Initiativen für sichere Smart Grids in Österreich und Europa

Thomas Bleier
Dipl.-Ing. MSc zPM CISSP CEH
Thematic Coordinator ICT Security
Safety & Security Department
AIT Austrian Institute of Technology GmbH

IKT-Sicherheitsthemen im Smart Grid

- Organisatorische Maßnahmen & Prozesse
  - ISMS, Risikomanagement, Audit
- Sichere Entwicklung von Komponenten
  - Security by Design, Secure Development Lifecycle, Tests, Zertifizierungen
- Sichere Inbetriebnahme & Betrieb
  - Security by Default, Trainings, Wartung, Patch Management, etc.
- Sichere Kommunikation
  - Paradigmenwechsel: inhärente Sicherheit statt Isolation
- Physische Sicherheit
  - Monitoring, Überwachung, Resilienz
- Behandlung von Sicherheitsvorfällen
  - Erkennung von Vorfällen, Informationsaustausch, angemessene Reaktion
- Wiederherstellung im Katastrophenfall
  - Wiederanlauf, Business Continuity, etc.

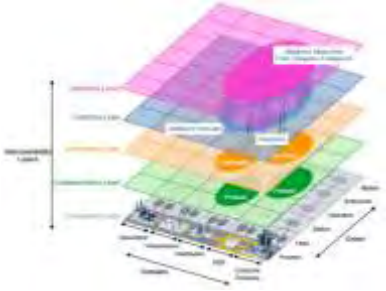
Standardisierung im Bereich SG Security

- Organisatorische Maßnahmen & Prozesse
  - ISO 27001/27005/27019, IEC 62443, NISTIR 7628, etc.
- Sichere Entwicklung von Komponenten
  - BSI Schutzprofile / Common Criteria, IEC 62443
- Sichere Inbetriebnahme & Betrieb
  - ? (IEC 62443)
- Sichere Kommunikation
  - IEC 62351, etc.
- Physische Sicherheit
  - Diverse – aber (Smart) Grid spezifisch?
- Behandlung von Sicherheitsvorfällen
  - ISO 27035, ISO 27010, etc.
- Wiederherstellung im Katastrophenfall
  - ISO 22301

(SG)² - Smart Grid Security Guidance

- Nationales Forschungsprojekt im Förderprogramm KIRAS (PL 2.4)
- Laufzeit: 2 Jahre (11/2012 – 10/2014)
- Budget: 1,2 Mio. EUR
- Projektpartner:
  - AIT Austrian Institute of Technology (Koordinator)
  - Technische Universität Wien
  - SECConsult Unternehmensberatung GmbH
  - Siemens AG, Corporate Technology
  - LINZ AG
  - Energie AG
  - Innsbrucker Kommunalbetriebe AG
  - Energieinstitut an der JKU Linz GmbH
  - Bundesministerium für Inneres
  - Bundesministerium für Landesverteidigung

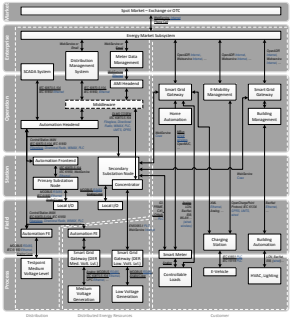
SG2 - Ansatz und Status

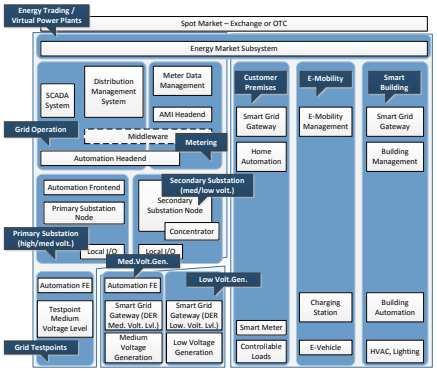


Bedrohungskatalog & Risiko-Assessment

Security Architektur Empfehlungen

Auswahl der Systemteile Aufgrund des Risikos





Nationales Referenzmodell

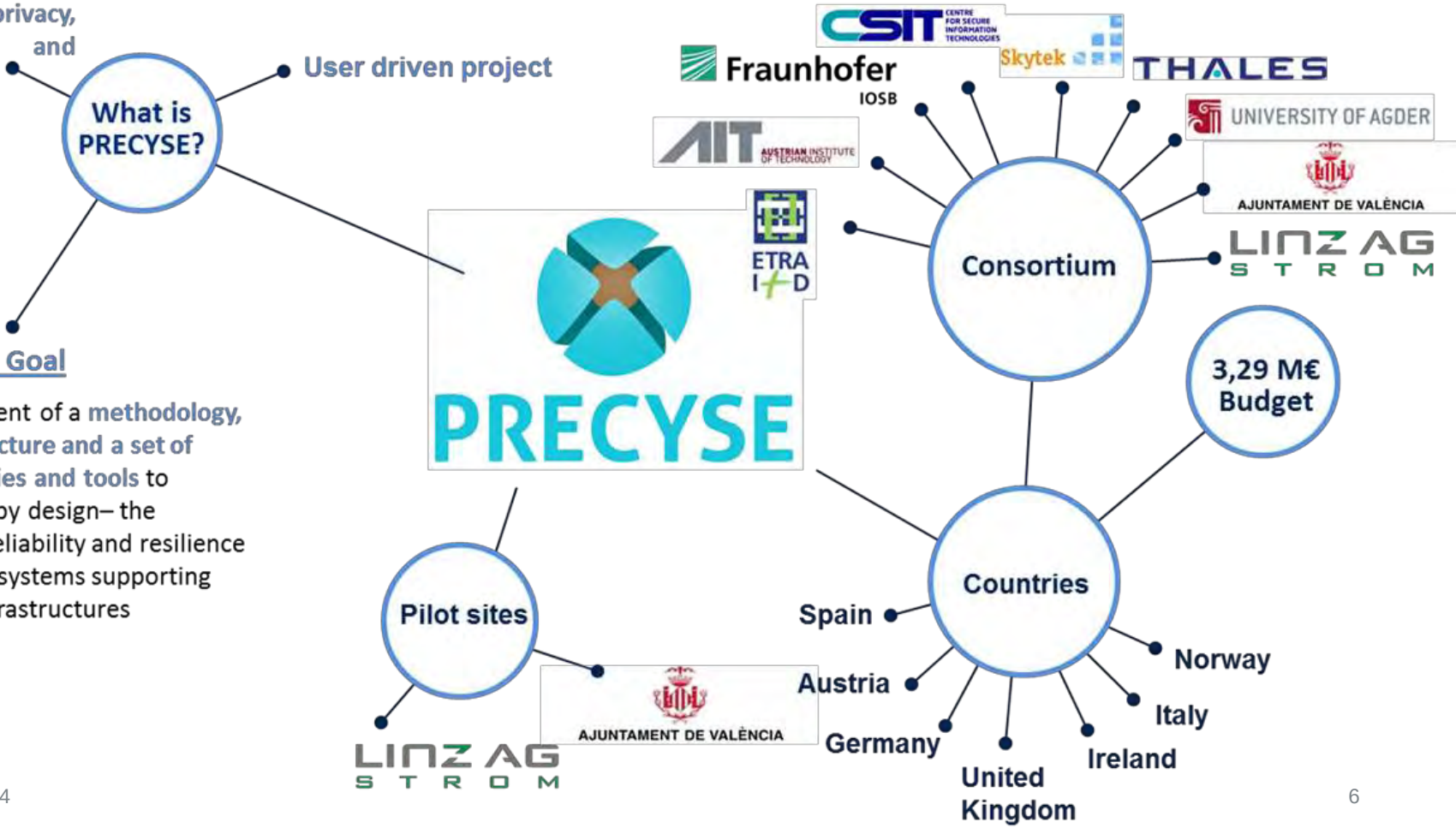
Security Implementierungs Empfehlungen

Verwundbarkeiten in konkreten Systemen

Penetrationstests: Risikowahrscheinlichkeit & Auswirkungen

Projekt “PRECYSE” – Prevention, protection and reaction to Cyber Attacks to Critical Infrastructures

Building on **previous research** and **existing standards**, and paying attention to **relevant privacy, policy, legal and ethical issues.**



Strategic Goal

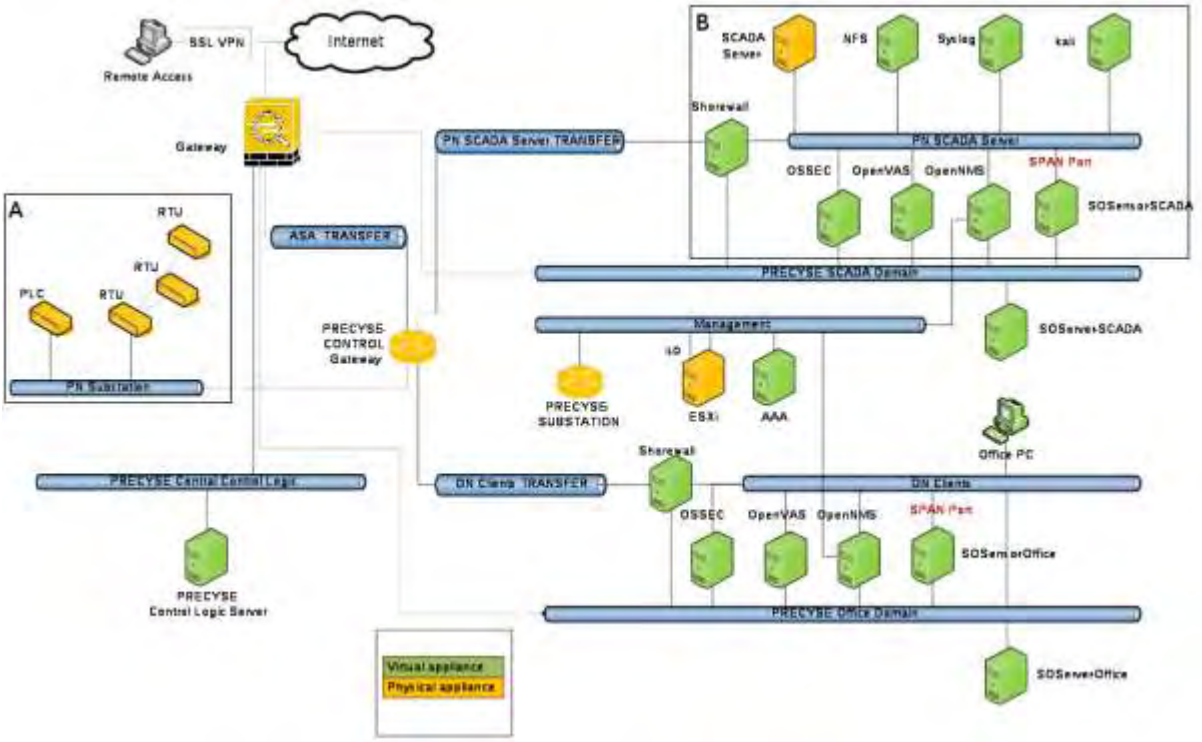
Development of a **methodology, an architecture and a set of technologies and tools** to improve –by design– the security, reliability and resilience of the ICT systems supporting Critical Infrastructures

PRECYSE - Schwerpunkte

- Risiko Assessment für SCADA Systeme
- Sichere Architekturen für SCADA Systeme
- Intrusion Detection und Anomalieerkennung in SCADA Netzwerken

Prevention, protection and REaction to CYber attackS to critical infrastructurEs

PRECYSE



SPARKS – SmartGrid protection against Cyber Attacks

Duration:
April 2014 – March 2017

Budget:
EUR 5 Mio.

sparks
SMART GRID PROTECTION AGAINST CYBER ATTACKS

Consortium

- AIT Austrian Institute of Technology
- Fraunhofer AISEC
- The Queen's University Belfast
- Royal Institute of Technology (KTH)
- Landis + Gyr
- Energy Institute at the J. Kepler University Linz
- EMC RSA
- United Technologies Research Centre
- SWW Wunsiedel GmbH

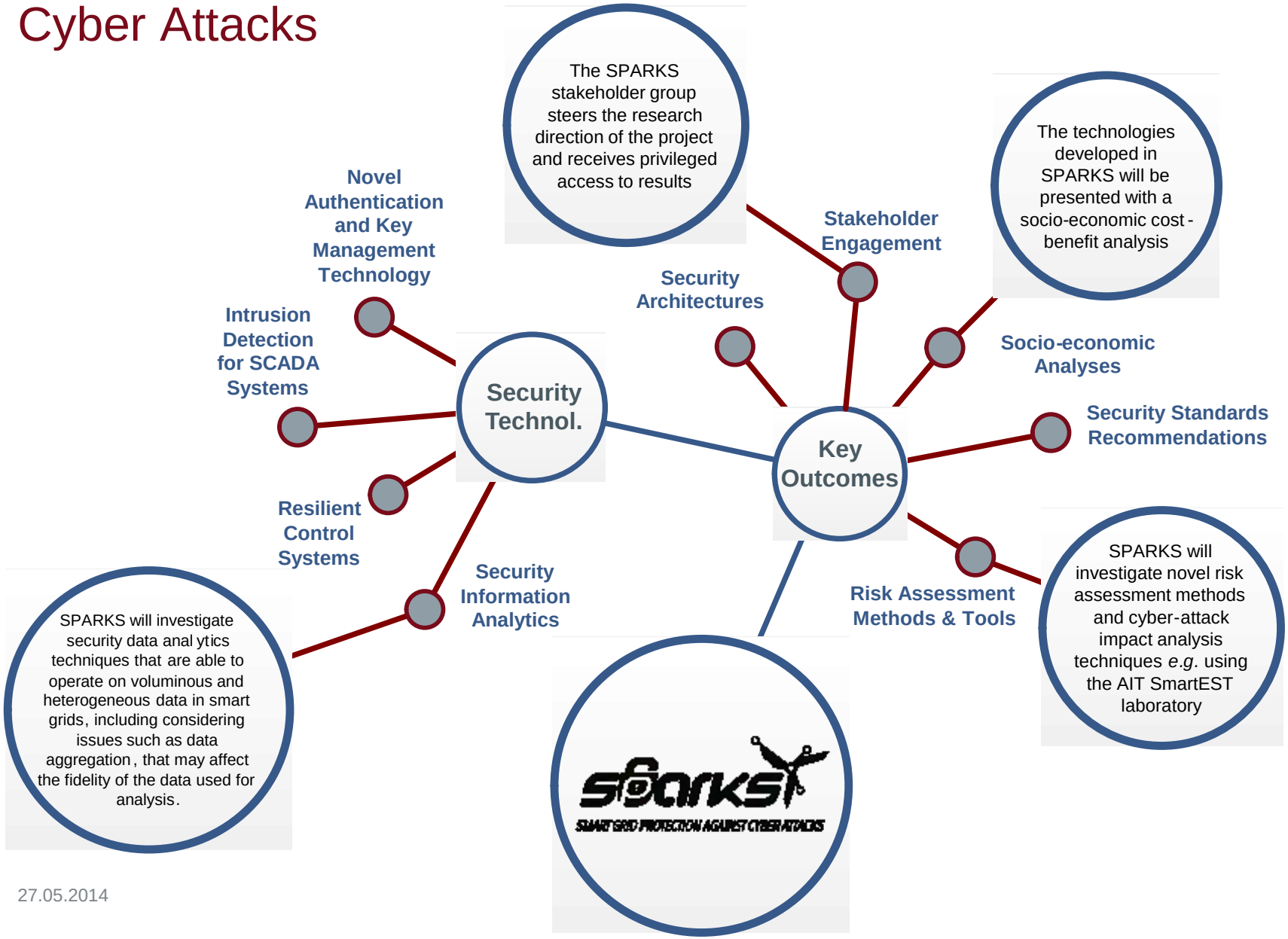
Demonstration Sites

- AIT SmartEST Laboratory

- Nimbus Microgrid

- SWW Wunsiedel Smart Grid

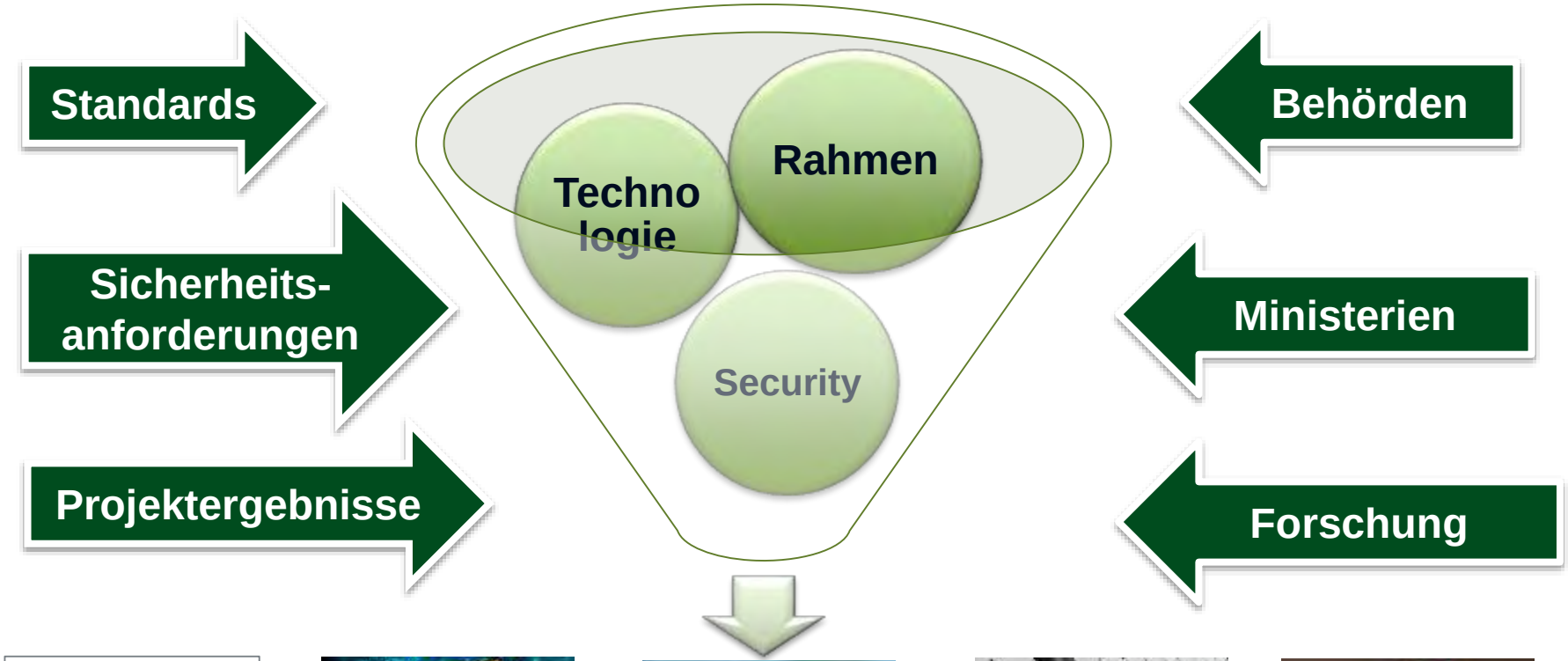
SPARKS – SmartGrid protection against Cyber Attacks



The SPARKS Stakeholder Group

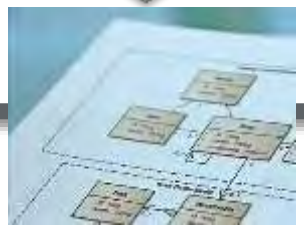
- Currently more than **30** organisations representing different groups:
  - Grid operators, technology providers, solutions providers, policy makers, end-user forum representatives, and standards organisations
- Primary outlet for project results and a vital source of requirements input
- A series of dissemination workshops are planned throughout the lifetime of the project
  - 1st Stakeholder Group Workshop was on Tuesday, May 20th

RASSA – Reference Architecture for Secure Smart Grids in Austria



Institutionelle Rahmenbedingungen

Security-Standards



Referenz-architektur

Validierte Konzepte

Akzeptierte Schnittstellen

RASSA Roadmap

Elektromobilität

Neue Energiemärkte (Virtuelle Kraftwerke etc.)

Anbindung flexibler Assets (Gebäude, Speicher etc.)

Sichere Verteilnetzautomatisierung

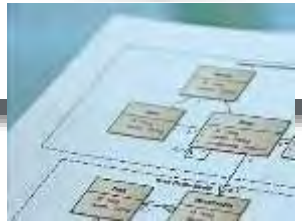
Prosumer Security & Privacy (User Domain)

Höhere Resilienz für vorhandene Infrastruktur

Smart Grid Gesamtarchitektur: Sicherheit und Resilienz des Gesamtsystems

Institutionelle Rahmenbedingungen

Security-Standards



Referenz-architektur

Validierte Konzepte

Akzeptierte Schnittstellen

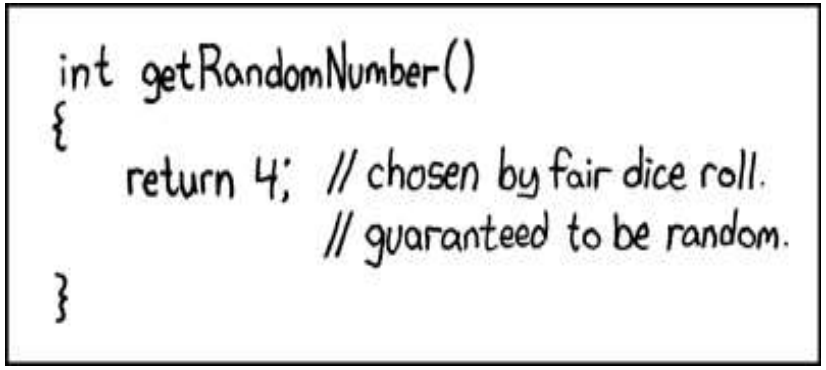
Angepasste Lösungen sind notwendig…

- Nicht das Rad neu erfinden!
- Aber: **spezifische Anforderungen**
  - Risiko vs. Security vs. Kosten
  - Safety & Security
  - Lebenszyklus von Systemen
  - Industrieautomatisierung vs. Internet of Things
- **Angepasste** Sicherheitslevel

- Neue Sicherheitskonzepte sind erforderlich

Security ist eine gemeinsame Verantwortung…

- Das Smart Grid ist ein „System of Systems“
- Sichere Komponenten zu erzeugen ist **nicht genug**
- Sichere **Implementierung** und **Betrieb**
- Security by Default
- Verantwortlichkeiten für spezifischer Sicherheits-aspekte müssen festgelegt werden



© XKCD

Vermeidung, Erkennung und Reaktion …

- Schutzmechanismen sind nutzlos ohne Erkennung und Reaktion auf Angriffe
- Security von Geräten in „feindlichen Umgebungen“
- Verantwortung vs. Kompetenz
- Situationsbewusstsein (situational awareness)
- Incident Reporting (NIS)

AIT Austrian Institute of Technology

your ingenious partner

Thomas Bleier

Dipl.-Ing. MSc zPM CISSP CEH

Senior Engineer, 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/ict-security