Cybersecurity in Smart Grids:
PRECYSE, NOBELGRID and WISEGRID

Santiago Cáceres

22/09/2016

etra

Initiatives led by ETRA

- Past… **PRECYSE**

- Ongoing… NOBEL GRID

- Future… WISEGRID

etra I+D

- STRONG SUPPORT ON ICT SYSTEMS OFFERING **MISSION CRITICAL SERVICES**

- **NEW DEMANDS OF** EXTERNAL **SERVICES** TO END USERS

- **INCREASING NUMBER OF ENTITIES** TO BE MANAGED

- **THREATS BECOMES UBIQUITIOUS AND GLOBAL**

etra I+D

PRECYSE **MISSION** was to define, develop and validate a methodology, an architecture and a set of technologies and tools to improve –by design– the security, reliability and resilience of the ICT systems supporting Critical Infrastructures (CI).

We built on previous research and existing standards, and paid due attention to performance demands of current CI systems, as well as to relevant security, privacy, policy, legal and ethical issues.
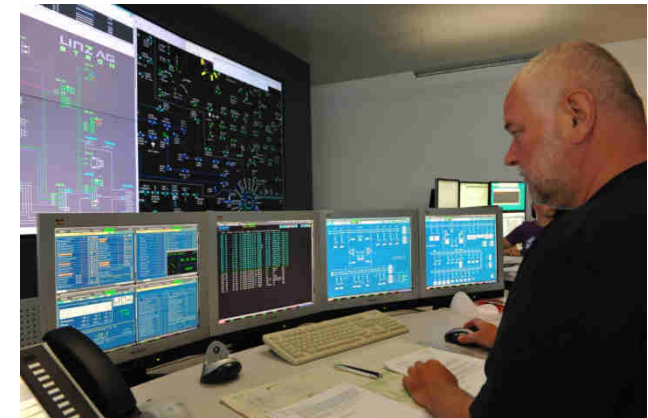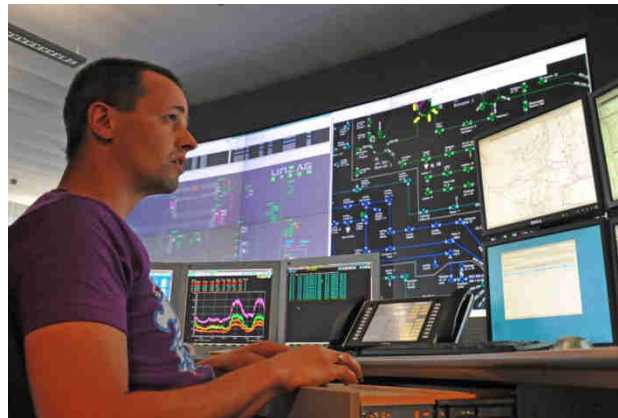
- Traffic Control Centre in the City of Valencia (Spain)
- 1.500.000 Inhabitants, 500.000 Vehicles Running

- Energy Demonstrator in the City of Linz (Austria)
- Power Supply and Related Services for 400.000 Inhabitants

etra I+D

PRECYSE Approach

Methodology Policy Benchmarking

1

Architectural Principles and Supporting Tools

2

Critical Infrastructure

3

Technologies to

Protect   Prevent

Diagnose   React

4

$P_i P_x$

P_y

D_x

$R_i R_u$

SECURE Critical Infrastructure

5

etra I+D

The PRECYSE Architecture diagram showing Processes, Methods & Techniques, and Tools:

Methodology / Policy / Benchmarking

Processes
1. Gather infrastructure details, including vulnerabilities
2. Perform a risk assessment
   a) Determine assets
   b) Determine threats
   c) Determine current safeguards and countermeasures
   d) Estimate impacts
   e) Estimate risks
3. Select security controls
4. Implement security controls
5. Measure control effectiveness
6. Make adjustments

Methods & Techniques
- Asset enumeration techniques: manual/automatic, active/passive
- *Magerit* as overarching risk assessment method
- Using attack and defence trees
- Threat & vulnerability analysis
- Gap analysis using security and resilience metrics and indicators
- Risk and cost-based control selection
- Access control, encryption, enclaves, IDS, integrity checking, multi-level security,…
- Benchmarking security controls
- Test-suites, metrics, indicators
- Change management

Tools (The PRECYSE Architecture)
- **PRECYSE tools**, Nmap,
- OpenVAS vulnerability scanner
- NVD/vulnerability databases
- **PRECYSE tools**
- ISMS tools (e.g., Verinice)
- Security Incident and Event Management
- Sharing cyber threat information
- Incident response handling, STIX
- XACML, Snort IDS, firewalls, AV software, OSSEC
- Test automation, OVAL
- **PRECYSE tools**
- Service orchestration, ebXML

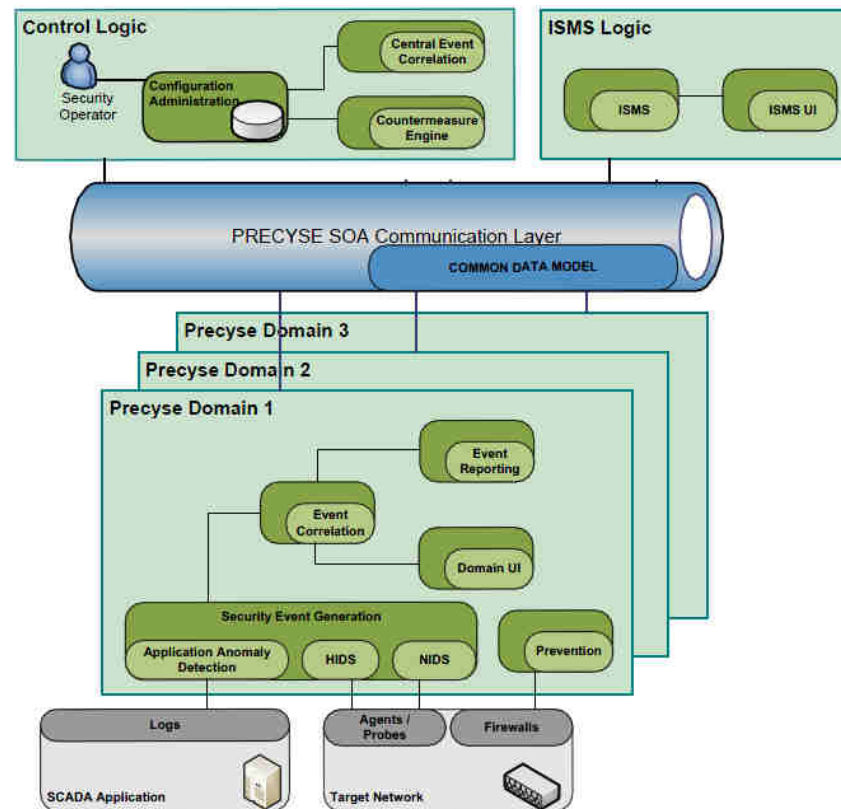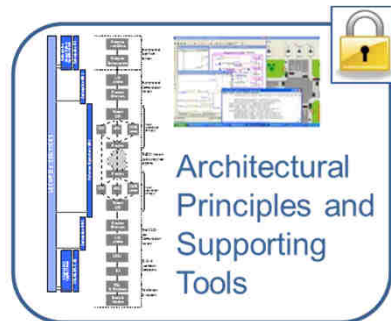**Security and Resilience Metrics**

PRECYSE Framework for ICS Security
- Methodology based on standards and best practices (metrics on privacy, security, resilience and trust)
- Benchmarking test suite (Interactive OCIL questionnaires and automated OVAL tests)
- Assessment of risks coming from APTs (like e.g. Stuxnet) based on public available vulnerability data
- PRECYSE catalogue of security controls based on MAGERIT (available on Verinice)

etra I+D

Architectural Principles and Supporting Tools

Control Logic
- Security Operator
- Configuration Administration
- Central Event Correlation
- Countermeasure Engine

ISMS Logic
- ISMS
- ISMS UI

PRECYSE SOA Communication Layer
COMMON DATA MODEL

Precyse Domain 3
Precyse Domain 2
Precyse Domain 1
- Event Reporting
- Event Correlation
- Domain UI
- Security Event Generation
  - Application Anomaly Detection
  - HIDS
  - NIDS
- Prevention

Logs — SCADA Application
Agents / Probes — Firewalls — Target Network

PRECYSE SSF Architectural model
- Complete specification
- Instantiation guidelines
- Information Model based on open security standards

etra I+D
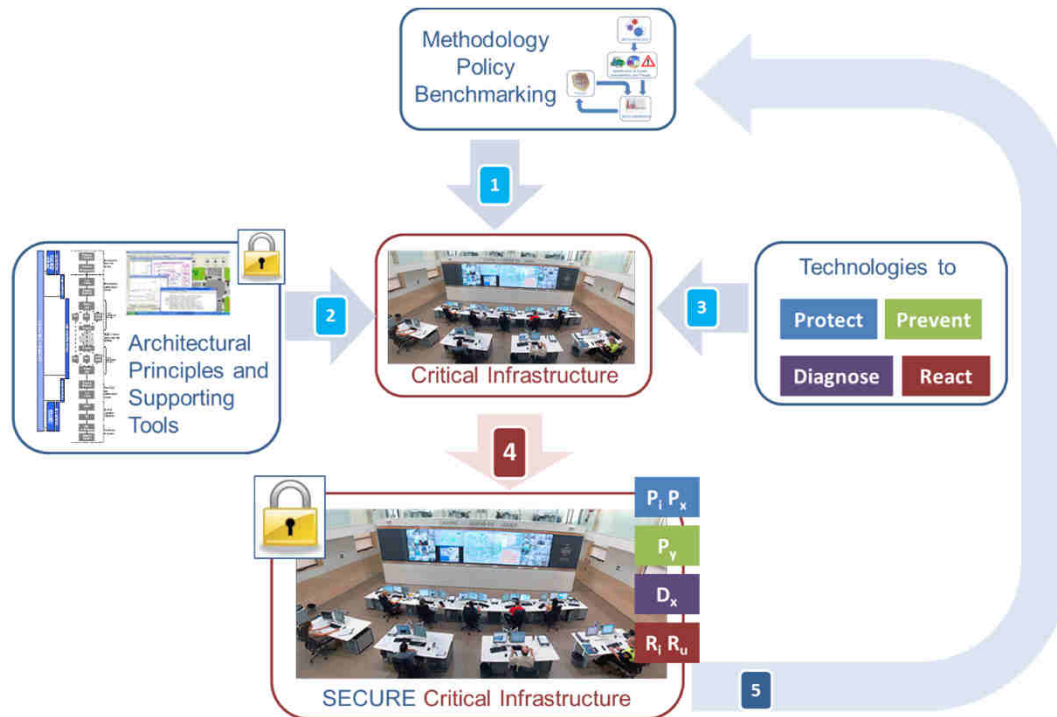
Technologies to

Protect | Prevent
Diagnose | React

Minimum IT security infrastructure required?
- Firewall
- Antivirus
- IPS
- IDS
- Authentication + Communications Encryption
- …

PRECYSE technologies to protect, prevent and react against cyber attacks

- SCADA Specific Ontology
- Privacy-Enhanced IDS (Anonymiser and Deanonymyser tool)
- Customised IDS for ICS (Monitoring IEC 60870-5-104 protocol)
- Specification of PRECYSE SSF deployment making use of open source tools
- Development of SOA based logic framework to run PRECYSE SSF

etra I+D

Methodology
Policy
Benchmarking

Architectural
Principles and
Supporting
Tools

Critical Infrastructure

Technologies to

Protect   Prevent

Diagnose   React

P_i P_x

P_y

D_x

R_l R_u

SECURE Critical Infrastructure

Prevention, protection and REaction to CYber attackS to critical infrastructurEs

PRECYSE

More info:
- www.precyse.eu

etra I+D

Initiatives led by ETRA

- Past… PRECYSE

- Ongoing… **NOBEL GRID**

- Future… WISEGRID

etra I+D

January 2015 Starting date

42 months Duration

Coordinator etra I+D

H2020 Topic

Challenge
To provide all actors of the **Smart Grid and energy market** with advanced tools and services to ensure more secure and stable grids and **cleaner and affordable electricity**.

Nobel Grid
Smart energy for people

13,9 M€ Budget

1774 PMs

Countries
- Romania
- UK
- Netherland
- Sweden
- Belgium
- Italy
- Greece
- Portugal
- Austria
- Germany
- Spain

Pilot sites
- Meltemi - Greece
- Terni - Italy
- Flanders - Belgium
- Manchester - UK
- Alginet - Spain

etra I+D
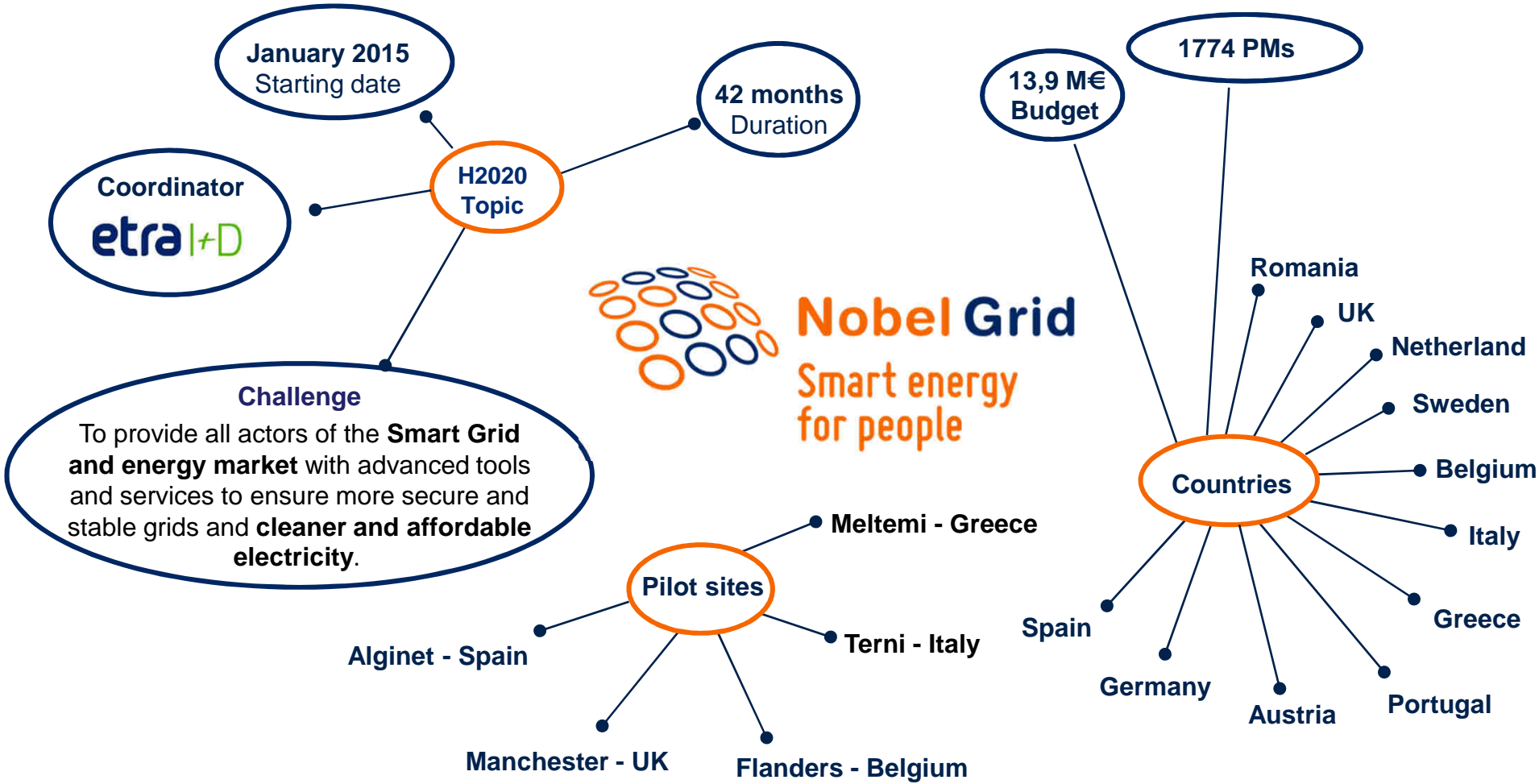
1. To provide **Secure, stable, clean and sustainable Smart Grids** allowing DSO:
   o To mitigate management, replacement and maintenance costs
   o In presence of large share of renewable energy

2. To develop **New services and Business models for all the actors of the distribution grid**, including new actors, such as prosumers, aggregators and ESCOs.
   o To facilitate integration of the next generation distributed renewable energy sources and
   o Active participation of citizens in the energy market (demand response schemas).

3. To design and develop from scratch an **Innovative and affordable** Smart Low-cost Advanced Meter allowing:
   o More extended functionalities for consumers and "prosumers"
   o Empowering and protecting European citizens

etra I+D

Tools and ICT services for Smart Grid actors

G3M Framework
A cockpit that facilitates and reduces the costs of the management, control and maintenance of the distribution grid to DSO.
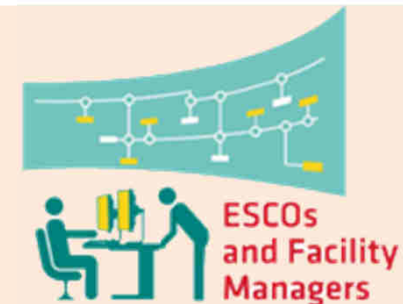

EMA App
An energy monitoring and active participation App for domestic and industrial prosumers

DRFM cockpit
A Demand Response cockpit for aggregators, energy service companies (ESCOS) and retailers.

etra I+D

Alginet, Spain

Flanders, Belgium

ASM Terni, Italy

Meltemi, Greece

Manchester, UK

etra I+D

Initiatives led by ETRA

- Past… PRECYSE

- Ongoing… NOBEL GRID

- Future… **WISEGRID**

etra I+D

- **WiseGRID** project objective is to put into the market, within a horizon of **24** months after project completion, a **set of solutions and technologies** to increase the **smartness, stability and security of an open, consumer-centric European energy grid**, with an enhanced use of storage technologies and a highly increased share of RES.

- WiseGRID integrated solution will be demonstrated and evaluated under **real life conditions in 4 large scale demonstrators** –in Belgium, Italy, Spain and Greece- **under different technical, climatological, regulatory, legislative and social conditions**.

etra I+D

WiseGRID results will be tested in real conditions **in four different demonstration sites** involving more than **1700 users**, **60 batteries** – totalling more than 300KWh of installed capacity-, **50 heat pumps** – totalling more than 160kWh of installed capacity-, **180 EV, 40 charging stations and more than 70MWh of RES** –PV, Wind Turbines and Hydro-.

Public DSO ASM Terni, Italy

RES cooperative Flanders, Belgium

Electric cooperative Crevillent, Spain

National DSO Greece

etra I+D

Thanks for your attention!

Santiago Cáceres Elvira

scaceres.etra-id@grupoetra.com

etra I+D

etra I+D

- **AWARENESS** NEEDED AT APPROPIATE LEVEL

- **NO SINGLE PRODUCT** IS COVERING THE CYBER SECURITY NEEDS

- NEW CYBER THREATS REQUIRE **INNOVATIVE SECURITY APPROACHES**

- **TECHNOLOGY** IS NOT ENOUGH, CHECK **PROCESSES AND PEOPLE**

Cyber Attacks Motivations

- Challenge
- Personal satisfaction

- Business
- Resources
- ROI (€, investments)

APT (Advanced Persistent Threat)

etra I+D