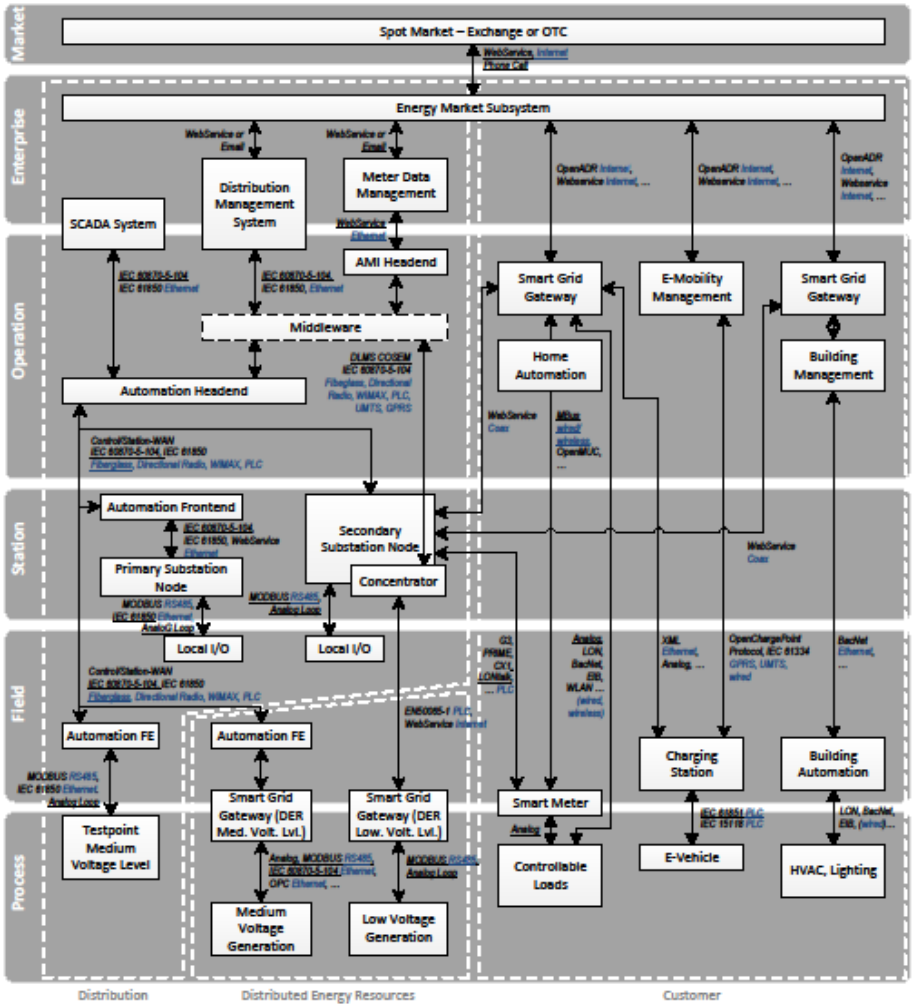
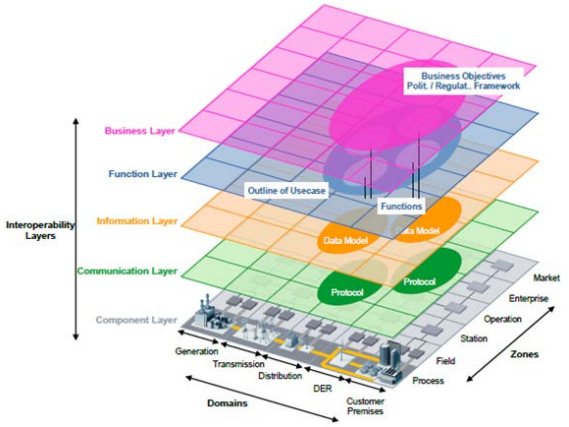
Cyber-security Risks for Smart Grids

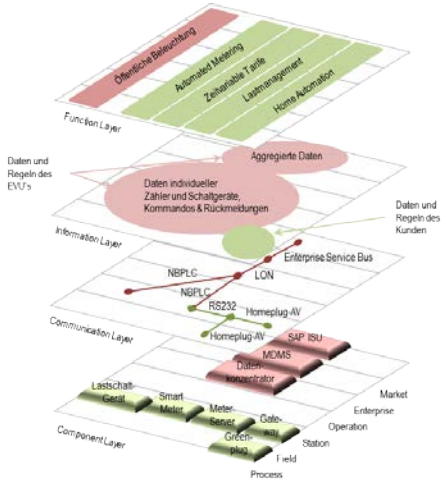
Lucie Langer and Paul Smith
firstname.lastname@ait.ac.at
AIT Austrian Institute of Technology

ComForEn Workshop
Monday 29th September, 2014

The (SG)² Architecture Model





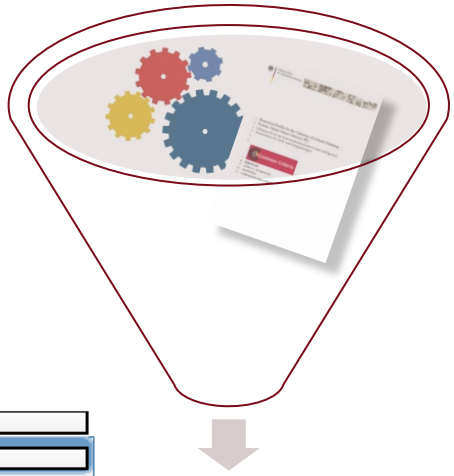


The (SG)² Threat Catalogue

(SG)² Smart Grid Security Guidance

Bundesamt für Sicherheit in der Informationstechnik

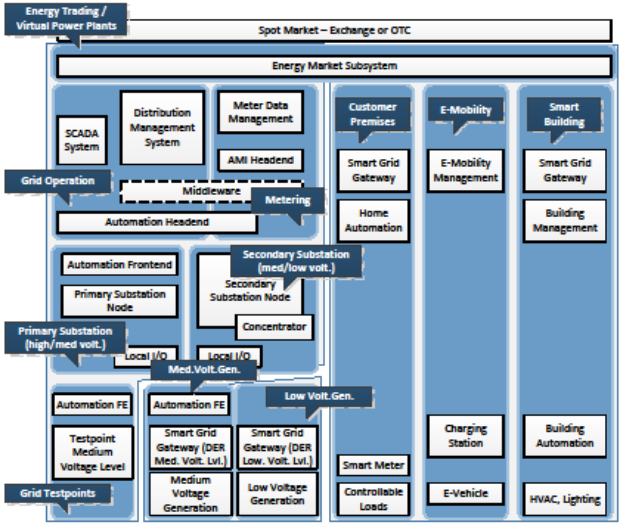
- BSI IT-Baseline-Protection and Common Criteria Protection Profiles
  - Consider 240 out of >500 threats
  - Only technical aspects, no force majeure, no organisational issues



- Outcome: 31 threats, grouped into the categories
  - Authentication / authorisation
  - Integrity / availability
  - Confidentiality / data protection
  - Security mechanisms applied
  - Internal / external interfaces
  - Maintenance / system monitoring

(SG)² threat catalogue

- Apply threats to architecture model
  - Matrix of threats vs system clusters



bmvit Bundesministerium für Verkehr, Innovation und Technologie

The (SG)² Risk Catalogue

- Probability
  - Number of successful attacks p.a.

very low (1) …. medium (3) …. very high (5)
<0.1 p.a. >1 p.a.

- Impact
  - Monetary loss
  - Impact on business continuity and customers
  - Range of effects (local, regional, global)

- Both based on DSO experience / estimation

The (SG)² Risk Catalogue (cont.)

Attacks on the WAN through smart grid gateway

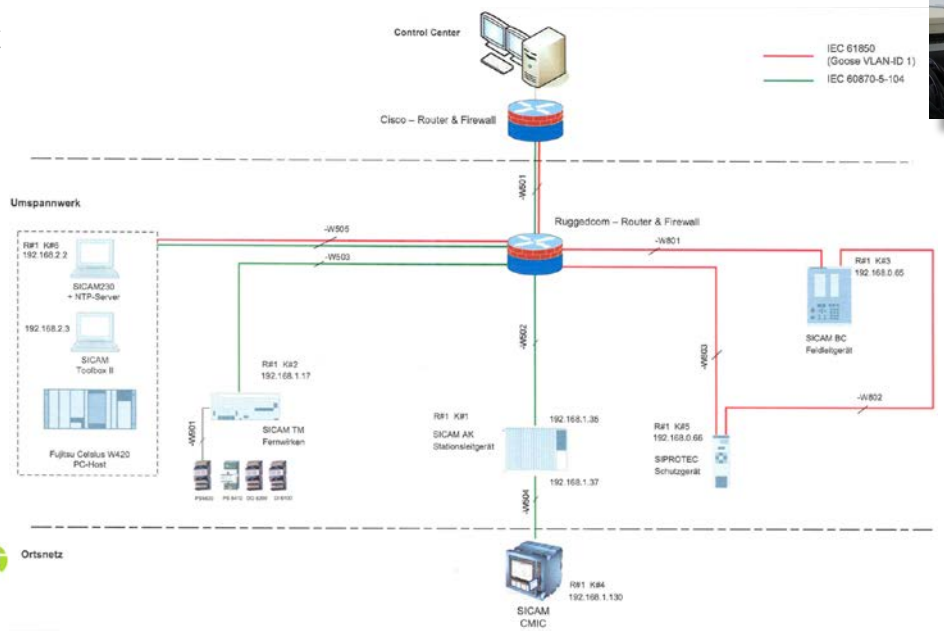
Attacks through remote maintenance access

Cluster / Threat to…	Smart Buildings	E-Mobility	Customer Premises	Low Volt. Gen.	Med. Volt. Gen.	Grid Testpoints	Primary Substation	Secondary Substation	Grid Operation	Metering	*Threat Category Avg.*
Authentication & Authorisation	3,50	4,00	3,00	6,00	6,00	6,25	5,25	8,25	7,00	5,00	5,43
Applied Security Mechanisms	9,50	4,15	7,50	6,40	4,60	4,70	5,05	5,90	7,05	3,00	5,79
Integrity & Availability	2,71	4,46	4,69	4,00	3,13	3,07	3,64	4,72	3,97	4,50	3,89
Internal & ext. Interfaces	2,67	3,50	6,33	6,67	4,00	3,33	5,00	4,00	5,83	2,33	4,37
Confidentiality & Data Protection	5,67	4,67	4,67	8,67	4,33	4,00	3,67	5,63	7,50	3,75	5,25
Maintenance of Equipment	4,43	3,50	4,60	3,75	4,15	3,31	3,94	5,33	5,83	3,60	4,24
Component Cluster Avg.	4,75	4,05	5,13	5,91	4,37	4,11	4,42	5,64	6,20	3,70	

Privacy issues of customer production data

Security Tests

- Secure Substation
- AMIS
- Interface analysis
  - Passive: protocols, sniffing, communication, encryption
  - Active: port scans, replay attacks, protocol manipulation
- In-depth analysis
  - AMIS: Smart Meter
  - SSA: CMIC



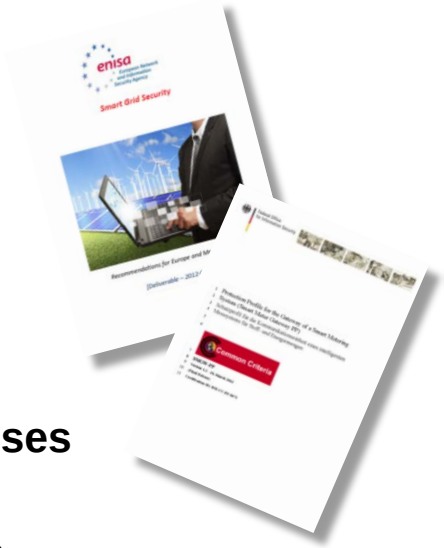
Security Measures

- Define general measures per threat
  + specific measures per component

Archi.komp. / Bedrohung	generische Maßnahmen	Funktionale Gebäude	E-Mobilität Ladeinfrastruktur & E-Mobilität-Management
Ausfall oder Störung von IT-Systemen	Configuration Management (Übersicht eingesetzter Geräte und deren Wartungszustand); Incident Management (kontrollierte Abwicklung von Incidents); Patchmanagement (Systemzustand aktuell halten); geeignete Wartungsintervalle für IT-Systeme vorsehen; regelmäßig technische & physische Audits durchführen (Auffinden möglicher Schwachstellen); Tests nach jeder Systemänderung (z.B. nach korrektivem Eingriff); redundante Auslegung kritischer (IT-)Systeme; abgesicherte Start-, Stopp- und Notlaufprogramme für Smart-Grid-Komponenten (Graceful Degradation, kein Totalausfall); Backup-/Restore-Strategien (z.B. für Mess- und Rechnungsdaten); Integritätscheck nach einem Ausfall (z.B. Messdaten); Notsignalgebung zum Netzbetreiber berücksichtigen (für z.B. schnelle Reaktion auf mögliche Lastprobleme); Disaster Recovery (DRP) & Business Continuity Plan (BCP)	Geringe Risikoklasse, da die Stromversorgung des Gebäudes nicht beeinträchtigt werden kann; im Falle eines Ausfalls funktioniert das Gebäude-Lastmanagement nicht mehr; dies führt vor allem zu negativen Auswirkungen beim Nutzer, jedoch nicht beim Netzbetreiber (EW: 2; AW: 2; RP niedrig)	Relevant für Ladestation und E-Mobility MS; Ausfall oder Störung des E-Mobility MS kann Störungen des Lastmanagements oder der Stromversorgung bewirken; unter Umständen könnten sogar alle Ladestationen in einem Gebiet (z.B. Stadtteil) gleichzeitig an- oder ausgeschaltet werden und Schwankungen oder Instabilitäten im Stromnetz bewirken (lokale Auswirkungen) (EW: 2-3; AW: 2; RP mittel)
Ausfall oder Störung von IT-Systemen	AIT	siehe generelle Maßnahmen	siehe generelle Maßnahmen

Security Measures (cont.)

- Evaluate (weighted) rate of occurence
  - Factor 0,1 / 0,5 / 1,0 for low / medium / high risk
- Results:
  - **46: Ensure authenticity and integrity**
  - **36: Perform security evaluation / pen testing**
  - **34: Define and follow change / patch / config mgmt processes**
  - 31: Provide for (network) segmentation
  - 25: Follow minimisation principle (access rights, functions, etc.)
  - 21: Apply strong protection measures to remote maintenance access points; perform incident mgmt
  - 19: Introduce multi-layer security; apply physical security measures
  - 18: Define security requirements for vendors / supply chain and require proof (e.g. certification)



Next steps

- Feed results from the security tests back into risk catalogue and define specific security measures

- Tool implementation of the risk catalogue

verinice.

Cluster / Threat to...	Smart Buildings	E-Mobility	Customer Premises	Low Volt. Gen.	Med. Volt. Gen.	Grid Testpoints	Primary Substation	Secondary Substation	Grid Operation	Metering	Threat Category Avg.
Authentication & Authorisation	3,50	4,00	3,00	6,00	6,00	6,25	5,25	8,25	7,00	5,00	5,43
Applied Security Mechanisms	9,50	4,15	7,50	6,40	4,60	4,70	5,05	5,90	7,05	3,00	5,79
Integrity & Availability	2,71	4,46	4,69	4,00	3,13	3,07	3,64	4,72	3,97	4,50	3,89
Internal & ext. Interfaces	2,67	3,50	6,33	6,67	4,00	3,33	5,00	4,00	5,83	2,33	4,37
Confidentiality & Data Protection	5,67	4,67	4,67	8,67	4,33	4,00	3,67	5,63	7,50	3,75	5,25
Maintenance of Equipment	4,43	3,50	4,60	3,75	4,15	3,31	3,94	5,33	5,83	3,60	4,24
Component Cluster Avg.	4,75	4,05	5,13	5,91	4,37	4,11	4,42	5,64	6,20	3,70	

bmvit
Bundesministerium für Verkehr, Innovation und Technologie

Questions?