Smart Grid Security

Use Case: Balancing MV renewable energy centrally

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

The future carries many new challenges for DSOs

Historical Challenges

Quality of Service

Operational Efficiency

- Supply customers with high quality of service
- Minimize OPEX and CAPEX

New Challenges

Advanced Metering Infrastructure

Renewables & Distributed Generation

MV/LV automation & sensoring

Smart Grid

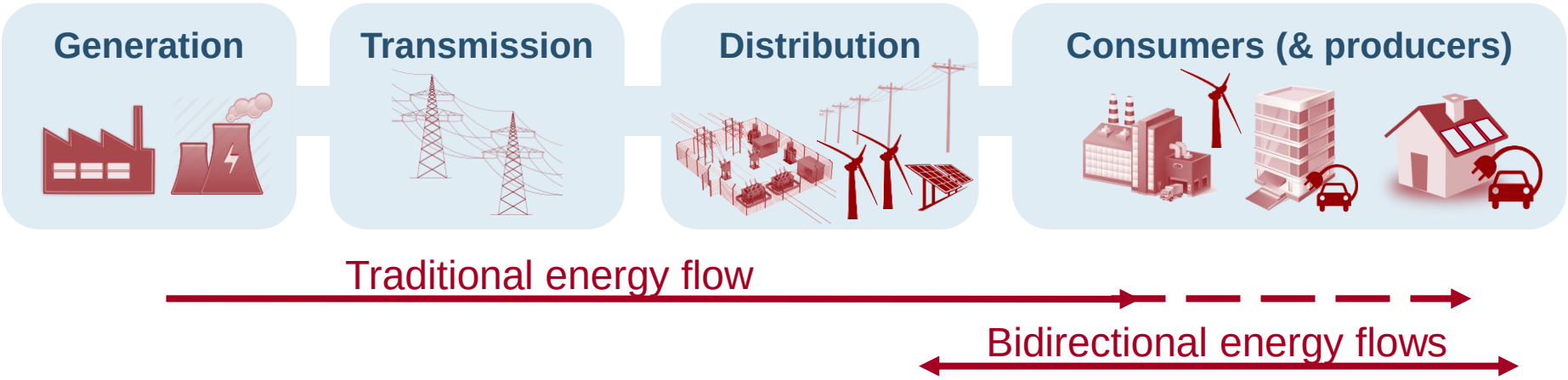
Electric vehicle

Energy efficiency and new business models

A smarter distribution grid to new challenges

- New ways of planning and managing the grid (e.g. DG, bidirectional energy flows...)
- More information to customer energy efficiency
- New technologies (e.g. energy storage) and new business models (e.g. DSM, dynamic energy prices...)
- EV integration (e.g. V2G, smart charging...)

Towards the Smart Grid

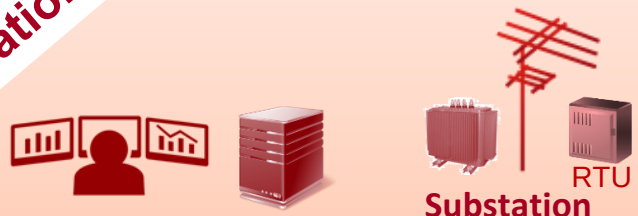


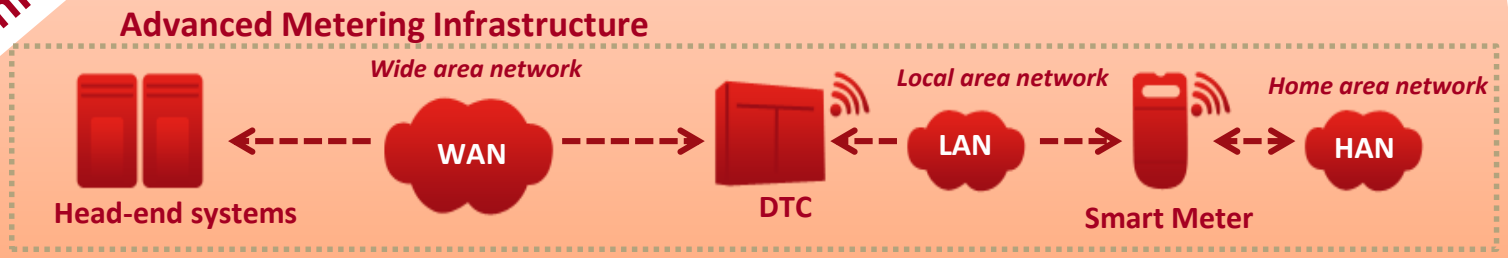
- Renewable and distributed generation
  - European Commission (EC) has set a goal to meet at least 40 percent of the continent's demand for electrical power with renewables by 2030.
- Electric vehicle charging
- Introduction of new stakeholders
- Distribution System Operators (DSO) will need to make major changes to the way they run their networks.

Towards the Smart Grid

New challenges for DSOs to manage the

Increase in monitoring and automation



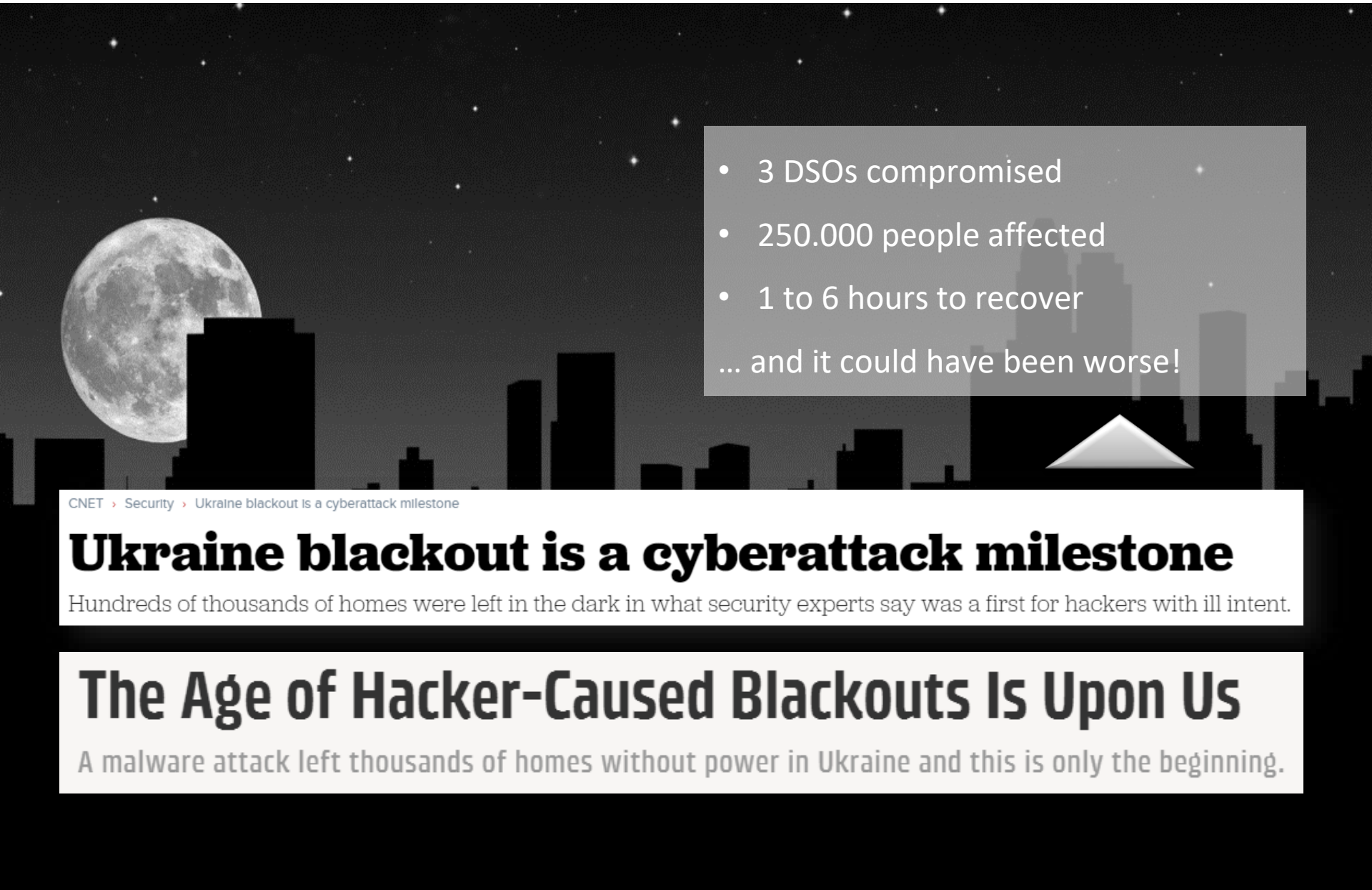


Increases the Complexity & the Exposure of the electricity grid to Cyber Threats

Cyber threats within the Electricity Grid are real.

Root causes for blackouts are no longer exclusively physical

SEGRID



- 3 DSOs compromised
- 250.000 people affected
- 1 to 6 hours to recover

… and it could have been worse!

CNET › Security › Ukraine blackout is a cyberattack milestone

Ukraine blackout is a cyberattack milestone

Hundreds of thousands of homes were left in the dark in what security experts say was a first for hackers with ill intent.

The Age of Hacker-Caused Blackouts Is Upon Us

A malware attack left thousands of homes without power in Ukraine and this is only the beginning.

And the challenges are not only technological.
EU regulations for Cybersecurity and Data Protection.

SEGRID

Network and Information Security (NIS) Directive
(entry into force in May2018)

Applicable to Operators of Essential Services

- Risk analysis methodologies;
- Security controls;
- Technical and organizational measures;
- Incident response capabilities;
- Incident reporting obligation.

General Data Protection Regulation (GDPR)
(entry into force in May 2018)

Applicable to personal data 'controllers' and 'processors'

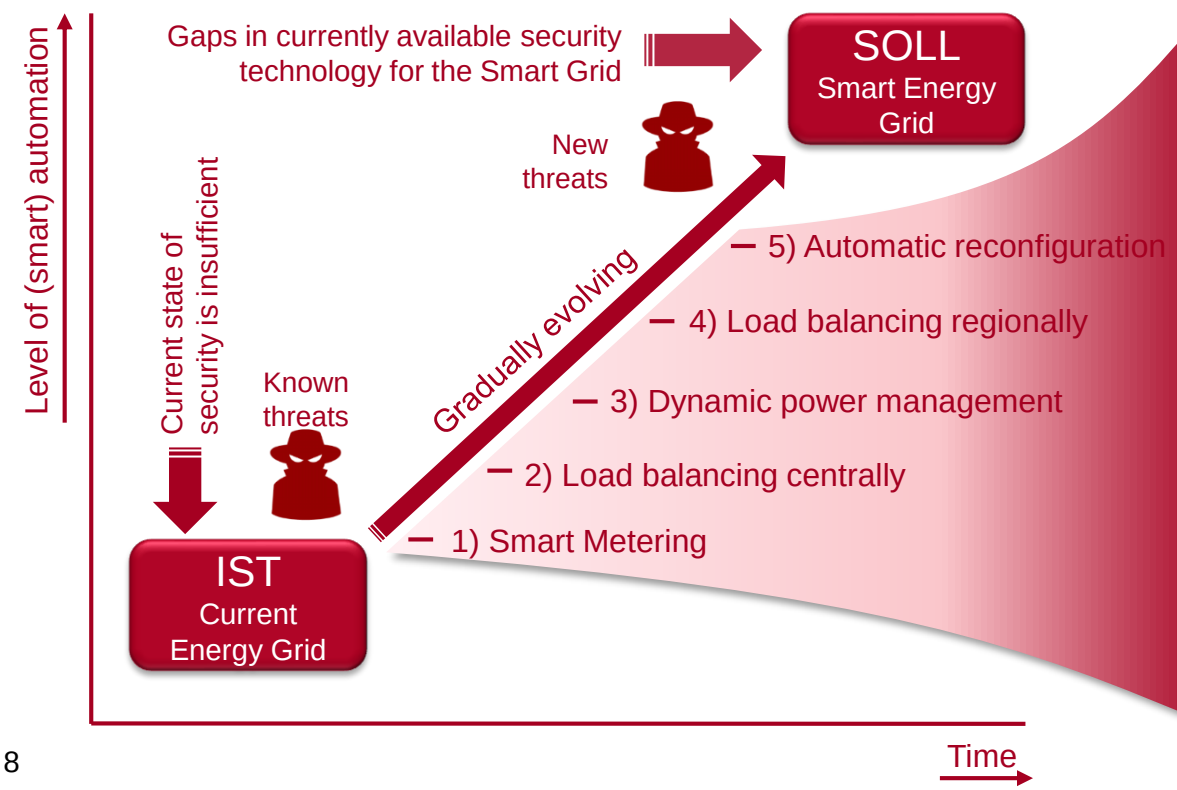
- Data Prot. Impact Assess. (DPIA);
- Data Protection Controls;
- Penalty in case of data breach: 20M€ vs 2%-4% annual turnover;
- Report on data breaches <72h;

SEGRID

SEGRID

How did SEGRID approach these challenges?

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



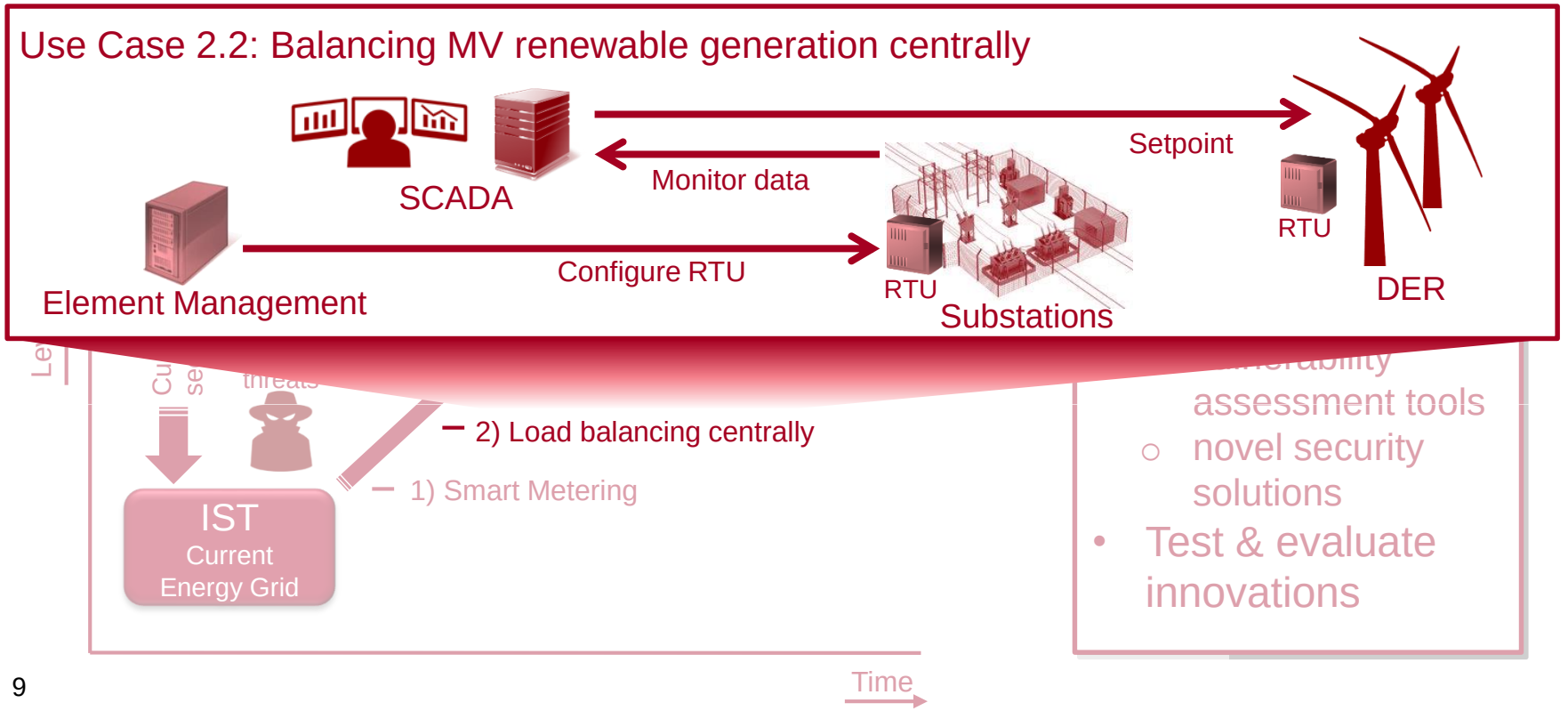
Use cases guided activities e.g.

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

SEGRID

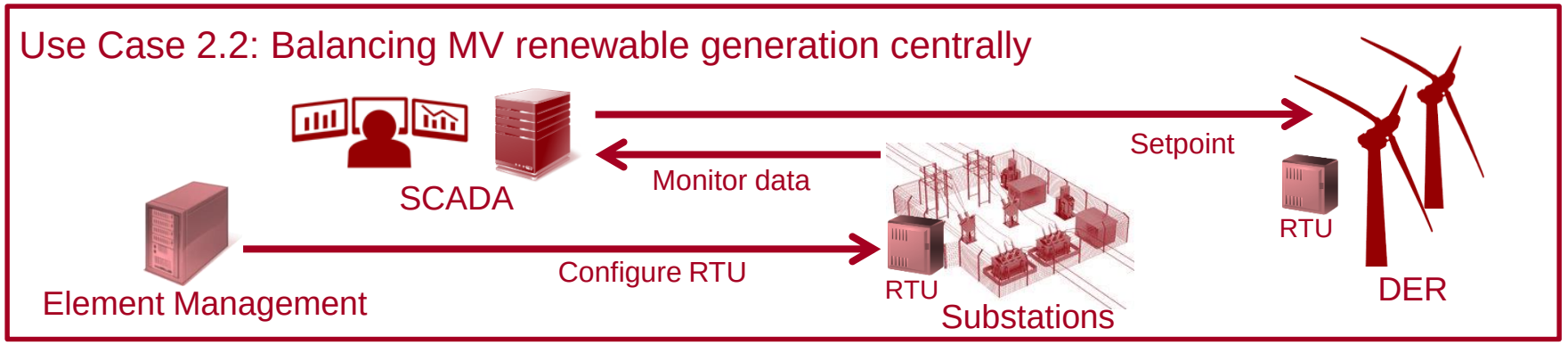
Demonstrate SEGRID result applied to Use Case 2.2

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

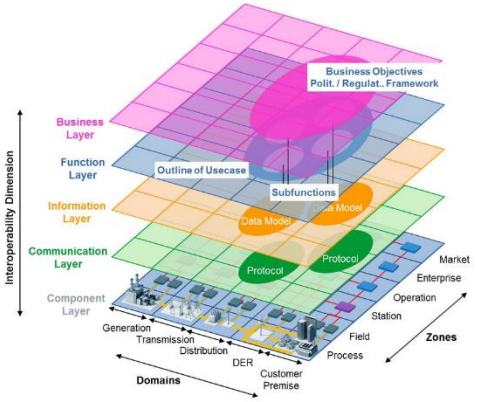


UC2.2: Balancing MV renewable generation centrally

Load balancing renewable energy is a way to automatically control and monitor both the distributed generation and consumption, and balance the renewable energy supply to the demand, to avoid regional congestion.

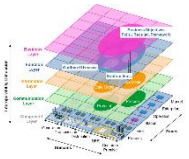


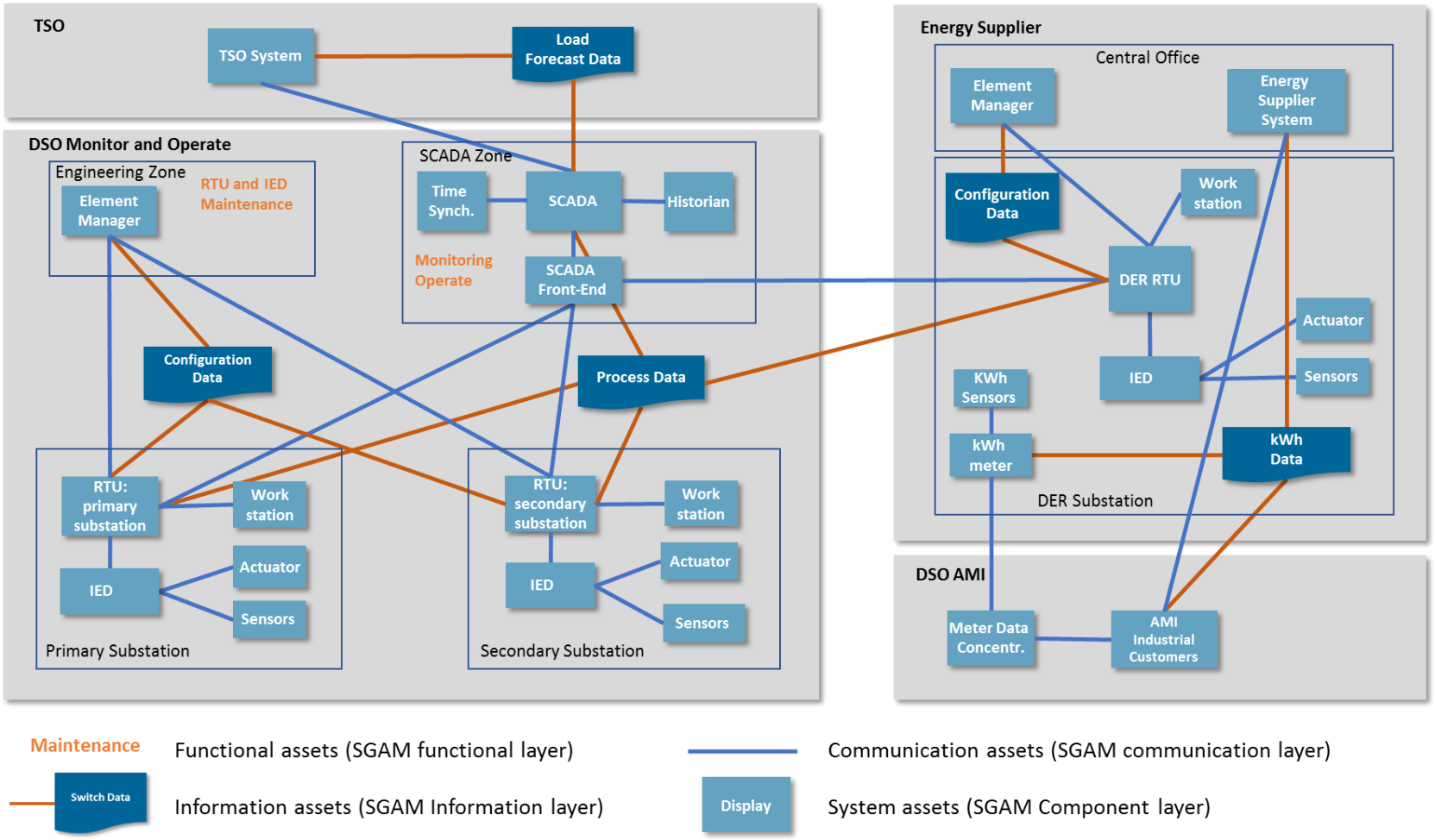
Elaborate on the use case by creating a M/490 Smart Grid Architecture Model (SGAM)



UC2.2: Balancing MV renewable generation centrally

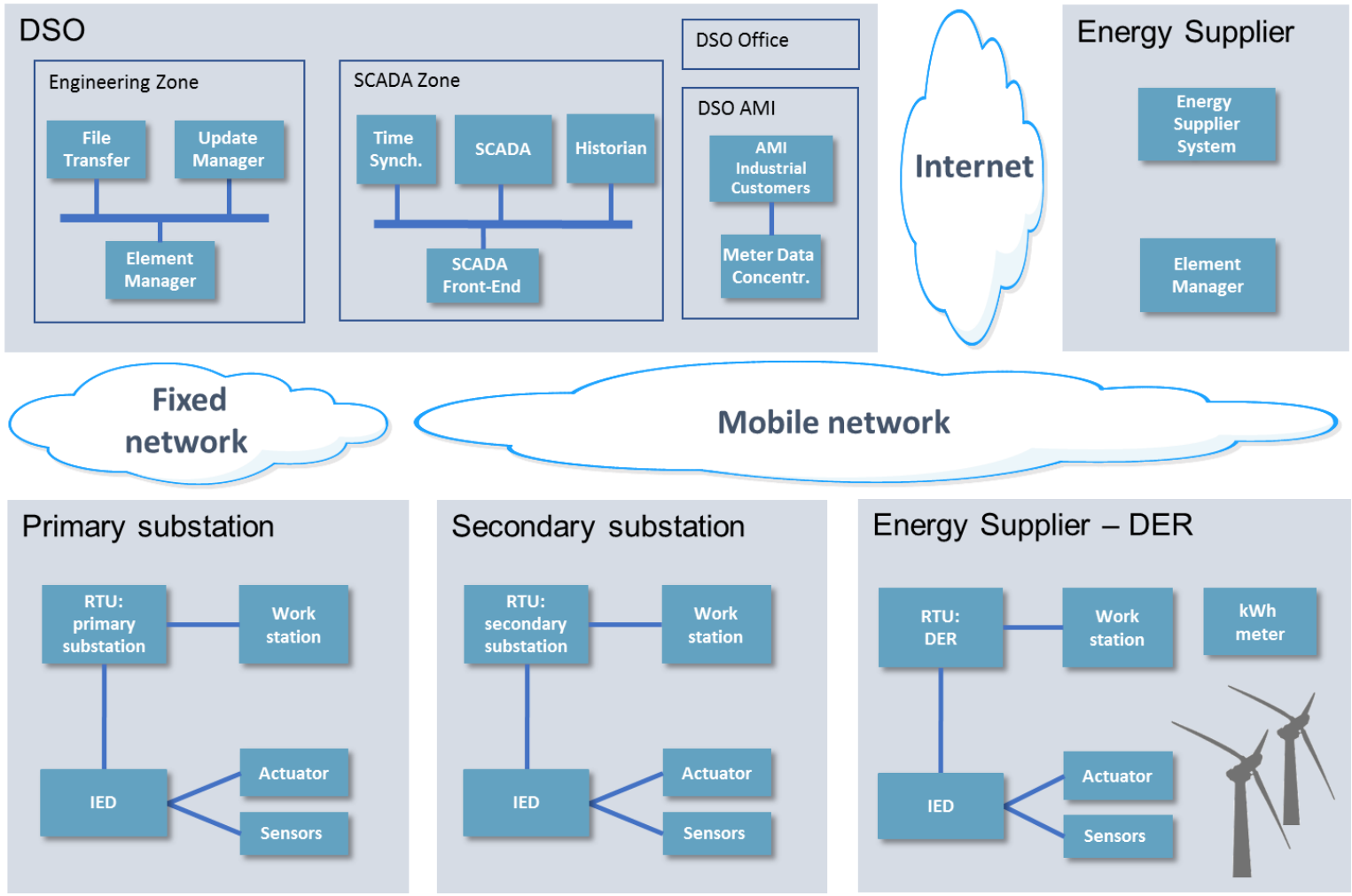
SGAM interoperability layers





UC2.2: Balancing MV renewable generation centrally

Towards a system architecture

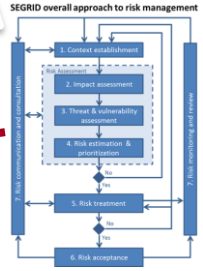


Risk Management & SEGRID Innovations

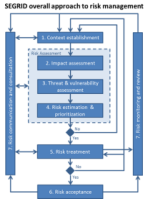
Risk management

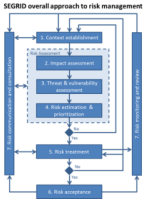
Periodic update

SRMM



Changes in:
- Threat landscape
- Infrastructure
- Business objectives
- Risk appetite





Power Grid Infrastructure

Power Grid Infrastructure

Power Grid Infrastructure

Operations

Development

Risk assessment

Add new functions to the Power Grid

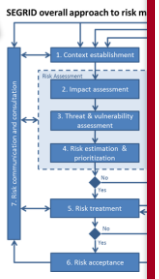
Development process

new system

time

Risk Management & 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

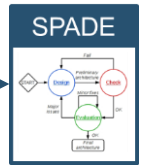
- Vulnerability Detection and Correction with WAP

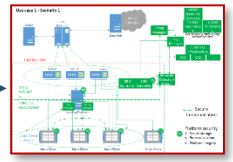
Operations

Power G
Infrastruc

Development

Risk assessment





Security & Privacy Architecture with *SEGRID security solutions*

Cost Assessment

Add new functions to the Power Grid

Development process

new system

time

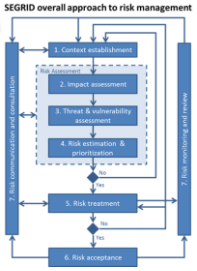
Security & Privacy Architecture DEsign

Risk Management & SEGRID Innovations

Risk management

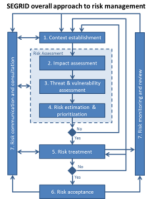
Periodic update

Toward dynamic / real-time risk management

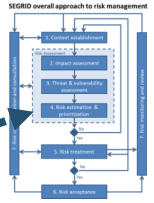


Changes in:

- Threat landscape
- Infrastructure
- Business objectives
- Risk appetite



securiCAD use



automatic model creation & updating

Power Grid Infrastructure

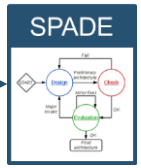
Power Grid Infrastructure

Power Grid Infrastructure

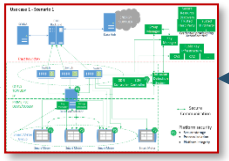
Operations

Development

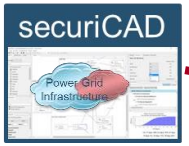
Risk assessment



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

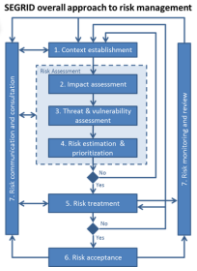
time

Risk Management & SEGRID Innovations

Risk management

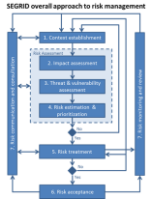
Periodic update

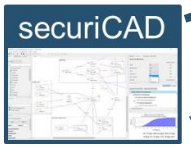
Toward dynamic / real-time risk management



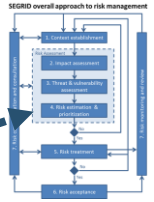
Changes in:

- Threat landscape
- Infrastructure
- Business objectives
- Risk appetite





use



Security Operations

Vulnerability Management, Security Incident Monitoring & Incident Response

automatic model creation & updating

Power Grid Infrastructure

Power Grid Infrastructure

Power Grid Infrastructure

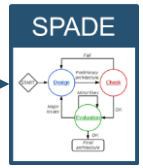
Operations

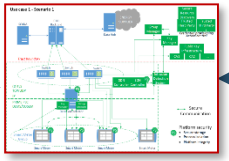
Development

Risk assessment

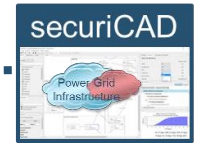
Security & Privacy Architecture with *SEGRID security solutions*

modelled





check



integration

Operational Security Capability Model

Add new functions to the Power Grid

Development process

new system

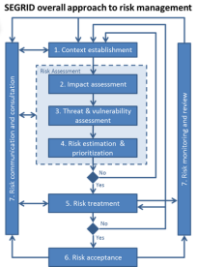
time

Risk Management & SEGRID Innovations

Risk management

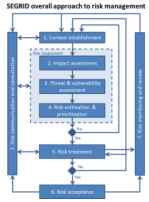
Periodic update

Toward dynamic / real-time risk management

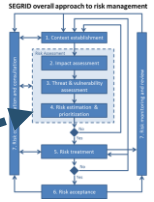


Changes in:

- Threat landscape
- Infrastructure
- Business objectives
- Risk appetite



securiCAD use



Security Operations

Vulnerability Management, Security Incident Monitoring & Incident Response

automatic model creation & updating

Power Grid Infrastructure

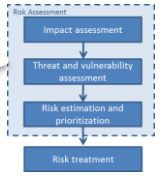
Power Grid Infrastructure

Power Grid Infrastructure

Operations

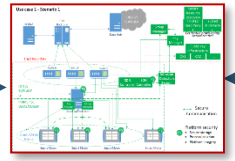
Development

Risk assessment



SPADE

Security & Privacy Architecture with *SEGRID security solutions*



check

securiCAD

modelled

integration

Add new functions to the Power Grid

Development process

new system

time

Questions

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

WP1 leader:

Medeiros, Nuno

EDP Distribuição

Phone: +351 934644128
E-mail: nuno.medeiros@edp.pt

Technical Coordinator:

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