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
Duration:	39 months
Coordinator:	TNO, The Netherlands

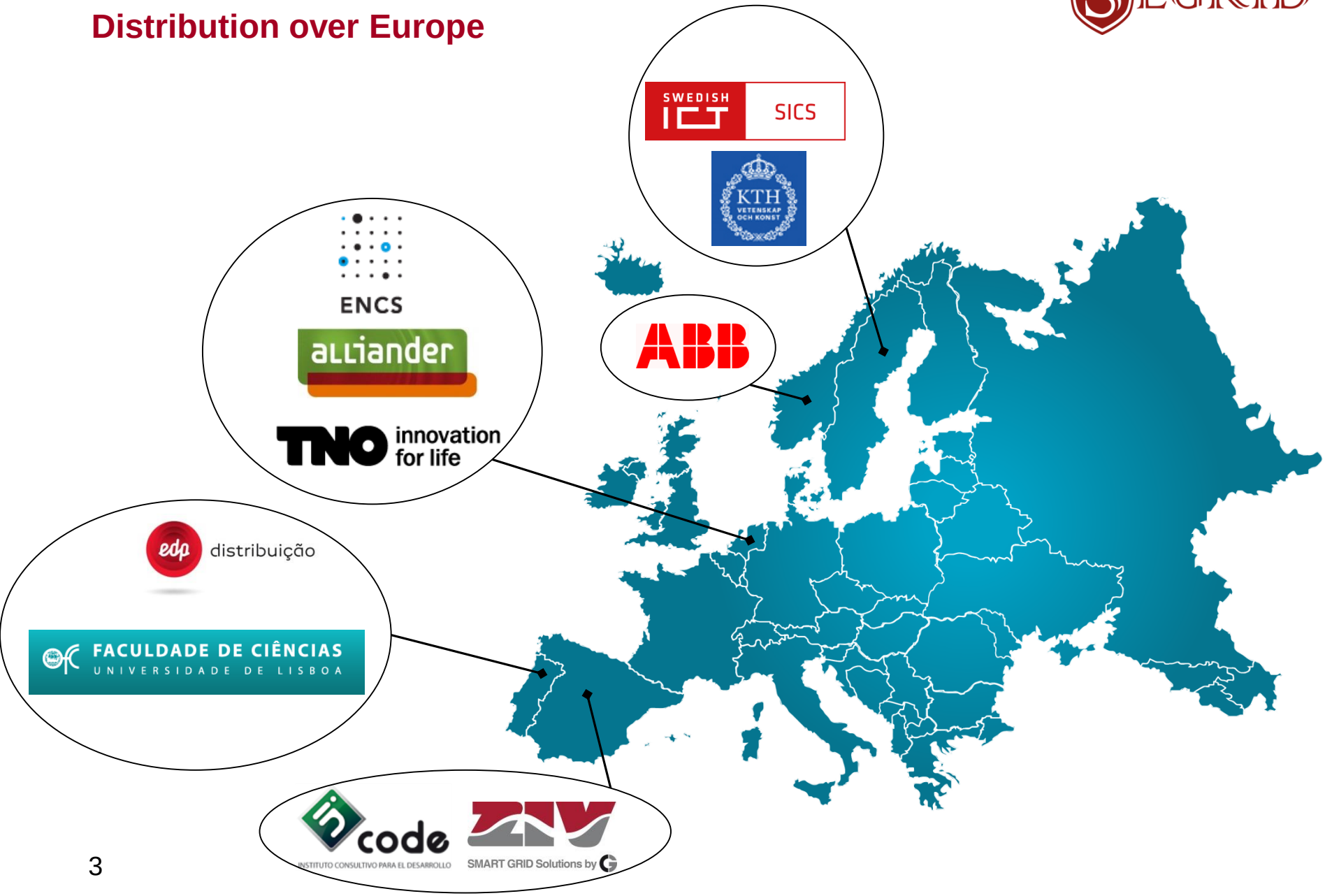
SEGRID is supported by the EU FP7 Programme under Contract No. 607109

Partners

Distribution System Operators	alliander, edp distribuição
Manufacturers	ABB, ZIV SMART GRID Solutions by
Knowledge institutes	TNO innovation for life, SWEDISH ICT SICS, incode INSTITUTO CONSULTIVO PARA EL DESARROLLO, ENCS
Universities	KTH VETENSKAP OCH KONST, FACULDADE DE CIÊNCIAS UNIVERSIDADE DE LISBOA

SEGRID

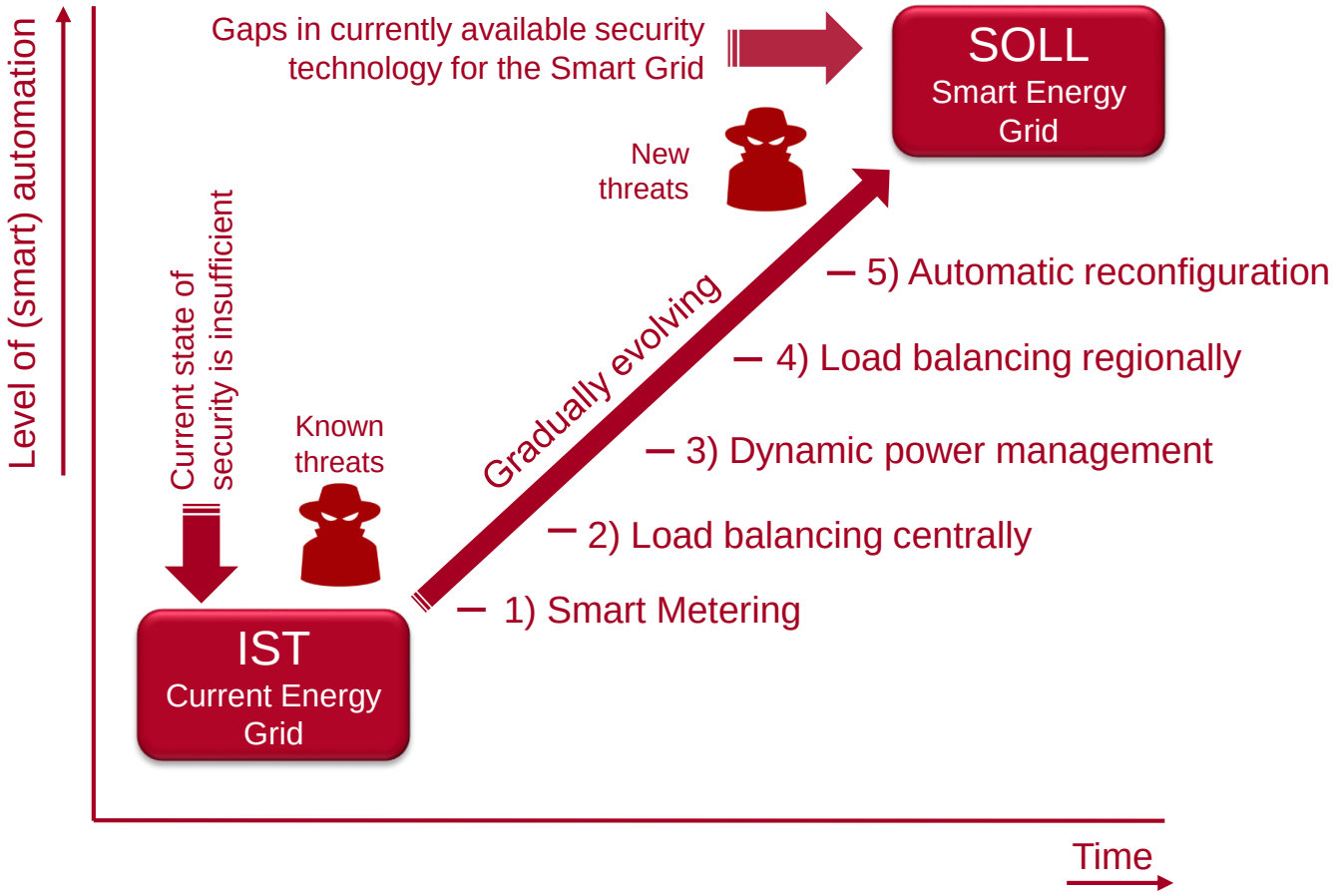
Distribution over Europe



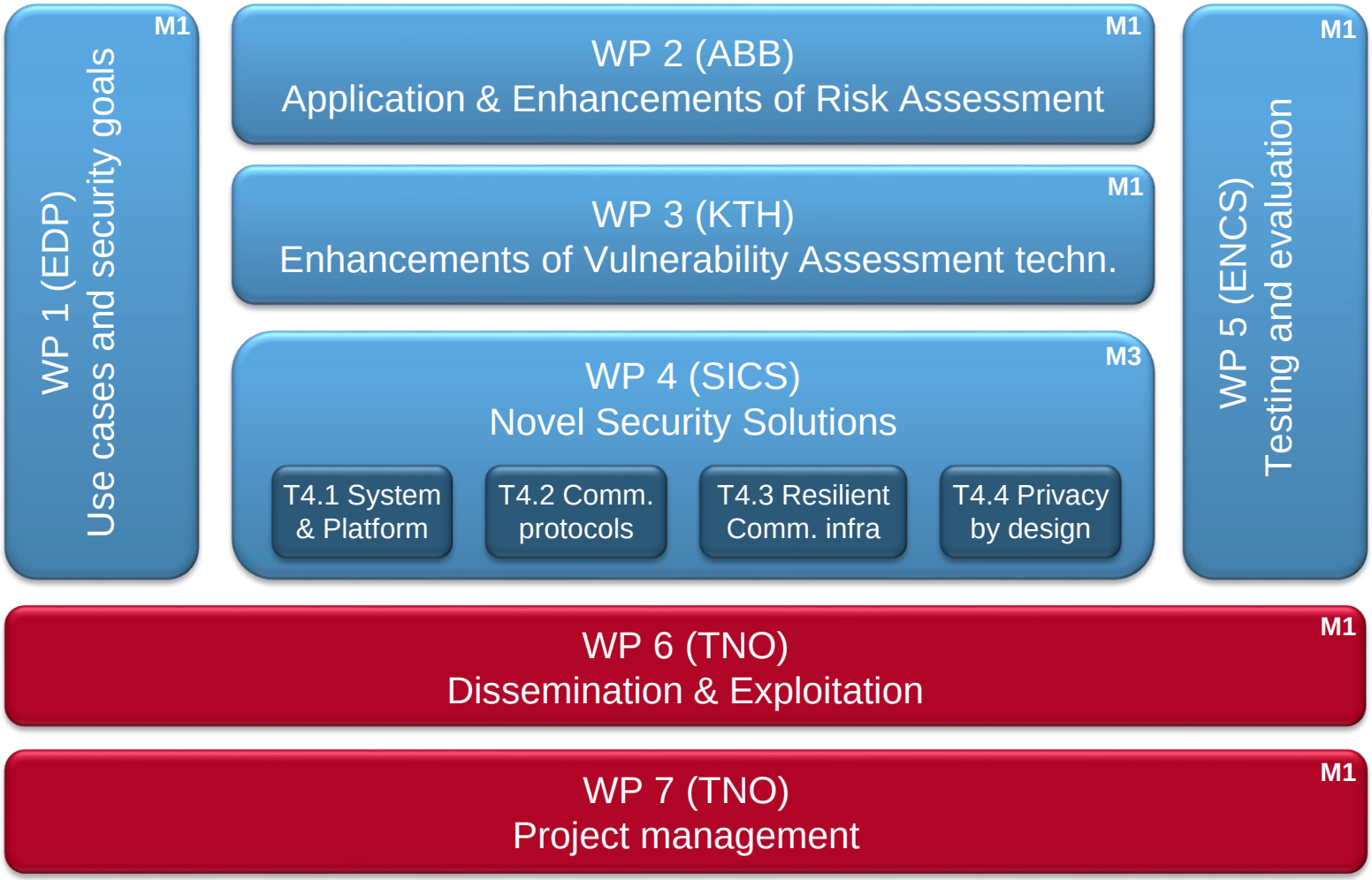
Project targets

1. Identifying threats and potential future cyber-attack pathways, for the SEGRID use cases;
2. Determining the gap between currently available security for smart grids and what is needed for the SEGRID use cases;
3. Developing the necessary new security methods and measures for privacy, communication and system security in smart grids;
4. Building up a realistic test environment (Security Integration Test Environment, SITE) to test and verify new security methods and measures;
5. Evaluating and improving current risk management methodologies in order to make them optimally suited to identify and address the key risk factors of smart grids of 2020;
6. Feeding the established results from the SEGRID project into European and global standardisation bodies, industry groups and smart grid suppliers.

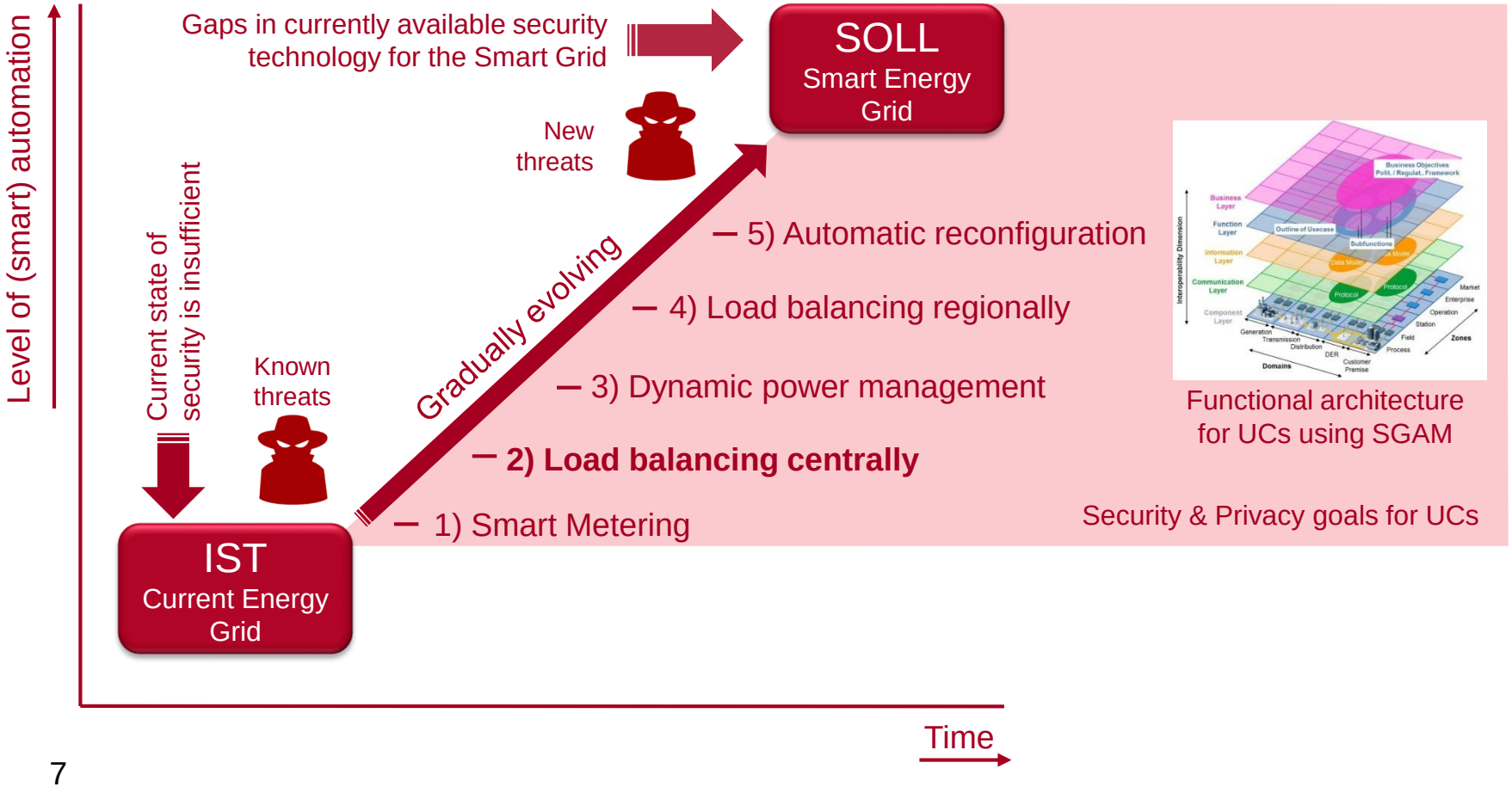
Storyline


Level of (smart) automation
Gaps in currently available security technology for the Smart Grid
SOLL
Smart Energy Grid
New threats
Current state of security is insufficient
Known threats
Gradually evolving
5) Automatic reconfiguration
4) Load balancing regionally
3) Dynamic power management
2) Load balancing centrally
1) Smart Metering
IST
Current Energy Grid
Time

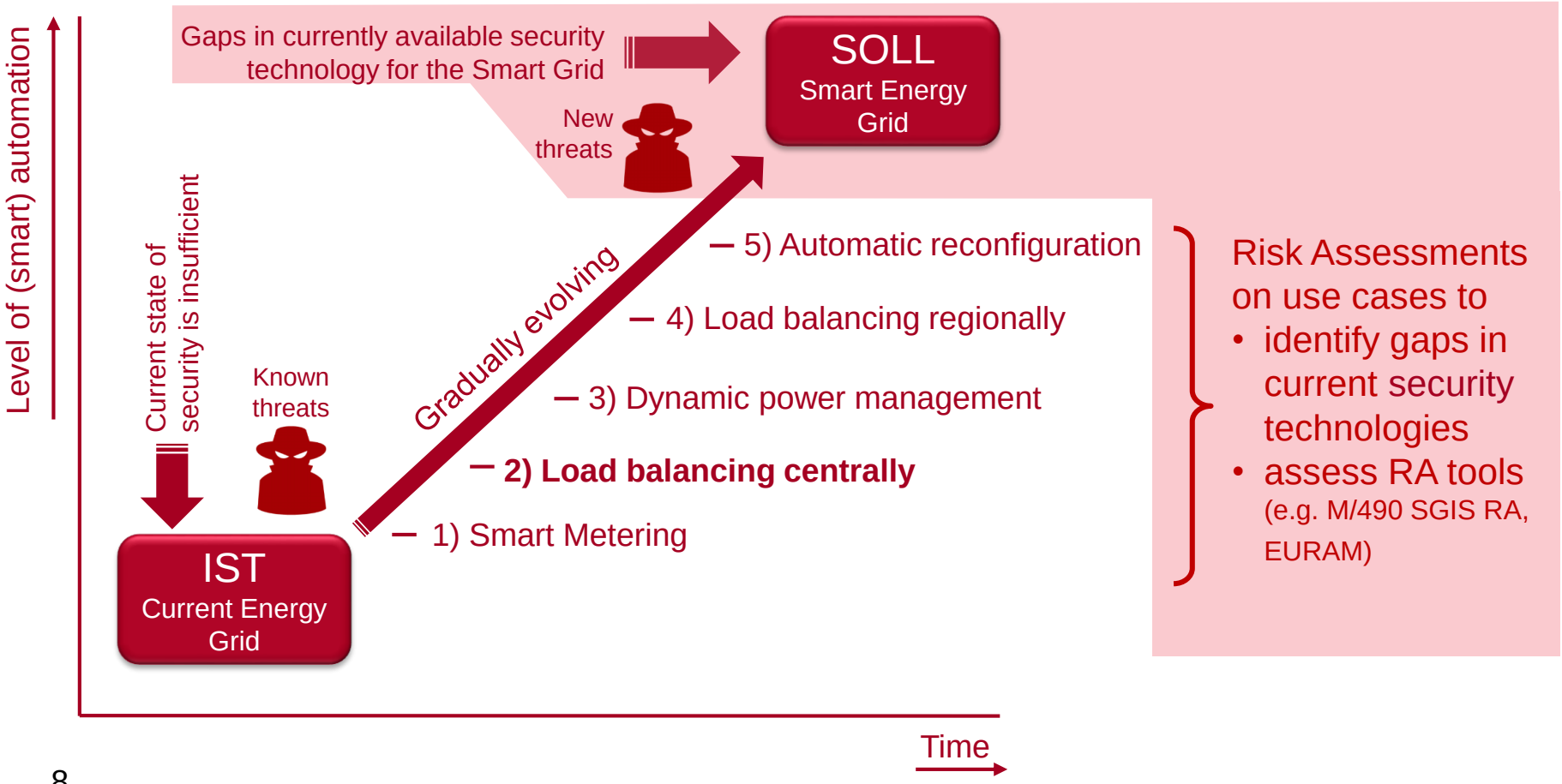
Work package structure



Use cases and security goals



Application & enhancement of Risk assessment



Develop vulnerability assessment technologies

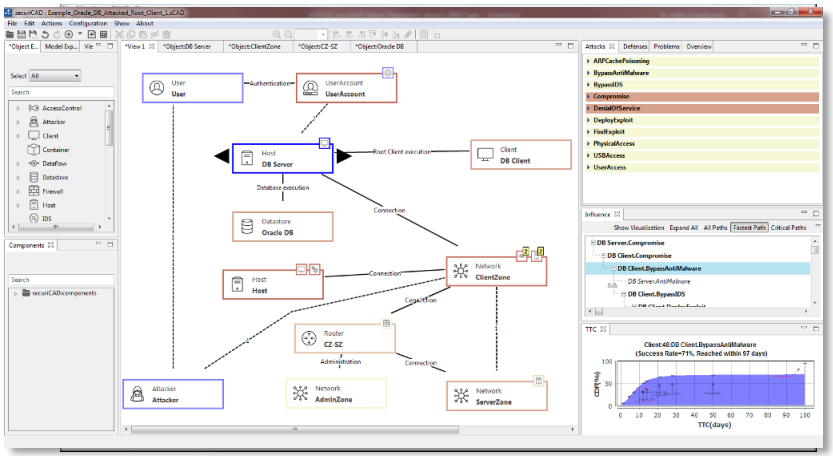
WP3 (KTH)
Vulnerability assessment tools

- T3.1 Enhancement of CySeMol
- T3.2 Automatic model generation
- T3.3 software vulnerability discovery & diagnosis

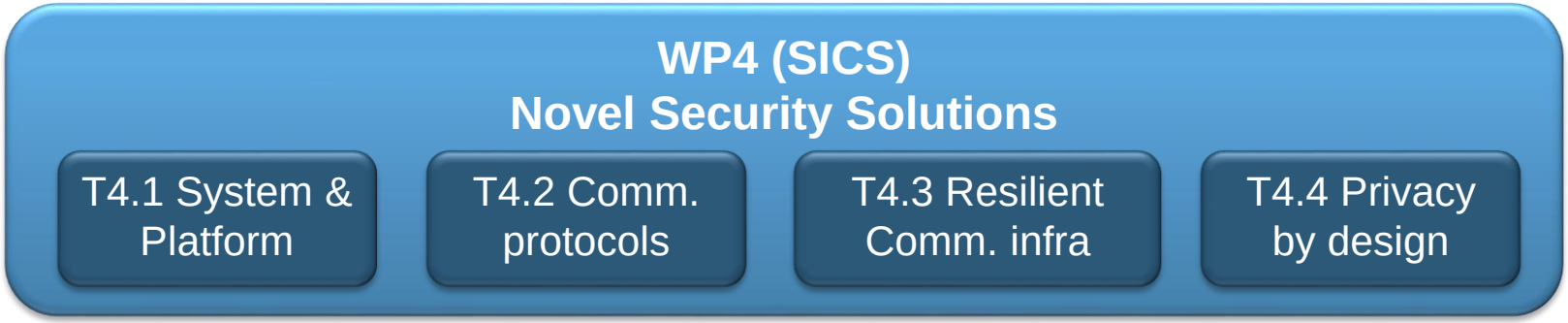
Cyber Security Modelling Language (~~CySeMoL~~ SecuriCAD)

- Developed by KTH in FP7 Viking
- Tool for assessing vulnerabilities in system architecture (using probabilistic attack graphs)

- SEGRID has enhanced the tool by
  - extending functionality more towards smart grids (e.g. use cases), and
  - automatic model generation



Develop novel security solutions (to fill some of the gaps)



- Design the *SEGRID Security and Privacy Architecture*, that includes security life-cycle management
- Current WP4 activities on novel security solutions
  a) Trusted Platform
  b) Resilient SCADA systems
  c) IDS and authentication in mesh networks
  d) Resilient communication infrastructure
  e) Robustness and scalable (D)TLS-based communication
  f) Key management for group software distribution
  g) Privacy by design

Develop novel security solutions (to fill some of the gaps)

WP4 (SICS)
Novel Security Solutions

- T4.1 System & Platform
- T4.2 Comm. protocols
- T4.3 Resilient Comm. infra
- T4.4 Privacy by design

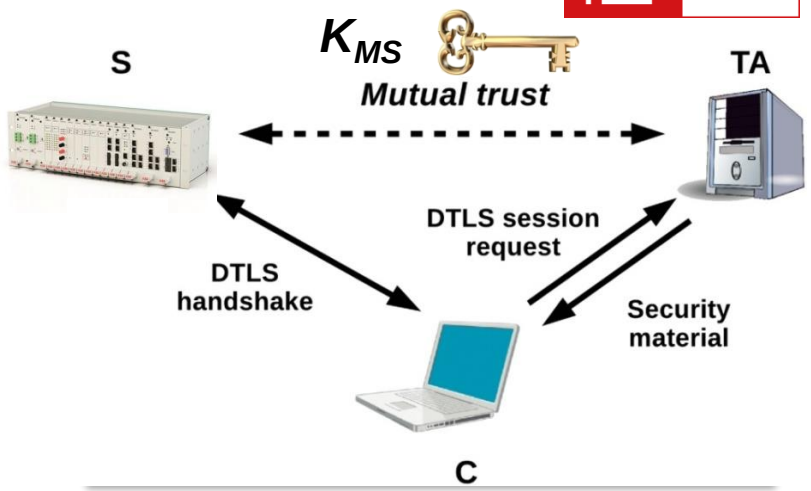
Robustness and scalable (D)TLS-based communication

SWEDISH ICT SICS

Problem:

- (D)TLS handshake (cookie exchange) is vulnerable for DoS attack.
- Pre-shared key establishment scales poorly

- SICS developed a solution that resolves both problems



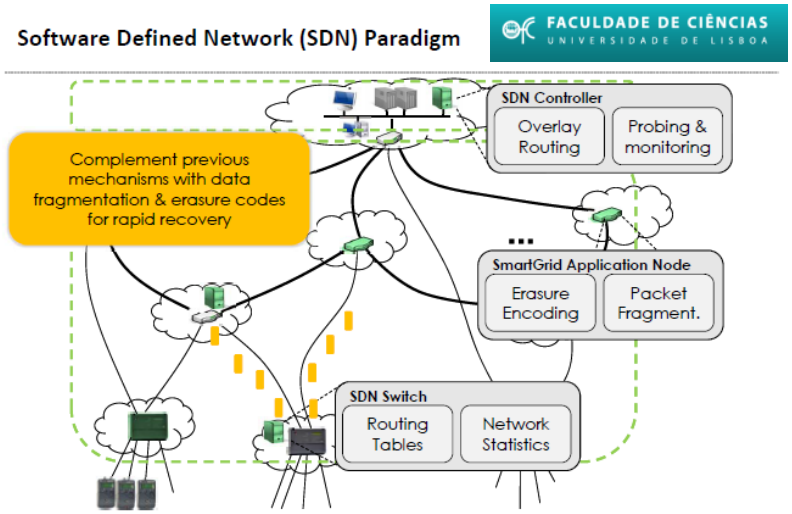
Develop novel security solutions (to fill some of the gaps)

WP4 (SICS)
Novel Security Solutions

- T4.1 System & Platform
- T4.2 Comm. protocols
- T4.3 Resilient Comm. infra
- T4.4 Privacy by design

Resilient comm. infrastructure

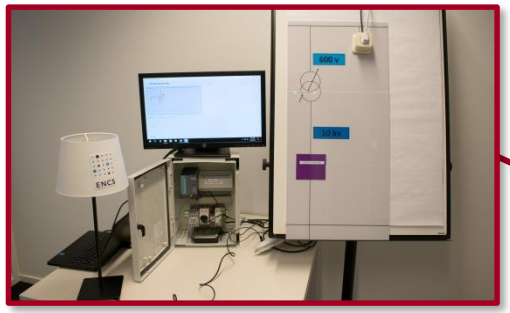
- Goal: Develop a number of mechanisms to support resilient communication infrastructure under attack and/or with accidental failures.
- SEGRID is developing technology for adaptive probing and monitoring to select the “best” available routes enabling rapid reaction after failures.
- Scope: SCADA ⇔ Primary Substation

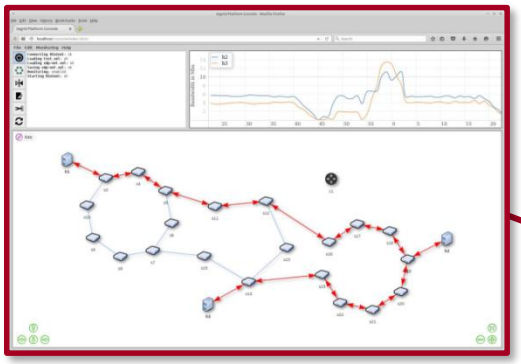


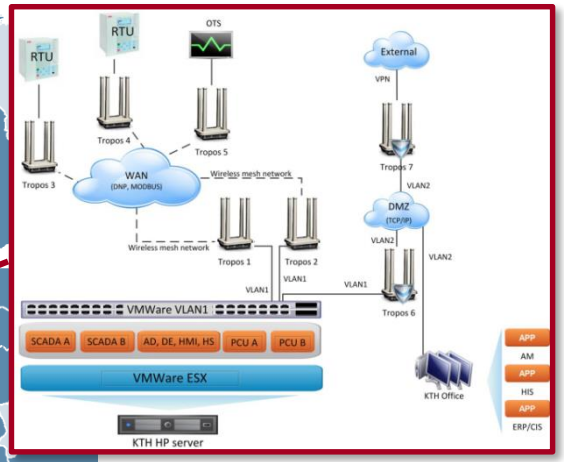
Security Integration Test Environment (SITE)

Robustness and scalable D(T)LS-based communication

SCADA (WP3) & secure wireless communication







Resilient communications infrastructure
Resilient SCADA systems

Key management for group software distribution

Questions

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

Project Coordinator:

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

Technical Coordinator:

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