Sichere IKT-Architektur im Smart Grid

Round Table

Thomas Bleier

Dipl.-Ing. MSc zPM CISSP CEH

Thematic Coordinator ICT Security

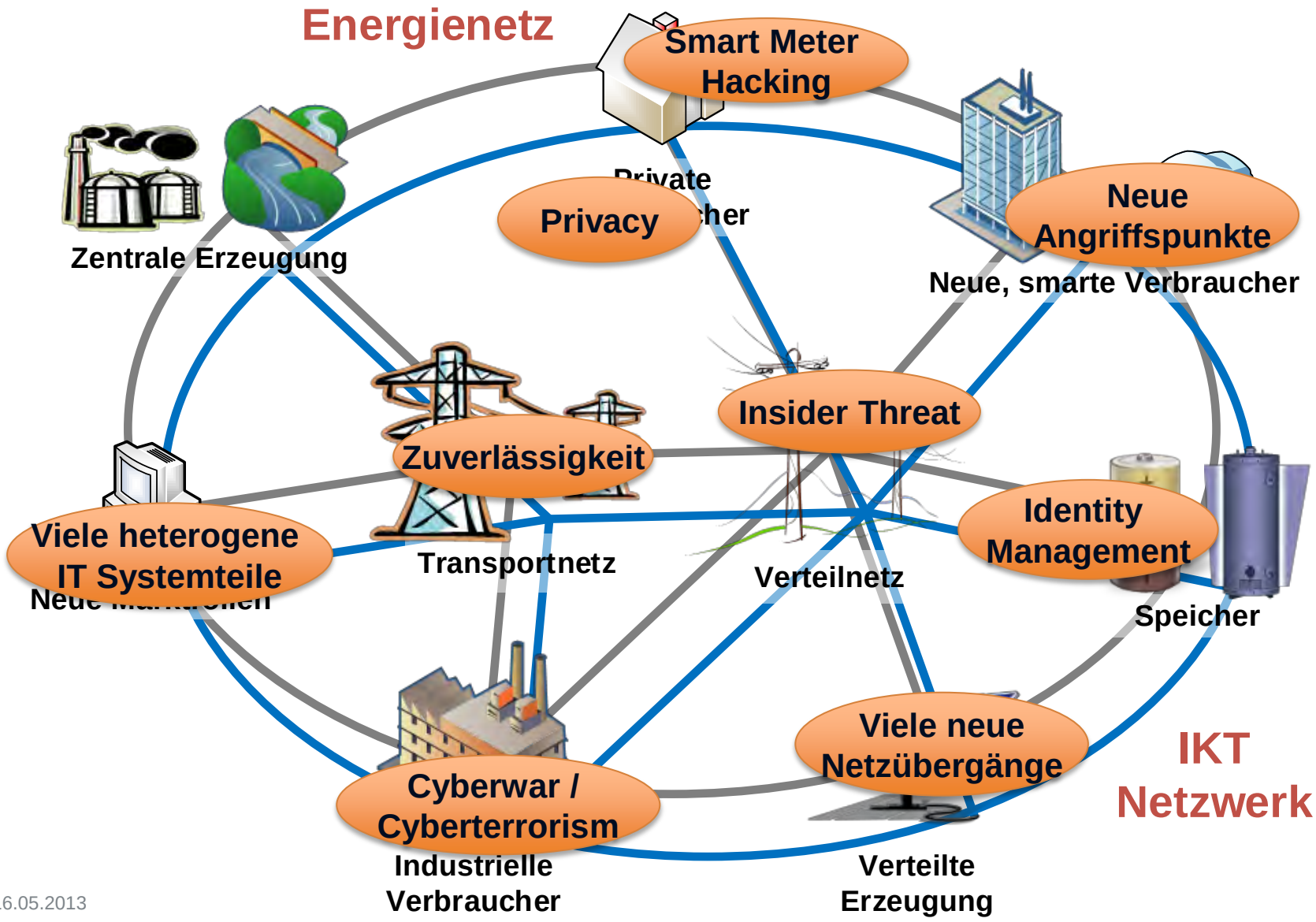
Safety & Security Department

AIT Austrian Institute of Technology GmbH

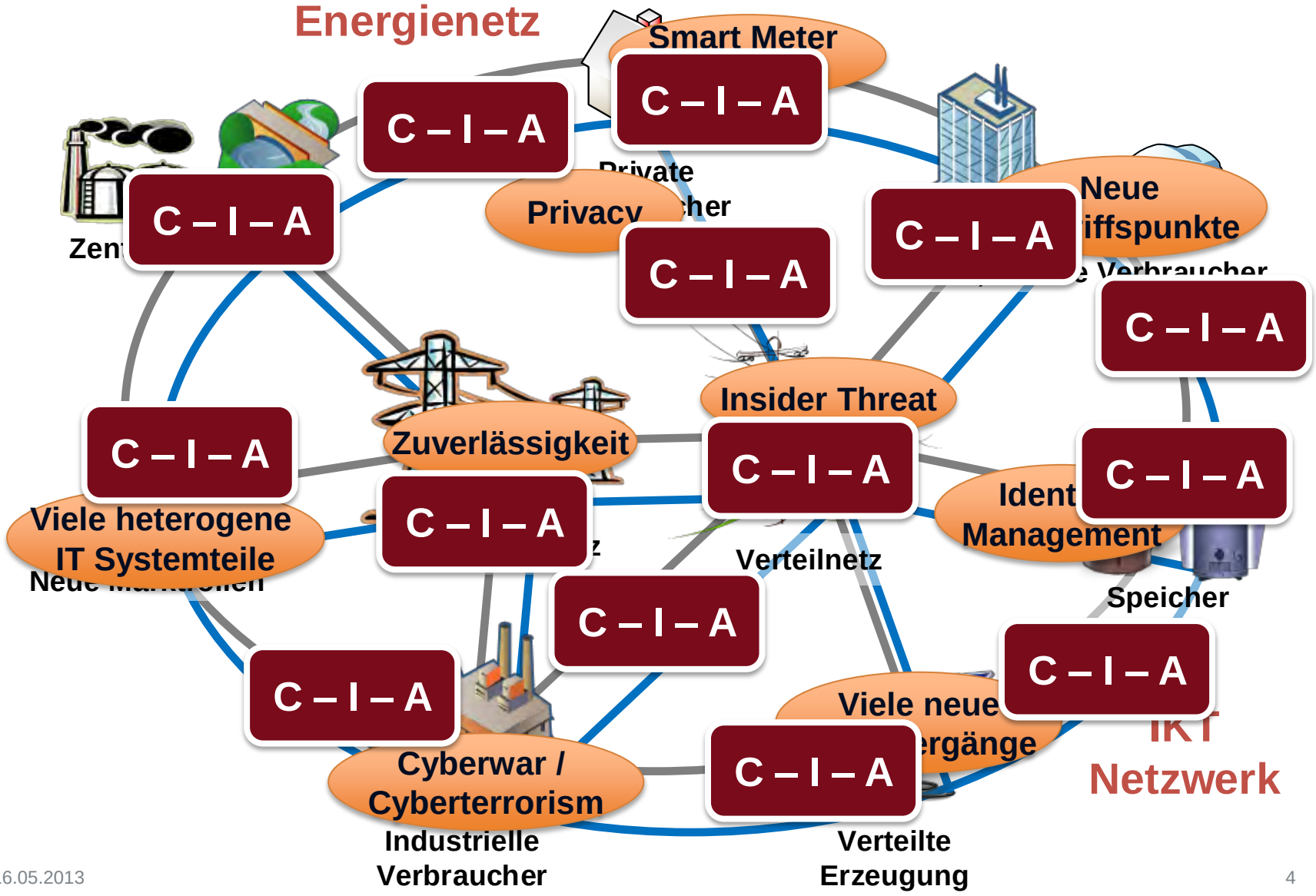
Agenda

- Kurzvortrag: Überblick über IKT-Sicherheitsthemen im Smart Grid
- Einleitungsstatements der Diskutanten
- Diskussion
- Zusammenfassung

Das sichere Smart Grid



Das sichere Smart Grid



Wissenschaftliche Darstellung

$$\forall\, x\ (x \in SmartGrid):$$

$$\lim_{n \to \infty} (C(x), I(x), A(x))$$

Confidentiality, Integrity, Availability

Soweit zur Theorie…

Praktische Problemstellungen:

- Unterschiedliche Rahmenbedingungen
- Unterschiedliche Sicherheitsniveaus
- Verschiedene Organisationen
- Wieviel Sicherheit braucht man?
- Komplexe interagierende Systeme

- Divide and Conquer – Aufteilung in Themenbereiche

IKT-Sicherheitsaspekte im Smart Grid

- Organisatorische Maßnahmen und Sicherheitsprozesse
- Sichere Entwicklung und Inbetriebnahme von Komponenten
- Sicherheit der Kommunikation
- Sicherheit des Betriebes
- Physische Sicherheit
- Behandlung von Sicherheitsvorfällen
- Wiederherstellung im Katastrophenfall

Angelehnt an existierende Standards und Guidelines wie ISO 27002, ENISA Appropriate security measures for Smart Grids, NIST Guidelines for Smart Grid Cyber Security, NERC CIP, IEC 62443, etc.

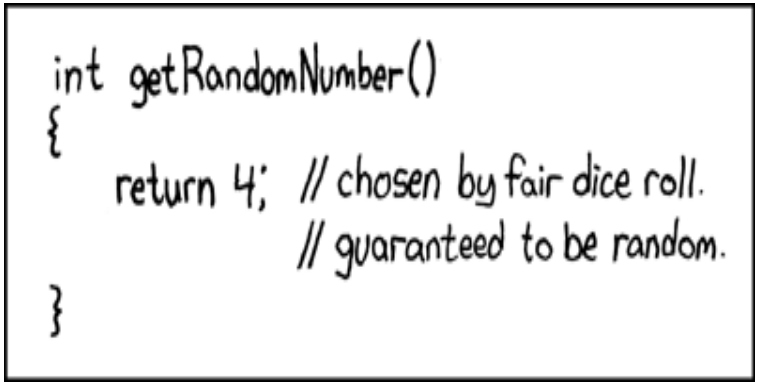
Organisatorische Maßnahmen und Sicherheitsprozesse

- Informationssicherheitsmanagement
  - ISO 2700x u. 27019, IEC 62443, BSI, NIST SP 800-53, 800-82, NERC CIP, BDEW Whitepaper, OE, etc.
- Risikomanagement
- Compliance und Zertifizierung
  - ISO 27001, NERC CIP bzw. spezifische – Verpflichtung?

- ISMS im Smart Grid:
  - Netzbetreiber, Kraftwerksbetreiber, Facility Management, etc
  - Private Haushalte?
  - Virtuelle Aggregatoren?
  - Komplexe Systeme?

Sichere Komponenten (Entwicklung, etc.)

- Secure Development Prozesse
  - NIST SDL, MS-SDL, ISSECO, etc.
  - Requirements, Threat Modelling, Codeanalyse, Penetrationstests, Incident Response Prozesse, etc.



- COTS vs. Industriekomponenten
- Bedrohungsszenarien und Vernetzung
- Functional Safety (IEC 61508) vs. IT Security (ISO/IEC 15408 Common Criteria)
- Kryptographie – Lebenszyklus, Low Power
- Tests und Zertifizierung
  - BSI Smart Meter Schutzprofil
- Supply Chain Management

Sichere Kommunikation

- Protokolle aus der Automatisierung/Energiewelt
  - IEC 61850, IEC 60870, DNP3, etc.
- vs. Protokolle aus der Business-IT
  - HTTP, SOAP, REST, etc.
- Security-Erweiterungen
  - SSL/TLS, IEC 62351, IPsec, SAML, XACML, etc.
- Verfügbarket vs. Verwendung in der Praxis
- Designziele der Protokolle vs. Anwendungsszenario
- Privacy-Anforderungen
- Sicherheit von Ad-Hoc Kommunikation (E-Mail)

Sicherer Betrieb

- Komplexität - Systemverständnis des Betriebspersonals
- Vulnerability Management, Patch Management
  - Konfigurationsmanagement
- User Awareness
  - Social Networks, Consumerization, etc.
- Dienstleister, Zuständigkeiten
- Zugriffskontrolle, AAA
- Auditing und Logging
- Separation of Duties, Least Privilege

Physische Sicherheit

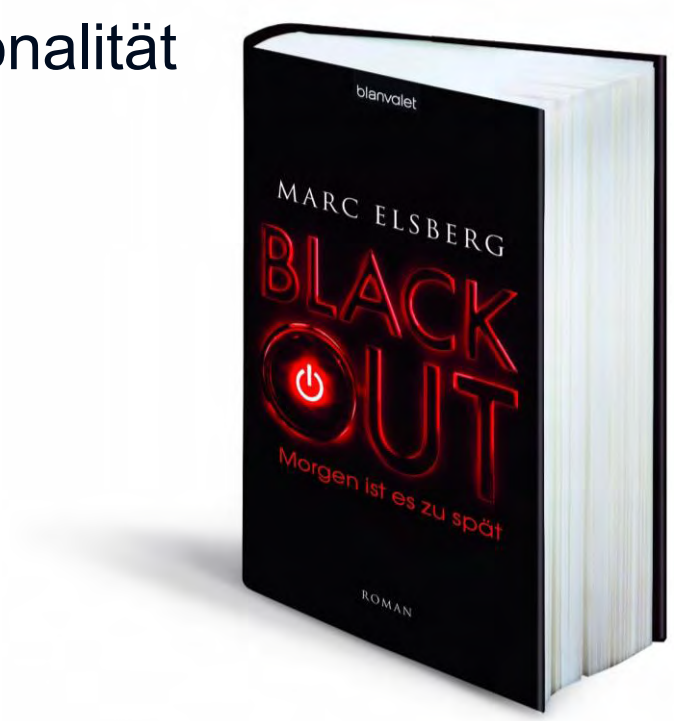
- Sicherheitszonen
  - Ausweitung der Infrastruktur
  - Neue Konzepte notwendig
  - Smart Meter, E-Mobility, etc.
- Sicherheit bei physischem Zugriff ist schwierig:
  - DVD
  - Spielekonsolen
  - Pay-TV
  - Chiptuning
  - Mobiltelefone
  - etc.
- Resilienz

Behandlung von Sicherheitsvorfällen

- Reaktion auf Sicherheitsvorfälle
- Logging, Monitoring
- Situational Awareness
- Incident Management
- Informationsaustausch
- Informationskultur – Verbesserungswille
- Meldepflicht?
- Preventive vs. Detective Bedrohungslage

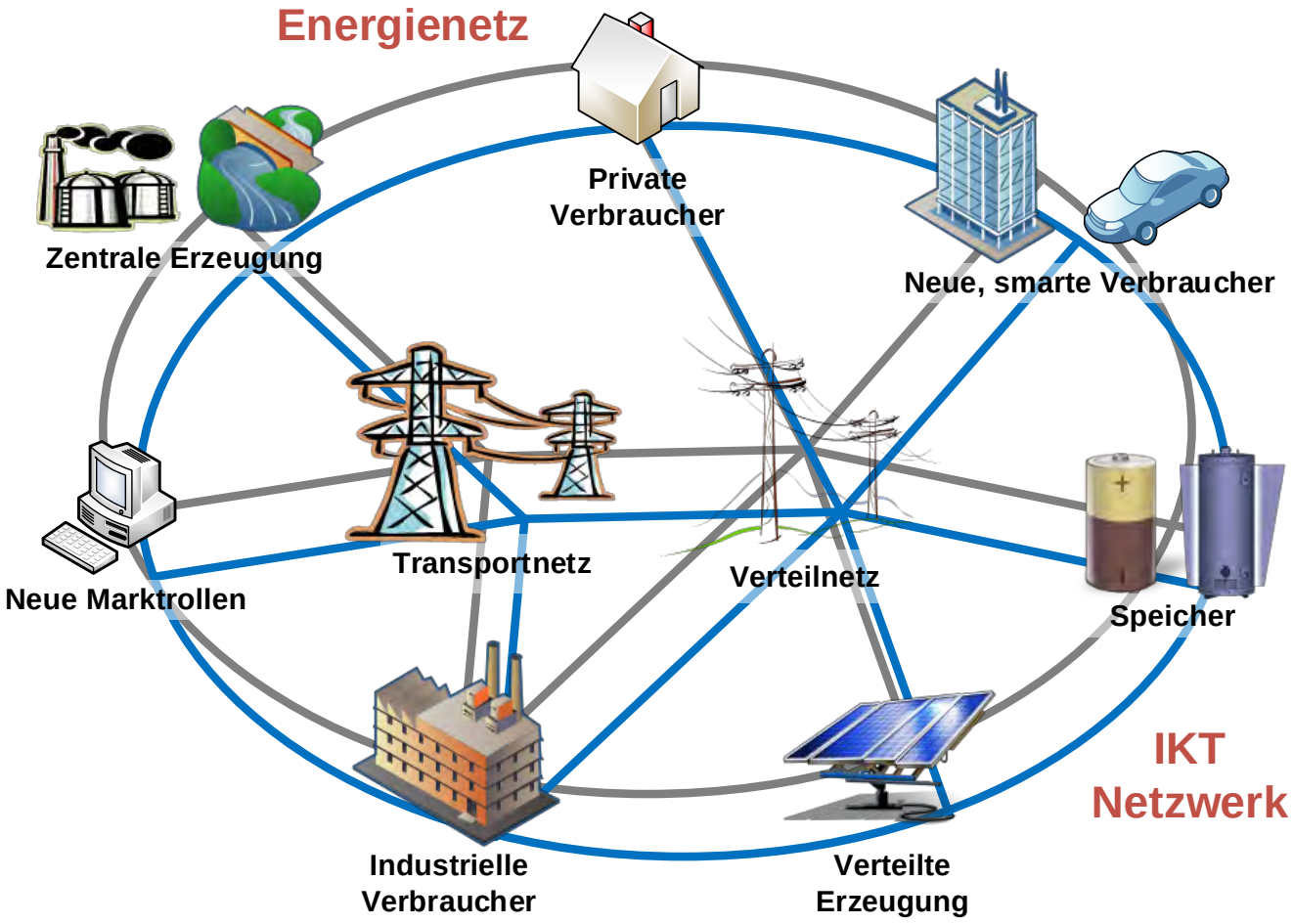
Wiederherstellung im Katastrophenfall

- Business Continuity
- Schwarzstartfähigkeit im Smart Grid
- Inselbetrieb?
- „Notbetrieb“ mit reduzierter Funktionalität
- Kommunikation im Krisenfall



Aufgabenteilung, Verantwortlichkeiten

- Wer ist zuständig für welche Sicherheitsaspekte?



Security als Innovationsmotor

Smart Grid ist der nächste große
Innovationsschritt im Energiesystem.

Adäquate Sicherheit ist Voraussetzung und
Enabler damit neue Technologien angenommen
und eingesetzt werden!

Erste Schritte sind gemacht,
aber ein weiter Weg liegt noch vor uns

Fragen?

Thomas Bleier
Dipl.-Ing. MSc zPM CISSP CEH
Thematic Coordinator ICT Security
Research Area Future Networks and Services
Safety & Security Department

thomas.bleier@ait.ac.at | +43 664 8251279 | www.ait.ac.at/it-security

Diskussionsrunde

- **Dominik Engel**
  Josef Ressel Zentrum Smart Grid Privacy & Security Salzburg
- **Stephan Flake**
  OFFIS e.V.
- **Markus Berger**
  Salzburg AG
- **Brian Korittnig**
  Energie Steiermark AG, Österreich
- **Richard Link**
  Siemens AG
- **Po-Wen Liu**
  RTR GmbH
- **Markus Robin**
  SEC Consult GmbH