SEGRID storyline

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 storyline

Objectives

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

- What is the smart grid?
- What are the security challenges in smart grids?
- What needs to be enhanced?

How does SEGRID addresses these question?

SEGRID storyline

Smart Grid

SEGRID partners

Load balancing renewable energy

SCADA

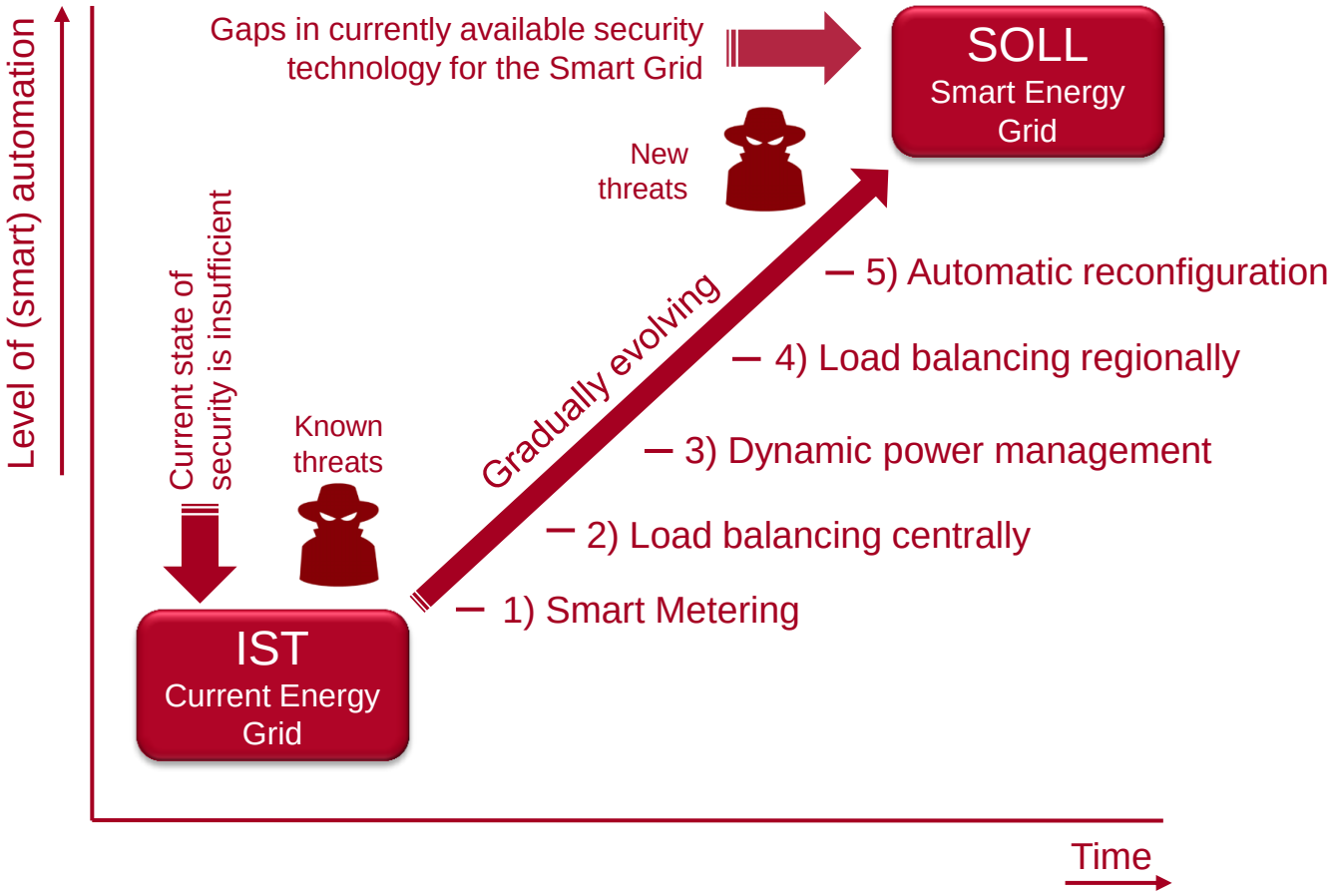
Smart metering

Dynamic power management for smart homes, smart offices, electric vehicles

Automatic reconfiguration of the power grid

Substation automation

SEGRID storyline



SEGRID storyline

Security challenges in smart grids

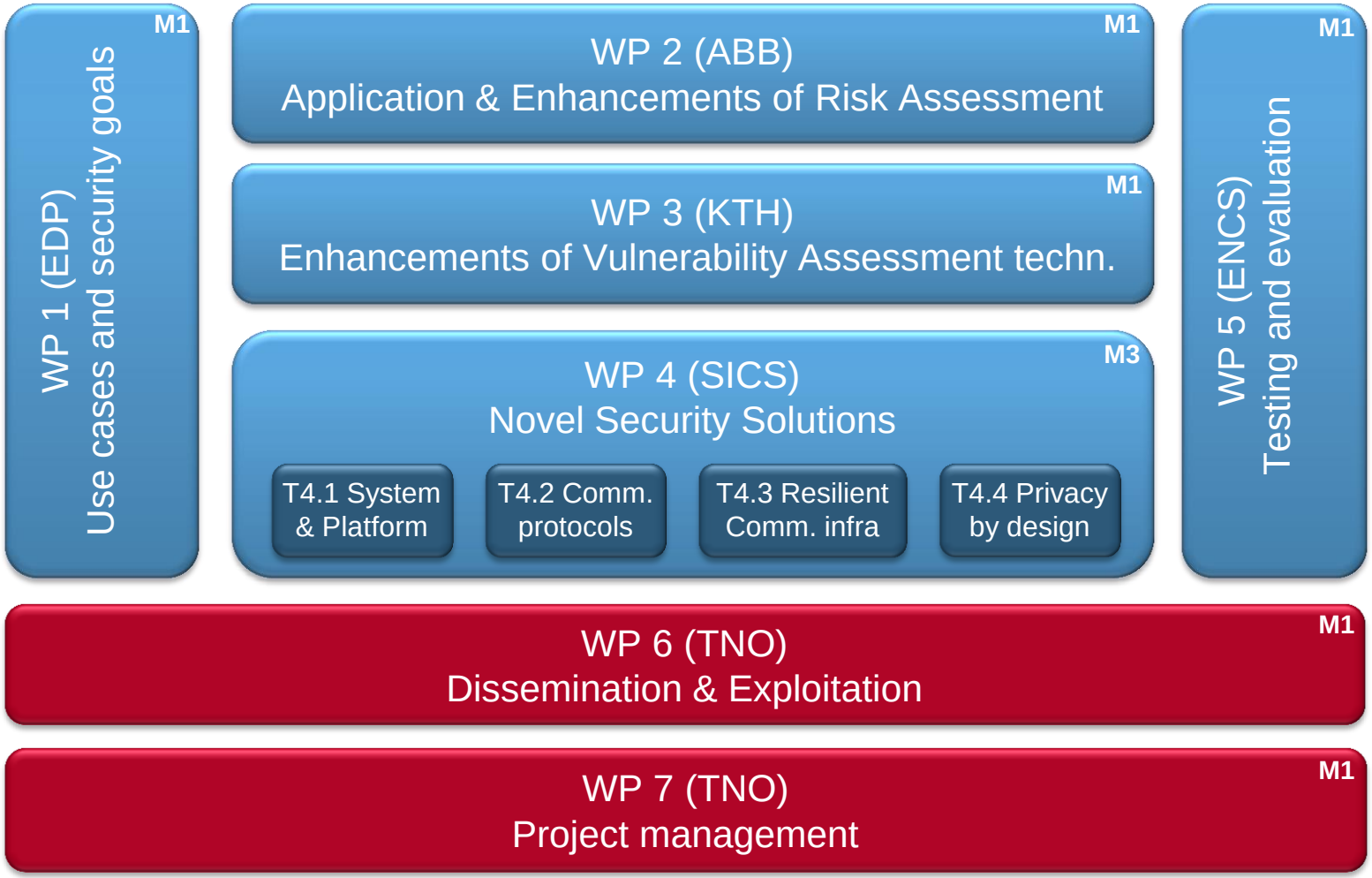
- Smart Grid engineers & Cyber Security experts speak different languages.
  - Availability, Integrity & Confidentiality
  - Safety (physical damage/death)

- Systems have different constraints
  - long component lifetime, but how about security updates / patches?
  - realtime requirements, some low bandwidth channels, legacy protocols, …
  - high dependability (don't touch a good system / vulnerability scanning?)

- Non-security / -crypto experts involved in security protocol design, standardization, software development, …
  - Incorrect use of algorithms, lack of message authentication, SQL injection, …

SEGRID

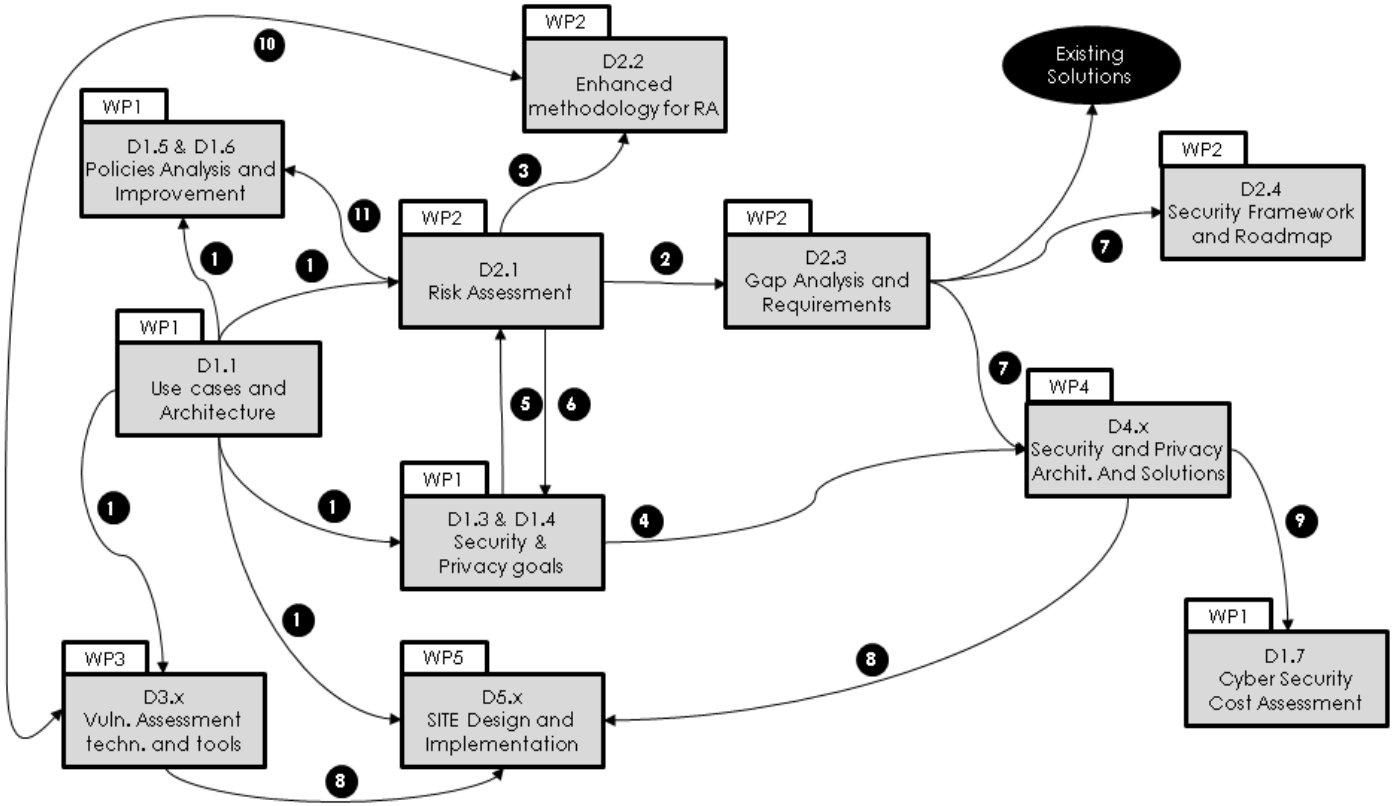
Work package structure



SEGRID – WP1

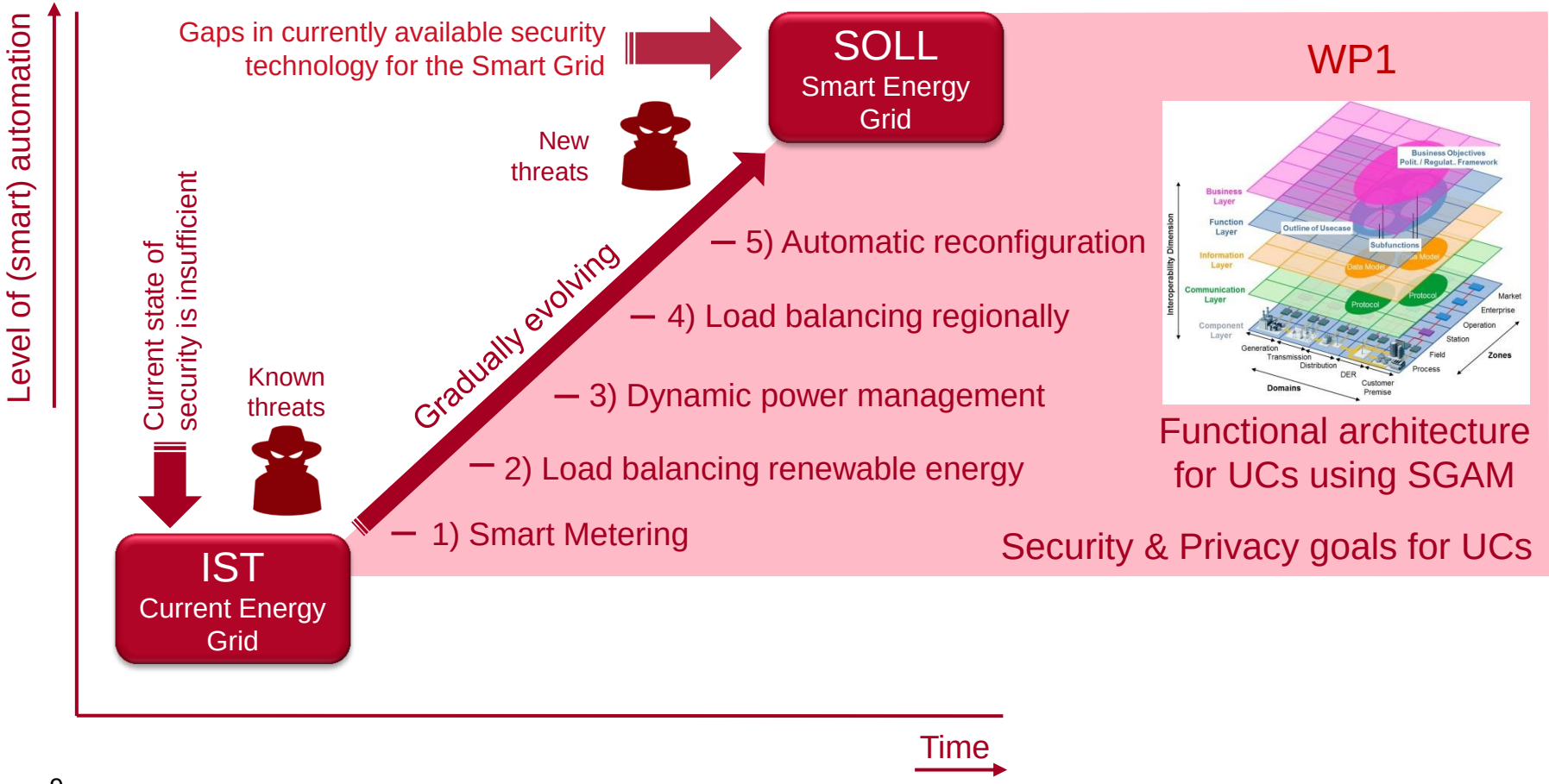
Deliverable 1.2 – SEGRID Smart Grid Security Roadmap

- Describes the SEGRID work package interdependencies



SEGRID – WP1

Use cases and security goals



SEGRID – WP1

Use cases & scenario's

UC1: Smart meter used for on-line reading of consumption and technical data
- 1.1 Metering
- 1.2 Remote power switching
- 1.3 Outage management

} **Scenario's**

UC2: Load balancing renewable energy centrally
- 2.1 Managing Power Quality
- 2.2 Balancing MV renewable generation centrally

UC3: Dynamic power management for smart homes, smart offices, EV
- 3.1 Centralised control of available loads
- 3.2 Load shifting – Centralised control and automation of home appliances
- 3.3 Optimised charging of EV

UC4: Load balancing renewable energy regionally (substation automation)
- 4.1 Balancing MV renewable generation
- 4.2 Balancing LV renewable generation
- 4.3 Balancing LV energy consumption locally

UC5: Automatic reconfiguration of the power grid
- 5.1 Centrally decided isolation and restoration at faults in MV network
- 5.2 Distributed isolation and restoration at faults in the MV network
- 5.3 Minimisation of losses in the MV network using switching

SEGRID – WP1

Functional architecture – according to SGAM interoperability layers

Use Case 1: Smart meter used for on-line reading of consumption and technical data

Legenda

Maintenance

Functional layer

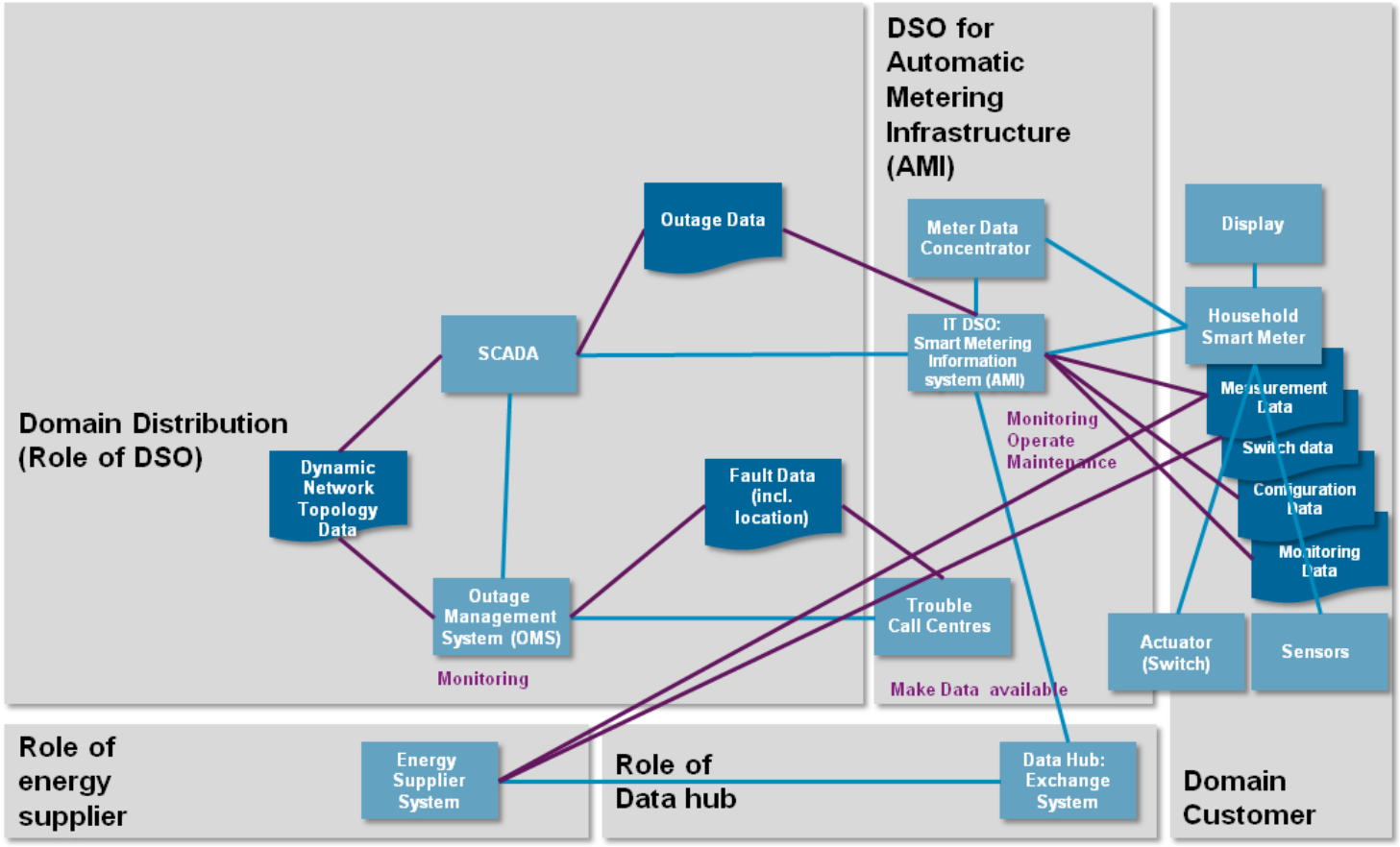
Switch Data

Information layer

Communication layer

RTU

Component layer



SEGRID – WP1

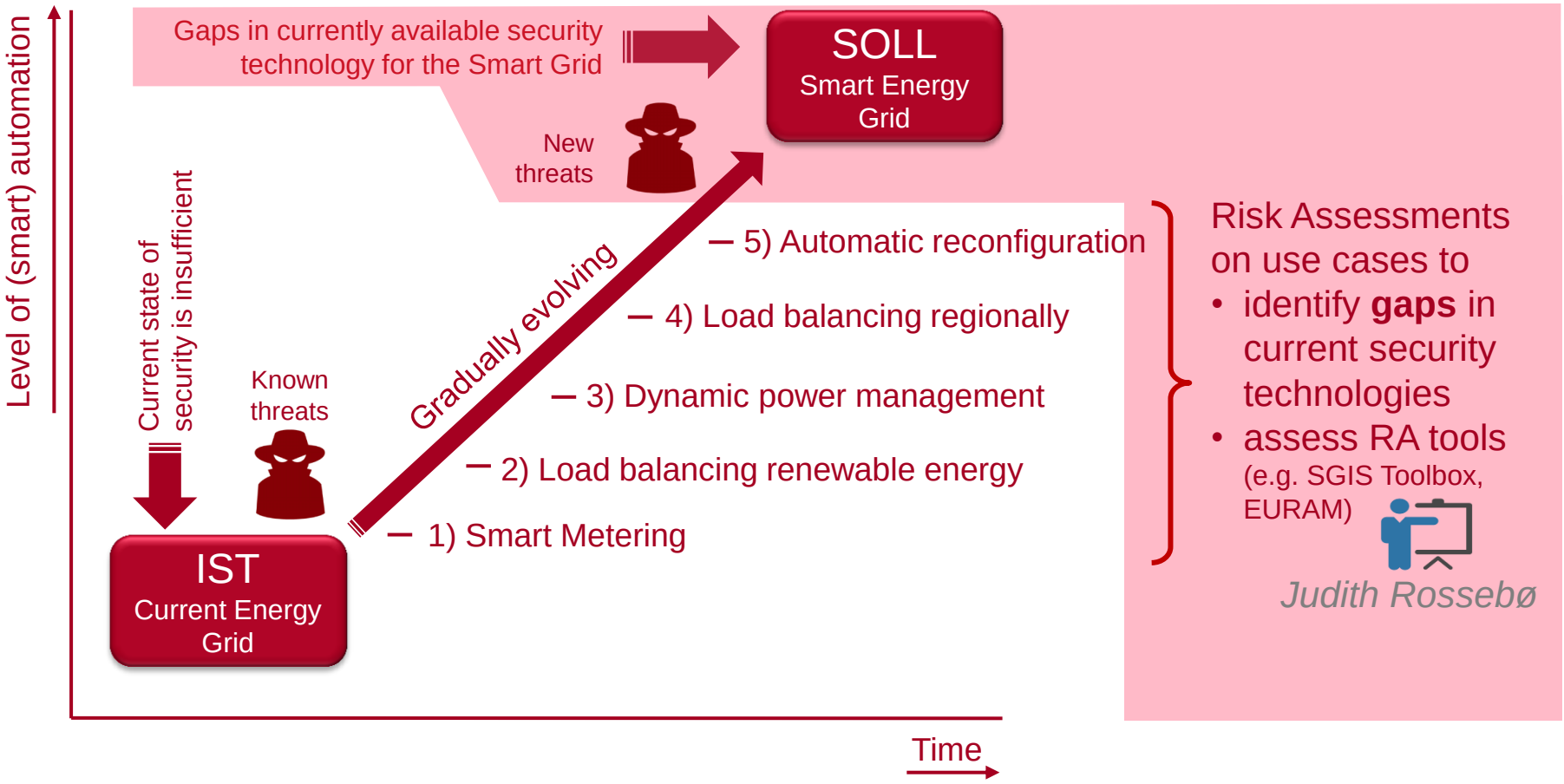
Security & Privacy goals for the use cases

- Defines WHAT is needed and WHY based on stakeholder interests.
  - A *security goal* is a specific need to protect a certain *interest of a stakeholder*.
  - A *privacy goal* is a specific need to *protect personal data* when it is collected, transferred, processed, and/or stored by a stakeholder.
- **Security Goals** have been defined on:
  - *Information Assets*
    - Properties: Availability, Data Integrity, Authenticity, Confidentiality, etc.
  - *System Assets*
    - Properties: Robustness, Resilience, System Integrity, Controlled Access, Physical Security, and `Security Lifecycle Aspects (e.g. Maintainability, Upgradability)
- **Privacy Goals** have been defined:
  - Properties (privacy design strategies): Minimise, Hide, Separate, Aggregate, Inform, Control, Enforce, Demonstrate

DSO_SG01	ensure *data integrity* and *authenticity* of measurement data (i.e. Measurement Data, Sensor Data, kWh Data) and monitoring data (e.g. Current Status Data) during transfer and storage.

SEGRID – WP2

Application & Enhancement of Risk Assessment



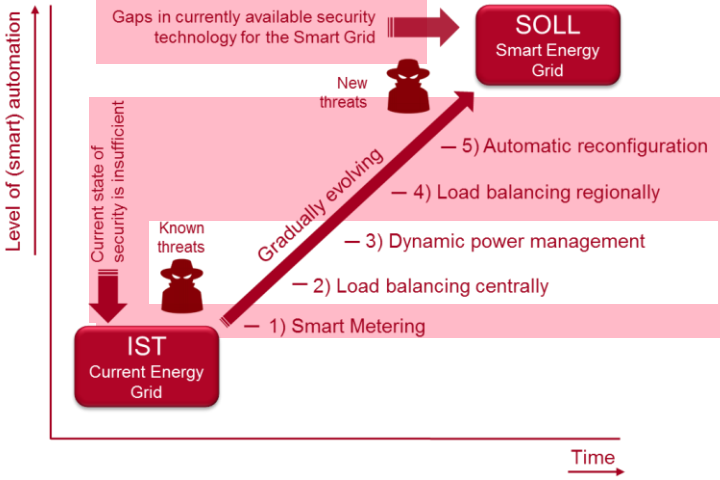
SEGRID – WP2

GAP Analysis & Roadmap

GAP Analysis consisted of two parts:

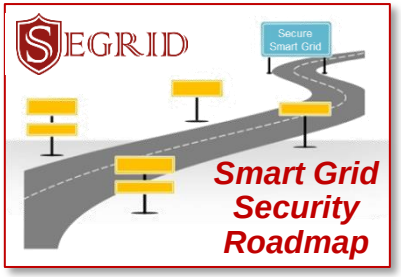
Security Technologies
- Intrusion Detection
- Platform Security
- Privacy
- Smart Grid Comm.
- SCADA

2) Assessed GAPs along needs in specific *security technologies* based on research efforts & research projects



1) Assessed GAPs (short comings) in current security technology to mitigate identified risks [D2.1] in use cases: ***UC1, UC4, and UC5***

GAP Analysis was basis for



Maarten Hoeve

SEGRID – WP3

Enhancements of Vulnerability Assessment technologies

WP 3 (KTH)
Enhancements of Vulnerability Assessment techn.

- Enhancements of vulnerability assessment techniques
- Develop vulnerability discovery and diagnosis tools

DEMO

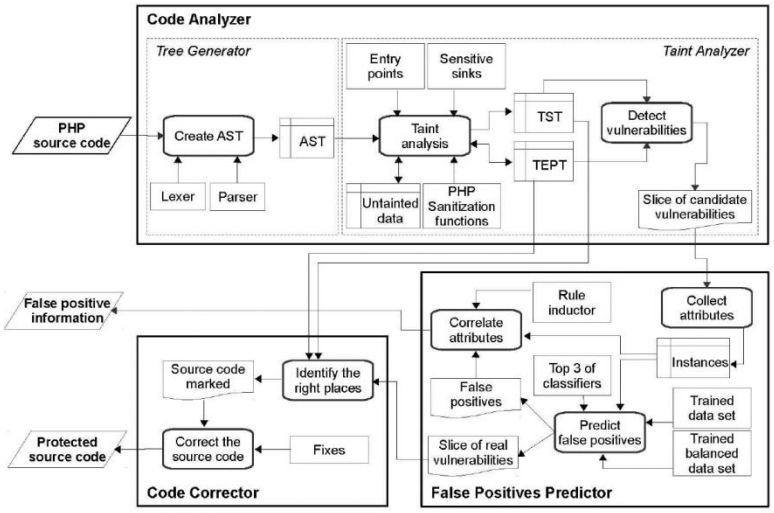
Web Application Protection (WAP) tool

FACULDADE DE CIÊNCIAS UNIVERSIDADE DE LISBOA

Smart Grid systems and components are increasingly using web technology. Web applications are prone to vulnerabilities

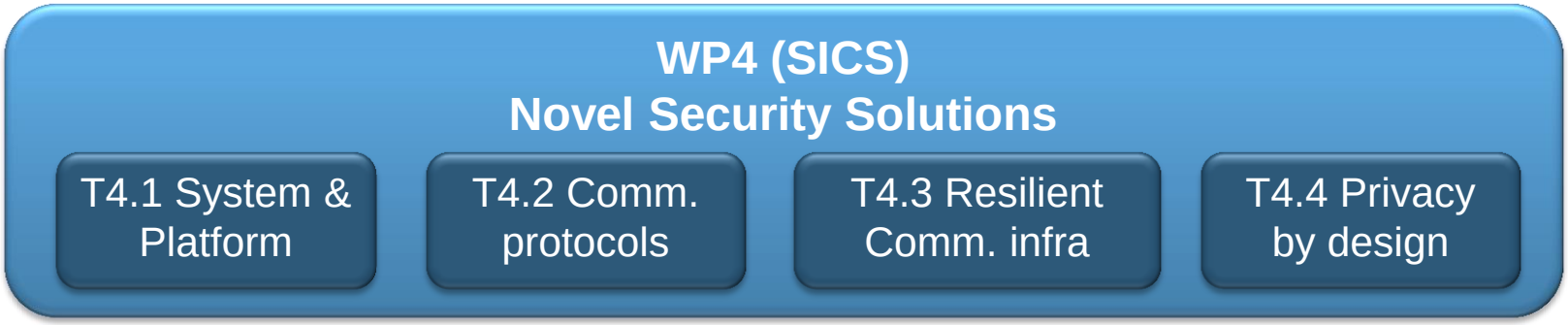
SEGRID is developing a source code vulnerability analysis tool that automatically discovers & corrects vulnerabilities.

- taint analysis for vulnerability discovery
- machine learning to reduce false positives



SEGRID – WP4

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(T)LS-based communication
  f) Key management for group software distribution
  g) Privacy by design

SEGRID – WP4

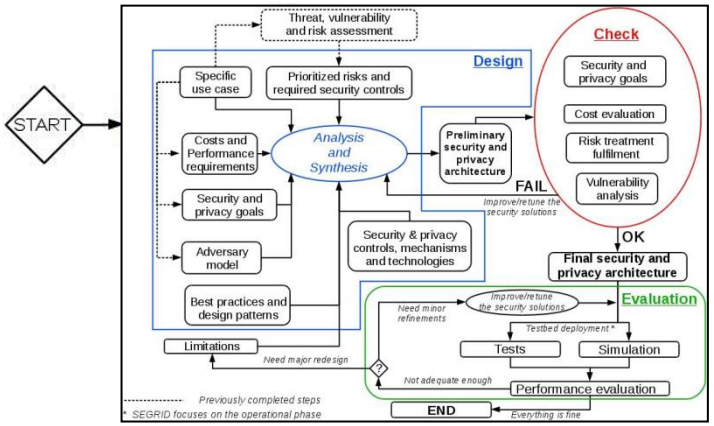
Develop novel security solutions (to fill some of the gaps)

WP4 (SICS)
Novel Security Solutions

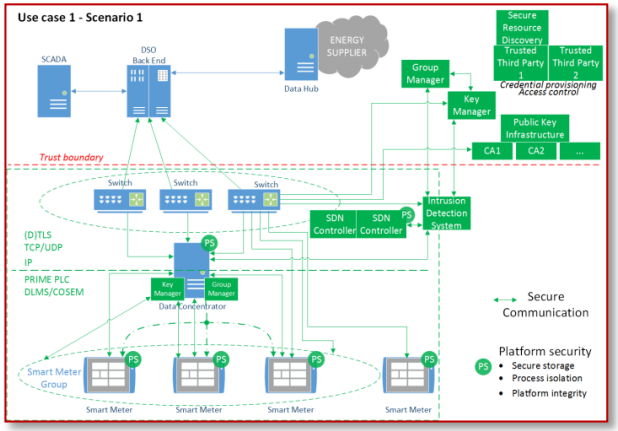
- T4.1 System & Platform
- T4.2 Comm. protocols
- T4.3 Resilient Comm. infra
- T4.4 Privacy by design

Security and Privacy Architecture DEsign process (SPADE)

- SPADE is a process to design a Security Architecture



apply



SEGRID – WP4

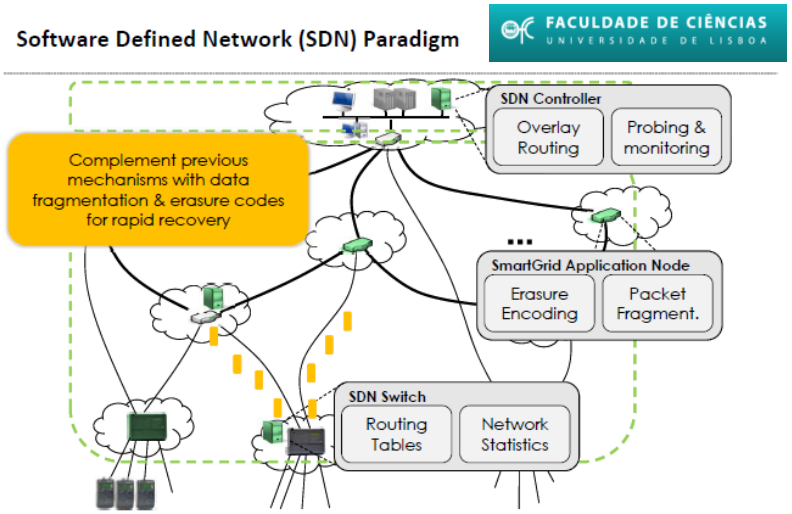
Develop novel security solutions (to fill some of the gaps)

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



SEGRID – WP4

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

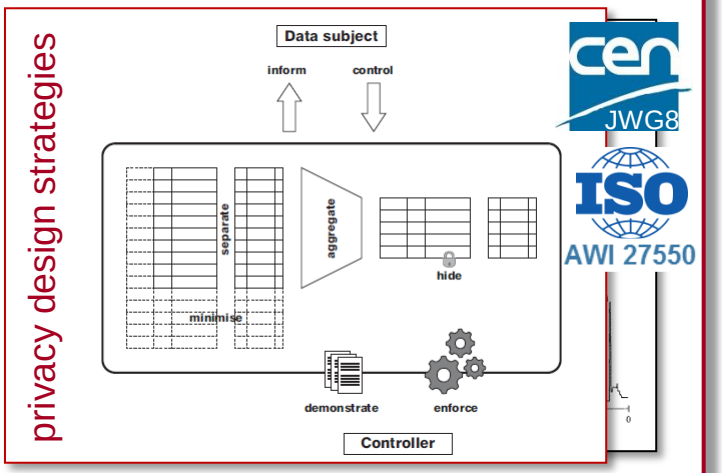
WP4 (SICS)
Novel Security Solutions

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

Privacy-by-design toolbox

- Goal: Support a paradigm shift towards collecting less personally sensitive data, while supporting all functionality needed.
- SEGRID is developing a privacy-by-design toolbox specific for future smart grid developments.
  - new privacy tactics & design patterns
  - privacy enhancing techniques

TNO innovation for life

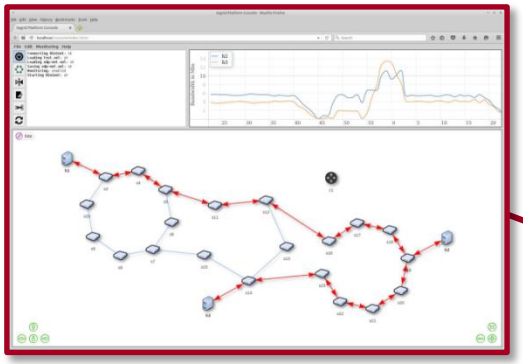


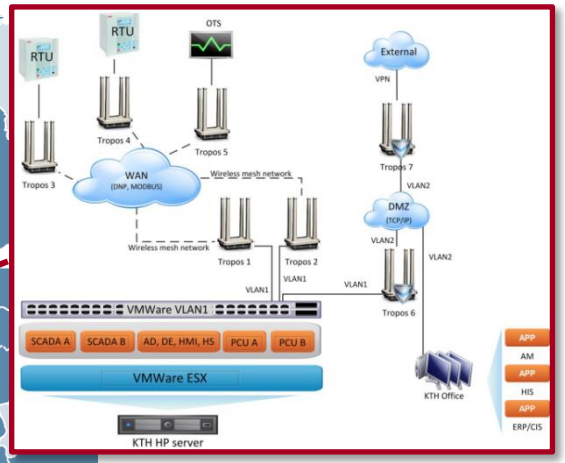
SEGRID – WP5

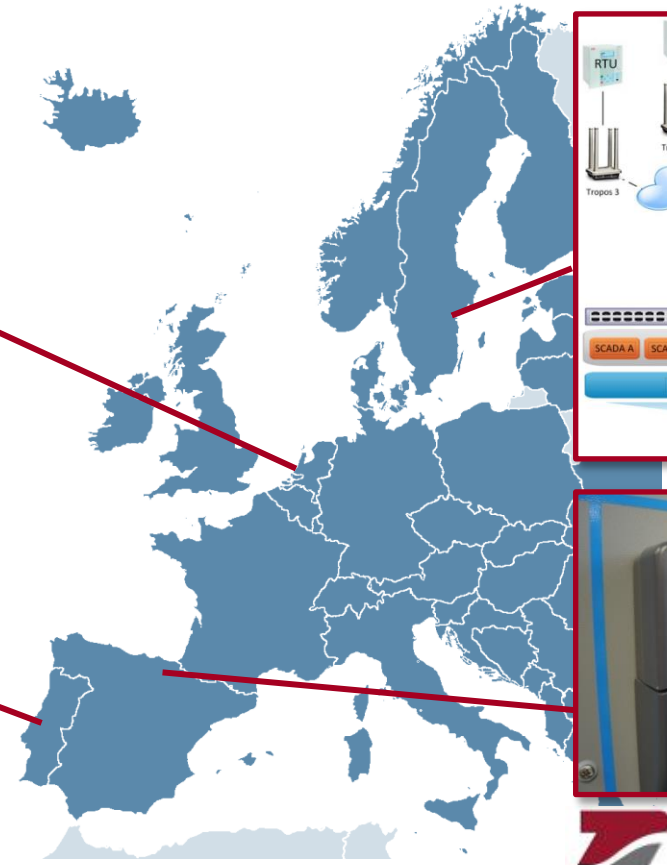
Security Integration Test Environment (SITE)

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:

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