SMART GRID PROTECTION AGAINST CYBER ATTACKS

The SPARKS Project
Motivation, Objectives and Results

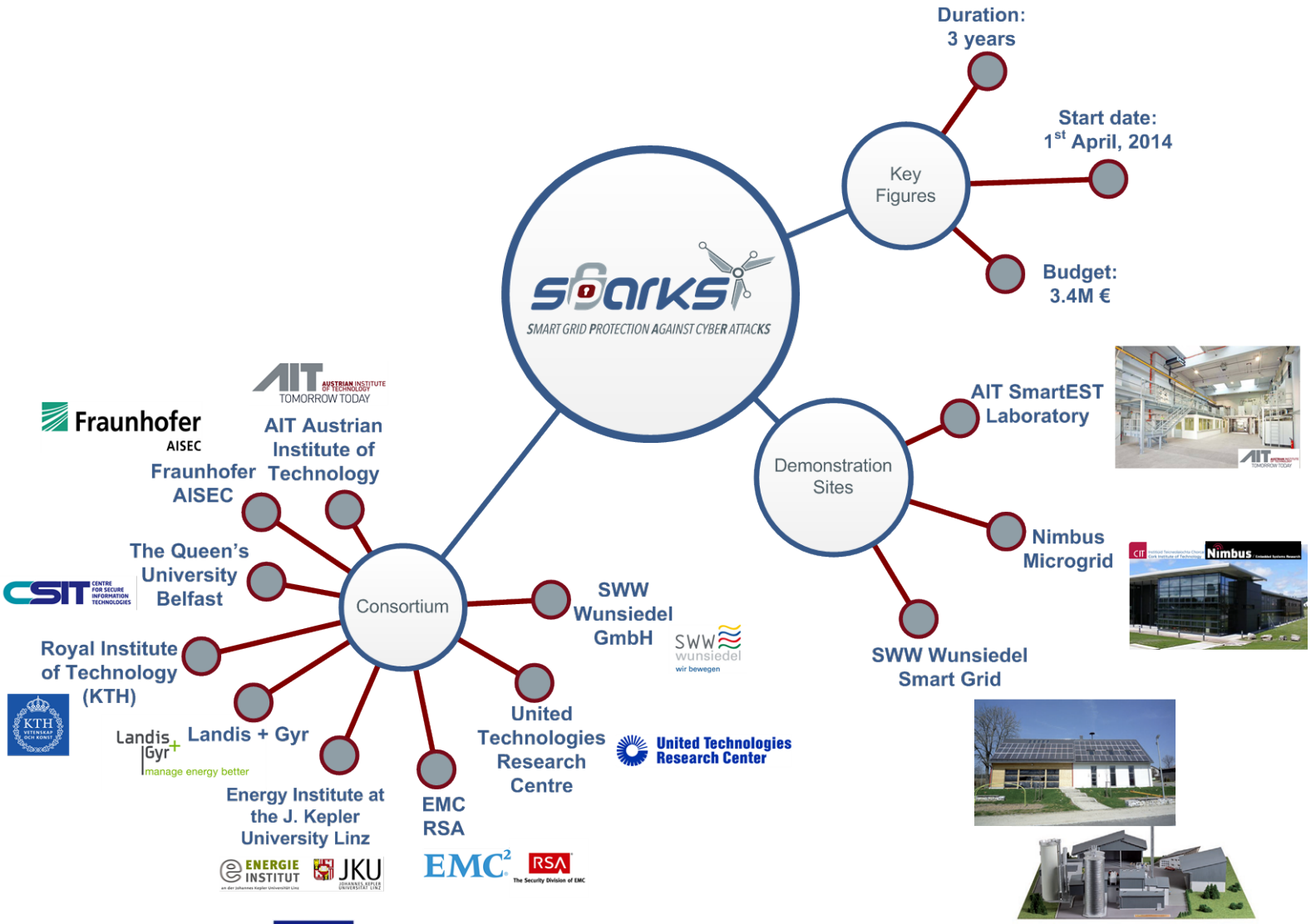
Paul Smith
paul.smith@ait.ac.at
AIT Austrian Institute of Technology

SEGRID Project Workshop
14th November, 2016, Barcelona, Spain

© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

The SPARKS Project

SMART GRID PROTECTION AGAINST CYBER ATTACKS

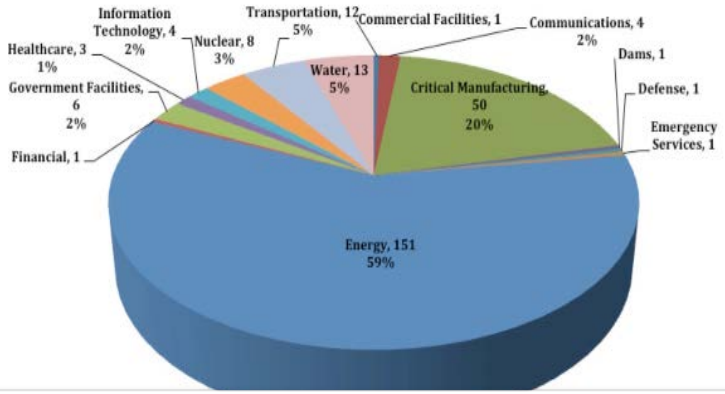


© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

Motivation: New Cybersecurity Concerns for Energy Utilities

SMART GRID PROTECTION AGAINST CYBER ATTACKS

Operational Risks



Analysis confirms coordinated hack attack caused Ukrainian power outage

BlackEnergy was key ingredient used to cause power outage to at least 80k customers.

by **Dan Goodin** - Jan 11, 2016 5:42am GMT

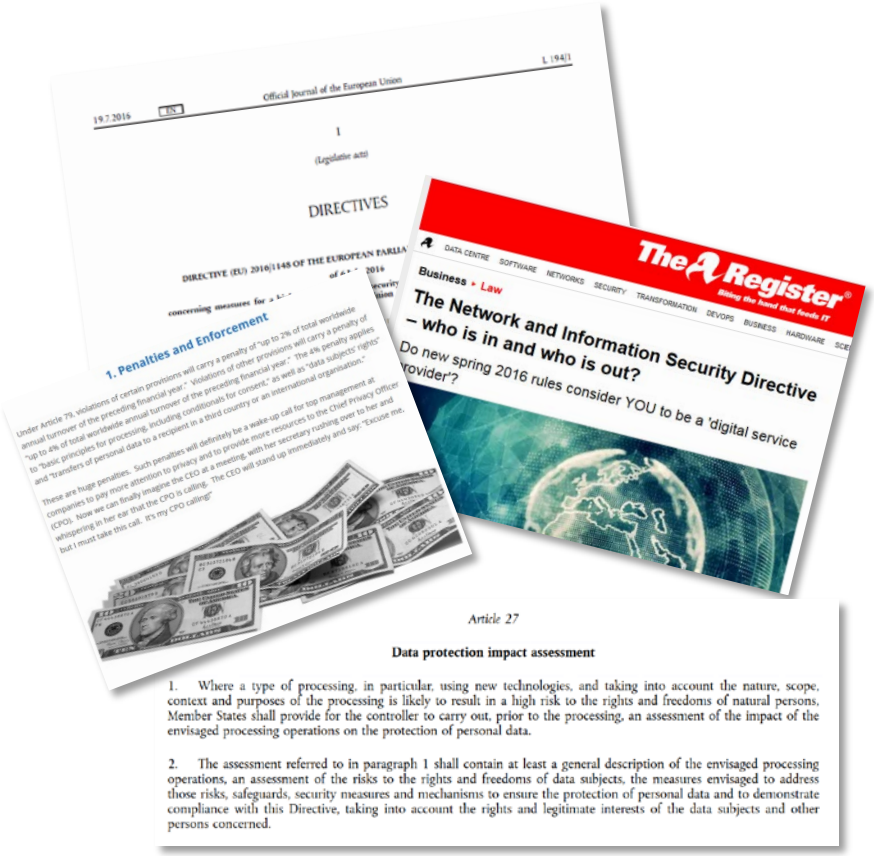
Share Tweet Email 33

The people who carried out last month's first known hacker-caused power outage used highly destructive malware to gain a foothold into multiple regional distribution power companies in Ukraine and delay restoration efforts once electricity had been shut off, a newly published analysis confirms.

The malware, known as BlackEnergy, allowed the attackers to gain a foothold on the power company systems, said the

FURTHER READING

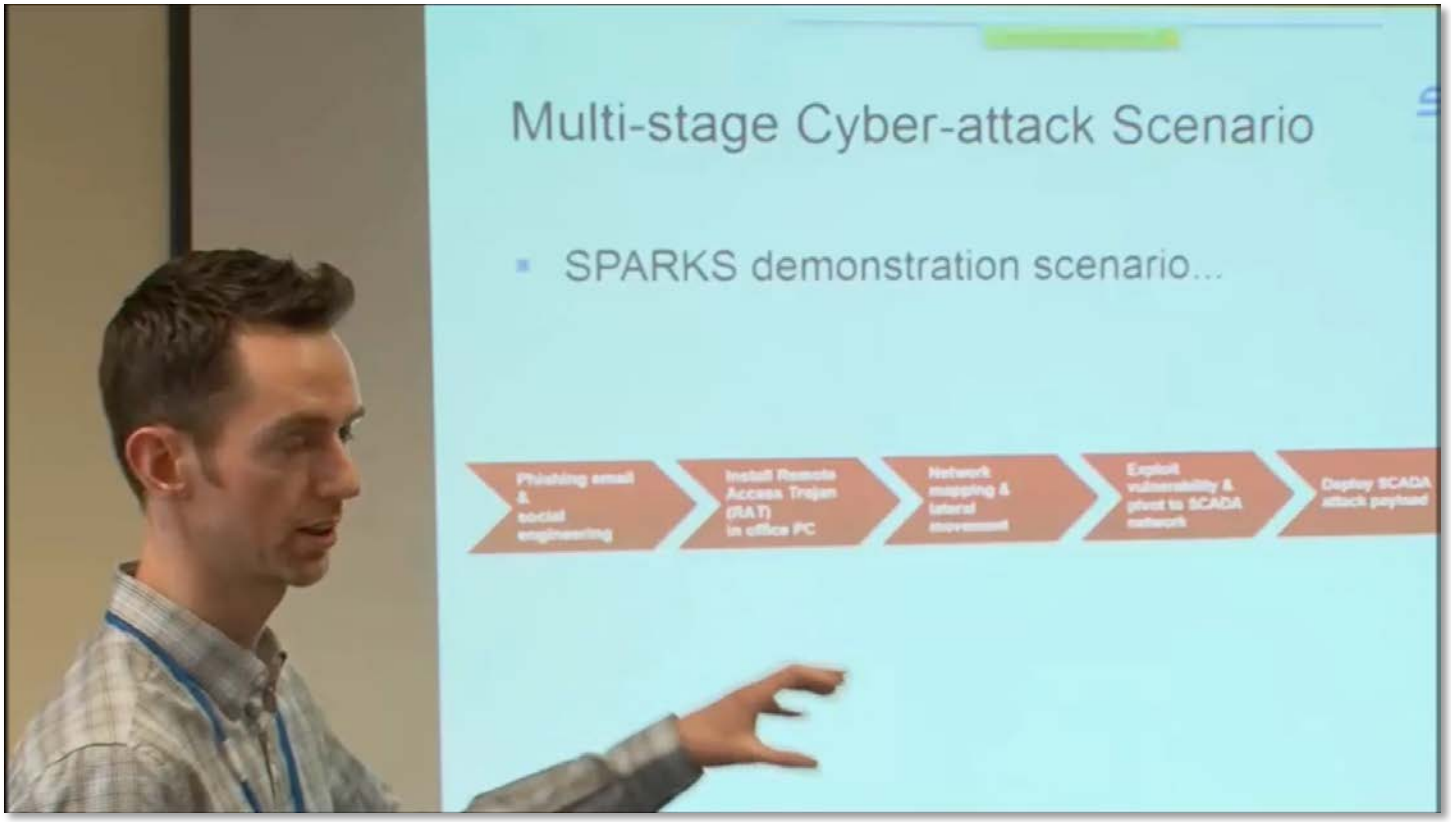
Compliance Concerns



© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

Advanced Persistent **Cyber-Physical** Threat: SPARKS Demonstration

SMART GRID PROTECTION AGAINST CYBER ATTACKS

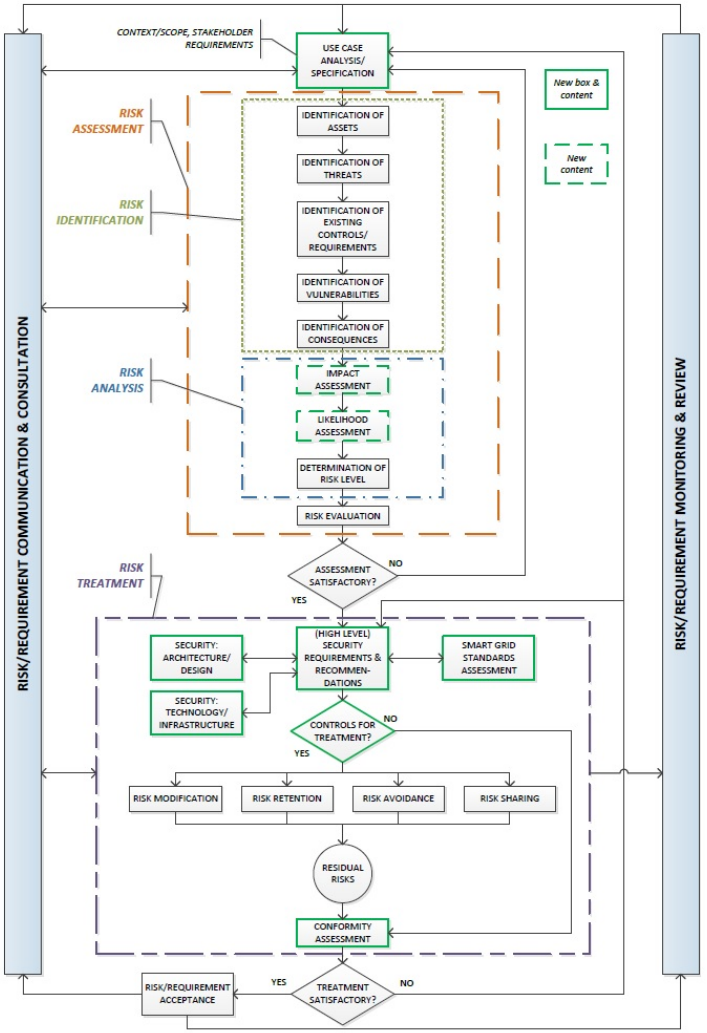


Phishing email & social engineering → **Install Remote Access Trojan (RAT) in office PC** → **Network mapping & lateral movement** → **Exploit vulnerability & pivot to SCADA network** → **Deploy SCADA attack payload** → **Attack physical system functions**

© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

SPARKS Risk Assessment Framework

- Based on ISO/IEC 27005
- Familiar to the information security community
- Well-aligned with emerging cyber security requirements and compliance needs for critical infrastructure protection
- Guidance on how to implement the risk management process for a set of smart grid use cases

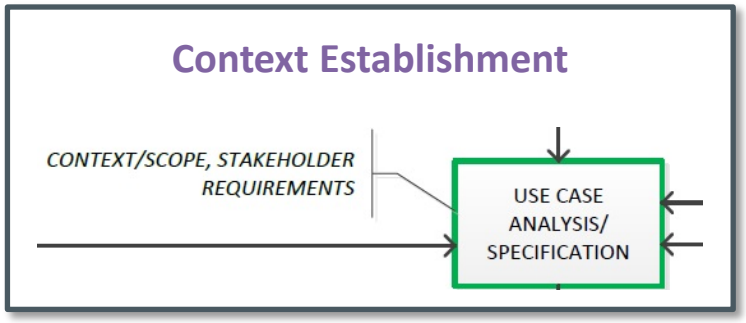


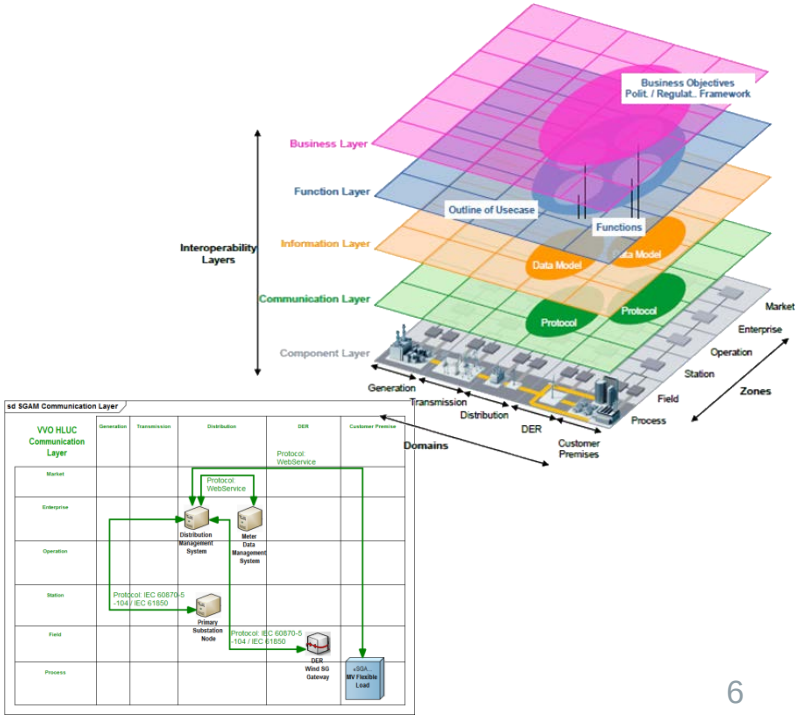
© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

Context Establishment

- Overview
  - Define the scope of the risk assessment, and the technical and organisational boundaries
  - Consider stakeholder requirements
  - Consider the underlying system architecture
  - Derive a smart grid use case to be analysed

- Approach
  - Use the SGAM Framework and Toolbox to define the context of the risk management exercise

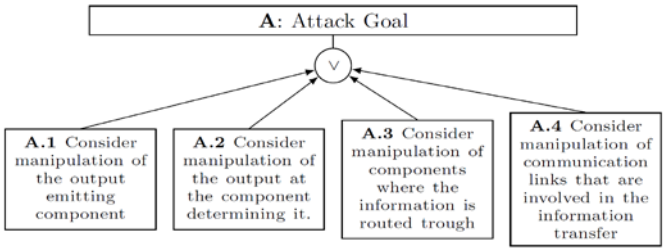


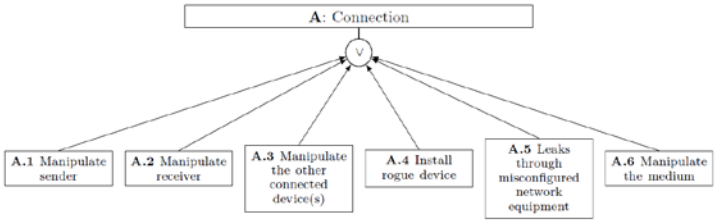


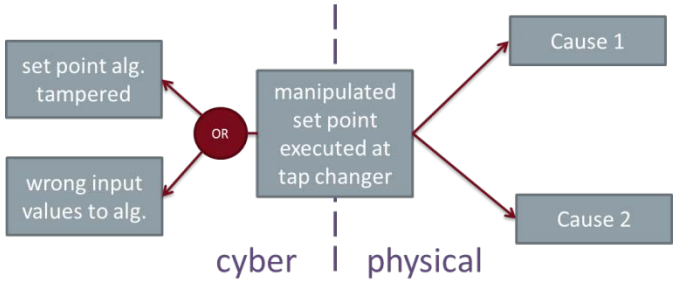
© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

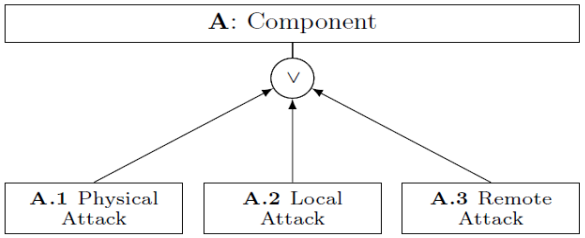
Identification of Threats: Attack Trees

- A deductive approach to analyse the steps that an attacker can take to realise their goal
- Developed re-usable attack patterns to support the development of trees
- Tool support for tree generation, using an Ontology that is created from an SGAM-based architecture description





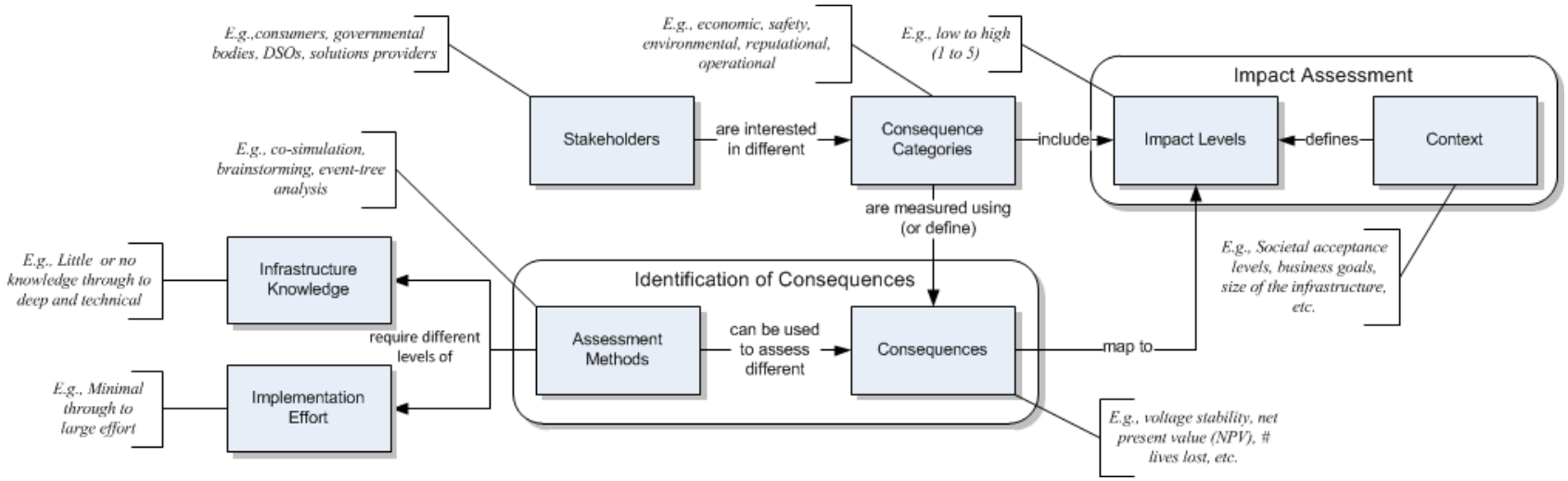




© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

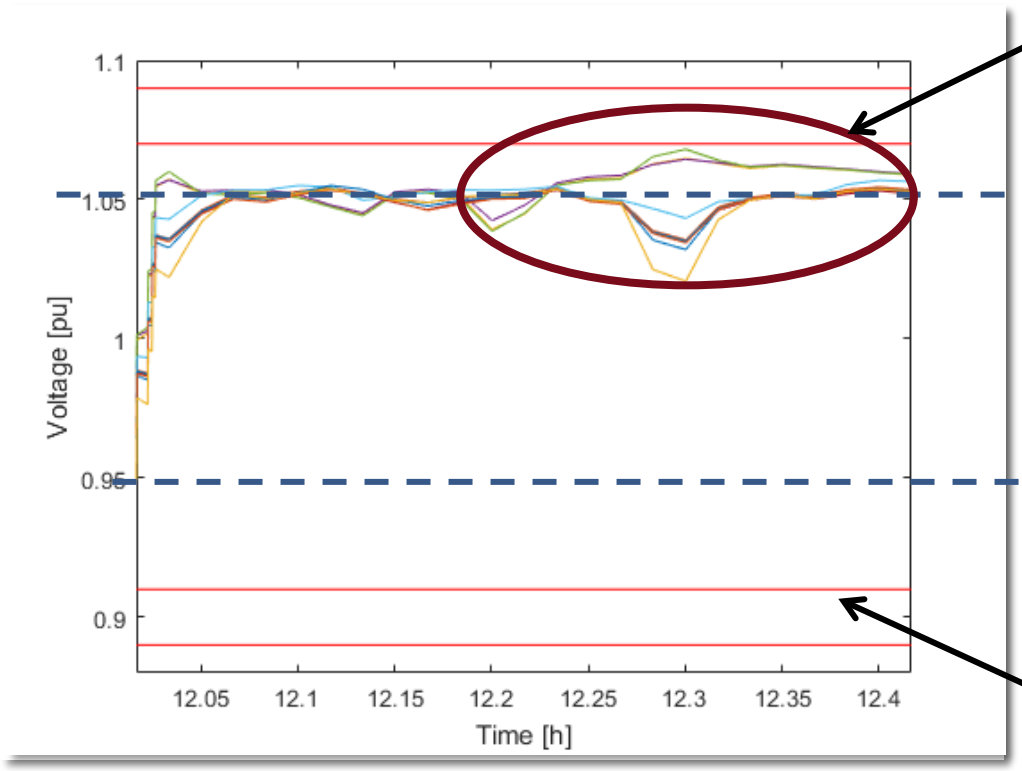
Consequence Identification

- Consequences identification for information security is largely concerned with data-related (CIA) losses
- In the smart grid, consequences can be wide-ranging, e.g., cyber-physical concerns, and challenging to identify
- Smart grid stakeholders have varied concerns and capacity to analyse consequences



© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

Co-Simulation of Power Systems Consequences



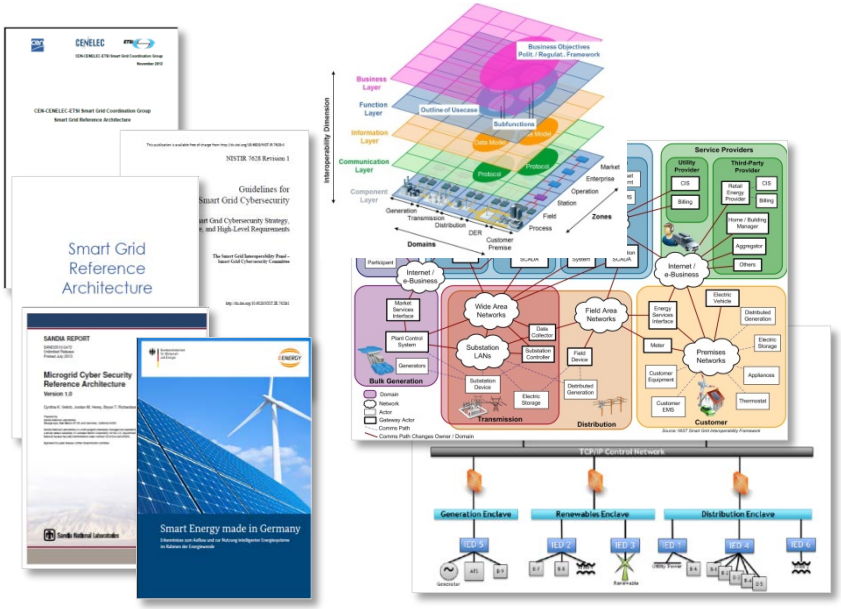
Overvoltage situation

±5% of the nominal voltage (230V)

Manipulated Q(U) curve parameters

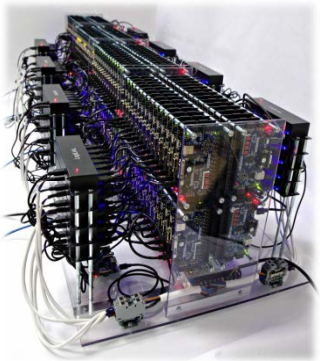
© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

Security Architectures and Technologies



- Consolidation an analysis of existing standards, architectural guidelines and best practices
- Guidance on the application of material to operators
- Recommendations regarding future topics that should be addressed

- Exploration of the use of PUF technology to secure smart meters and gateways
- Unique testbed to evaluate PUF designs and their robustness to side channel attacks, etc.

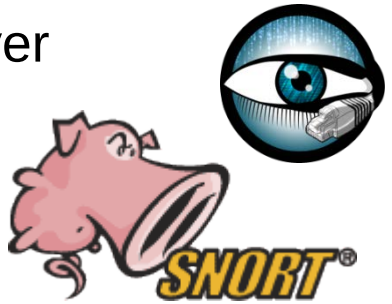


© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

Intrusion Detection for SCADA Systems

SMART GRID PROTECTION AGAINST CYBER ATTACKS

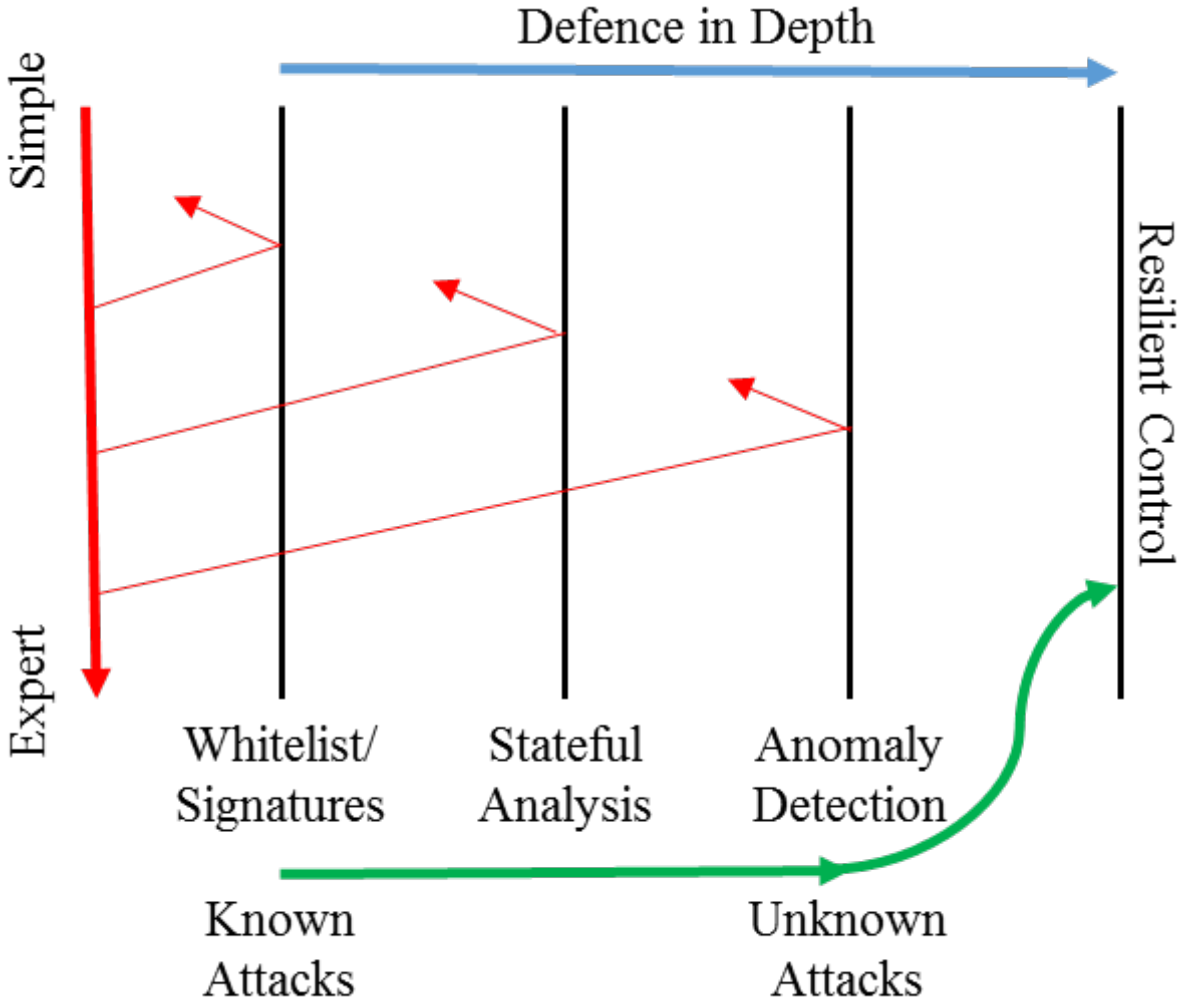
- Current approaches:
  - Security solutions generally lack awareness of power systems properties
  - Deployment of SCADA systems often realised without security extensions enabled (e.g., IEC 62351)
  - Lack of deep analysis at SCADA application layer



- Our aim is to combine SCADA and power systems knowledge to effectively monitor application layer data

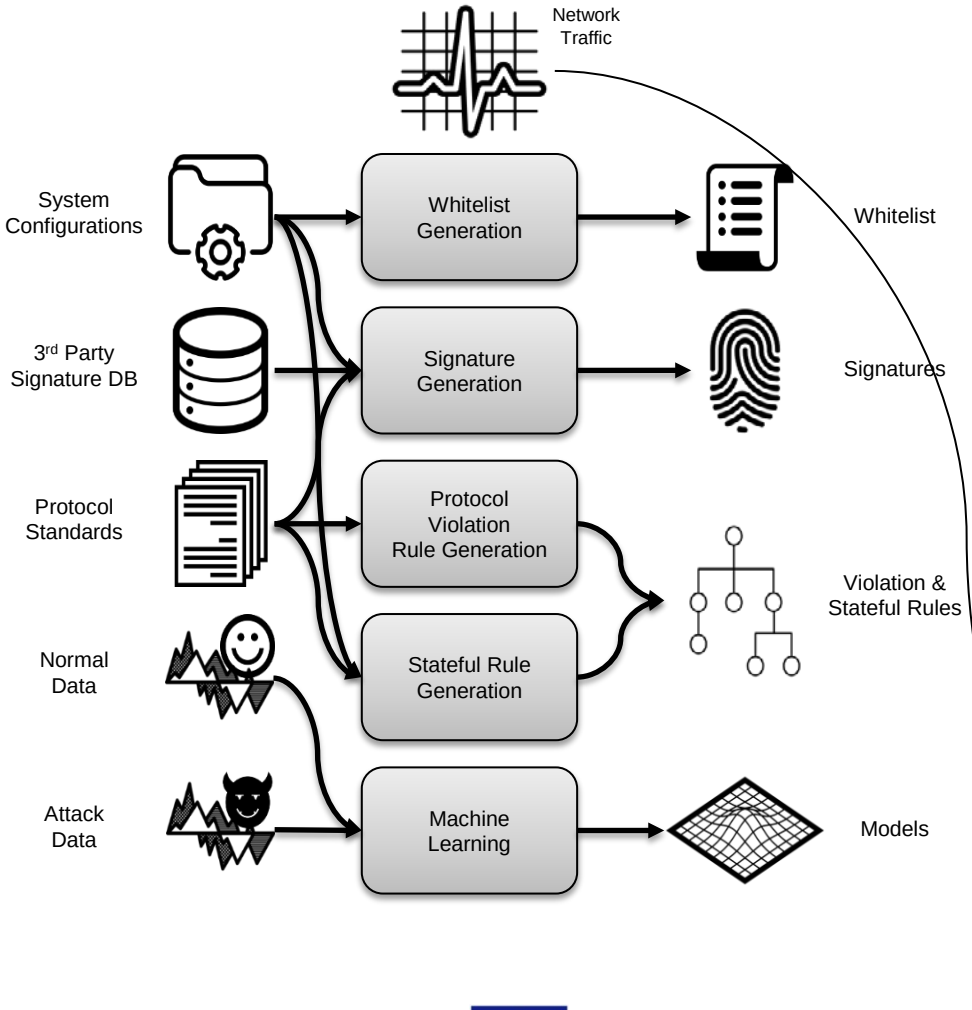
© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

Multi-Attribute SCADA IDS Concept

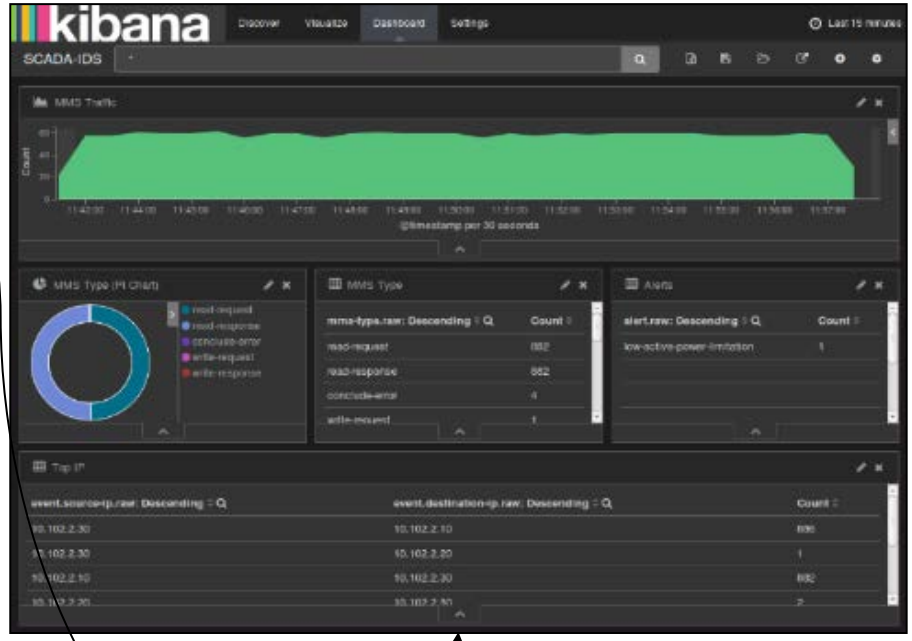


© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

Multi-Attribute SCADA IDS Implementation



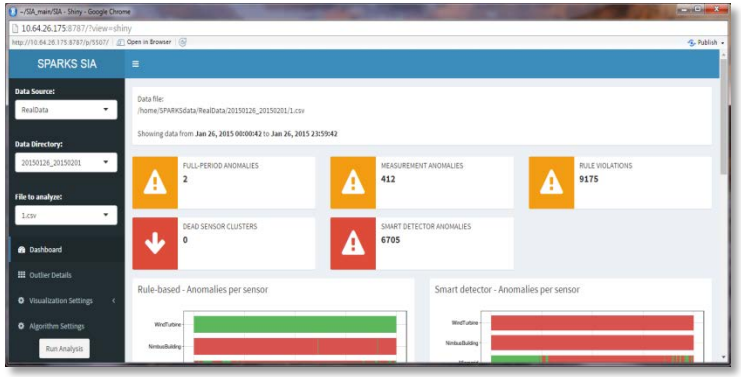
ELK (Elasticsearch, Logstash, Kibana)



© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

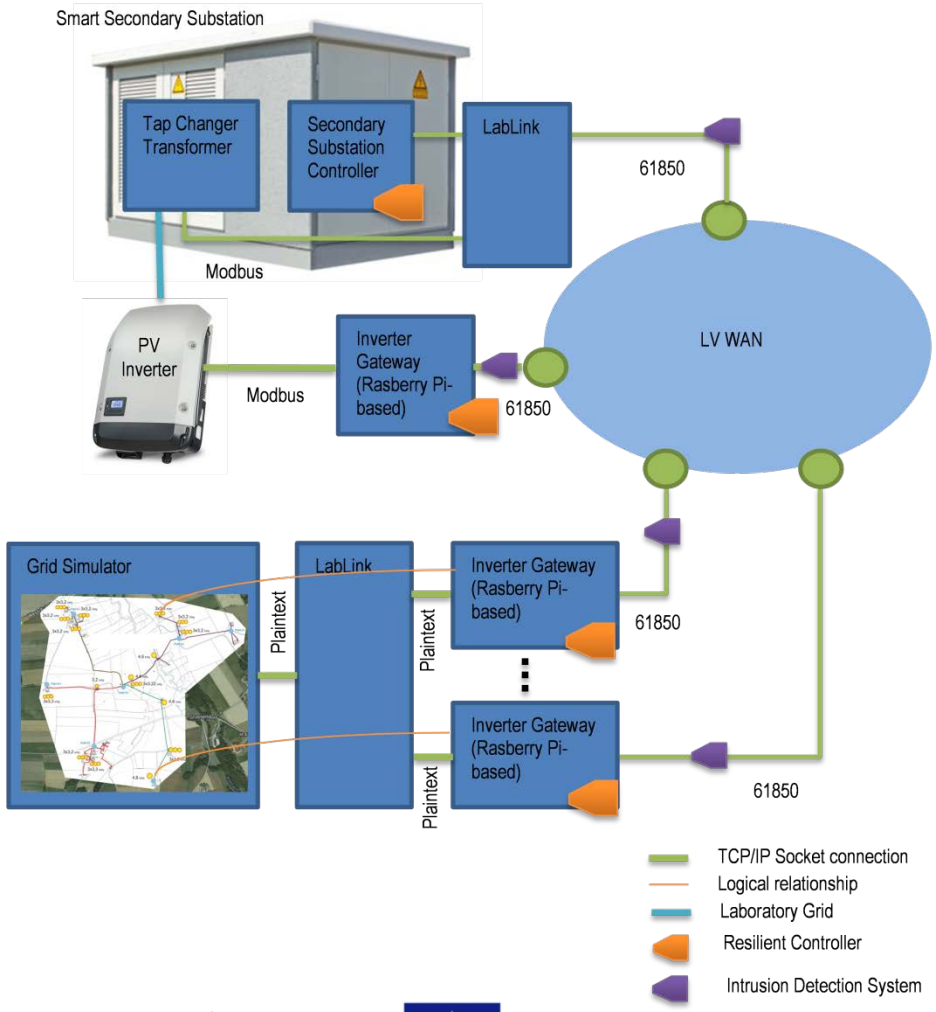
Security Information Analytics Platform

- **Knowledge-based** (needs domain expertise):
  - **Deviation from set-point** (grid specifications)
  - **Rule violations** (physical laws; system model)
  - **Dead-sensor clustering** (operator-selected time windows)
- **Data-driven** (implicitly learns “normal” patterns):
  - **Kullback–Leibler divergence** (histogram over full day)
  - **Single-class SVM** (classification – normal vs anomalous)



© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

Resilient Control in Low Voltage Grid



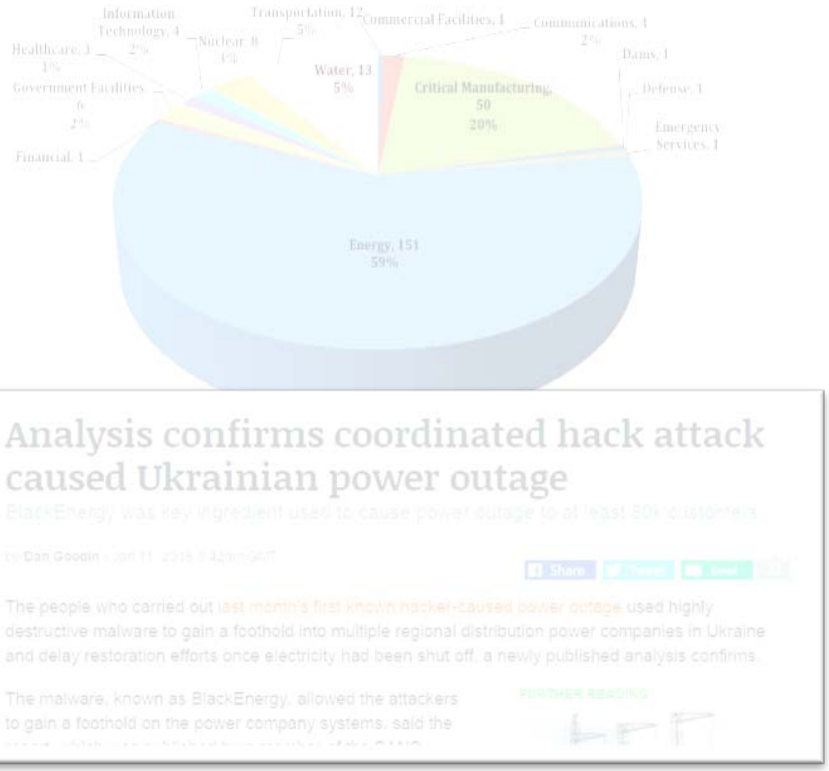
- Adaptation of PV controller behaviour, based on security information
- Evidential network used to determine system state
  - Dempster-Shafer Theory used to address alert uncertainty
- Demonstration in the AIT SmartEST Lab

© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

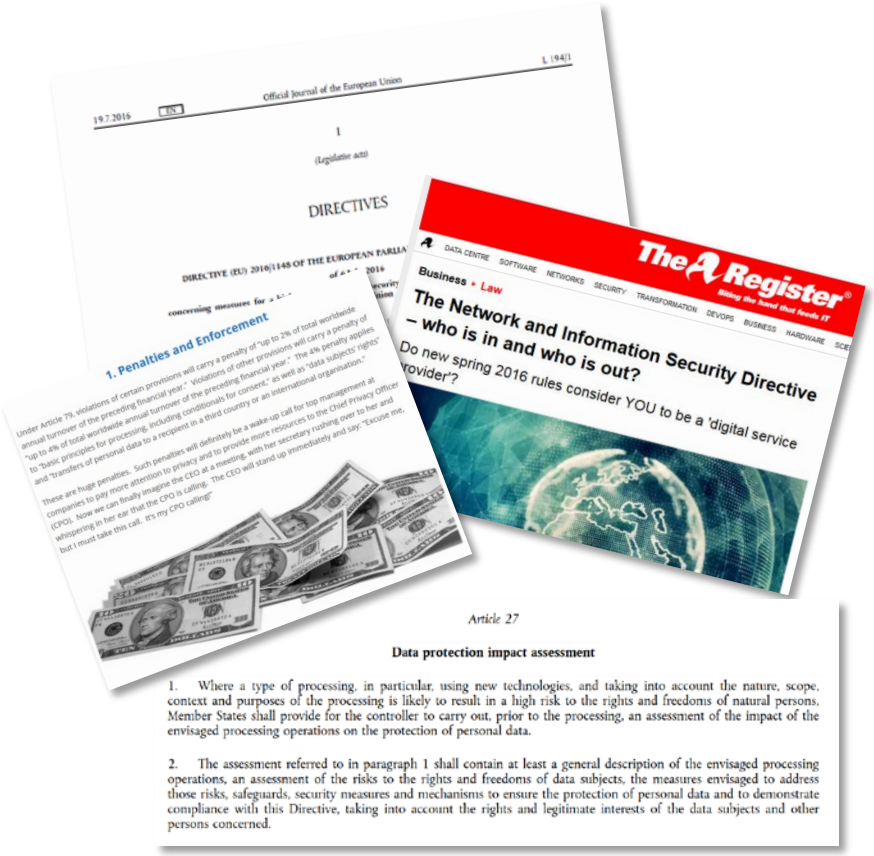
Motivation: New Cybersecurity Concerns for Energy Utilities

SMART GRID PROTECTION AGAINST CYBER ATTACKS

Operational Risks



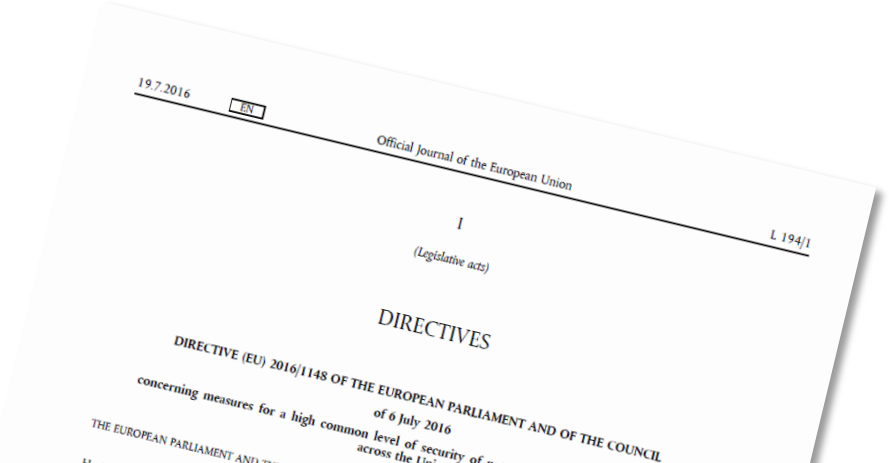
Compliance Risks



© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

The Network and Information Security (NIS) Directive

- Entered into force in August 2016
  - Member States have 21 months to transpose the Directive into national laws
- The aims of the Directive:
  - Ensure a high common level of network and information security
  - Improve the security of the Internet and the private networks and information systems
  - Increase preparedness and cooperation between MSs


19.7.2016 EN Official Journal of the European Union L 194/1

I

(Legislative acts)

DIRECTIVES

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 6 July 2016

concerning measures for a high common level of security of

THE EUROPEAN PARLIAMENT AND

across the

© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

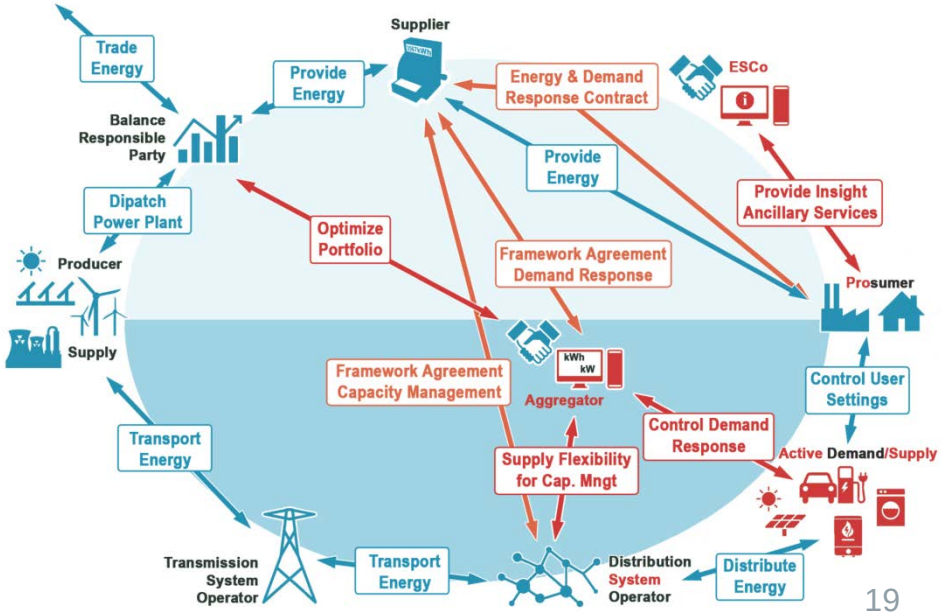
Cornerstones of the NIS Directive

- A National NIS Strategy
- A Cooperation Group to support and facilitate strategic cooperation and exchange of information
- National Computer Security Incident Response Team (CSIRTs) to facilitate effective operational cooperation
- Security and notification requirements for **operators of essential services** and **digital service providers**
- National Competent Authorities, Single Points of Contact and CSIRTs, with tasks related to the security of networks and information systems

© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

NIS Directive: Open Questions

- Which smart grid actors does the Directive apply to – who are providers of essential services and digital services?
- Which incidents should be reported to the competent authority?
- What should minimal security requirements be?



© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

General Data Protection Regulation and Data Protection Impact Assessment

SMART GRID PROTECTION AGAINST CYBER ATTACKS

Article 27

Data protection impact assessment

1. Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Member States shall provide for the controller to carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data.

2. The assessment referred to in paragraph 1 shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Directive, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC

(15) The 'Proposed Data Protection Regulation' replacing Directive 95/46/EC would render Data Protection Impact Assessments mandatory under certain conditions, as a key instrument to enhance data controllers' accountability. In this respect, the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems, albeit itself non-compulsory, will serve the purpose, as an evaluation and decision-making tool, of supporting data controllers in the smart grids sector to comply with a future legal obligation under the 'Proposed Data Protection Regulation'.

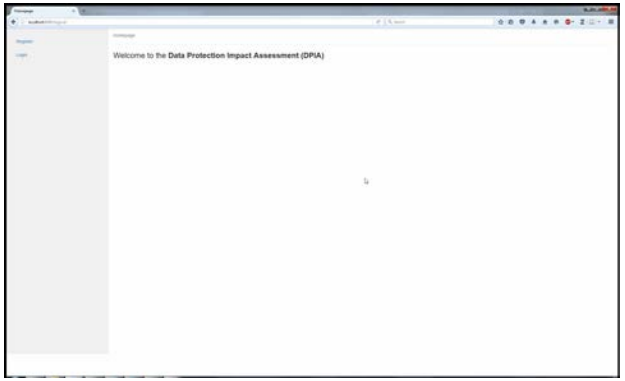
2014/724/EU: Commission Recommendation of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014H0724&from=EN

© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

Data Protection Impact Assessment (DPIA) Template

SMART GRID PROTECTION AGAINST CYBER ATTACKS

- Introduced by the Smart Grid Task Force (EG2)
- Guidance on how to perform privacy impact assessment in the smart grid
  - What data is being collected and how is it processed?
  - What are the risks to rights and freedom of data subjects?
  - What are the measures, privacy targets and controls to ensure privacy?



Nobel Grid
Smart energy for people

© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

Conclusions and Next Steps

- Smart grid stakeholders face two major new concerns:
  - New compliance-related obligations
  - Advanced Persistent ***Cyber-Physical*** Threats
- These threats are likely to become more prevalent and sophisticated
  - Energy systems become more open
  - Barrier to entry is reduced; attacker tools become commoditized
- Enabling **situational awareness** and **resilience** is critical
- Major next steps:
  - Cost-benefit analysis of SPARKS solutions
  - Demonstration of smart grid resilience using the AIT SmartEST lab
  - Provide guidance on the socio-legal aspects of smart grid security

© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

Symposium on Innovative Smart Grid Cybersecurity Solutions

SMART GRID PROTECTION AGAINST CYBER ATTACKS

- Presentations on:
  - Risk assessment, situational awareness, privacy issues, smart grid resilience, …
- Live demonstrations
- **13th – 14th March, 2017 in Vienna**

© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

Questions

Website

https://project-sparks.eu

Follow Us

@eusparks

Email

paul.smith@ait.ac.at

Telephone

+43 (0) 664 883 90031

© The SPARKS Consortium
EU FP7 Programme Contract No. 608224