Fraunhofer
AISEC

SPARKS
SMART GRID PROTECTION AGAINST CYBER ATTACKS

Risk Assessment for Cyber-Physical Smart Grid Systems

The SPARKS project approach

Martin Hutle

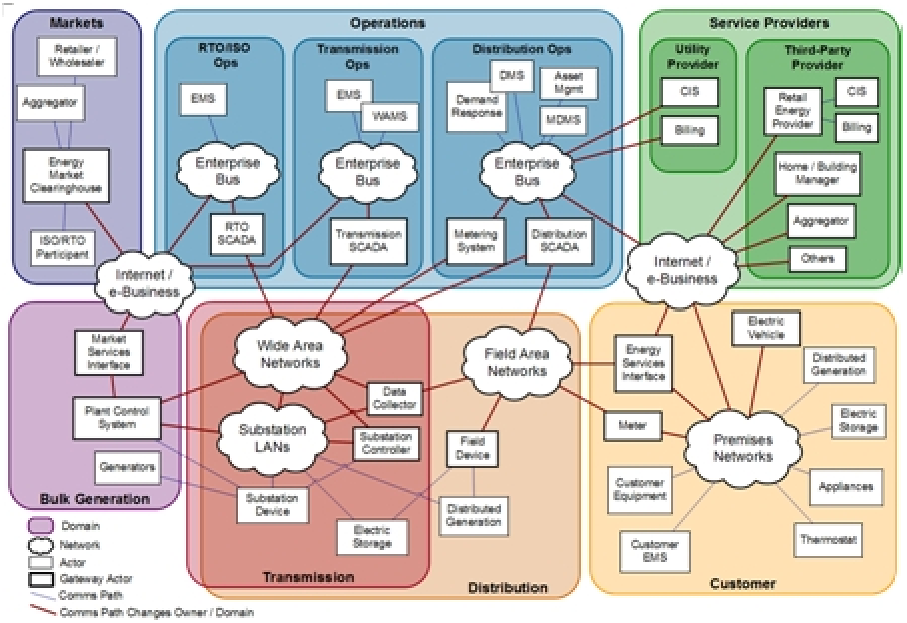
Symposium on Innovative Smart Grid Cybersecurity Solutions 2017, Vienna, Austria

EU FP7 Programme Contract No. 608224

Risk assessment for the smart grid

sparks
SMART GRID PROTECTION AGAINST CYBER ATTACKS

- The smart grid is a networked cyber-physical system
  - heterogeneous (technology, ownership, functionality)
  - complex dependencies (data network, grid, administrative)
- An adequate risk assessment considers
  - multi-stage attacks → SPARKS demo
  - combined attacks → Ukraine 2015

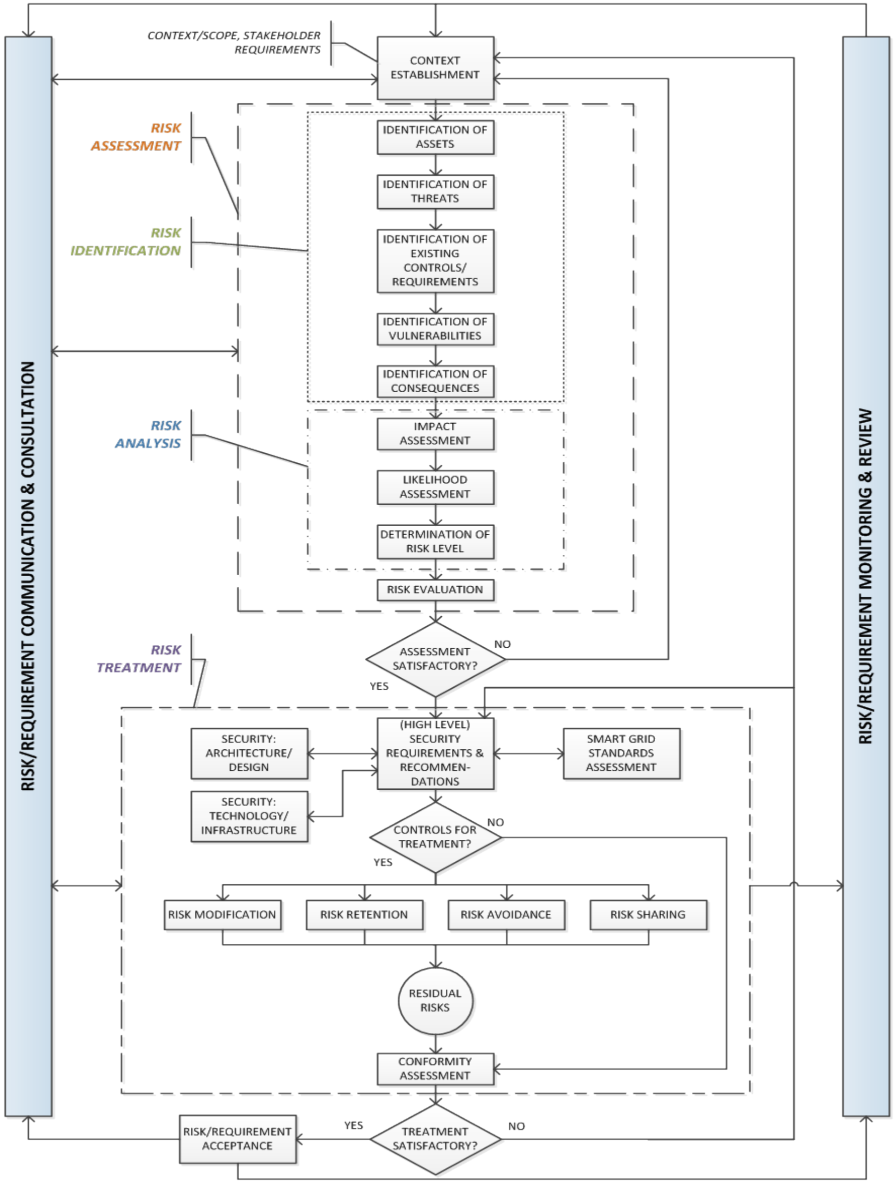


EU FP7 Programme Contract No. 608224

The SPARKS risk assessment approach

SPARKS
SMART GRID PROTECTION AGAINST CYBER ATTACKS

- ISO 27005 framework
  - asset driven approach
- we populate various steps with smart grid specific implementations
- partially from existing methods where useful
  - SGIS Toolbox
  - HMG IS1
- own methods
- supporting tools



RISK/REQUIREMENT COMMUNICATION & CONSULTATION

CONTEXT/SCOPE, STAKEHOLDER REQUIREMENTS

CONTEXT ESTABLISHMENT

RISK ASSESSMENT

IDENTIFICATION OF ASSETS

IDENTIFICATION OF THREATS

RISK IDENTIFICATION

IDENTIFICATION OF EXISTING CONTROLS/ REQUIREMENTS

IDENTIFICATION OF VULNERABILITIES

IDENTIFICATION OF CONSEQUENCES

RISK ANALYSIS

IMPACT ASSESSMENT

LIKELIHOOD ASSESSMENT

DETERMINATION OF RISK LEVEL

RISK EVALUATION

RISK TREATMENT

ASSESSMENT SATISFACTORY?

NO

YES

SECURITY: ARCHITECTURE/ DESIGN

(HIGH LEVEL) SECURITY REQUIREMENTS & RECOMMEN-DATIONS

SMART GRID STANDARDS ASSESSMENT

SECURITY: TECHNOLOGY/ INFRASTRUCTURE

CONTROLS FOR TREATMENT?

NO

YES

RISK MODIFICATION

RISK RETENTION

RISK AVOIDANCE

RISK SHARING

RESIDUAL RISKS

CONFORMITY ASSESSMENT

RISK/REQUIREMENT ACCEPTANCE

YES

TREATMENT SATISFACTORY?

NO

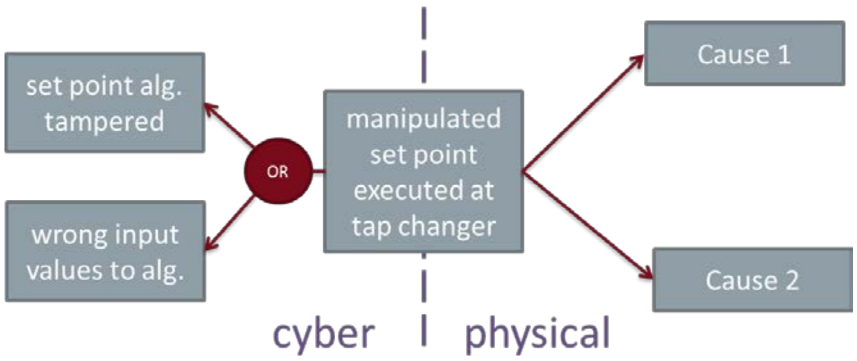
RISK/REQUIREMENT MONITORING & REVIEW

EU FP7 Programme Contract No. 608224

Identifying assets and security objectives

SPARKS
SMART GRID PROTECTION AGAINST CYBER ATTACKS

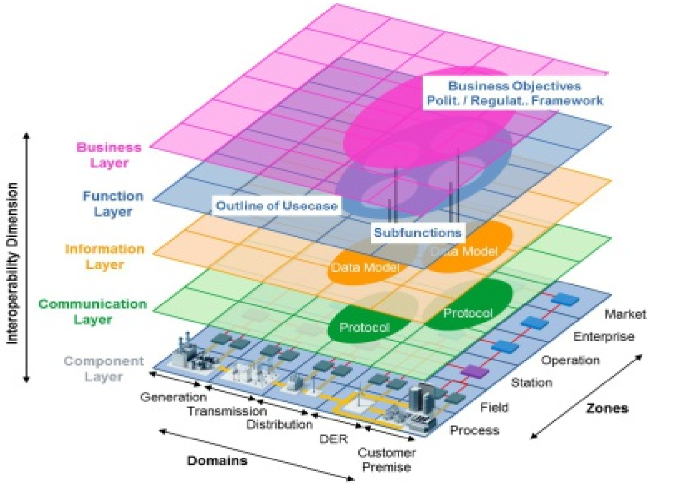
- In the smart grid the most important assets are located at the edge between “cyber” and “physical”
  - integrity has direct impact on grid stability
  - standard IT: confidentiality is more in the focus
- Start analysis with focus on these primary assets
  - security analysis (“likelihood”)
  - consequence and impact analysis
- Reduces the number of assets for the analysis
- Secondary assets are implicitly identified by the threat analysis

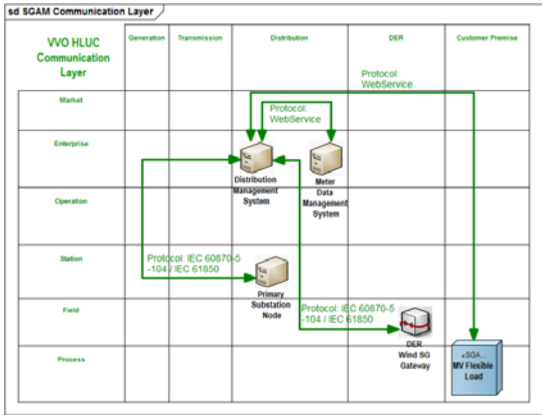

set point alg. tampered
wrong input values to alg.
OR
manipulated set point executed at tap changer
Cause 1
Cause 2
cyber
physical

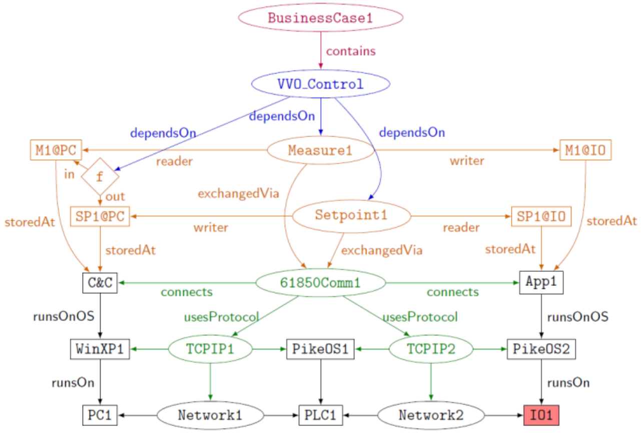
Model-based approach for asset identification and threat analysis

SMART GRID PROTECTION AGAINST CYBER ATTACKS

- Description in the Smart Grid Architecture Model (SGAM)
- Precise language (Ontology representation of SGAM elements)
- Tool:
  - Plug-in for Enterprise Architect
  - Export to RDF







EU FP7 Programme Contract No. 608224

Handling the complexity of threat analysis

- Complex attack vectors
  - multi-stage attacks
  - combined attacks
- Many assessment methods look on individual assets only
  - neglects these interdependencies
  - are not able to capture countermeasures such as isolation or zoning
- Attack trees
  - allow representation of these scenarios
  - become quickly intractable with growing system size
- SPARKS: Tool-based approach
  - use machine-based reasoning to identify attack vectors
  - implicit representation
  - uses ontology-based description
  - reusability
  - combination with vulnerability databases, threat catalogues

Impact categories

SMART GRID PROTECTION AGAINST CYBER ATTACKS

Category	PM	P	ICTP	ESCO	TSO	DSO
Economic		●		●	●	●
Safety	●					●
Quality of Supply				●	●	●
Infrastructures	●					
Regulatory	●		●	●	●	●
Reputational		●	●	●	●	●
Data Protection and Privacy		●	●	●	●	●
Equipment		●	●		●	●
Population	●					

Impact is stakeholder-dependent!

policy makers (PM), producers (P), ICT equipment producers (ICTP), energy service companies (ESCO), transmission system operators (TSO), distribution system operators (DSO)

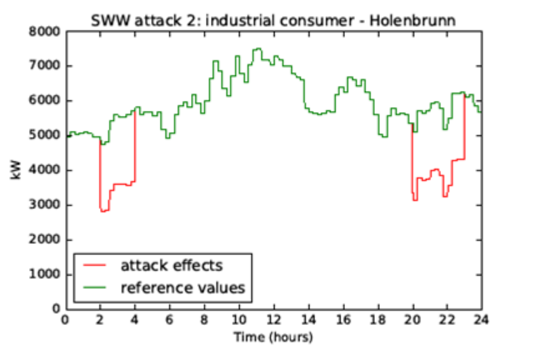
EU FP7 Programme Contract No. 608224

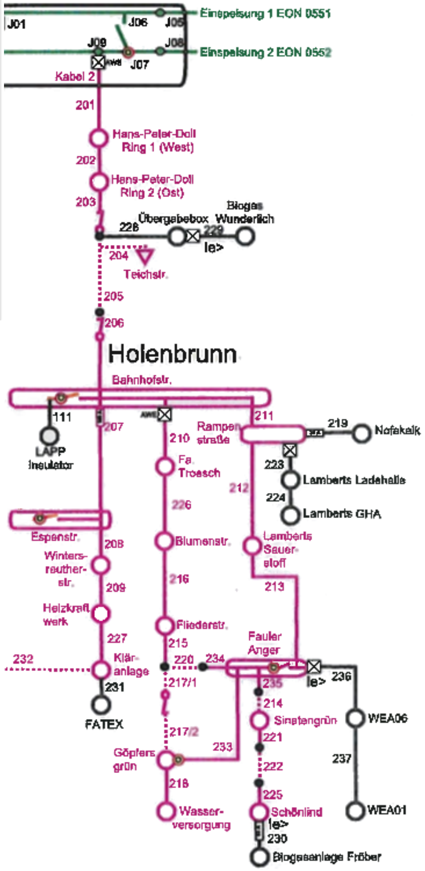
Impact analysis

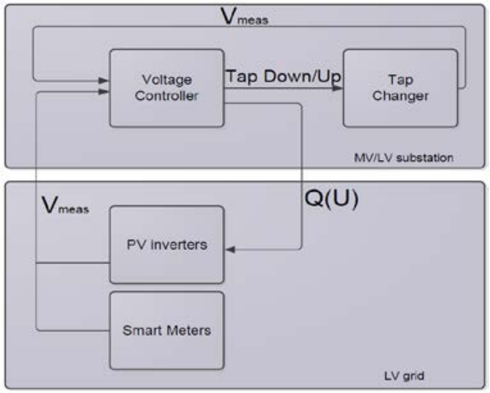
- Expert Analysis
- Safety and Security Analysis
  - Event tree analysis
  - FMVEA
  - System theoretic process analysis (STPA)
  - Bayesian networks.
- System analysis
  - mathematical (differential) equations to model the electrical system
  - looks for analytical solutions to these equations
- Simulation
  - allows solutions for systems that are too complex for an analytical solution
  - allows combination with data network simulation (co-simulation)
  - allows including real hardware in the simulation (hardware-in-the-loop).

SPARKS Impact Analysis

- Co-simulation environment for MV grid
  - SWW Holenbrunn area
  - attack: price manipulation scenario
- System theoretic impact analysis on LV grid
- Simulation of LV grid
  - simulation with hardware in the loop
  - voltage control use-case
- Customized impact tables

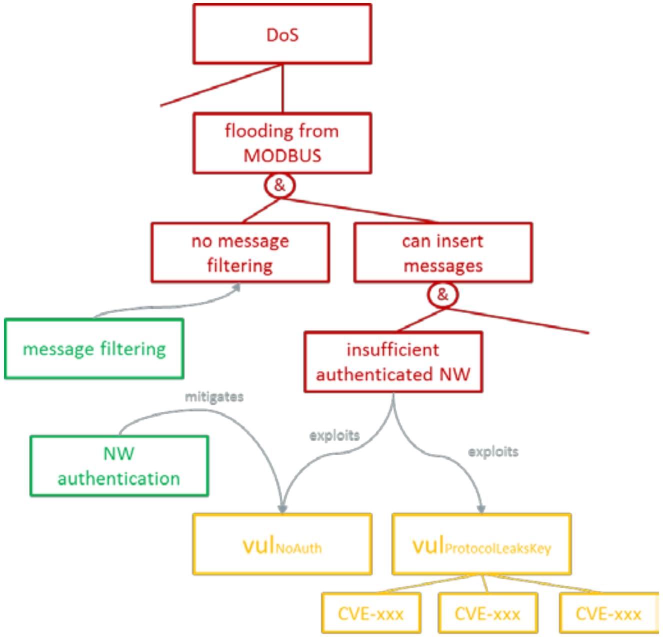






Risk treatment

- Problem with existing risk assessment methods: missing link between technical risk analysis and mitigation measures
  - often measures are based on risk level only
  - connection to actual threats gets lost
- Semantic threat graphs
  - offer possibility to deduce tailored countermeasures by machine-based reasoning
  - combination of attack graphs and semantic threat graphs
  - input from best-practice catalogues



Summary

- SPARKS risk assessment
  - ISO 27005 framework
  - context establishment using SGAM modelling
  - security analysis with machine-based reasoning
  - impact analysis: simulation, analytical
  - deduction of countermeasures with semantic threat graphs
- Exercised the method on the SPARKS demonstration sites
  - Stadtwerke Wundsiedel
  - NIMBUS Microgrid

Thank you for your attention!

Dr. Martin Hutle
Deputy Head of Department
Product Protection and Industrial Security

Fraunhofer AISEC
Parkring 4
85748 Garching bei München, Germany

Phone: +49 89 3229986-135
Fax: +49 89 3229986-222
E-Mail: martin.hutle@aisec.fraunhofer.de
Internet: www.aisec.fraunhofer.de