Critical Information Infrastructure Protection – A Research Perspective

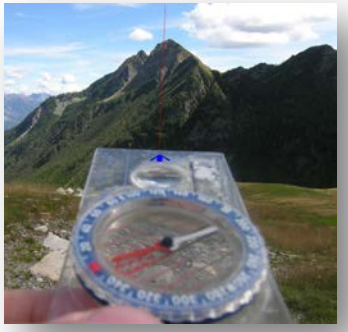
Past, Present and Future Perspectives

Dr Paul Smith
paul.smith@ait.ac.at

Senior Scientist
AIT Austrian Institute of Technology
Safety & Security Department

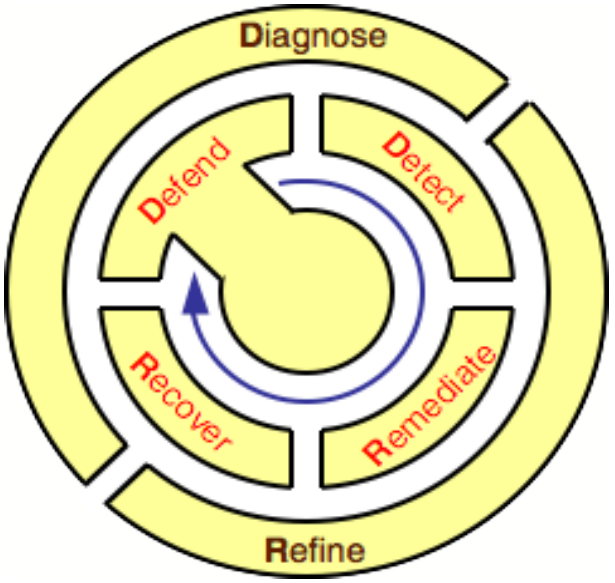
Overview

- **Past**
  - Future Internet Resilience
    - The ResumeNet Project
- **Present**
  - Cyber Security and Resilience of Critical Information Infrastructures
    - The PRECYSE Project
- **Future**
  - Smart Grid Cyber Security and Resilience
    - $(SG)^2$ and The SPARKS proposal



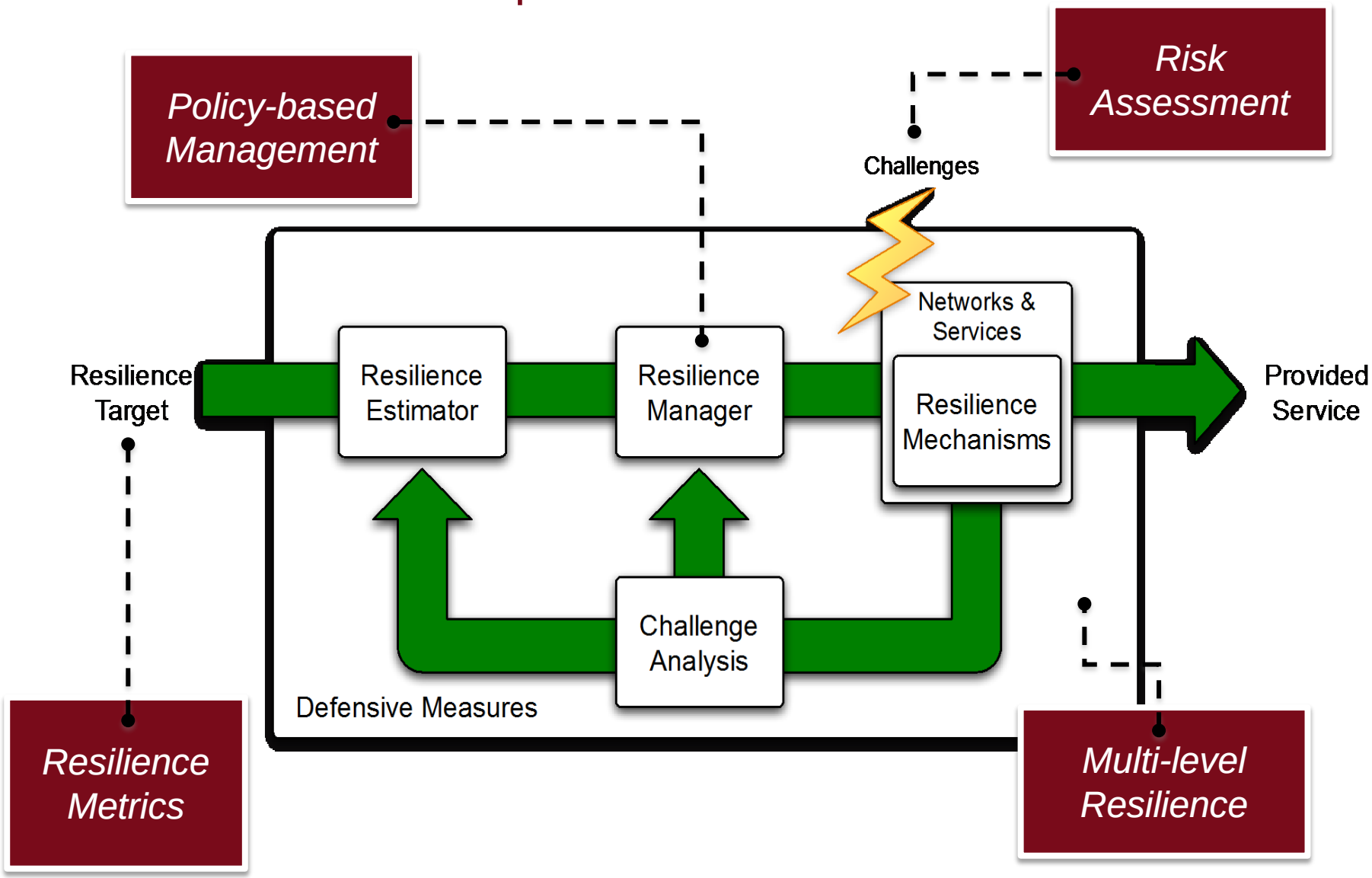
The EU-funded ResumeNet Project

- 3 year project, running from 2008 – 2011
- Investigating a systematic approach to network resilience
- Website: http://www.resumenet.eu
- Real-time Control Loop
  - **D**efend
  - **D**etect
  - **R**emediate
  - **R**ecover
- System Enhancement
  - **D**iagnose
  - **R**efine



The D^2R^2+DR Resilience Strategy

Resilience Control Loop



P. Smith, D. Hutchison, J. P.G. Sterbenz, M. Schöller, A. Fessi, M. Karaliopoulos, C. Lac, and B. Plattner, Network Resilience: A Systematic Approach, IEEE Communications Magazine, vol. 49, no. 7, pp. 88 – 97, July, 2011.

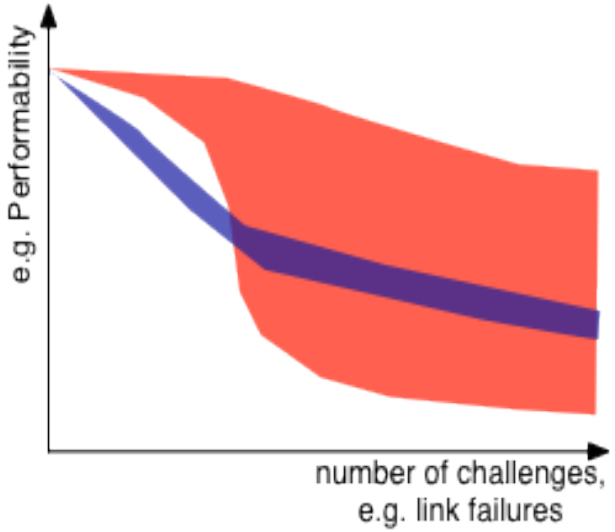
Motivation for Resilience Metrics

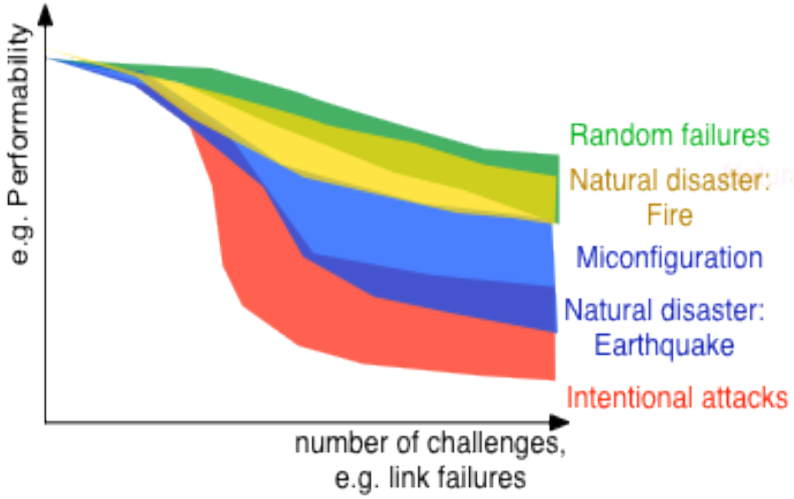
- Resilience metrics are fundamental to enable decision making
  - During risk assessment processes to determine the effect of high-impact challenges
  - To understand the potential resilience benefit of some capital expenditure
  - During network operation to understand the health of the network and the services it supports
  - …

these challenges. At the end we present the detailed feedback received from the stakeholders.
The most important challenges identified were:

- **The lack of a standardised framework**, even for the most basic resilience measurements. There are not that many frameworks available and none of them are globally accepted
- **No standard practices** were identified within the different organisations for the baseline resilience metrics. Different organisations all use their own specific approaches and means of measuring resilience, if they measure at all. This impedes the usage of those metrics for overall assessment of resilience, or the aggregation and composition towards higher levels (such as a national or a pan-European assessment of resilience)
- **Lack of knowledge and awareness of resilience metrics**. This results in severe difficulties for organisations when deploying resilience metrics

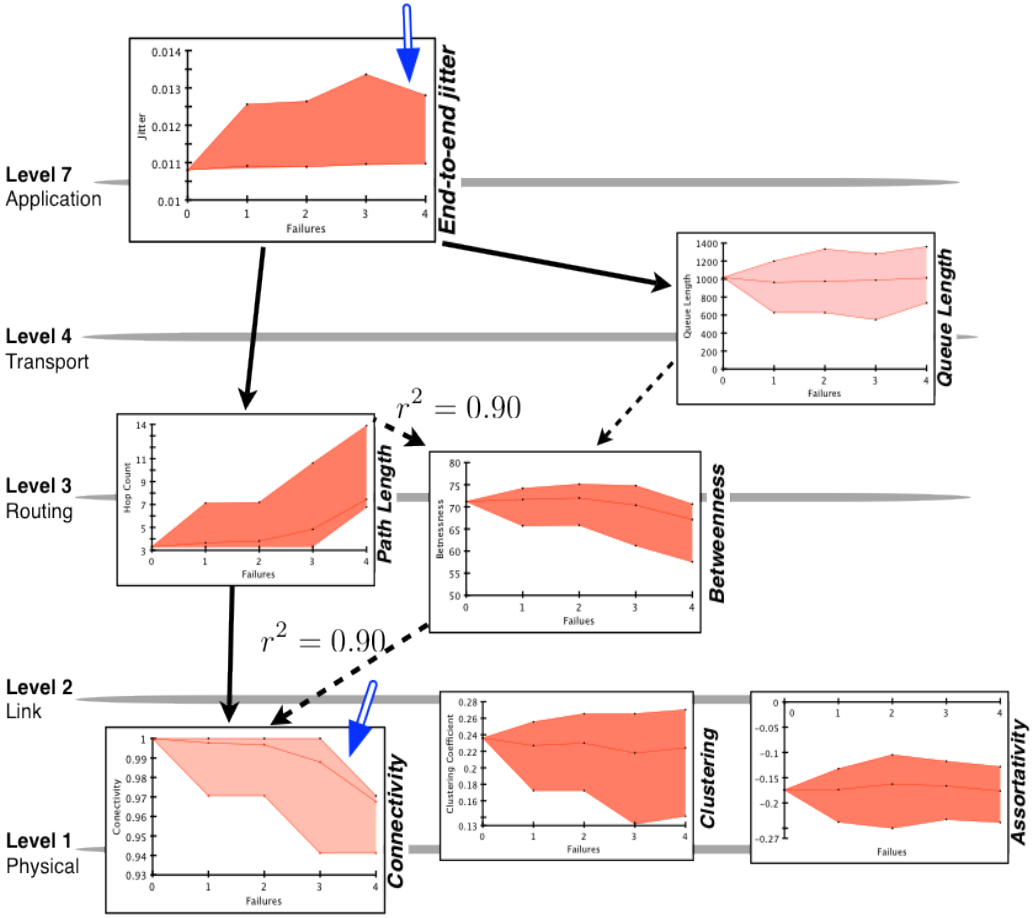
Resilience Metric Envelopes





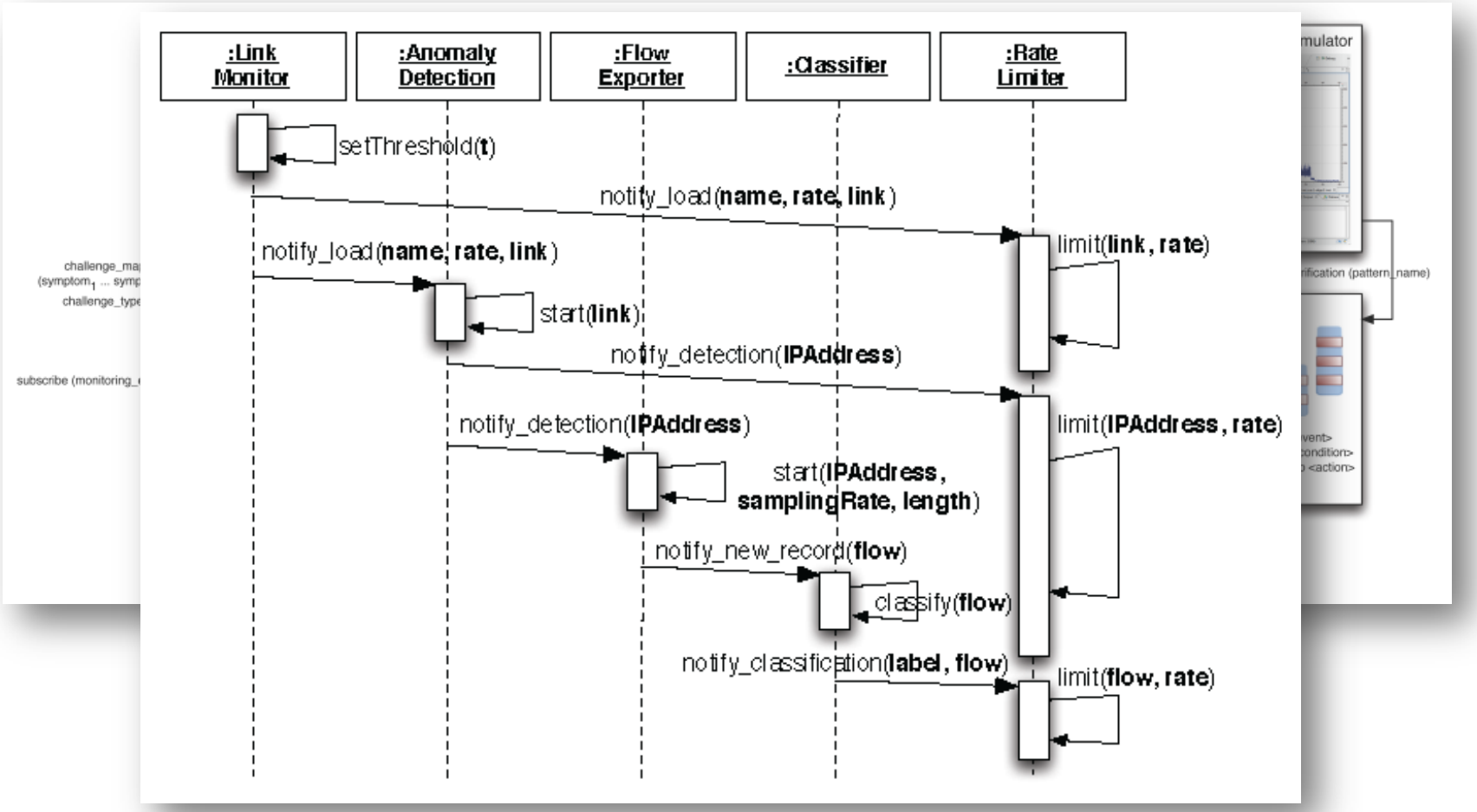
- Comparing resilience based on metric envelopes get a visual explanation of the network degradation process
- Depending on the application domain a more bounded envelope might be preferable
- The effect of various failure sources on the evaluated metric can be revealed

GÉANT2 – Multi-level Metric Envelopes



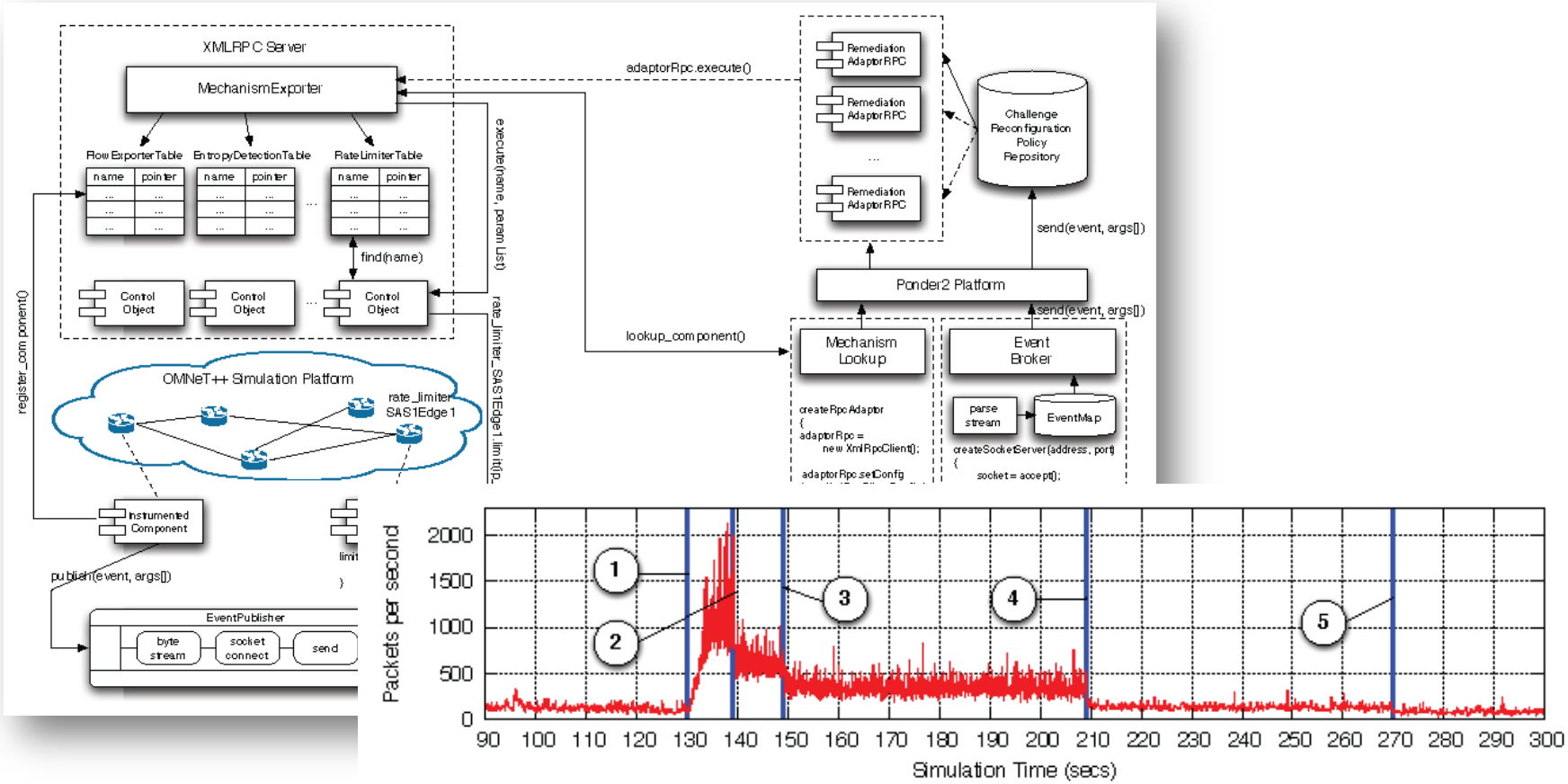
C. Doerr, and J. Martin-Hernandez, “A computational approach to multi-level analysis of network resilience”, DEPEND 2010, Venice, Italy, July 18-25, 2010

Architectures for Network Resilience



A. Schaeffer-Filho, P. Smith, A. Mauthe, D. Hutchison, Y. Yu and M. Fry, "A Framework for the Design and Evaluation of Network Resilience Management," in 13th IEEE/IFIP Network Operations and Management Symposium (NOMS 2012), Maui, Hawaii, USA. April 2012, pp.401-408.

PReSET: Simulating Policy-based Resilience Strategies

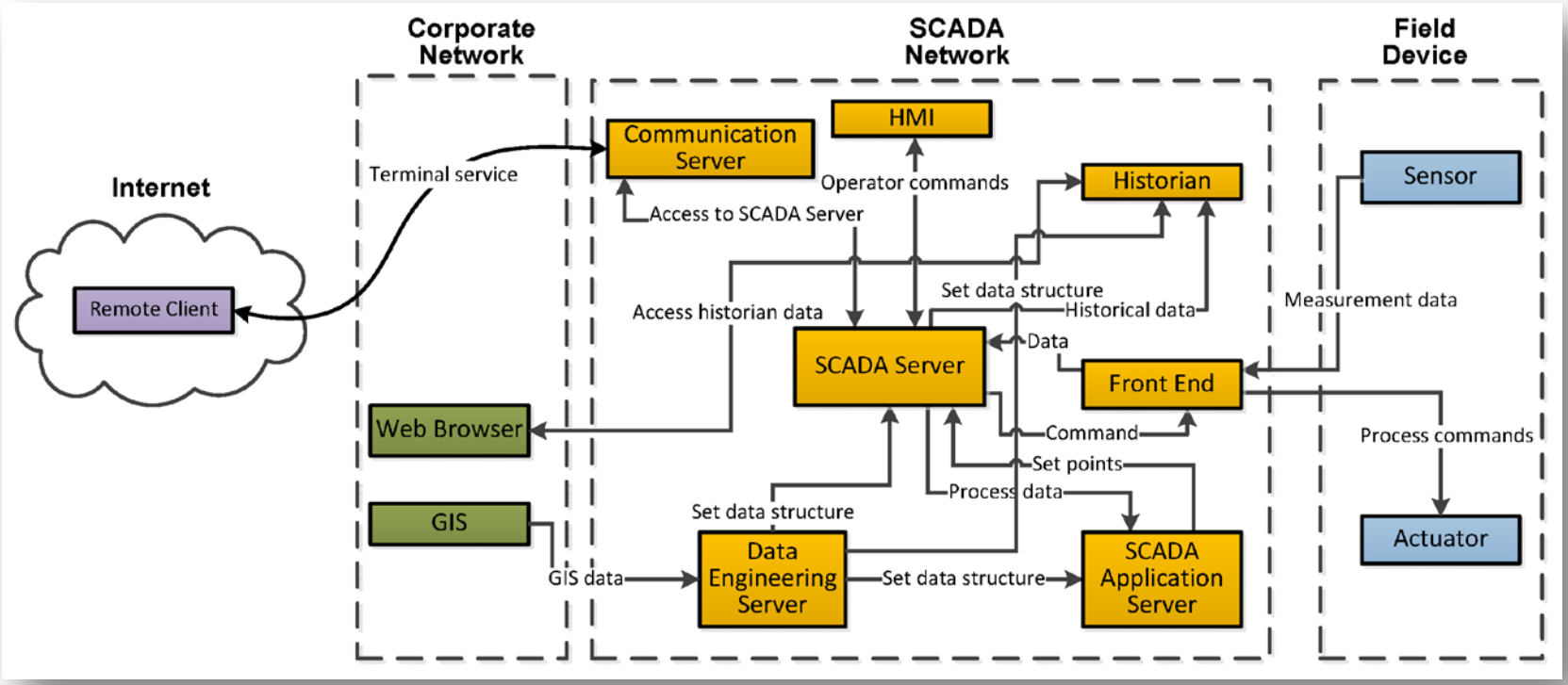


A. Schaeffer-Filho, P. Smith, Y. Yu, A. Mauthe, D. Hutchison, M. Fry, "PReSET: A Toolset for the Evaluation of Network Resilience Strategies," to appear in IFIP/IEEE International Symposium on Integrated Network Management, Ghent, Belgium, May, 2013.

Reflections on ResumeNet

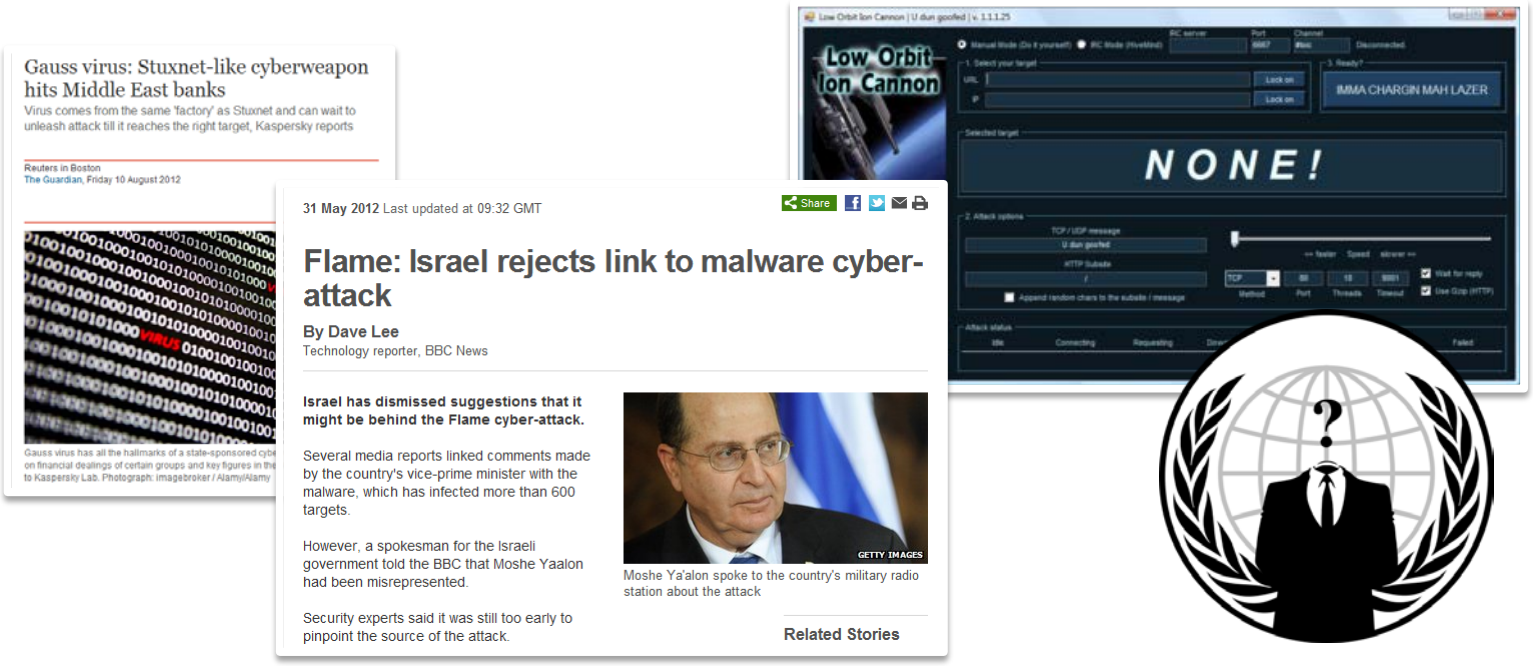
- Overall, we found the D^2R^2+DR resilience strategy and the resilience control loop useful concepts to hang our research efforts on…
- …our endeavours on resilience metrics were well-received by network operators, and the wider community…
- …however, we had a hard time convincing network operators about the value of some aspects of our research:
  - Many considered resilience a “solved problem” – a number of best practices exist that have historically been sufficient for 98% of the problems
  - The autonomic aspects of our work were received with some reservations
- On-going work on Future Internet Resilience in the EINS NoE in JRA7
  - http://www.internet-science.eu/

The Present – Critical Infrastructure Information Systems

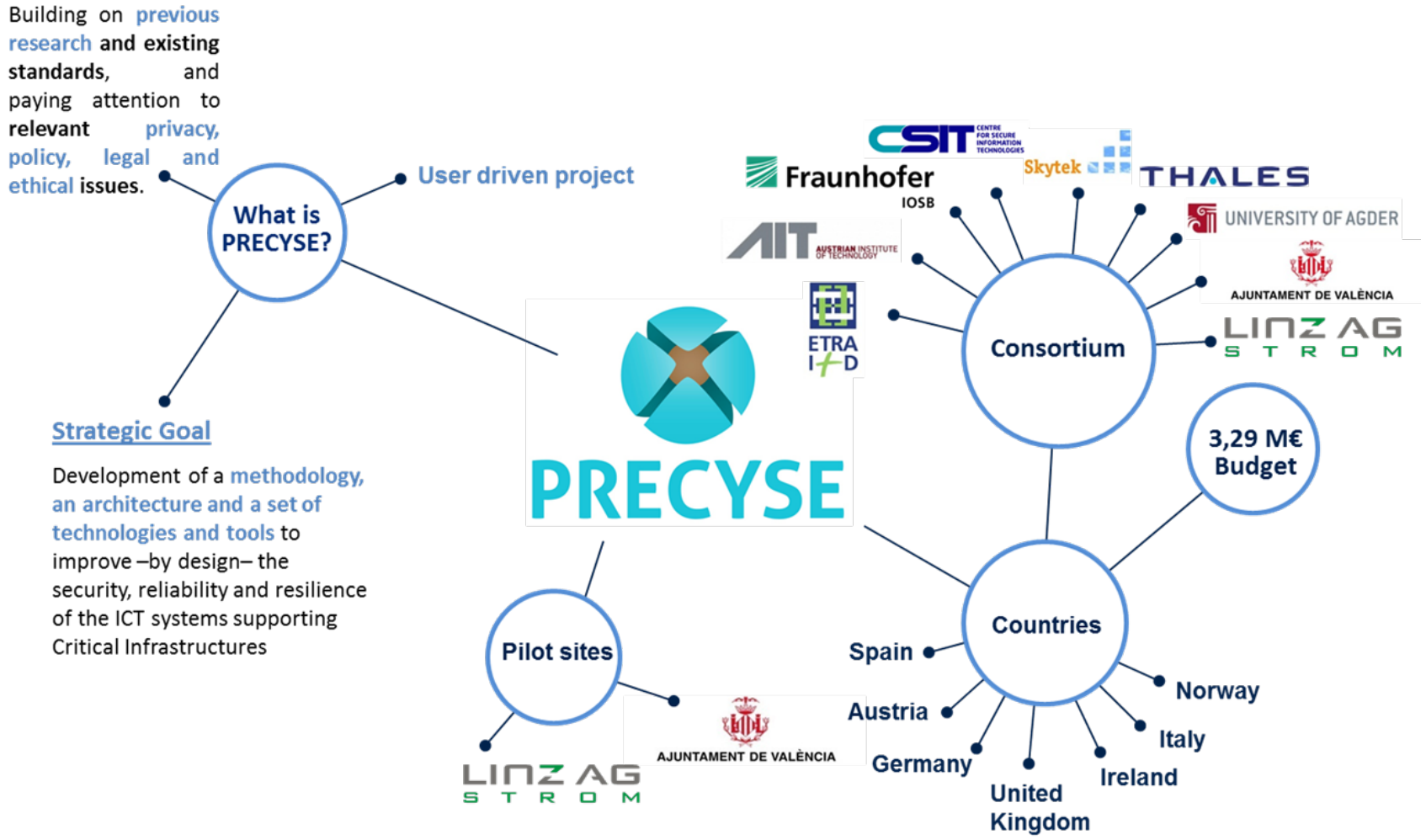


Critical Information Infrastructure Systems Challenges

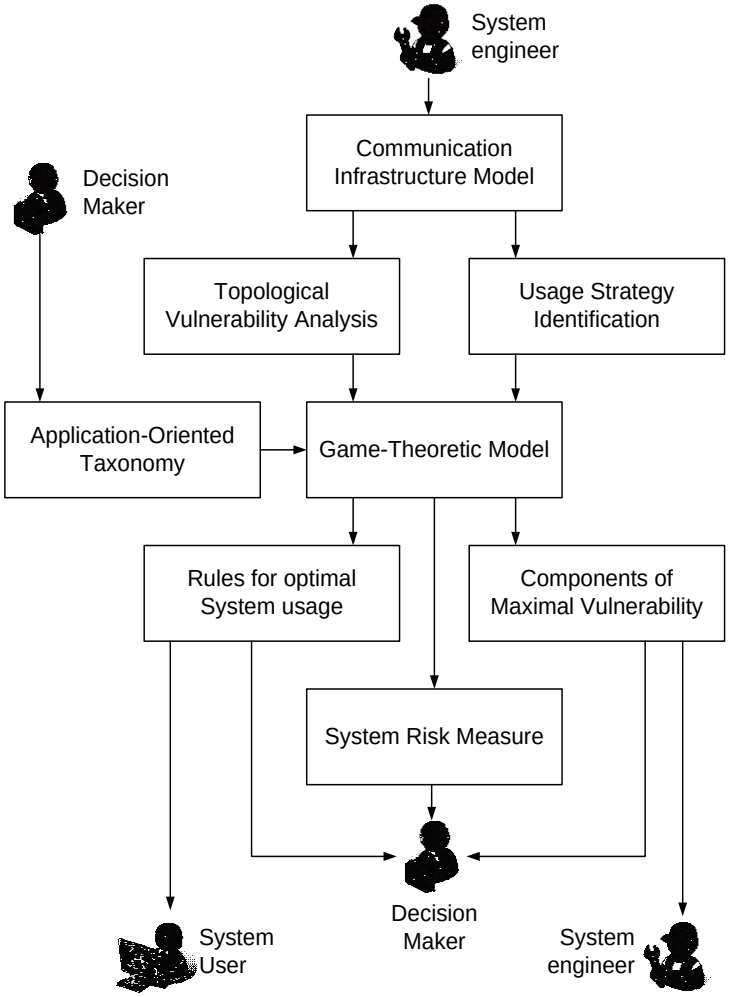
- Critical infrastructures are increasingly dependent on and connected to ICT systems
- Threats are becoming increasingly sophisticated and occurring more often
- Industry lacks tools and methodologies to systematically address this new threat landscape



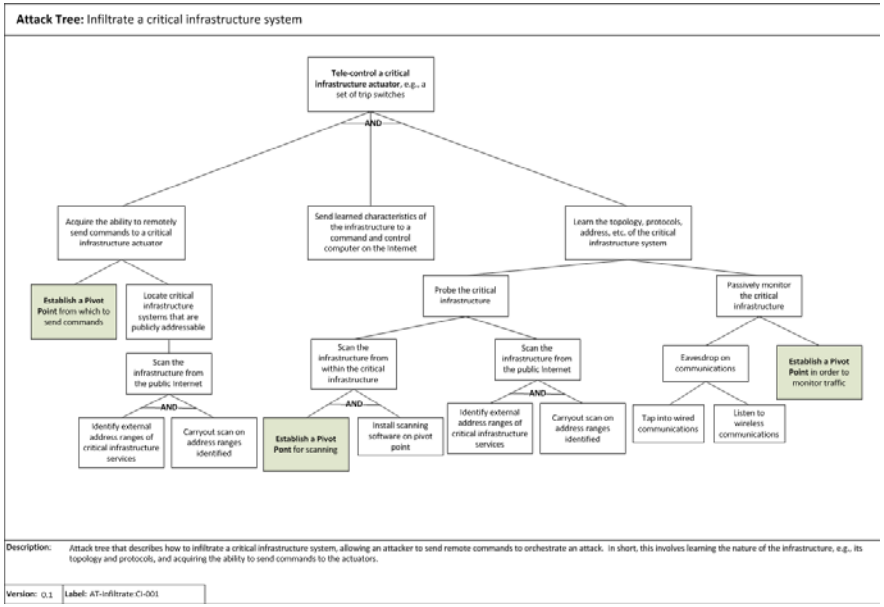
The PRECYSE Project



Security Risk Analysis based on Decision Theory



A challenge for cyber-security risk analysis for smart grids and critical infrastructures is identifying the likelihood of an attack occurring and being successful…



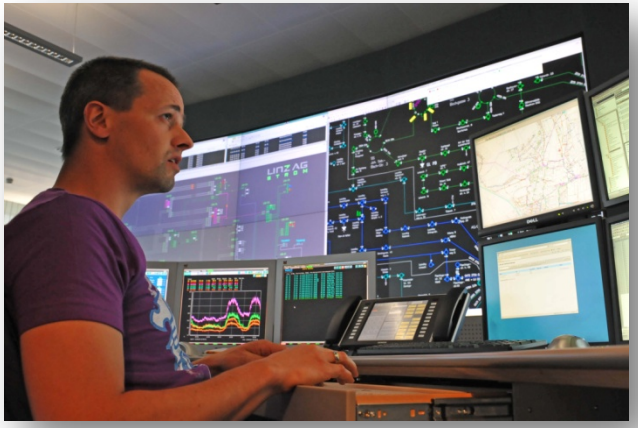
The PRECYSE Project Demonstrators

Traffic control centre in the city of Valencia (Spain)

1.5 million inhabitants, 500 000 vehicles

Energy demonstrator in the city of Linz (Austria)

Power supply and related services for 400 000 inhabitants



The CRISALIS Project

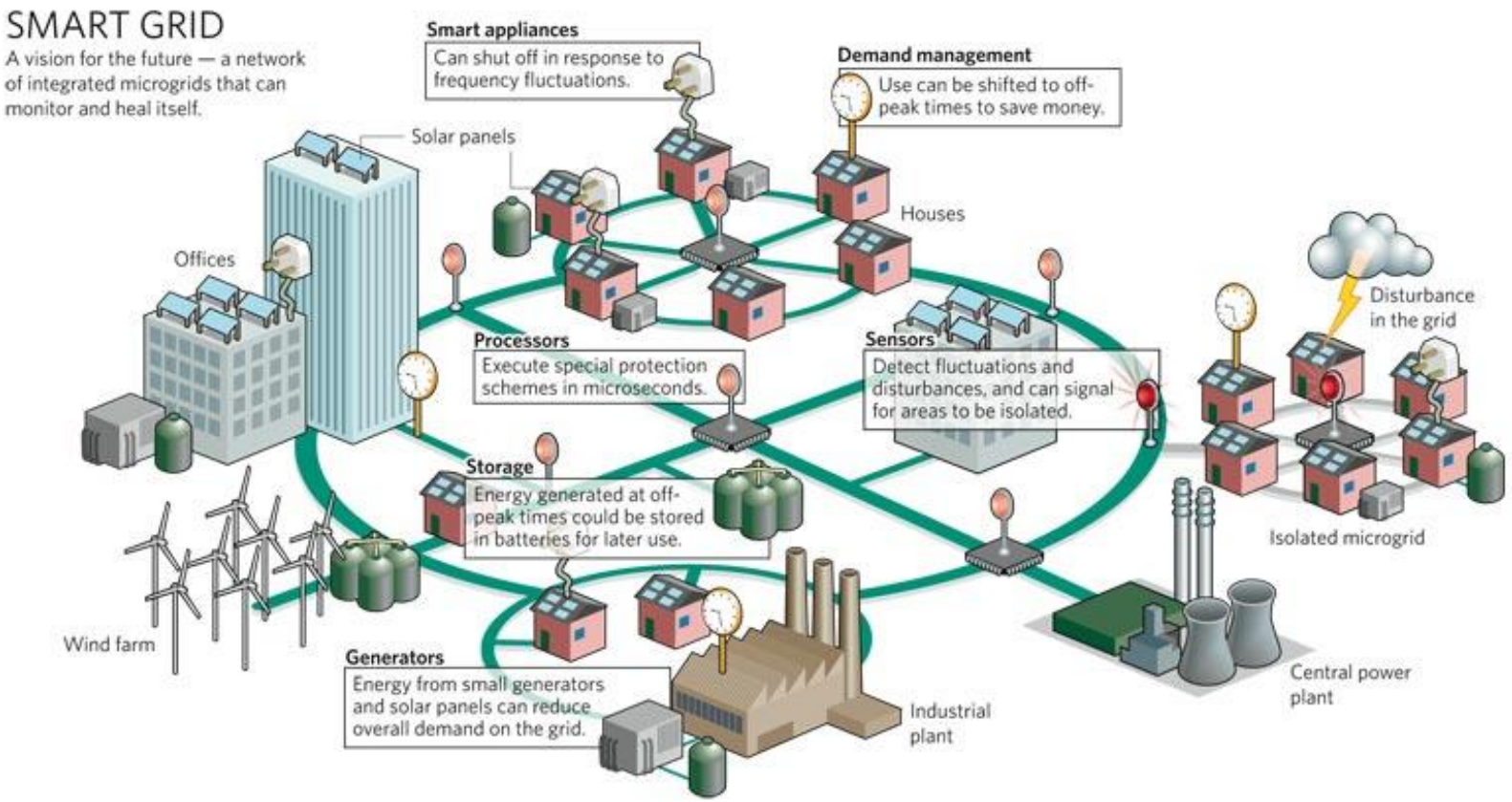
- 3 year EU-funded Project
  - http://www.crisalis-project.eu

Research Objectives:

1. Securing the systems
   - tools to facilitate the *automated* analysis of critical infrastructure environments and the discovery of possible threat vectors
2. Detecting intrusions
   - build new detection techniques that detect targeted, unknown threats
3. Analysing successful intrusions
   - new techniques to facilitate the "post-mortem" analysis of critical infrastructure environments and the involved devices, inc. forensic techniques

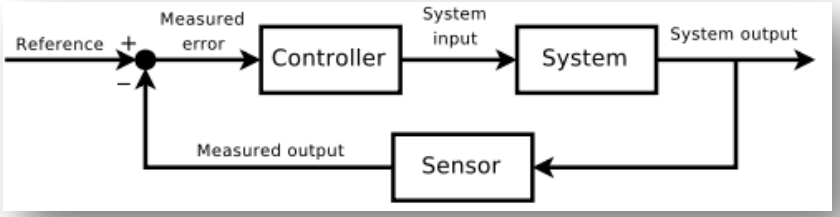
Consortium


The Future – Smart Grids



….a much more open and ICT-dependent power grid

Smart Grid Security Concerns



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

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

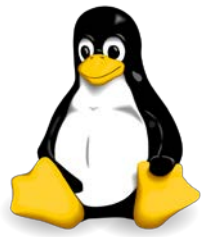

Smart energy meter will not be compulsory

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

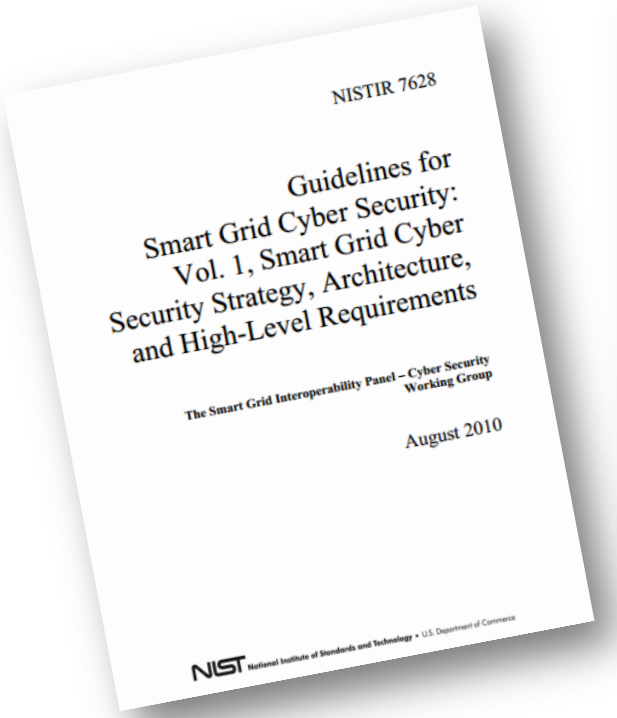
Privacy concerns emerging from smart meters & increased risks associated with tampering

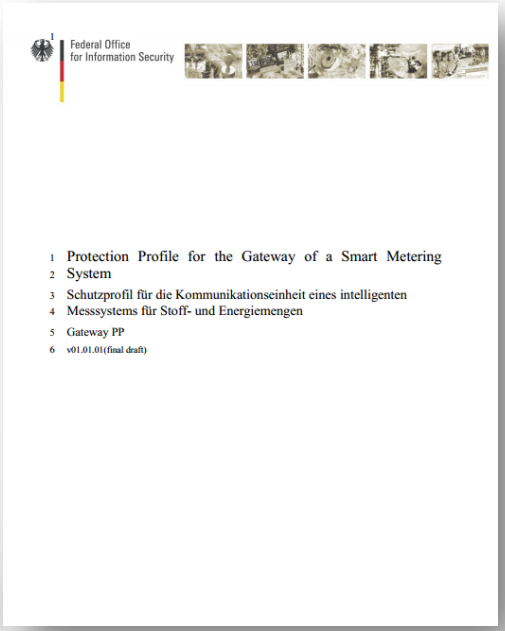
Microsoft



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

Notable Smart Grid Security Guides





Smart Grid Security Guidance (SG)² Project

- Nationally-funded research project
- Project Duration: 2 years, 11/2012 – 11/2014
- Aim to produce practical guidelines for Smart Grid security for Austria
- Partners from research, industry and government:
  - AIT Austrian Institute of Technology
  - Technische Universität Wien
  - SECConsult Unternehmensberatung GmbH
  - Siemens AG, Corporate Technology Österreich
  - LINZ STROM GmbH
  - Energie AG Oberösterreich Data GmbH
  - Innsbrucker Kommunalbetriebe AG
  - Energieinstitut an der JKU Linz GmbH
  - Bundesministerium für Inneres
  - Bundesministerium für Landesverteidigung und Sport

Conclusions

- The ResumeNet project investigated a systematic approach to network resilience, focusing on a future Internet
  - There were some well-received results from industry
    - But other aspects less so, especially around autonomic control
  - Many open issues: energy consumption *vs.* resilience trade-offs, emerging Internet architectures, …

- Critical information infrastructure systems are becoming increasingly open and dependent on ICT systems, thus introducing potential new threats
  - Risk assessment is a challenge in this domain that must be addressed

- Smart grids represent a considerably more connected and open power grid, with significant potential impact, if successfully attacked

- It will not be possible to make smart grids secure against all threats, i.e., we cannot expect a perfect *Defend* phase to be implemented…
  - …therefore approaches to making them resilient are required, including autonomic behaviours?

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

AIT Austrian Institute of Technology

your ingenious partner

Dr Paul Smith
Senior Scientist
Research Area Future Networks and Services
Safety & Security Department

paul.smith@ait.ac.at | +43 664 883 90031 | www.ait.ac.at/it-security