Critical Energy Infrastructures Security & Resiliency Management

Massimo Bertoncini, Director of R&D for Smart Energy Systems
Engineering Ingegneria Informatica

Terni, 22 September 2016

ENGINEERING

www.eng.it

Engineering: a global worlwide player

- ✓ **Foreign Customers account for a 7% share of the global revenue**
- ✓ **More than 7000 full time employees**
- ✓ **More than 400 employees working in the *Energy & Utilities General Direction***

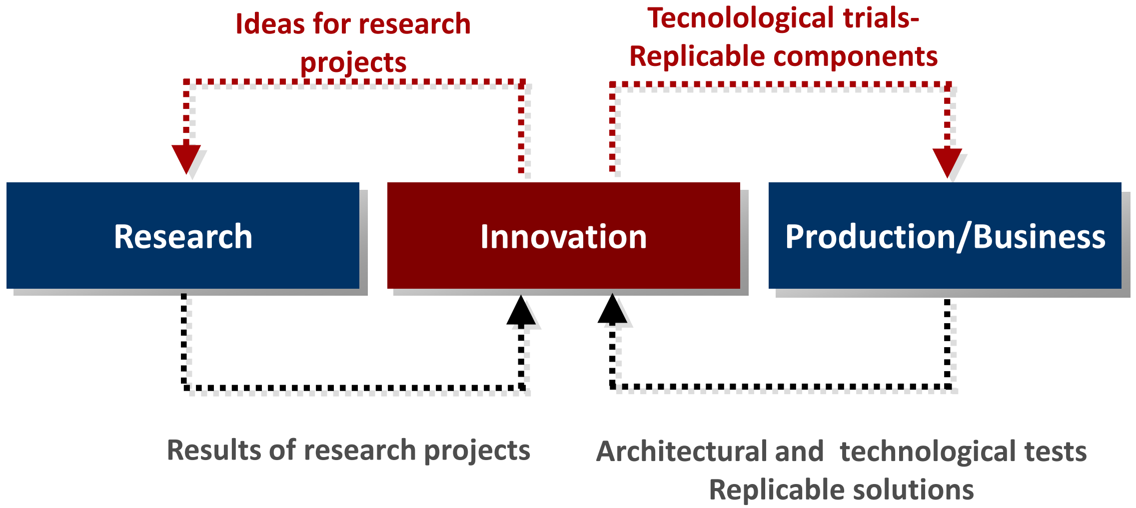
MARKETS AND COMMERCIAL OFFER: MAIN CUSTOMERS

FINANCE Intesa Sanpaolo Group Monte Paschi Siena Group	OIL & SERVICES ENI Group Autostrade per l'Italia Costa Crociere Poste Italiane	INDUSTRY Fiat Group Whirlpool Piaggio Ferrero Lavazza Benetton	
CENTRAL GOVERNMENT Ministries Public Bodies and Agencies Defence and Homeland security authorities and agencies EU bodies and agencies	LOCAL AUTHORITIES All the Italian Regions Italian main Municipalities Provinces Consortiums	HEALTHCARE 51% of hospitals 64% health operators Regions Universities Consortia	ENERGY & UTILITIES Hera Acea Enel THÜGA Group Iride Group

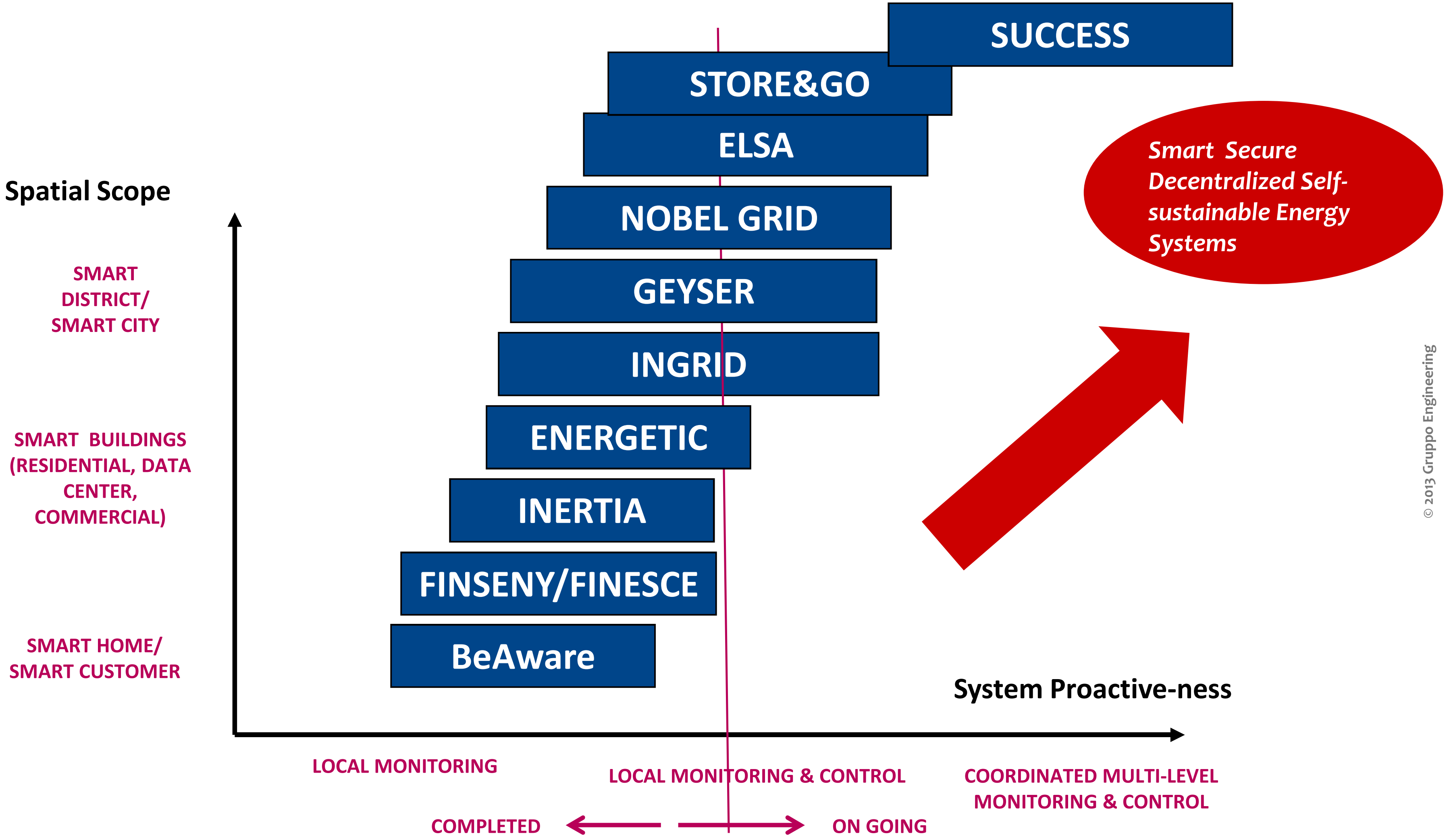
ENGINEERING

- We leverage research and innovation as strategic way to turn on innovative technologies into state-of-the-art commercial products

- Engineering is a very active stakeholder in the European research and innovation on Smart Grid/Smart Energy Systems & Security



Our Smart Grid Innovation Roadmap



ENGINEERING

Security Intelligence

Fight against crime and terrorism

Border and External Security

Digital and Cyber Security

Disaster Resilience (DRS) and
Critical Infrastructure Protection (CIP)

Security Intelligence (Fighting against crime and terrorism)

Video surveillance

ADVISE
Advanced Video Surveillance archives search Engine for security applications

SURVANT
SURveillance Video Archives iNvestigation assisTant

Multimedia forensic data analysis and exploitation

ASGARD
Analysis System for Gathered Raw Data

LASIE
Large Scale Information Exploitation of Forensic Data

SINTESYS
Security Intelligence System
(Open Source Framework for Open Source Intelligence)

DANTE
(Detection of terrorist-related contents over Internet, including Deep Web and Dark Net)

Multimedia analysis in Deep Web and Dark Net

Crowd-sensing/crowd-sourcing in security

TRILLION
Trusted Citizens LEAs Collaboration over Social Networks

Community policing

2012 2014 2016 2018 2020

Disaster Resilience and Critical Infrastructure Protection

Cyber physical protection

IntelliSEC
EIT 2016-17
Toolbox for Security of Critical Infrastructures

SUCCESS
Securing Critical Energy Infrastructures

Physical Protection

STORM
Safeguarding Cultural Heritage through Technical and Organisational Resources Management

SECURE!
Early Warning Detection of critical events for critical infrastructure protection

Crowd-sensing/crowd-sourcing in CIP

2012	2014	2016	2018	2020

ENGINEERING

Digital and Cyber Security - Projects

Research agenda
in cyber security

CAPITAL
Cyber security research Agenda for PrIvacy and Technology chALlenges

COURAGE
Cybercrime and cyberterrOrism (E)Uropean Research AGEnda

Cyber crime and cyber terrorism

Botnets

ACDC
Advanced Cyber Defense Centre

Cyber Communities: knowledge sharing and collective intelligence

CYSPA
European CYber Security Protection Alliance

DOGANA
Advanced Social Engineering and Vulnerability Assessment Framework

Social Engineering

2012 | 2014 | 2016 | 2018 | 2020

Border and External Security - Projects

Earth Observation

SAGRES
Services Activations For Growing Eurosur's Success

Maritime Surveillance Systems

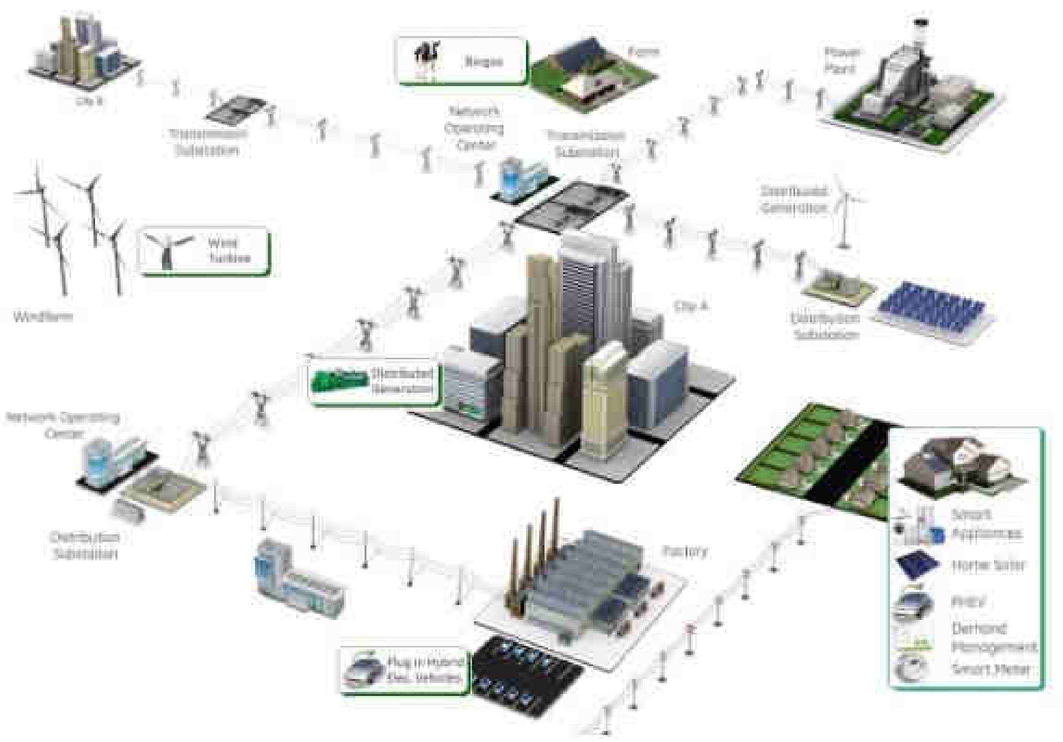
PERSEUS
Protection of EuRopean borders and Seas through the intelligent Use of Surveillance

(Counter-)Piracy

PROMERC
Protection Measures for Merchant Ships

2012 | 2014 | 2016 | 2018 | 2020

- **Critical Energy Infrastructures (CEI)** consist of a dispersed asset of either bulk either decentralized power generation plants, infrastructures for electricity transmission and distribution, and energy prosumers with their smart meters
- CEIs are characterized by vast, widely-diverse infrastructure of assets forming a multifaceted operational environment
    - with complex ownership and regulatory structures,
    - large scale **human involvement** at different levels (O&M, monitoring & control)



- Internet of Everything and Fog Computing
  - rising proliferation of smart devices
  - everyday life depending more and more from power availability

- Critical Energy infrastructures (CEI) are more and more becoming smart infrastructures, where **physical and IT layers are** tightly **interconnected**
  - the latter one in charge for **effective management of the asset** with a view to optimize network technical operation

- Energy sector is ranked first in the **incident lists** with 79 incidents (32%)

- Consequences of CEI outages largely negatively affect our everyday life

...CEI operators/owners are struggling to achieve **appropriate yet cost-effective security and protection for their infrastructures** over the time

- **Disjoint management** of **cyber** and **physical/technical security**

- "**Unlimited capacity**" models for security management
  - Security as a resource with limited availability -> Life Cycle Assessment models yet to come

- Static governance models for security and static risk/vulnerability assessment

- Insufficient **HILT (Human-In-The-Loop)**

- Small yet insufficient emphasis on resilience

- Impact of **Smart grid and decentralization** not adequately reflected into the current paradigms for CEI protection

•Nowadays **cyber and system-theoretic** approaches, as **individually used** for CEI protection, build on **incomplete attack models**, thus resulting in **silos-like** security management fragmented operational policies, and failing to provide appropriate security- and resilience-by-design.

•The system and attack models of both approaches are incomplete:

•**cyber security** approaches do not model the physical system, concentrating on the protection of the integrity of data measurements by using secure devices and secure communication protocols

•However, integrity of sensors and related managed data security can be broken by modifying the physical state of the system (e.g. via meters by-passing or due to unstable grid performance)

•On the other hand **cyber-attacks (es over the SCADA)** may result in false network state representation, potentially creating technical problems to the power network components, like feeder, transformers etc.

CEI as Resilient Cyber Human-enriched Physical Systems

• critical energy infrastructures modelled as distributed, large scale complex **resilient and human-enriched Cyber-Physical systems** which

•are able to take into due consideration the **potential reciprocal effects of cyber versus physical threats**

•operate within the framework of a **novel dynamic and adaptive security governance model**, which leverages on lifecycle assessment to manage security as a limited yet costly resource to be managed over the time

•bring **humans center stage** by empowering people as **virtual sensors** to contribute to threat detection and/or as **situated first order emergency responders** to accidents, disasters or attacks, or by simultaneously considering workforce as potential threats to CEi security

• suitably addresses how the **emerging decentralization of energy systems** challenge affect CEI protection (es NORM decentralized smart meter in SUCCESS)

  - •reduced information exchange with the central processing hub against extra threats due to insufficient DER security enforcement
  - •replacement of proprietary protocols and closed networks with standard open Internet protocols and shared networks ->Malicious attackers capable of exploiting protocol and network insecurities can target CPS operations

•Our framework manages:

• **information gathered through a range of** devices/technologies for situational awareness (fixed sensors like PMUs, mobile devices like drones and advanced video surveillance) for **situation awareness** (layer 1)

• **intelligent processing** for cyber-physical threat detection combined with a toolbox for incident mitigation, emergency response and fast restoration, and Human-In-The-Loop for managing humans interaction with CEI (layer 2)

•Blue prints, guidelines/lesson leants as knowledge sharing/spreading (layer 3)

Layer 1: CEI Situational Awareness

Layer 1 combines **fixed and mobile sensors and devices for physical and cyber information** gathering with **humans acting as decentralized nearby virtual sensors**

- **Physical information gathering** sensors: integrating audio-visual information from visual and laser technologies and swarms of drones with infrared/thermal or corona cameras to get close-up, 3-D images of
  - wind blades to find out if there are any scratches or imperfections without having to stop the turbines
  - PV parks for inspecting surface grazes and
  - transmission and distribution networks for damaged isolators.
- **Cyber information gathering**: managing combined data from existing IDS, SCADA, Smart Meters and Advanced Metering Infrastructure (AMI), and low cost Phasor Measurement Unit (PMU).
- **Human Sensors information gathering**: managing human sensors (crowd-sensing), with a view to empower citizens living in the vicinity of the power network installations, to act as “decentralized sensors and acting as first level emergency responders

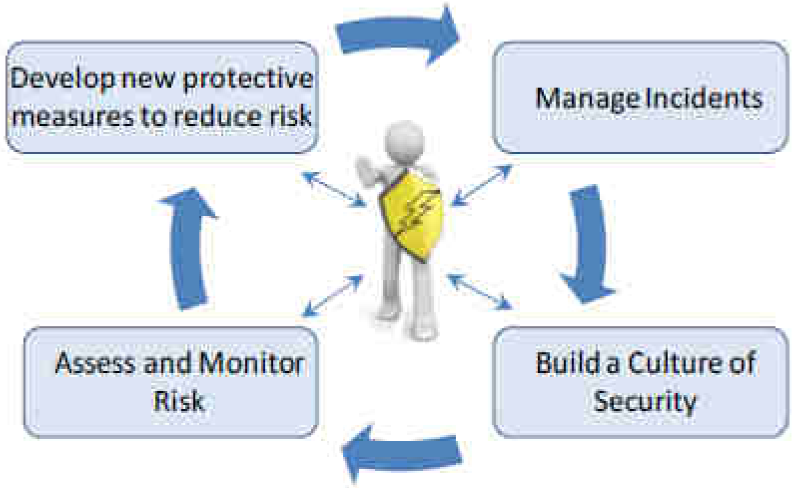
ENGINEERING

•Central in this framework is **dynamIc adaptable contermeasures toolbox**, in charge of:

•**anticipated physical and cyber-physical threat/ attack prevention,** while prioritizing the more relevant information (availability, integrity, privacy/ confidentiality) and infrastructure security objectives achievements along their effect in the network

•**dynamically triggering the most suitable countermeasures** for the detected attack, depending from the deployed scenario and the actual context-based security need

•**Risk and vulnerability assessment:** thorough understanding of their current security posture, enabling them to continually assess evolving cyber/physical threats and vulnerabilities, their risks, and potential countermeasures (continuous security state monitoring)

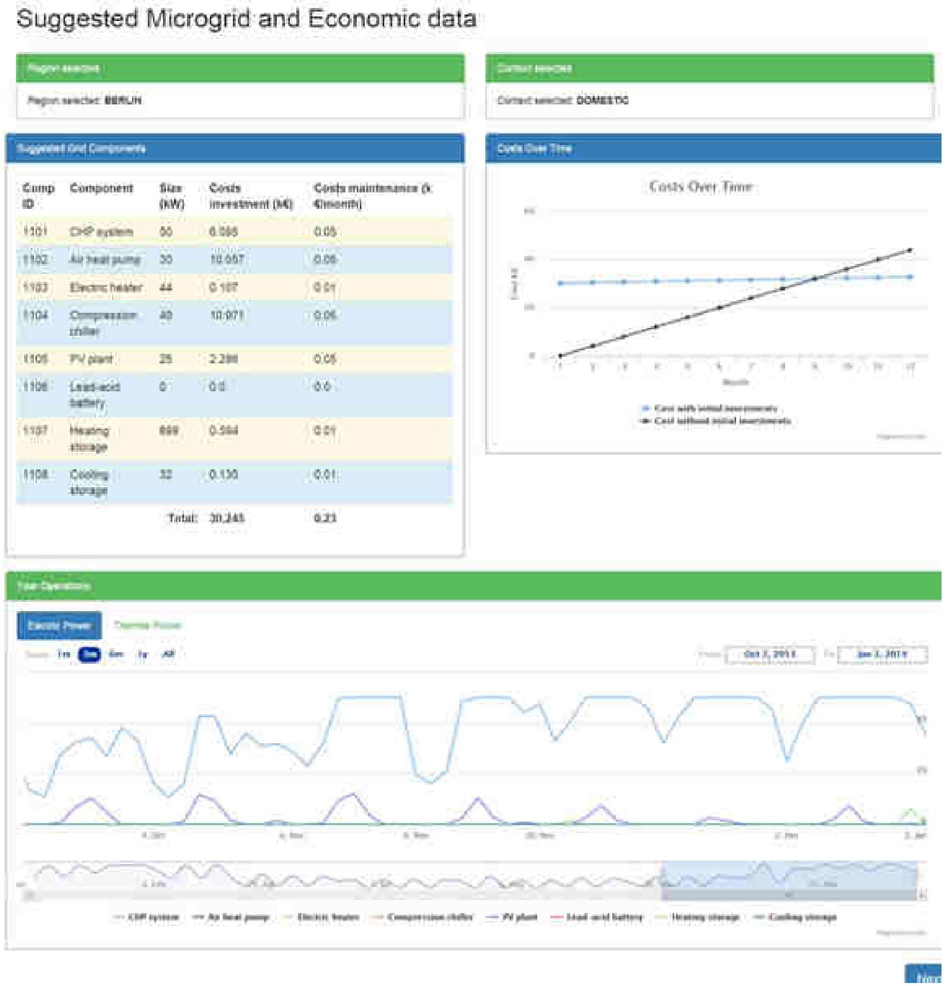


•New **protective measures for risk mitigation** to reduce risk by design. (including vulnerabilities and emerging threats assessment and preventive mitigation strategies)

•**Incidents management for fast CEI secure operation restoration**: when protective measures are not applied or fail to prevent an incident, detection, remediation, recovery, and restoration activities will minimize its impact and quickly return to normal operation

- •Integration among outage management systems and DER flexibility management to mitigate grid outages (es prosumer microgrids or storage for black start) is fundamental to ensure CEI resilience by-design

•**Culture of Security Spreading**: Post-incident analysis and forensics enable CEI stakeholders to learn from the incident, integrated with reliability practices, Human-In-The-Loop management



ENGINEERING