AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

(SG)² Smart Grid Security Guidance

Smart Grid Security Guidance

Architekturmodelle und Sicherheitsmaßnahmen für Smart Grids in Österreich

Dr. Lucie Langer
AIT Austrian Institute of Technology

AIT Austrian Institute of Technology • Technische Universität Wien • Energieinstitut an der JKU Linz
SECConsult Unternehmensberatung • Siemens AG • Linz Strom
Energie AG Oberösterreich • IKB Innsbrucker Kommunalbetriebe
Bundesministerium für Landesverteidigung und Sport • Bundesministerium für Inneres

bmvit Bundesministerium für Verkehr, Innovation und Technologie

KIRAS Sicherheitsforschung

FFG

Elektrische Energieinfrastruktur der Zukunft

- **Smart Grids** sind Stromnetze, welche durch ein abgestimmtes Management mittels zeitnaher und bidirektionaler Kommunikation zwischen Netzkomponenten, Erzeugern, Speichern und Verbrauchern einen energie- und kosteneffizienten Systembetrieb für zukünftige Anforderungen unterstützen

Aus Sicherheitssicht kritischer Punkt:
Aufbau eines IKT Netzes
parallel zum und mit enger Kopplung an
das Energienetz

Herausforderungen

- Energieversorger werden in Zukunft Ihre Netze zu Smart Grids umbauen

- Viele Sicherheitsfragen in diesen zukünftigen Netzen sind noch ungeklärt
  - Welche Auswirkungen haben die neuen IT-Komponenten auf die Sicherheit?
  - Welche neuen Angriffsszenarien (und Risiken) ergeben sich dadurch?
  - Erste Lösungsansätze existieren weltweit – wie können diese in Österreich umgesetzt werden?
  - Wie sieht es mit der Sicherheit der in den ersten Pilotprojekten verwendeten Komponenten aus, und wo muss diese noch verbessert werden?

Projektziele Smart Grid Security Guidance

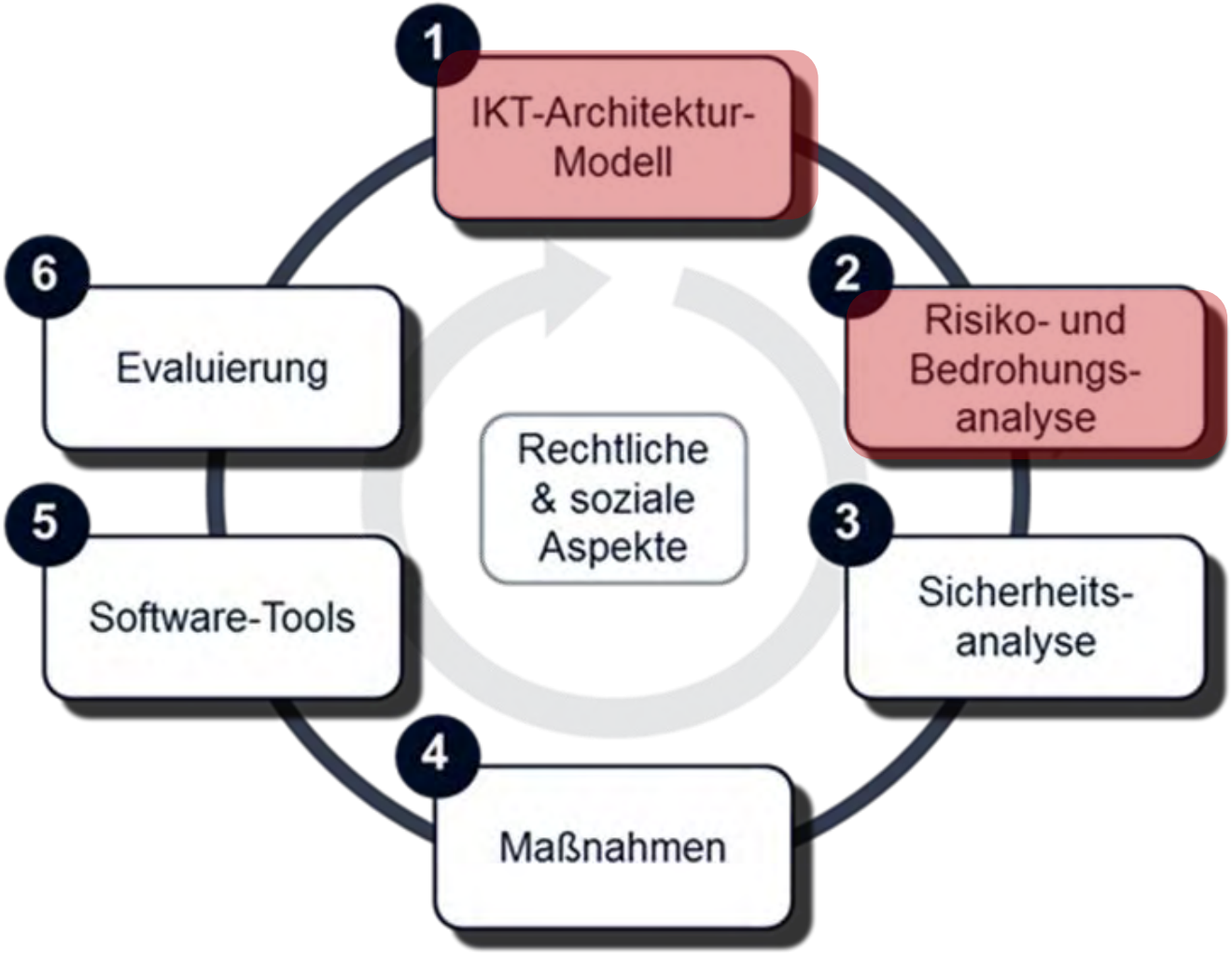
- Systematische Erforschung der Sicherheitsaspekte von Smart-Grid-Technologien
  - aufbauend auf existierenden Ansätzen und Ergebnissen
  - unter Berücksichtigung der spezifischen nationalen Gegebenheiten in Österreich

- Erarbeitung von Sicherheitsmaßnahmen für österreichische Energienetzbetreiber
  - Absicherung zukünftiger Energienetze gegenüber IKT-basierten Bedrohungen

Eckdaten (SG)²

- Nationales Forschungsprojekt im Förderprogramm KIRAS (PL 2.4)
- Laufzeit: 2 Jahre (11/2012 – 10/2014)
- Budget: 1,2 Mio. EUR
- Projektpartner:

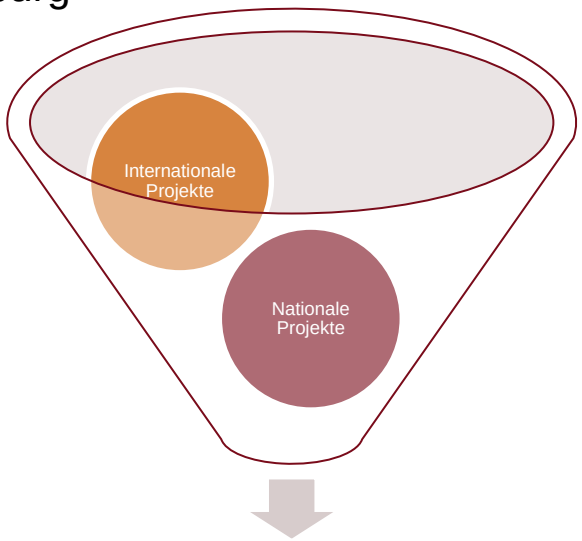
Forschungsthemen & Vorgehensmodell



Definition geeigneter Architekturmodelle (1/3)

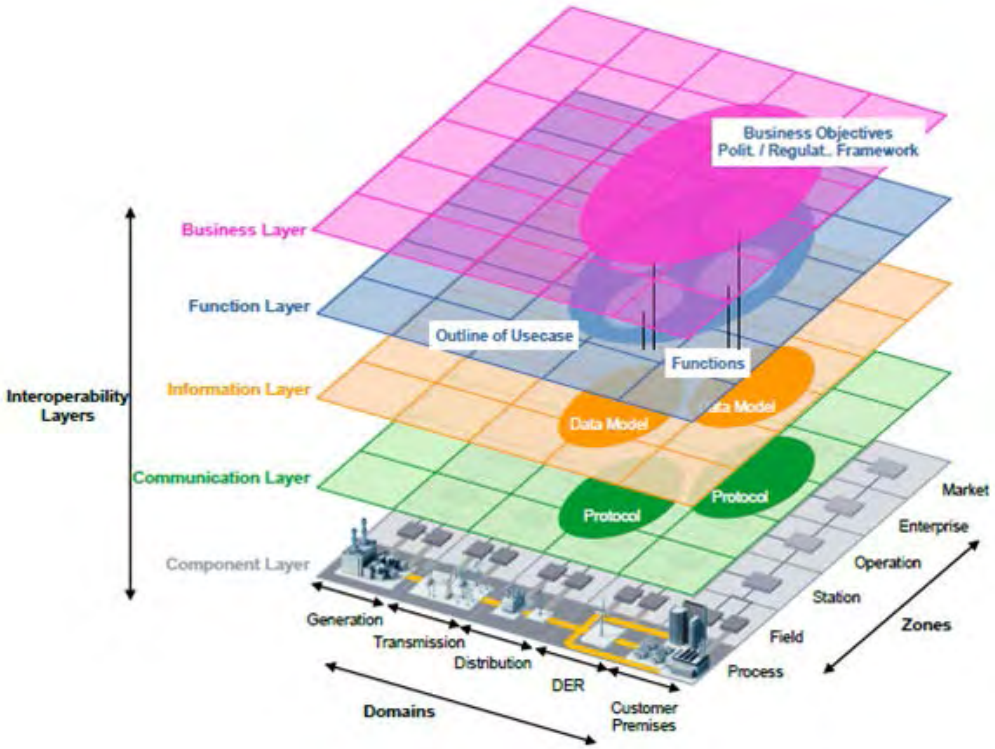
- Analyse relevanter Pilotprojekte
  - IEM: Intelligent Energy Management
  - Smart Web Grid
  - DG DemoNetz Smart LV Grid
  - DG DemoNetz Validierung
  - ZUQDE: Zentrale Spannungs- und Blindleistungsregelung mit dezentralen Einspeisungen in der Demoregion Salzburg
  - EMPORA: E-Mobile Power Austria
  - AMIS Smart Metering Rollout

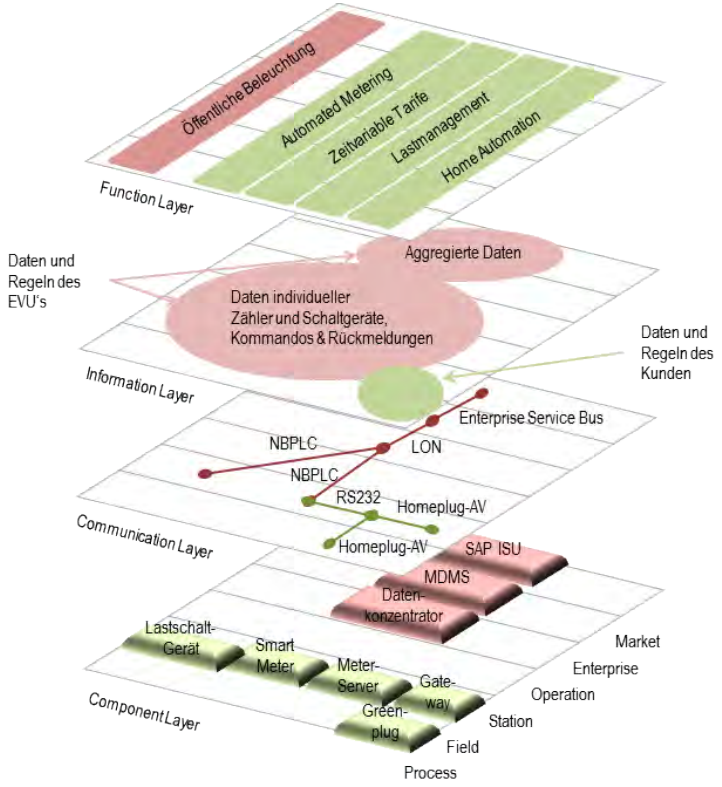
  - OpenNode (EU FP7)
  - EcoGrid EU (EU FP7)
  - OGEMA (DE)
  - Demand Response Automation Server (USA)



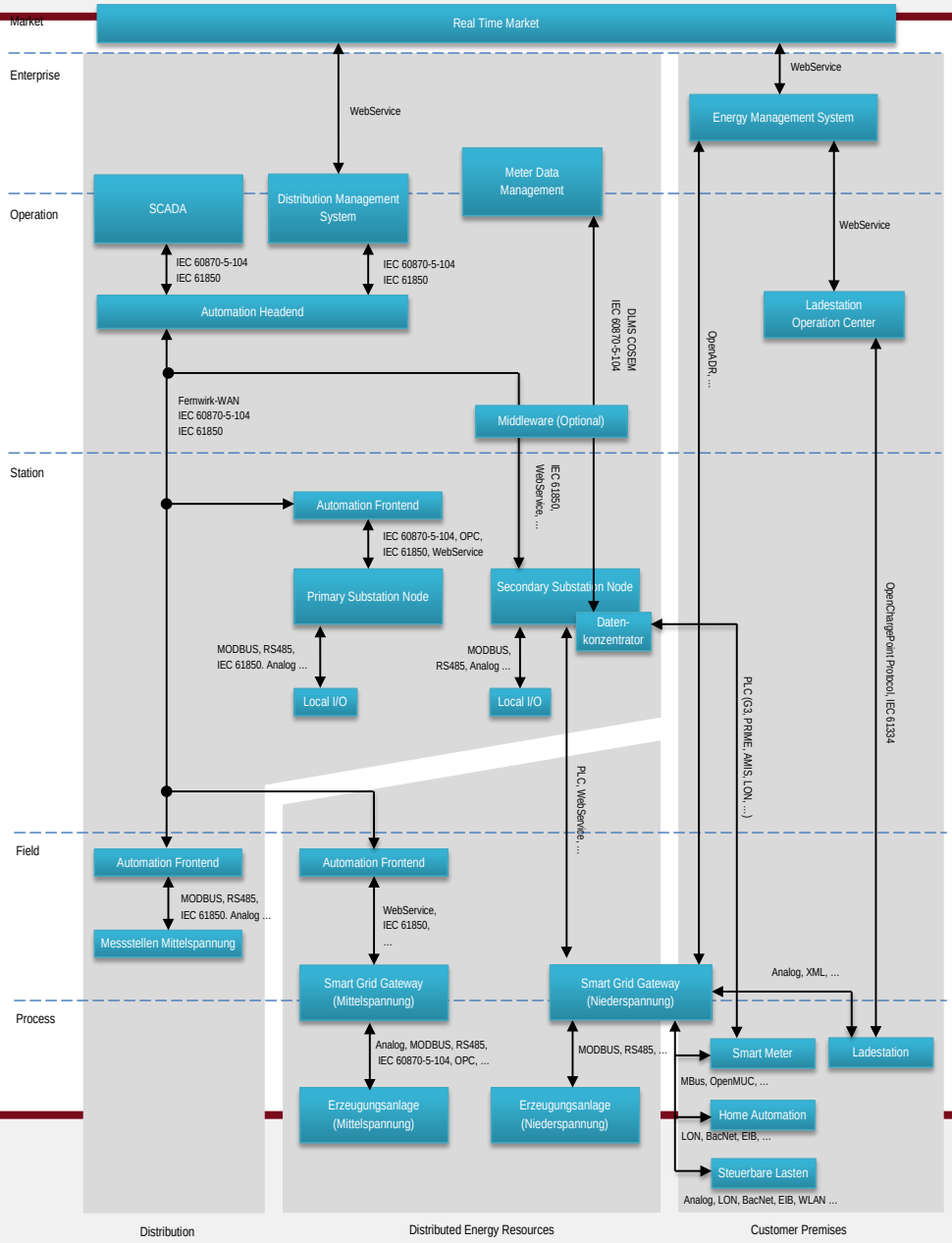
Definition geeigneter Architekturmodelle (2/3)

- Abbildung der Projektarchitekturen auf SGAM





Definition geeigneter Architekturmodelle (3/3)



Bedrohungs- und Risikokatalog (1/3)

- Definition eines Katalogs möglicher Bedrohungen und Risiken im Smart Grid
  - Basis: IT-Grundschutz-Kataloge und Smart Metering Schutzprofile
  - Fokus auf IKT-Aspekte & technische Bedrohungen
- Aus anfangs über 500 Bedrohungen ca. 260 Bedrohungen zur Weiterbetrachtung identifiziert
- Inhaltliche Zusammenfassung ergab **48 Bedrohungen** für den Bedrohungskatalog

Bedrohungs- und Risikokatalog (2/3)

- Authentifikation / Autorisierung
- Kryptographie / Vertraulichkeit
- Fehlende / falsche Sicherheitsmechanismen
- Interne / externe Schnittstellen
- Wartung / Instandhaltung / Systemzustand
- Integrität / Verfügbarkeit
  - Ausfall von IT-Systemen oder Netzwerken
  - Ausfall interner Versorgungsnetze
  - Datenverlust oder -verfälschung durch physische Eingriffe
  - Datenverlust oder -verfälschung durch Fehlbedienung oder SW-Probleme
  - Physische (fahrlässige oder mutwillige) Zerstörung von Geräten
  - Logische (fahrlässige oder mutwillige) Zerstörung von Daten
  - Gebührenbetrug

Bedrohungs- und Risikokatalog (3/3)

- Definition des Wirkungsbereichs jeder Bedrohung gemäß Architekturmodell aus AP1
- Definition von Kategorien für Auswirkungen und Wahrscheinlichkeit
- Bewerten der Architekturkomponenten im Hinblick auf die Bedrohungen
  - Welche Bedrohungen treffen potentiell zu?
  - Wie hoch ist die Wahrscheinlichkeit dafür, welche Auswirkungen kann es geben?
- Fragebogen für Feedback der Netzbetreiber

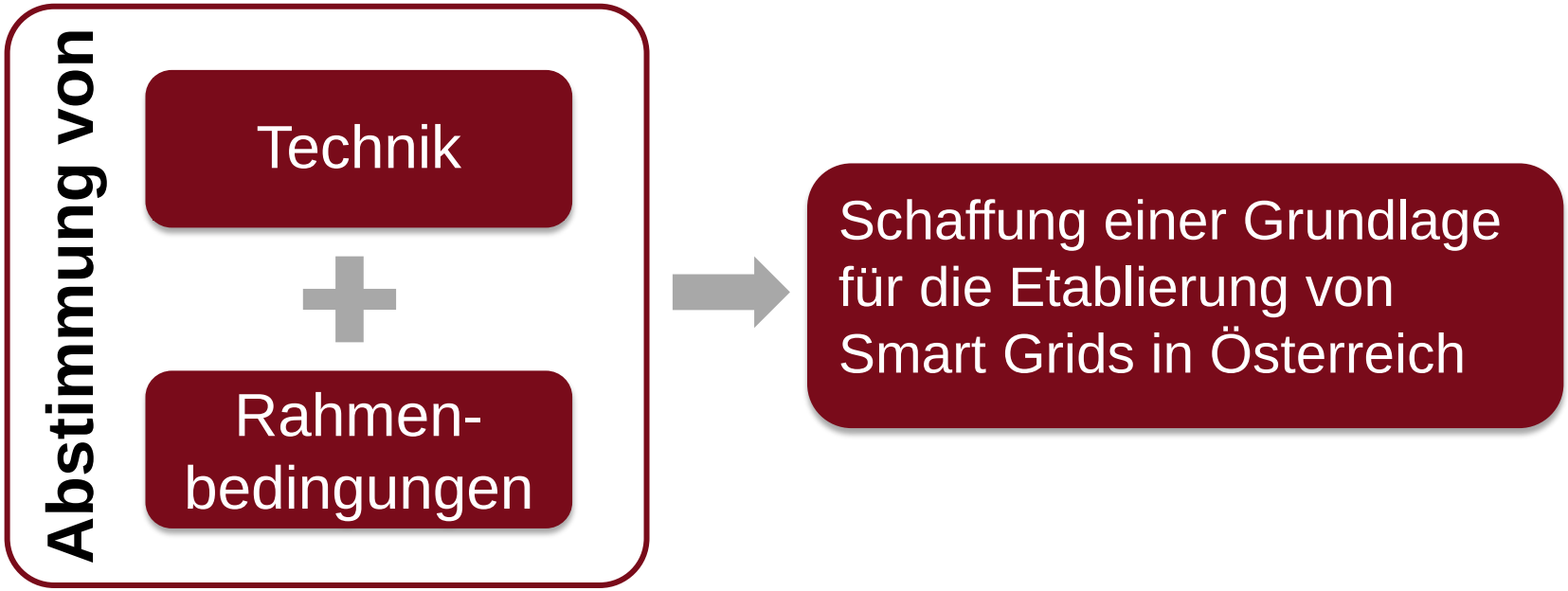
$(SG)^2$ vs. RASSA

- Schwerpunkt von $(SG)^2$ liegt auf Sicherheitsmaßnahmen für Verteilnetzbetreiber, Zeithorizont kurz- bis mittelfristig
- abgestimmtes Gesamtkonzept für die Zukunft sicherer Smart Grids in Österreich fehlt
- **eine gemeinsame** Referenzarchitektur für **Österreich** nötig
  - Welche speziellen Rahmenbedingungen gibt es in Österreich?
  - Wie leitet man eine konkrete Architektur ab?
  - Wie gelangt man vom Status quo dorthin (Migrationspfad)?

Reference Architecture for Secure Smart Grids in Austria (RASSA)

- Entwicklung einer Referenzarchitektur für sichere Smart Grids in Österreich
  - abgeleitet von bzw. kompatibel zu bestehenden Arbeiten wie z.B. M/490, NIST, BSI, etc.
  - Abgleich mit der internationalen, europäischen Ebene (D-A-CH, EU) und darüber hinaus
  - unter Einbeziehung sämtlicher relevanter Stakeholder in AT
- Entwicklung eines Migrationspfades ausgehend vom aktuellen Stand
- Entwicklung von Guidelines für konkrete Umsetzung
- Schaffung einer Standardisierungsgrundlage

Reference Architecture for Secure Smart Grids in Austria (RASSA)



RASSA Methodik

- Top-Down-Ansatz:
  breite Analyse bestehender Standards, Drafts, Publikationen
  - Smart-Grid-Referenzarchitekturen
  - Security, Smart Grid Security
  - nationale und internationale Forschungsprojekte / Pilotversuche
- ganzheitlich: IKT *und* Energie
- durchgängige Betrachtung von Sicherheits- und Privatsphäre-Aspekten (*Security by Design*, *Privacy by Design*)
- Stakeholderprozess

AIT Austrian Institute of Technology

your ingenious partner

Dr. Lucie Langer
Scientist
Research Area Future Networks and Services
Safety & Security Department

lucie.langer@ait.ac.at | +43 664 8251 438 | www.ait.ac.at/ict-security