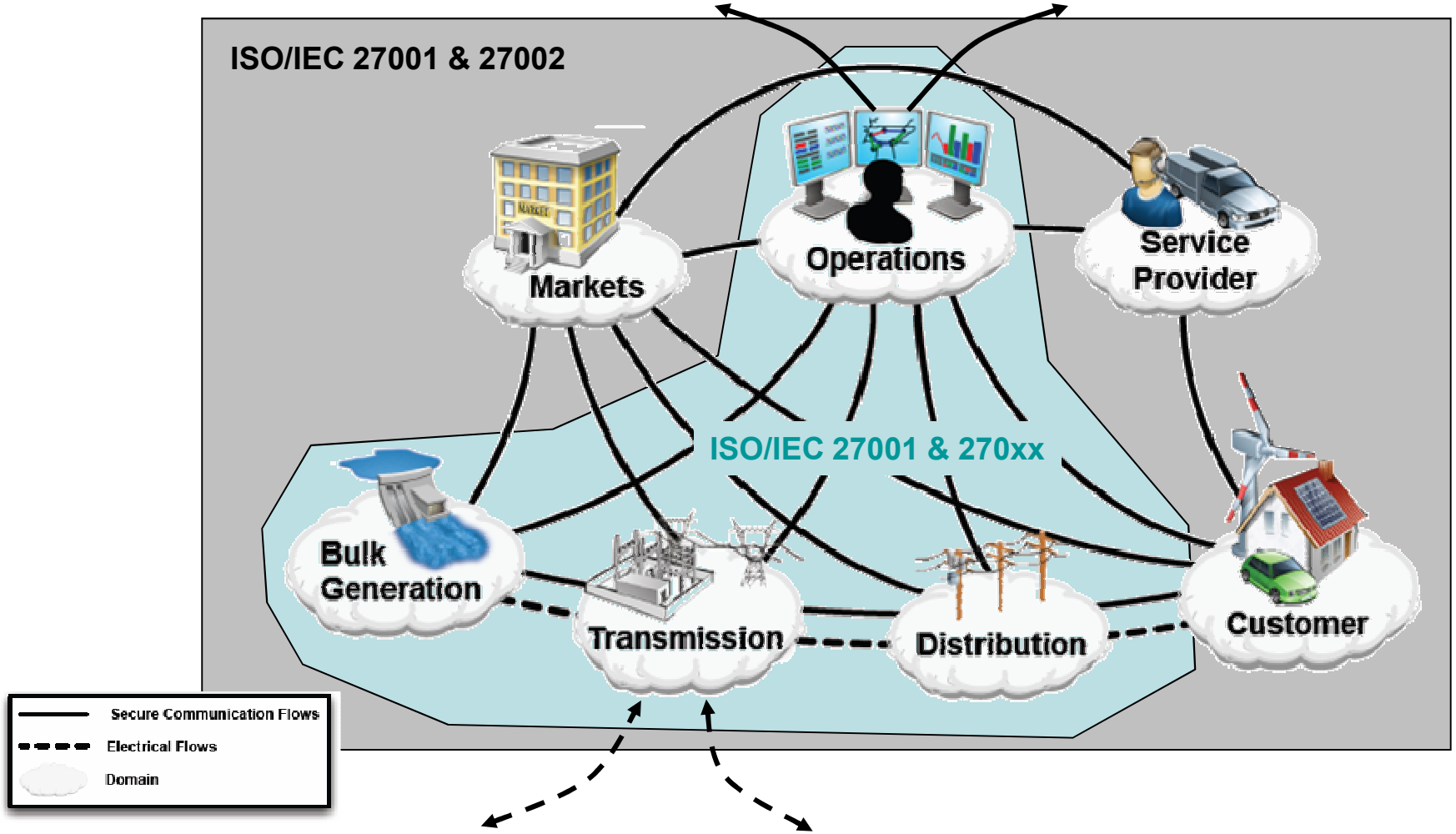
DIN 270xx: Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung
(Standardisierung nach ISO/IEC 27000)

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

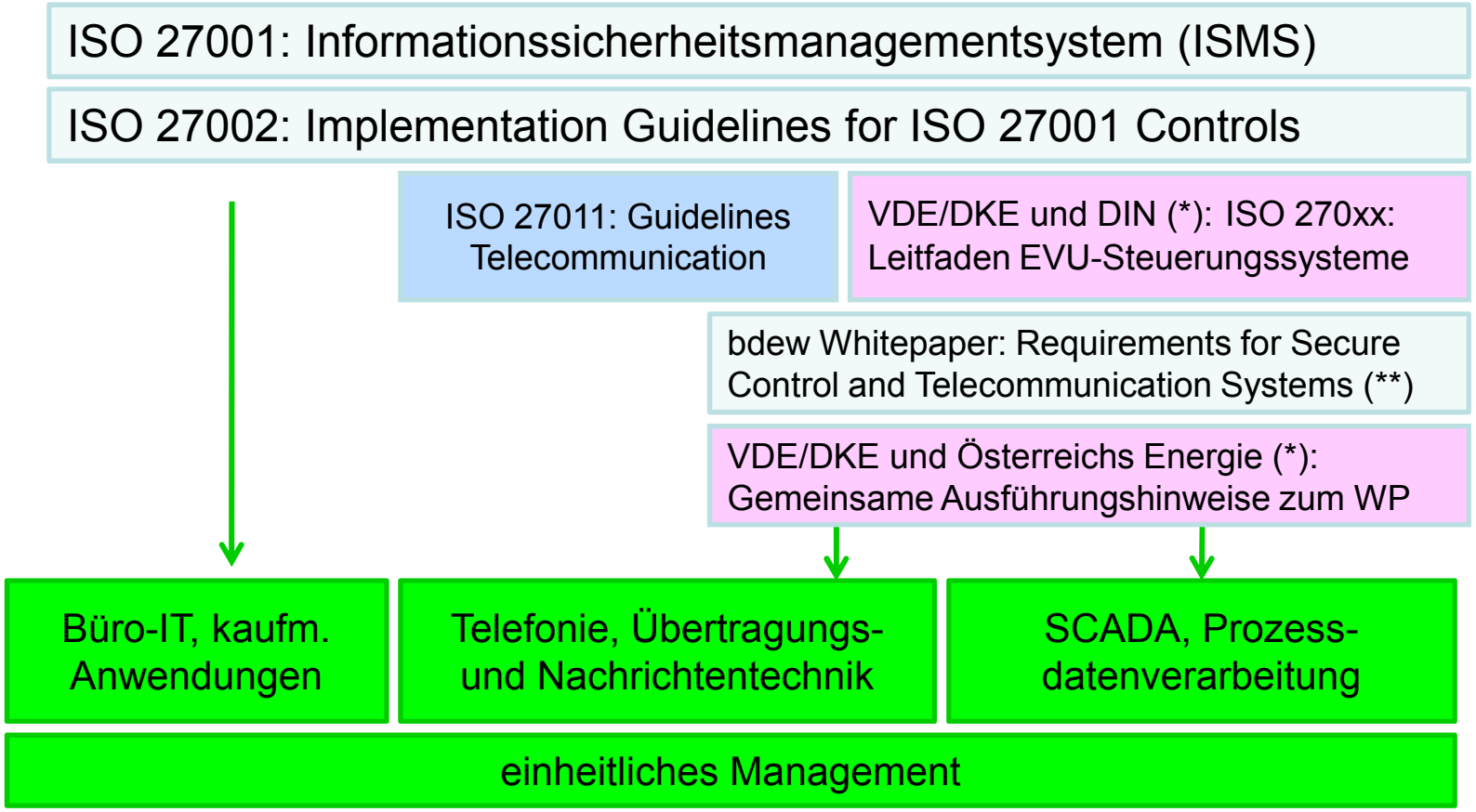
Charakteristika der PDV-Systeme im EVU-Umfeld Unterschiede zu herkömmlichen IT-Umgebungen

- 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“)

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

- Wartung
  - Laufzeit Steuerungssysteme bis zu 20 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

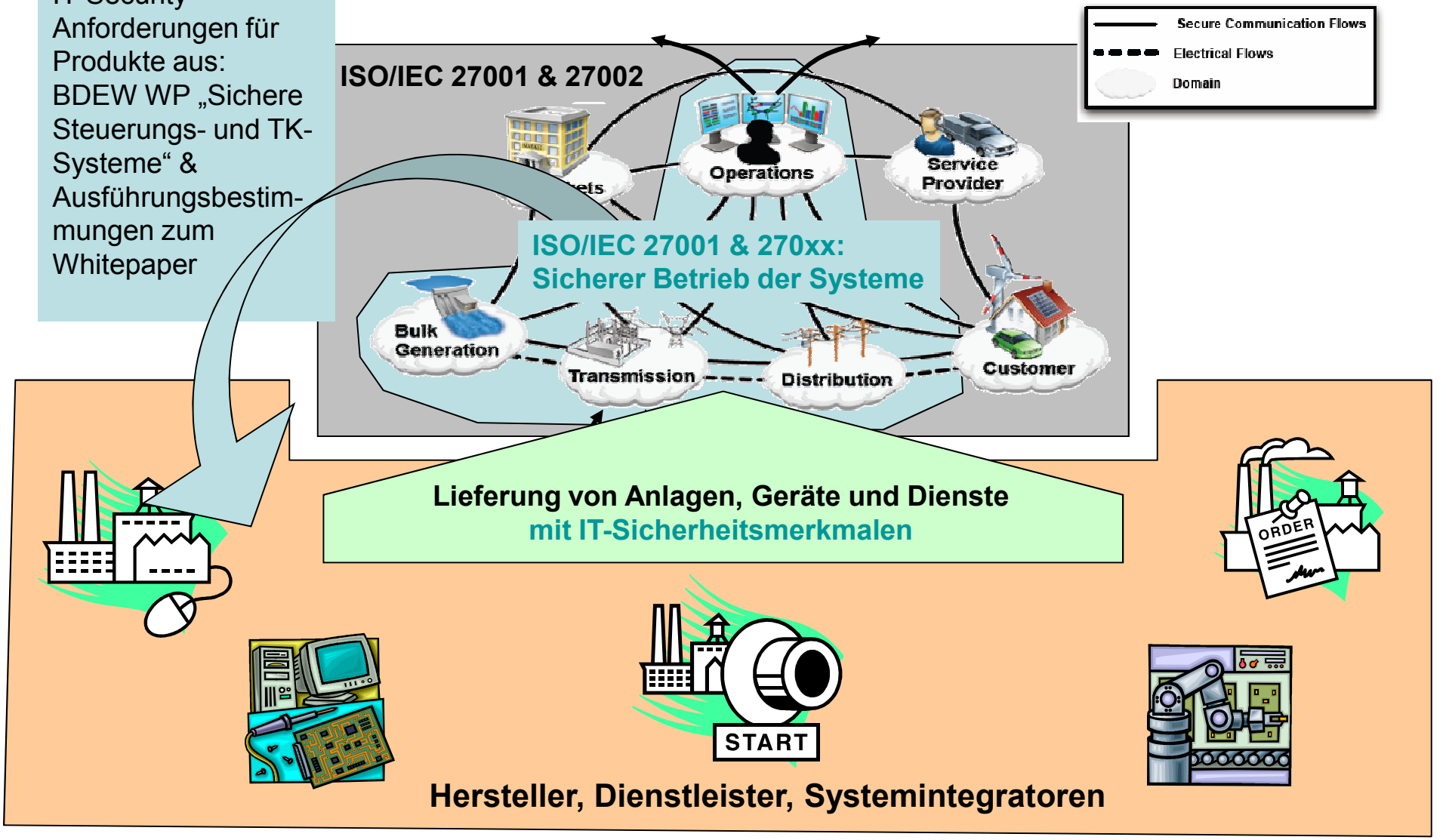
- Berücksichtigung von EVU-typischen Organisationsstrukturen
  - Erzeugung und Netzbetrieb, Asset-Owner ggf. ungleich Betreiber
- Berücksichtigung von Anforderungen aufgrund von Regulierung
- Konkretisierung von Anforderungen und Maßnahmen, z.B.
  - Berücksichtigung weitreichender Netzausfälle und Telekommunikation, 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

BDEW Whitepaper und Ausführungshinweise

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

IT-Security Anforderungen an Produkte und Dienstleistungen

IT-Security Anforderungen für Produkte aus: BDEW WP „Sichere Steuerungs- und TK-Systeme“ & Ausführungsbestim-mungen zum Whitepaper



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

Grundlegende Regeln

Regeln zur Sicherung der Rechnersysteme

Regeln zur sicheren Netzeinbindung

Regeln für sichere IT-Anwendungen

Regeln für sichere Programmierung beim Lieferanten

Regeln für den Fall der Fälle

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

Fazit:

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