IT-Resilienz und Risiko-Management von Energienetzen

Prof. Dr.-Ing. Hermann de Meer

Lehrstuhl für Informatik mit Schwerpunkt
Rechnernetze und Rechnerkommunikation

Lehrstuhl: Vorstellung

UNIVERSITÄT PASSAU
Fakultät für Mathematik und Informatik

- Personal
  - Prof. Dr.-Ing. Hermann de Meer
  - 9 wissenschaftliche Mitarbeiter
- Forschung
  - **IT-Sicherheit / Funktionale Sicherheit**
    - Risikoanalyse in kritischen Infrastrukturen
    - Analyse von Sicherheitsimplikationen durch Vernetzung (z.B. Smart Grid)
  - **Energieeffizienz**
    - Intelligente Demand-Response Mechanismen im Smart Grid
    - Trade-Off-Analysen zwischen Energieeffizienz/Performance/Sicherheit
  - **Selbstorganisation**
  - **Virtualisierung**

Energienetz: „Smart Grid“

UNIVERSITÄT PASSAU
Fakultät für Mathematik und Informatik

- Das heutige Energienetz wird sich in den kommenden Jahren in ein „Smart Grid“ verwandeln
  - Integration und Verflechtung von Energienetz mit Informations- und Kommunikations-Technologie (IKT)
- Netz von Netzen: Energienetz wird mit öffentlichen IT-Netzen (z.B. Internet) verbunden
  - Gegenseitige Abhängigkeit der Netze
  - Neues Netz besitzt zuvor unbekannte, komplexe Eigenschaften
  - Kombination beider Netze bildet ein neues komplexes System

➔ Verschmelzung von IT- und Energienetz erzeugt neuartige Risiken und Bedrohungen

Smart Grid: Kritische Infrastruktur

UNIVERSITÄT PASSAU
Fakultät für Mathematik und Informatik

- Energie- und Kommunikationsnetz unabhängig voneinander eine kritische Infrastruktur
  - Ständige Verfügbarkeit nicht optional, sondern obligatorisch
  - Störung ökonomisch, sozial und politisch-administrativ katastrophal
- Risikoabschätzung im Smart Grids enorm anspruchsvoll
  - Mögliche Fehlerausbreitung zwischen IKT und Energienetz
  - Vielfältige Fehlerquellen:
    - Unfälle / Menschliches Versagen
    - Defekte an Hard- / Software
    - Absichtliche Angriffe (Physikalisch / IT-basierend)

➔ Großflächiger, langfristiger Ausfall des Smart Grid muss unter allen Umständen verhindert werden!

Motivation

UNIVERSITÄT PASSAU
Fakultät für Mathematik und Informatik

- Stromausfall in Nord-Ost-Amerika 2003
  - Ursachen:
    - Software-Fehler in Überwachungssystemen
    - Überlastung und Ausfall von IT-Backup-Systemen
    - Mangelndes Risikobewusstsein
    - Veraltete Versorgungsnetzwerk-Infrastruktur
    - Mangelhafte Kommunikation
  - Folgen:
    - Mehr als 55 Millionen Personen ohne Strom
    - Ausfall öffentlicher Telekommunikations- / Versorgungsnetze
    - Geschätzte Kosten: 6 Milliarden US-$

➔ Wie können solch katastrophale Ausfälle verhindert werden?

(Fotos: Huffington Post, 2003)

Smart Grid: Lösungsansätze

UNIVERSITÄT PASSAU
Fakultät für Mathematik und Informatik

- Resiliente Realisierung eines Smart Grid benötigt:
  - Widerstandsfähiges Stromnetz
  - Widerstandsfähige Kommunikationinfrastruktur:
    - Vorsorge
    - Fehlererkennung
    - Fehlerabwehr
    - Fehlerbeseitigung
  - Neuartige Risiko-Bewertung notwendig:
    - Integration und Interaktion von Energienetz und IKT
    - Analyse von funktionalen Abhängigkeiten der Netze
    - Identifikation von Gefahrenpotential für vernetzte Energienetze

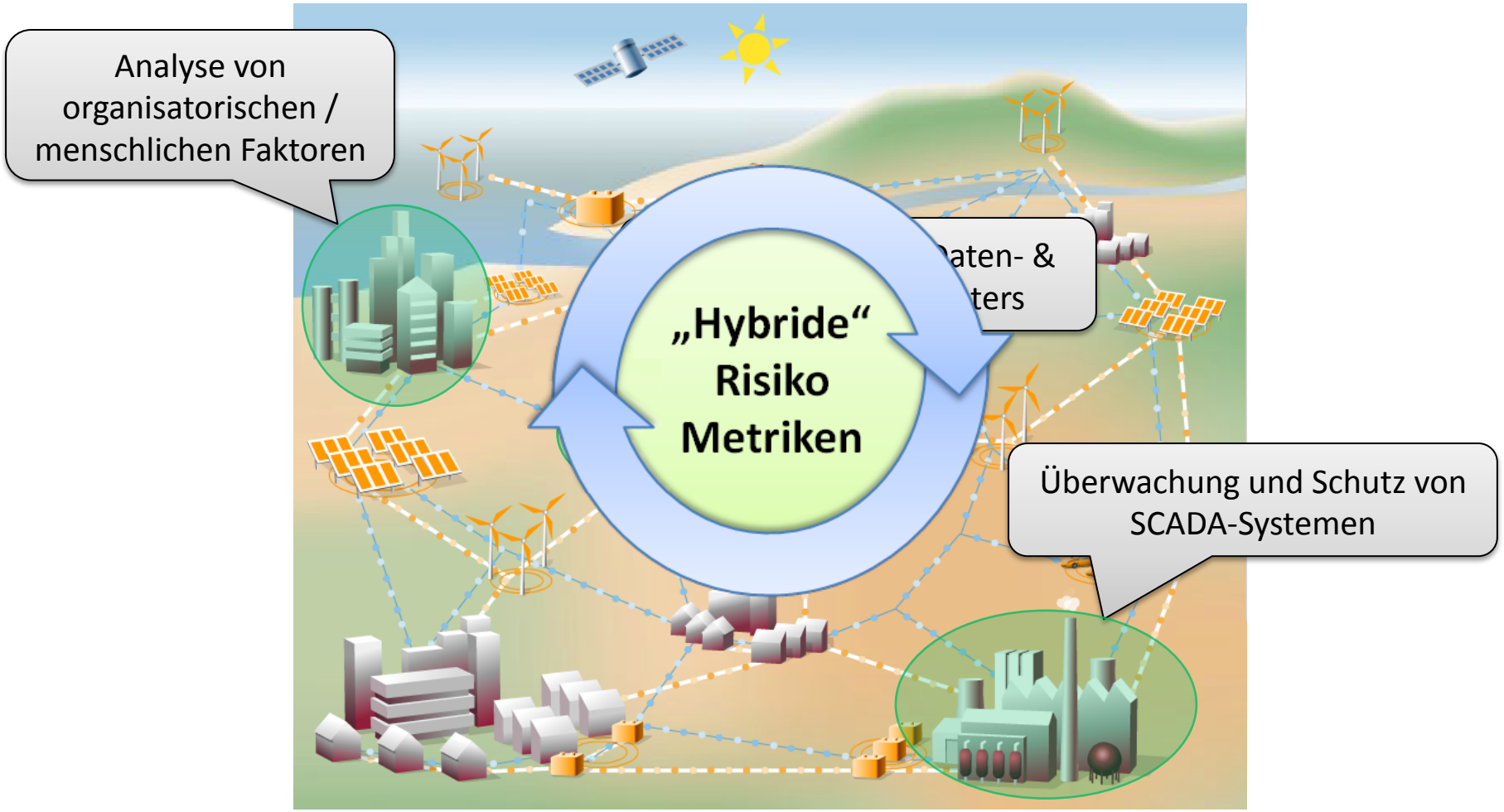
➔ Entwicklung ganzheitlicher Strategien, die den vielfältigen Bedrohungen Rechnung tragen

HyRiM: Projektübersicht

UNIVERSITÄT PASSAU
Fakultät für Mathematik und Informatik

- HyRiM = Hybrid Risk Management for Utility Networks
- EU FP7-Forschungsprojekt (Call FP7-SEC-2013.2.5-4)
- Laufzeit: 36 Monate (2014-2016)
- Kooperation zwischen 7 Projektpartnern
  - **Austrian Institute of Technology**
  - Lancaster University
  - ETRA Investigación y Desarrollo, S.A.
  - Akhela S.R.L.
  - Suministros Especiales Alginetenses, Coop. V.
  - Linz AG
  - Universität Passau

HyRiM: Projektübersicht



(Grafik: Föderprogramm E-Energy des BMWi)

HyRiM: Ziele (1/2)

UNIVERSITÄT PASSAU
Fakultät für Mathematik und Informatik

- Analyse von organisatorischen / menschlichen Faktoren
  - Untersuchung von organisatorischen / menschlichen Faktoren auf die Entwicklung von Risiken in Energienetzen
  - Minimierung von Risiken in Unternehmen, die durch neuartige Technologien oder durch menschliches Fehlverhalten ausgelöst werden
- Überwachung des Daten- & Energienetz Perimeters
  - Untersuchung von neuartigen Überwachungstechnologien (z.B. Sensornetze) zur Absicherung des Energienetz-Perimeters
  - Entwicklung von Selbstdiagnose-Systemen zur Fehlererkennung in Versorgungsinfrastrukturen
  - Klassifizierung und Empfehlungen für IT-basierte Schutzsysteme nach Anwendbarkeit und Effektivität in Versorgungsnetzwerken

HyRiM: Ziele (2/2)

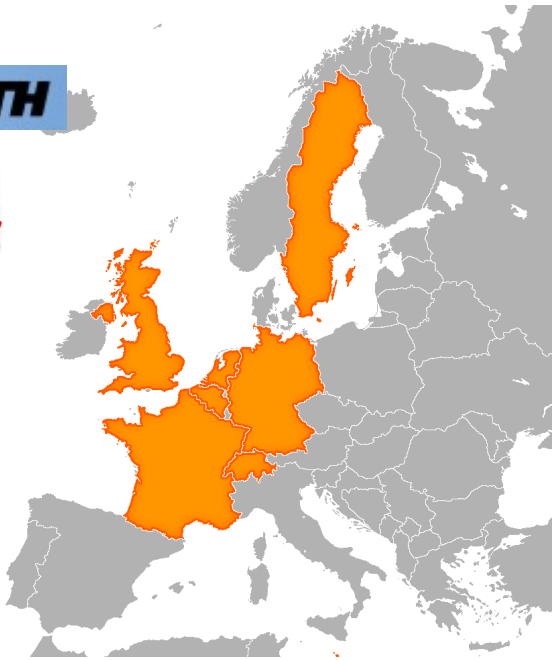
UNIVERSITÄT PASSAU
Fakultät für Mathematik und Informatik

- Überwachung und Schutz von SCADA-Systemen
  - Klassifikation von Attacken gegen SCADA-Systeme (z.B. Bedrohungen durch Smartphones, PDAs, USB-Sticks, …)
  - Analyse von unterschiedlichen Ansätzen zur Bedrohungsanalyse in SCADA-Systemen (z.B. Penetration-Tests, Firewalls, ...)
  - Entwicklung von präventiven Ansätzen und Policies zur Risikominimierung (z.B. Sicherheits-Audits, Risikoanalysen, ...)
- Entwicklung „hybrider“ Risikometriken
  - Verbindung von Risiken des Energienetzes und der IT-Infrastruktur
  - Ausfälle zufälliger Natur und intentionale Angriffe
  - Berücksichtigung des „Faktor Mensch“
  - Entwicklung von Analysemethoden / Metriken zur Beurteilung von Risiken

ResumeNet

UNIVERSITÄT PASSAU
Fakultät für Mathematik und Informatik

- ResumeNet = Resilience and Survivability for future networking: framework, mechanisms, experimental evaluation
- EU FP7-Forschungsprojekt (Call FP7-ICT-2007.1.6)
- Laufzeit: 40 Monate (2008-2011)
- Kooperation zwischen 9 Projektpartnern
  - **Swiss Federal Institute of Technology Zurich**
  - Lancaster University
  - Munich University of Technology
  - France Telecom
  - NEC Europe Ltd
  - Delft University of Technology
  - University of Uppsala
  - University of Liege
  - Universität Passau



Was ist Widerstandsfähigkeit? (1/2)

UNIVERSITÄT PASSAU
Fakultät für Mathematik und Informatik

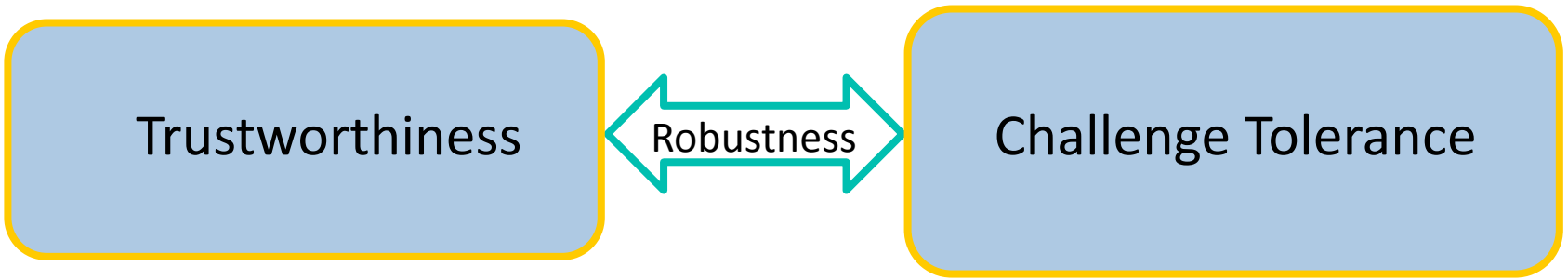
"The ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges."

"Die Fähigkeit eines Netzwerks auch unter Einfluss von Fehlern und Beeinträchtigungen ein angemessenes Dienstniveau zu erbringen und aufrecht zu erhalten."

Was ist Widerstandsfähigkeit? (2/3)

UNIVERSITÄT PASSAU
Fakultät für Mathematik und Informatik

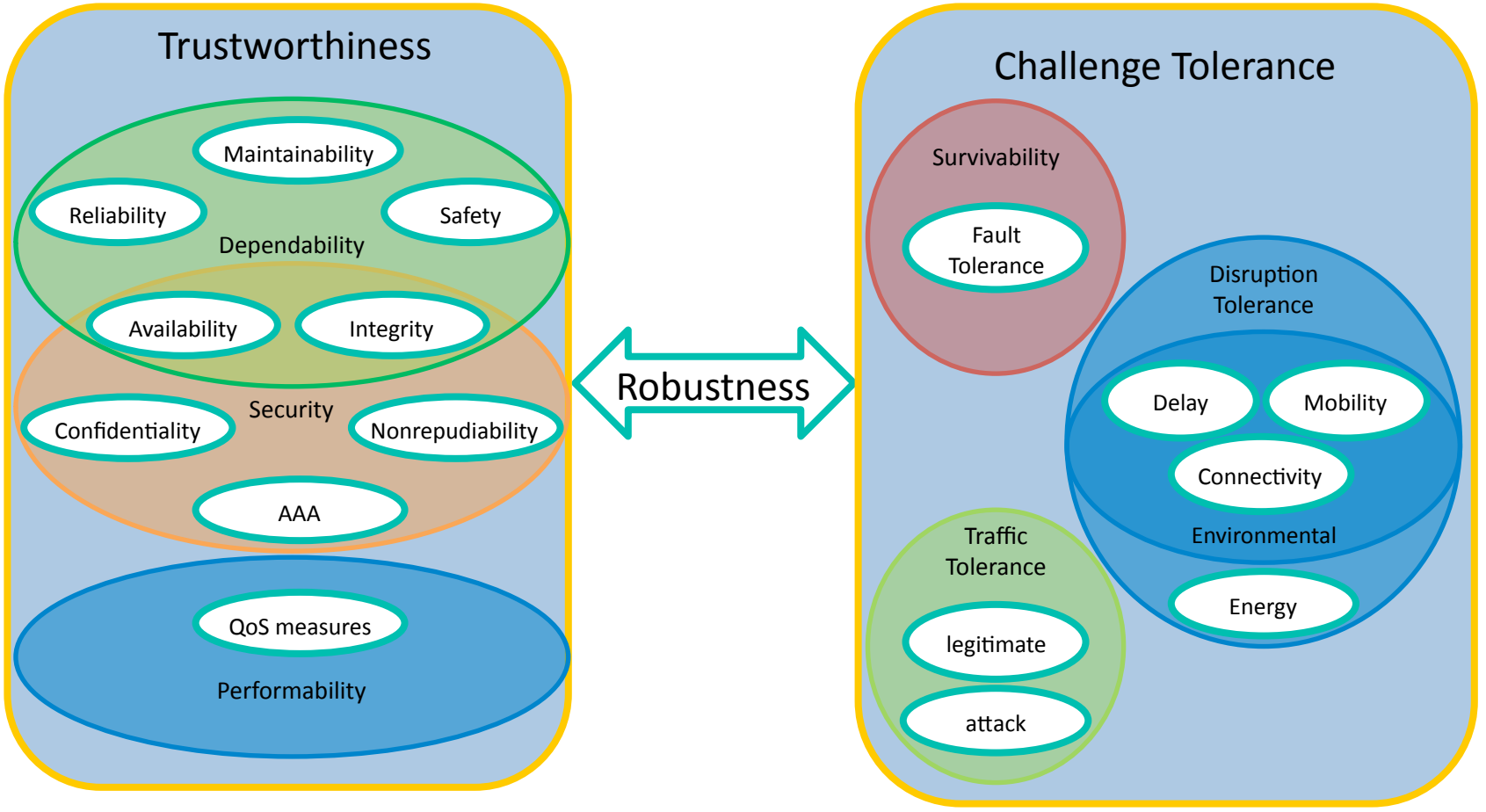
- Zwei Hauptkategorien der Widerstandsfähigkeit:
  - Trustworthiness: Messbare Eigenschaften bezgl. Widerstandsfähigkeit
  - Challenge Tolerance: Entwurfskriterien für Widerstandsfähigkeit
- Beziehung wird hergestellt durch Robustness
  - Systemperformanz im kritischen Zustand
  - Zuverlässigkeit eines beeinträchtigten Systems



Was ist Widerstandsfähigkeit? (3/3)

UNIVERSITÄT PASSAU
Fakultät für Mathematik und Informatik

Viele Unterdisziplinen subsumiert

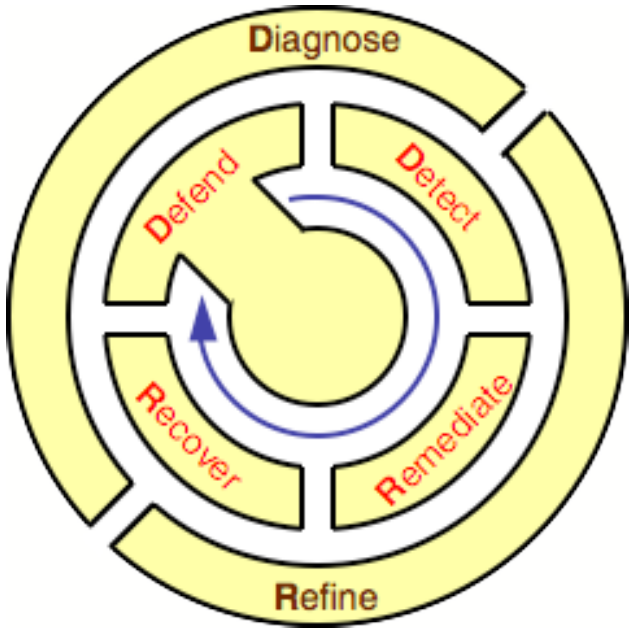


(1) Sterbenz et al. (2010)

Der ResumeNet Ansatz (1/2)

UNIVERSITÄT PASSAU
Fakultät für Mathematik und Informatik

- Widerstandsfähige Netzwerkarchitektur: **D^2R^2+DR**
- Zwei ineinandergeschachtelte Regelkreise
  - **"Defend, Detect, Remediate, Recover"**
    - Echtzeit-Regelkreis
    - Reagiert auf kurzfristige Änderungen im Netzwerk
  - **"Diagnose, Refine"**
    - Längerfristige Aktionen
    - Verbessert die langfristige Widerstandsfähigkeit des Netzwerks

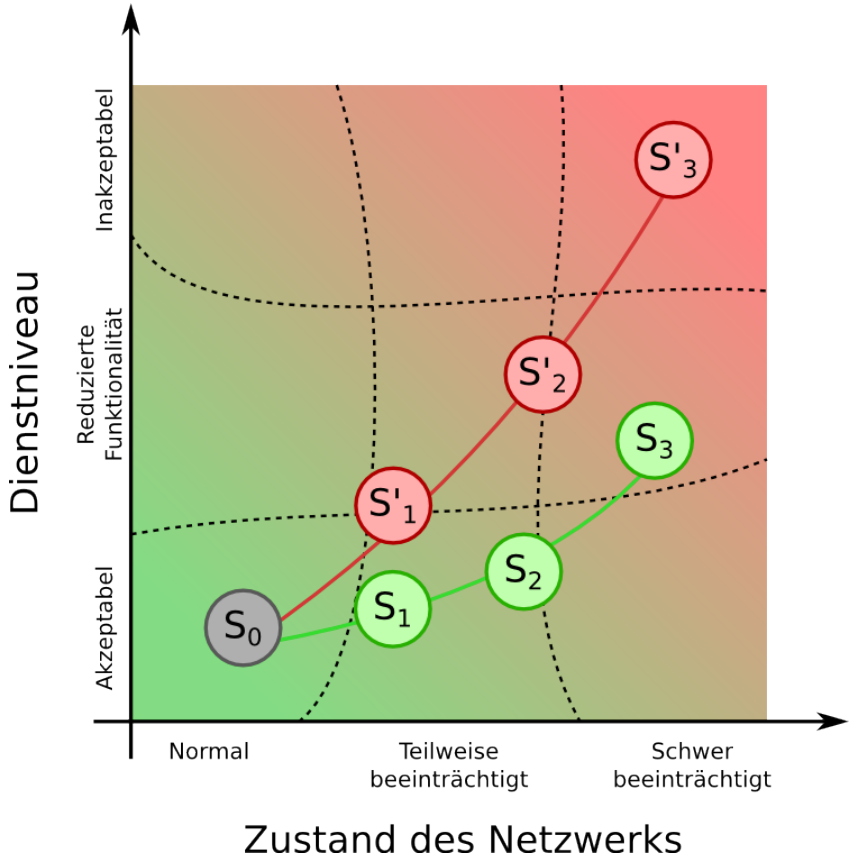


(2) Hutchison and Sterbenz (2009)

Der ResumeNet Ansatz (2/2)

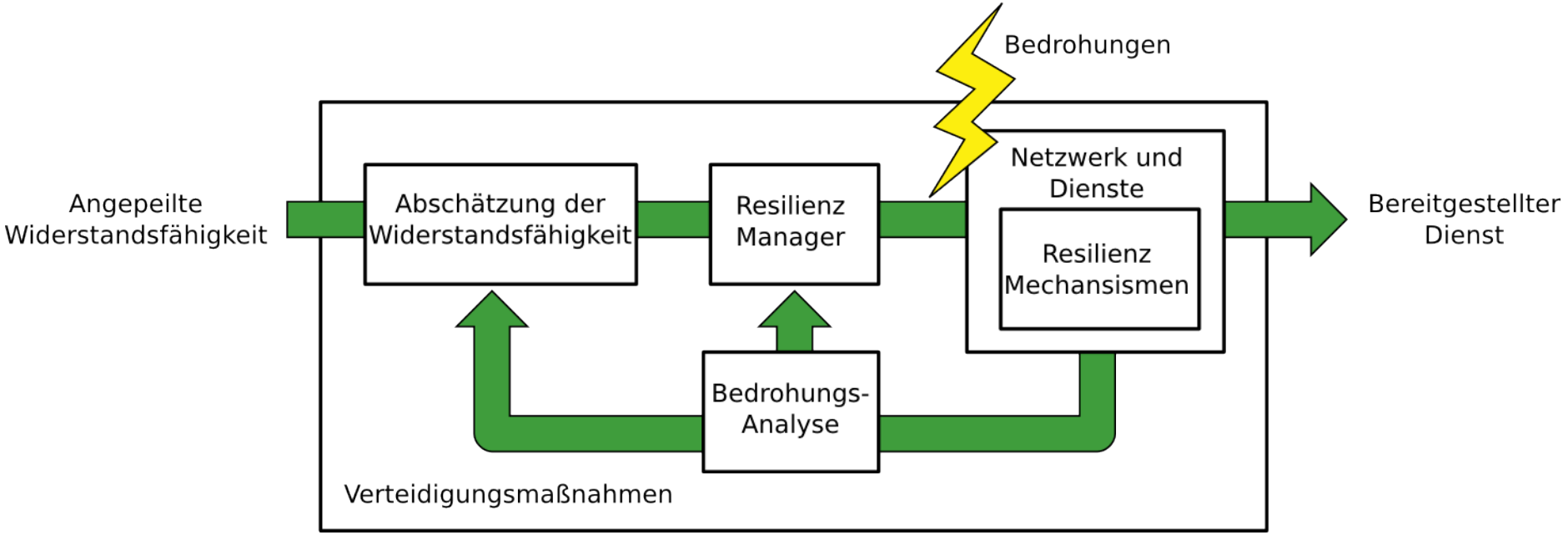
UNIVERSITÄT PASSAU
Fakultät für Mathematik und Informatik

- Widerstandsfähigkeit des Netzwerks und seiner Dienste
  - Zustand des Netzwerks
    - Normal
    - Teilweise beeinträchtigt
    - Schwer beeinträchtigt
  - Dienstniveau
    - Akzeptabel
    - Reduzierte Funktionalität
    - Inakzeptabel
  - Ziel
    - Dienstniveau im akzeptablen Bereich zu halten
    - Beeinträchtigung des Netzwerks tolerieren



(3) Smith et al. (2011)

Regelkreis für Widerstandsfähigkeit



- Anwendung des D^2R^2+DR Prinzips
  - Erwartete Widerstandsfähigkeit wird vorgegeben
  - Bedrohungsanalyse zeigt Gegenmaßnahmen auf
  - Durch Resilienz-Mechanismen kann der Dienst bereitgestellt werden

(3) Smith et al. (2011)

Offene Problemstellungen

UNIVERSITÄT PASSAU
Fakultät für Mathematik und Informatik

- Anwendung der HyRiM Konzepte
  - Wie können menschliche und organisatorische Probleme im Smart Grid vermieden werden?
  - Wie können Smart Grid Infrastrukturen räumlich gesichert werden?
  - Wie können die SCADA Systeme des Smart Grid abgesichert werden?
- Anwendung der ResumeNet Konzepte
  - Wie kann das Internet ein zuverlässiges Kommunikationsmedium für das Smart Grid werden?
  - Wie können Mechanismen der Widerstandsfähigkeit für Kommunikationsnetze auf das Smart Grid übertragen werden?

➔ Viele Fragen bleiben zu klären

Zusammenfassung

UNIVERSITÄT PASSAU
Fakultät für Mathematik und Informatik

- Zukünftige Szenarien noch nicht voll absehbar
  - Zunehmende Verflechtung von IT- und Versorgungsnetzen
  - Steigende Abhängigkeit zwischen Netzkomponenten problematisch
  - Unvollständige Analyse von Risiken und Bedrohungen
- Aktuell keine ausreichende Absicherung
  - Steuerungssysteme in Versorgungsnetzen nicht auf IT-Vernetzung ausgelegt
  - Keine ausgereifte Strategie im Falle eines Schwarzstarts

➔ Umfassende Risikoanalyse des Smart Grid

➔ Gemeinsame Absicherung von IT- und Energienetz notwendig

➔ Pläne für einen Schwarzstart des Smart Grid

Ausblick

UNIVERSITÄT PASSAU
Fakultät für Mathematik und Informatik

- Entwicklung eines dualen Ansatzes
  - Derzeitiges zentrales Stromnetz absichern
  - Dezentrale Lösungen ermöglichen und weiter ausbauen
- Aufbau einheitlicher Standards für Sicherheit und Zuverlässigkeit in Smart Grids
  - Interoperabilität für ein Netz von Netzen
  - Anwendung von Know-How aus dem Internet-Bereich
- Integration neuartiger Konzepte
  - Energiespeicher
  - Elektromobilität
  - Demand-Side Management (DSM)

Referenzen

(1) J.P.G. Sterbenz, D. Hutchison, E.G. Cetinkaya, A. Jabbar, J.P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in communication networks: strategies, principles, and survey of disciplines", Computer Networks, Special Issue on Resilient and Survivable Networks, Vol. 54, N° 8, June 2010, pp. 1245-1265

(2) D. Hutchison and J.P.G. Sterbenz, "ResiliNets: resilient and survivable networks", ERCIM News 77, April 2009

(3) P. Smith, D. Hutchison, J.P.G. Sterbenz, M. Schöller, A. Fessi, M. Karaliopoulos, C. Lac, and B. Plattner, "Network resilience: a systematic approach", IEEE Communications Magazine, Vol. 49, N° 7, 2011, pp. 88-97