Security for smart Electricity GRIDs

Project type:	Collaborative project – small or medium scale focused research project
Grant agreement no:	607109
Thematic Priority:	FP7-SEC-2013-1
Start date of project:	October 1st, 2014
End date of project:	December 31st, 2017
Coordinator:	TNO, The Netherlands

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 607109

SEGRID

Partners

Distribution System Operators	
Manufacturers	
Knowledge institutes	
Universities	

Towards the Smart Grid

- Renewable and distributed generation
  - European Commission (EC) has set a goal to meet at least 40 percent of the continent's demand for electrical power with renewables by 2030.
- Electric vehicle charging

Distribution System Operators (DSO) will need to make major changes to the way they run the distribution network.

Towards the Smart Grid

New challenges for DSOs

Increase in monitoring and automation

SCADA

Substation automation

RTU

Collection of data

Energy efficiency services for customers

Advanced Metering Infrastructure

Wide area network

WAN

Head-end systems

DTC

Local area network

LAN

Smart Meter

Home area network

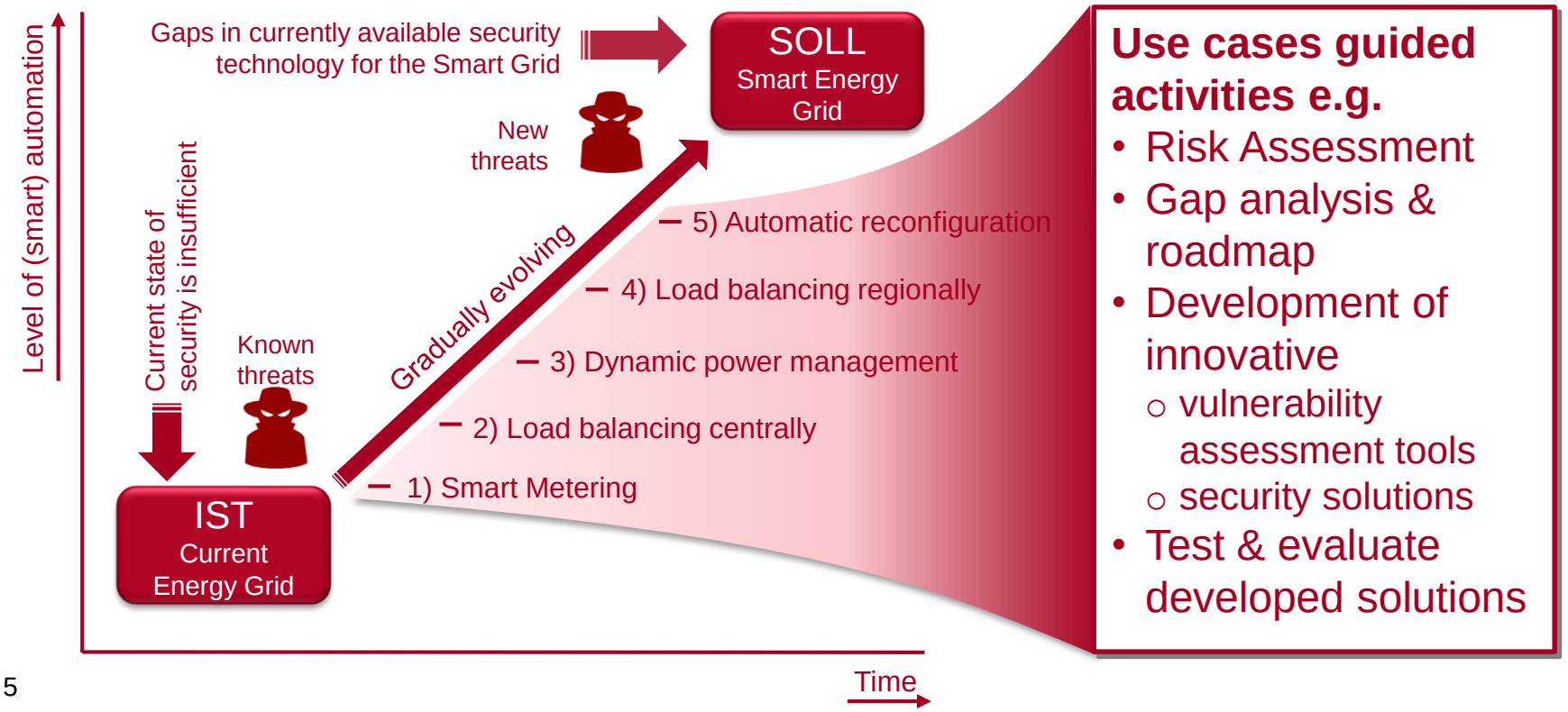
HAN

Increases the Complexity & the Exposure of the electricity grid to Cyber Threats

SEGRID

How did SEGRID approach these challenges?

SEGRID's main objective is to enhance the protection of smart grids against cyber-attacks.



Use cases guided activities e.g.

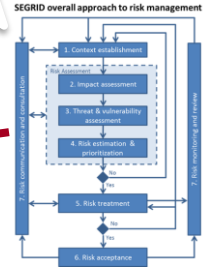
- Risk Assessment
- Gap analysis & roadmap
- Development of innovative
  - vulnerability assessment tools
  - security solutions
- Test & evaluate developed solutions

SEGRID Innovations

Risk management

Periodic

SRMM



Changes in:

- Threat lan
- Infrastruct
- Business c
- Risk appet

Power Grid Infrastructure

Operations

Development

Risk assessment

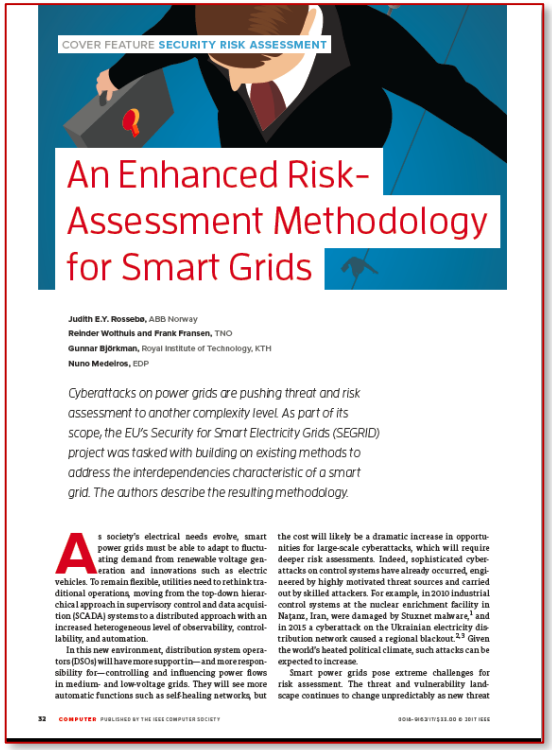
Add new functions to the Power Grid

system

Development process

time

You can read more about SRMM In IEEE Computer; April 2017



COVER FEATURE SECURITY RISK ASSESSMENT

An Enhanced Risk-Assessment Methodology for Smart Grids

Judith E.Y. Rossebø, ABB Norway
Reinder Wolthuis and Frank Pransen, TNO
Gunnar Björkman, Royal Institute of Technology, KTH
Nuno Medeiros, EDP

Cyberattacks on power grids are pushing threat and risk assessment to another complexity level. As part of its scope, the EU's Security for Smart Electricity Grids (SEGRID) project was tasked with building on existing methods to address the interdependencies characteristic of a smart grid. The authors describe the resulting methodology.

As society's electrical needs evolve, smart power grids must be able to adapt to fluctuating demand from renewable voltage generation and innovations such as electric vehicles. To remain flexible, utilities need to rethink traditional operations, moving from the top-down hierarchical approach in supervisory control and data acquisition (SCADA) systems to a distributed approach with an increased heterogeneous level of observability, controllability, and automation.

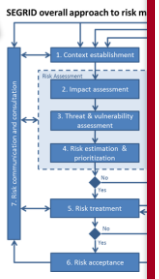
In this new environment, distribution system operators (DSOs) will have more support in—and more responsibility for—controlling and influencing power flows in medium- and low-voltage grids. They will see more automatic functions such as self-healing networks, but the cost will likely be a dramatic increase in opportunities for large-scale cyberattacks, which will require deeper risk assessments. Indeed, sophisticated cyberattacks on control systems have already occurred, engineered by highly motivated threat sources and carried out by skilled attackers. For example, in 2010 industrial control systems at the nuclear enrichment facility in Natanz, Iran, were damaged by Stuxnet malware,[1] and in 2015 a cyberattack on the Ukrainian electricity distribution network caused a regional blackout.[2,3] Given the world's heated political climate, such attacks can be expected to increase.

Smart power grids pose extreme challenges for risk assessment. The threat and vulnerability landscape continues to change unpredictably as new threat

0018-9162/17/$33.00 © 2017 IEEE

SEGRID Innovations

Risk management



Security solutions & technologies developed by SEGRID

- Trusted Platform
- Resilient SCADA systems
- IDS and authentication in mesh networks
- Robustness and scalable (D)TLS
- Resilient communication infrastructure
- Key management for group software distribution
- Privacy by design - privacy design patterns
- Prevention of Injection Attacks in DBMS

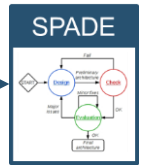
- Vulnerability Detection and Correction with WAP

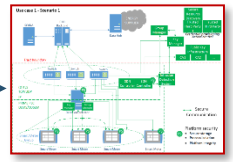
Operations

Power G
Infrastruc

Development

Risk assessment





Security & Privacy Architecture with *SEGRID security solutions*

Add new functions to the Power Grid

Development process

new system

Cost Assessment

time

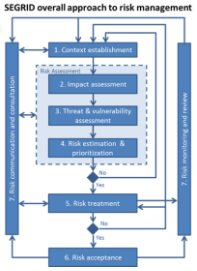
Security & Privacy Architecture DEsign

SEGRID Innovations

Risk management

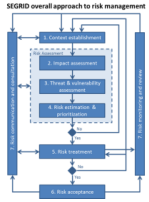
Periodic update

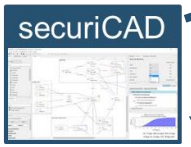
Toward dynamic / real-time risk management



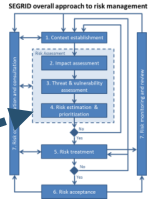
Changes in:

- Threat landscape
- Infrastructure
- Business objectives
- Risk appetite





use



automatic model creation & updating

Power Grid Infrastructure

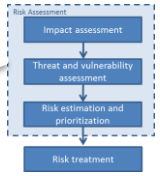
Power Grid Infrastructure

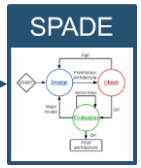
Power Grid Infrastructure

Operations

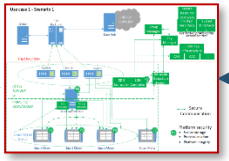
Development

Risk assessment

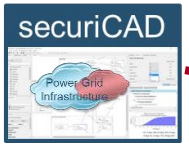




Security & Privacy Architecture with *SEGRID security solutions*



check



modelled

Vulnerability assessment tool (based on CySeMol, KTH)

Add new functions to the Power Grid

Development process

new system

time

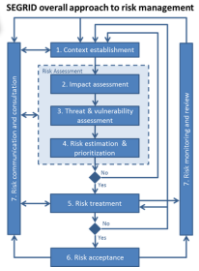
SEGRID Innovations

Risk management

Periodic update

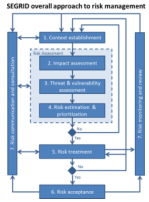
Toward dynamic / real-time risk management

Security Operations



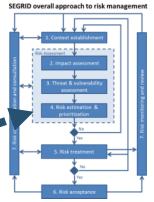
Changes in:

- Threat landscape
- Infrastructure
- Business objectives
- Risk appetite



securiCAD

use



automatic model creation & updating

Vulnerability Management, Security Monitoring & Incident Response

Power Grid Infrastructure

Power Grid Infrastructure

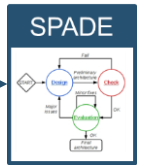
Power Grid Infrastructure

Operations

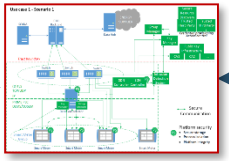
Development

Risk assessment

SPADE



Security & Privacy Architecture with *SEGRID security solutions*



check

securiCAD

modelled

integration

Operational Security Capability Model

Add new functions to the Power Grid

Development process

new system

time

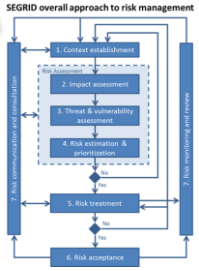
SEGRID Innovations

Risk management

Periodic update

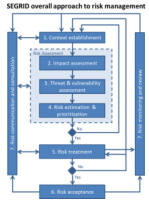
Toward dynamic / real-time risk management

Security Operations



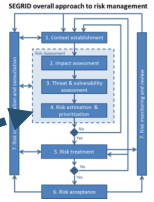
Changes in:

- Threat landscape
- Infrastructure
- Business objectives
- Risk appetite



securiCAD

use



automatic model creation & updating

Vulnerability Management, Security Monitoring & Incident Response

Power Grid Infrastructure

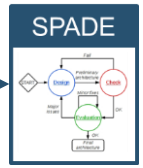
Power Grid Infrastructure

Power Grid Infrastructure

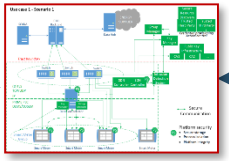
Operations

Development

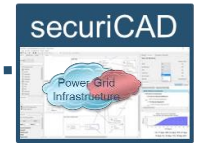
Risk assessment



Security & Privacy Architecture with *SEGRID security solutions*



check



modelled

integration

Add new functions to the Power Grid

Development process

new system

time

SEGRID Innovations

SEGRID Whitepaper

SEGRID Summit
October 2nd, 2017

Questions

Mail: info@segrid.eu
Website: www.segrid.eu
Telephone: +31 8886 67758

Project Coordinator:

TNO innovation for life

Reinder Wolthuis
+31 6 5191 33 79
reinder.wolthuis@tno.nl

Technical Coordinator:

TNO innovation for life

Frank Fransen
+31 6 53 72 49 00
frank.fransen@tno.nl