SMART GRID PROTECTION AGAINST CYBER ATTACKS

The SPARKS Project

1st Stakeholder Workshop

20th May, 2014

Energie Steiermark, Graz

EU FP7 Programme Contract No. 608224

Workshop Objectives

SMART GRID PROTECTION AGAINST CYBER ATTACKS

- SPARKS just started on 1st April, so we're just getting underway
- We present the proposed research activities that will be carried out in the project
- We have time for discussion in the programme
  - We have prepared questions, which will be presented after each talk
  - Are we asking the right questions, if not tell us!?

➢ **A desired outcome of this workshop is that we better understand our stakeholder's needs, which will influence our research**

Programme

Time	Item
09:00 – 09:20	Welcome and roundtable introduction
09:20 – 09:40	Motivation and introduction to the SPARKS project *Dr Paul Smith, AIT Austrian Institute of Technology*
09:40 – 10:20	Smart grid security architectures and standards *Dr Lucie Langer, AIT Austrian Institute of Technology*
10:20 – 11:00	Smart grid security analysis *Dr Paul Smith, AIT Austrian Institute of Technology*
11:00 – 11:30	Intrusion detection for SCADA systems *Dr Kieran McLaughlin, The Queen's University Belfast (CSIT)*
11:30 – 12:00	Coffee break
12:00 – 12:30	Smart meter (gateway) authentication and key management using hardware PUFs *Dr Martin Hutle, Fraunhofer AISEC*
12:30 – 13:00	Smart grid security information analytics *Dr Robert W Griffin, RSA an EMC Company*
13:00 – 14:00	Lunch break

Programme (contd.)

Time	Item
14:00 – 14:30	Cyber-attack resilient control systems *Mr André Teixeira, Royal Institute of Technology (KTH)*
14:30 – 15:00	Legal and social issues *Dr Michael Schmidthaler, Energy Institute at the J. Kepler University Linz*
15:00 – 15:30	SPARKS demonstration activities *Dr Friederich Kupzog, AIT Austrian Institute of Technology*
15:30 – 16:00	Coffee break
16:00 – 16:30	Roundtable discussions and wrap-up

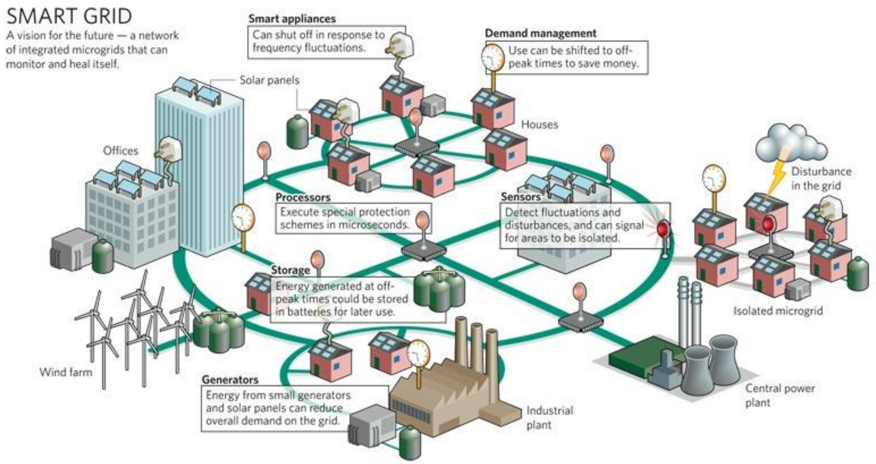
The SPARKS Project: Motivation and Introduction

Paul Smith
paul.smith@ait.ac.at

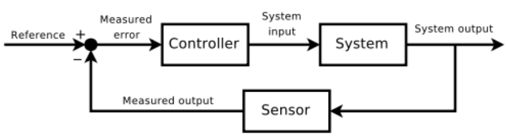
SPARKS Kick-off Meeting
28th April, 2014, Vienna

EU FP7 Programme Contract No. 608224

The Smart Grid and Security



Increased use of ICT systems, e.g., to support *prosumer* communities and advanced energy services



A greater degree of monitoring and automatic control at electricity network edge

Greater use of COTS systems to implement parts of a more open grid

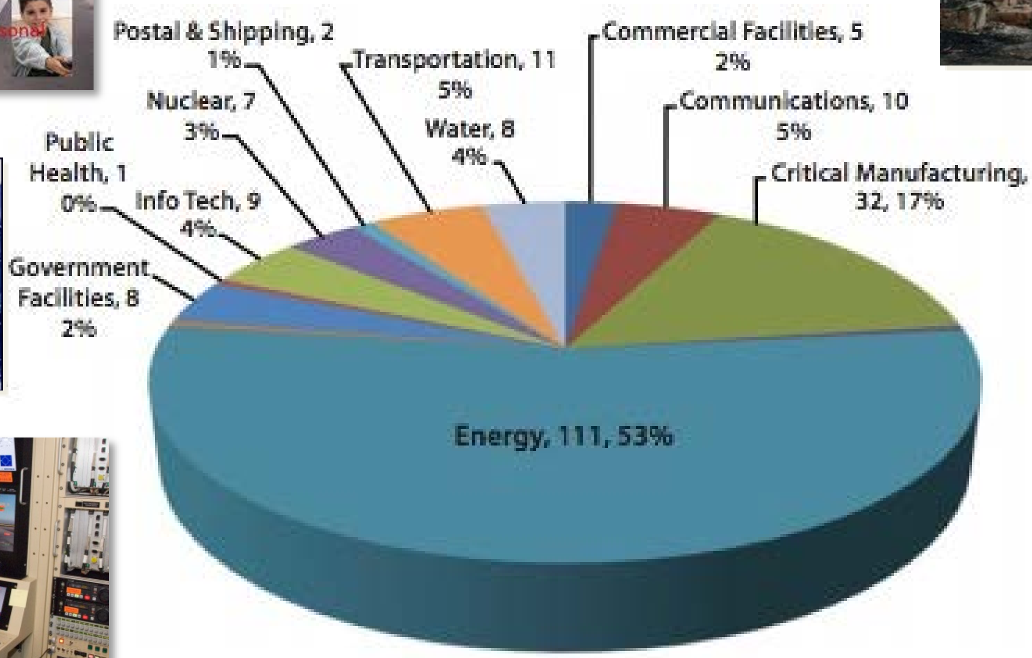

Smart energy meter will not be compulsory

The 'smart energy meter' will not be compulsory in the Netherlands. Minister of economic affairs Maria van der Hoeven backed down after consumer groups raised privacy concerns.

By Wilmer Heck

Privacy concerns emerging from smart meters & increased risks associated with tampering

SCADA-related Incidents



Incidents the US ICS-CERT responded to from Oct 2012-May 2013, Source: ICS-CERT

Topic: Security   Follow via:

Former Pentagon analyst: China has backdoors to 80% of telecoms

Summary: A former Pentagon analyst reports the Chinese government has "pervasive access" to about 80 percent of the world's communications, and it is looking currently to nail down the remaining 20 percent. Chinese companies Huawei and ZTE Corporation are reportedly to blame for the industrial espionage.

By Emil Protalinski for Zero Day | July 14, 2012 -- 18:43 GMT (11:43 PDT)
Follow @emilprotalinski

The Chinese government reportedly has "pervasive access" to some 80 percent of the world's communications, thanks to backdoors it has ordered to be installed in devices made by Huawei and ZTE Corporation. That's according to sources cited by Michael Maloof, a former senior security policy analyst in the Office of the Secretary of Defense, who now writes for WND:

In 2000, Huawei was virtually unknown outside China, but by 2009 it had grown to be one of the largest, second only to Ericsson.

Potential for Significant Financial Damage

28th September 2003, Italy (except Sardinia) blackout started on Sunday at 3 am and lasted up to 24 hours.

Cause: transmission line between Switzerland and Italy was cut by tree, and additional minor events

Blue area: supply restored at 12 o‘clock

White area: still unsupplied at 12 o‘clock

Green area: initially successful restoration failed and blackout continued

Overall economic damage: **1.180m €**

Thereof household damage: **285m €**

Project Information

Partners:

1	**AIT Austrian Institute of Technology GmbH (Coordinator)**	**AIT**	**Austria**
2	Fraunhofer AISEC	AISEC	Germany
3	Centre for Secure Information Technologies - Queen's University Belfast	CSIT	UK
4	Energy Institute at the Johannes Kepler University Linz	EI	Austria
5	EMC Corporation, with the security division RSA	EMC/RSA	Ireland
6	KTH Royal Institute of Technology	KTH	Sweden
7	Landis + Gyr	L+G	Switzerland
8	United Technologies Research Centre	UTRC	Ireland
9	SWW Wunsiedel GmbH	SWW	Germany

Work programme topic: Topic SEC-2013.2.2-3 Protection of smart energy grids against cyber attacks
Proposed duration: 36 months
Requested budget: €3.4M

SPARKS Objectives

1. **Engage Stakeholders & Perform Demonstrations**
   – SPARKS stakeholder group workshops
   – Demonstration of vulnerabilities and protection measures on test beds
   – Contributions towards standards

2. **Analyse Smart Grid Security and Risk**
   – Produce vulnerability, threat and risk assessment methods
   – Develop tools to evaluate smart grid security and resilience

SPARKS Objectives (contd.)

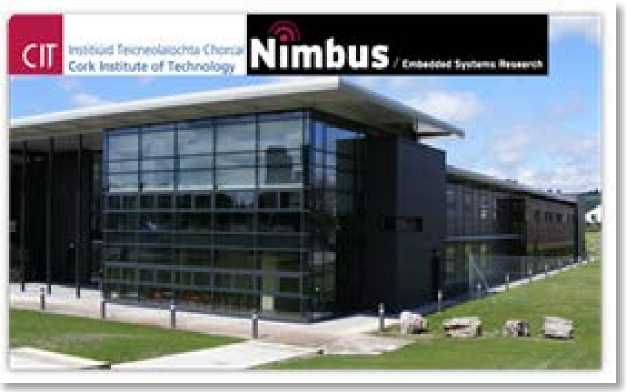
3. **Propose Smart Grid Security Standards**
   - Establish a common and consistent view of a smart grid architectural model
   - Definition of best practices and engagement with standards activities

4. **Develop Security Measures and Procedures**
   - Propose and develop novel security and resilience technologies and measures

5. **Investigate Financial, Legal and Social Issues**
   - Cost assessment, legislative and societal examination of technologies and security measures
   - Development of business cases

SPARKS Demonstration Facilities

SMART GRID PROTECTION AGAINST CYBER ATTACKS



The Nimbus Microgrid

Wunsiedel Smart Grid

AIT SmartEST lab

The SPARKS Stakeholder Group

- Currently, **29** organisations representing different stakeholder 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
  - We are here today for the very first!

Questions?