

DEFENDER

Defending the European Energy Infrastructures

Critical Infrastructure Protection Topic 1

Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe

Dr. Massimo Bertoncini, Senior Innovation Manager for Smart Energy
Engineering Ingegneria Informatica (ENG)



This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 740898



1

DEFENDER Consortium

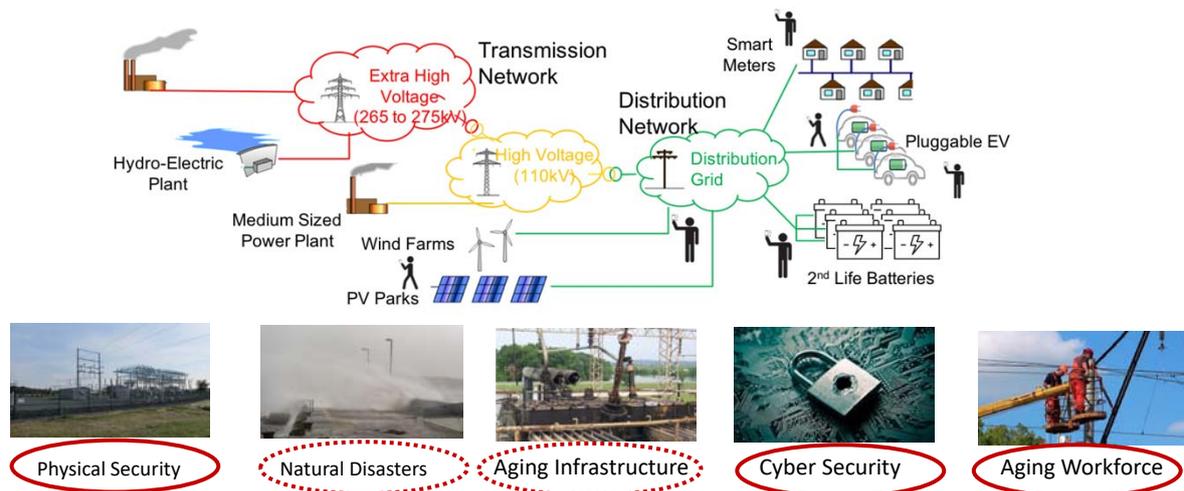
Defending the European Energy Infrastructures

- **Call Identifier:** CIP-2016-2017-1
- **Starting Date:** 1 May 2017
- **Duration:** 36 months
- **Action Type:** Innovation Action
- **EU Maximum financial grant:** 6.790.837,50 €
- **Partners:** 18 (from 9 countries)
- **Country coverage:** Italy, Greece, France, Romania, Germany, Slovenia, Portugal, UK, Israel



2

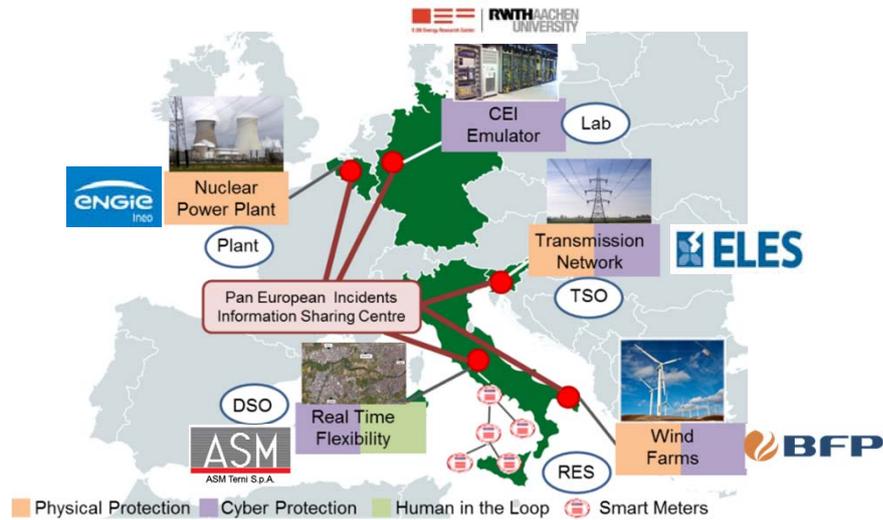
DEFENDER Scope



DEFENDER Main Objectives

1. Analyse CEI **threats and risks**, create methodology for **predicting new/et unknown risks**
2. Gain **CEI situation awareness, perception** and **comprehension** by interfacing Physical & Cyber sensors and metering devices and by utilising a Cyber-Physical Social System (CPSS) co-simulator
3. Develop methodologies and tools for innovative, **trusted, private and traceable bidirectional information flows**
4. Implement a novel dynamic **countermeasures toolbox** for physical and cyber threat/ accidents/ attack prevention
5. Integrate dynamic threat, vulnerability analysis and attack detection to **trigger the most suitable countermeasures**
6. Coordinate, synchronize and cross-validate information exchange on physical and cyber attacks patterns and countermeasures, via a **CEI Incidents Information Sharing Platform (I2SP)**
7. Initiate and coordinate the **Critical Energy Infrastructure Security Stakeholders Group (CEIS-SG)**

DEFENDER Trials and Testbeds



5

Main DEFENDER Innovations

The content of this slide has been omitted

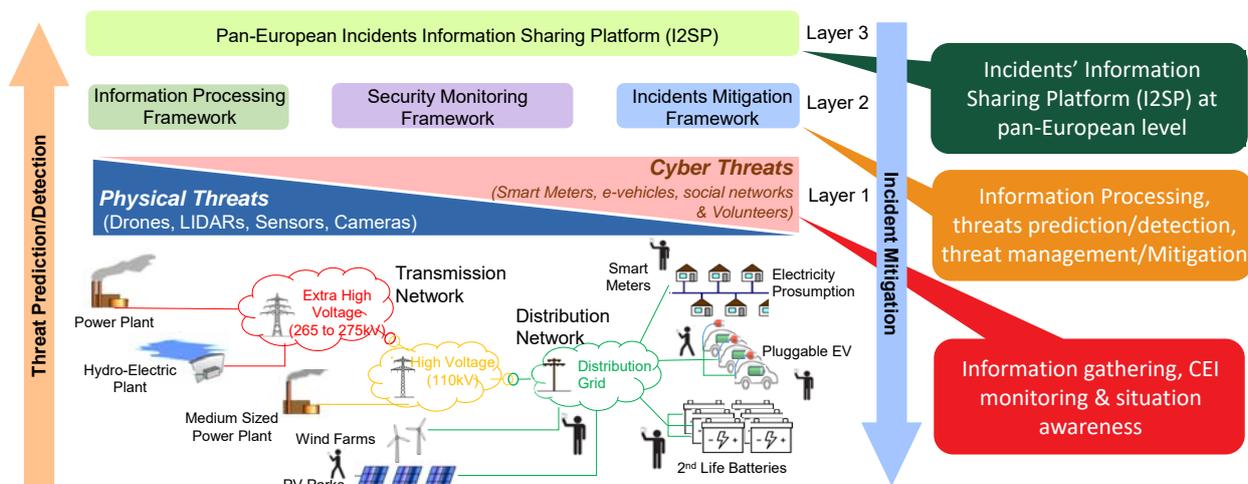
6

Main DEFENDER Innovations

The content of this slide has been omitted

7

DEFENDER Overall Architecture



8

Towards securing CEI

From CEI monitoring to attack mitigation



This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 740898



9

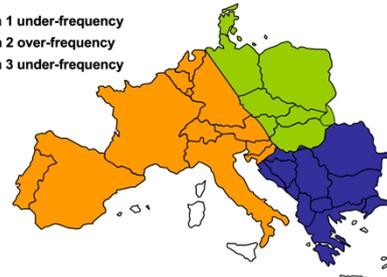
Examples of attacks on smart grid infrastructures

Ukrainian grid cyber attack (Dec. 2015)

1. Compromise of corporate networks via emails infected with phishing malware (**at least 6 months!**)
2. Took **SCADA control**, then remotely switching off 43 substations
3. Disabled **IT infrastructure components**
4. Destructed of files stored on servers and workstations with the **KillDisk** malware
5. Denial-of-service **attack on call centres** to deny consumers updating on the blackout.

European blackout (Nov. 2006)

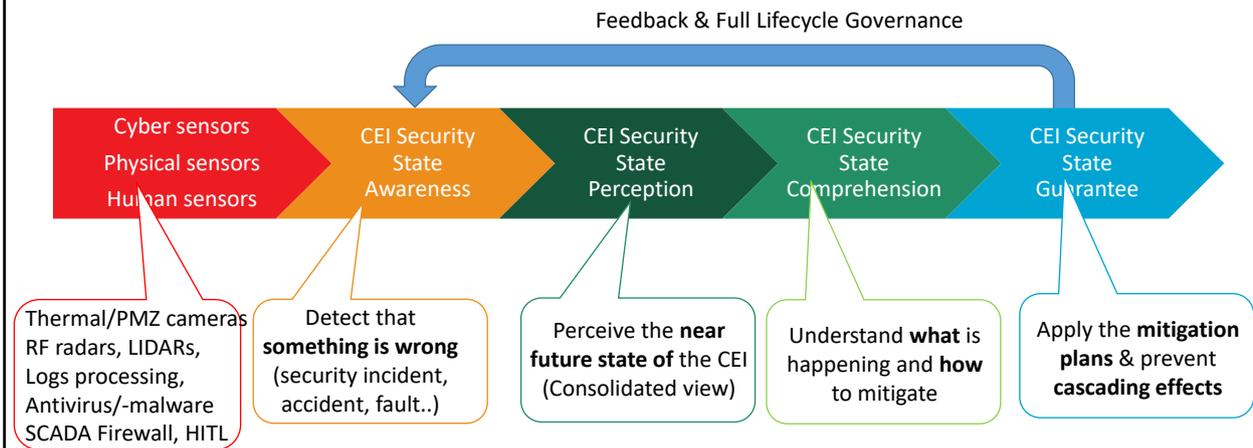
- Area 1 under-frequency
- Area 2 over-frequency
- Area 3 under-frequency



- Accidental
- Non fulfilment the N-1 criterion
- Insufficient inter-TSO co-ordination

10

From Monitoring to CEI Security Guarantee



From CEI security state Awareness to Comprehension

The content of this slide has been omitted

CEI Security Guarantee



The content of this slide has been omitted

People acting as cyber security sensors

The content of this slide has been omitted

Towards satisfying CEI communications requirements

The content of this slide has been omitted

CEI Security Stakeholders Group (CEIS-SG)

A group of **executive volunteers** and **decision makers** to ...

- ✓ **share information & best practices** on CEI risks, threats, countermeasures, ...
- ✓ **periodically review & challenge** risk management practices
- ✓ **confirm** that emerging threats do not diminish their effectiveness ...
- ✓ coordinate **CEI security preparedness planning** and **roadmap**

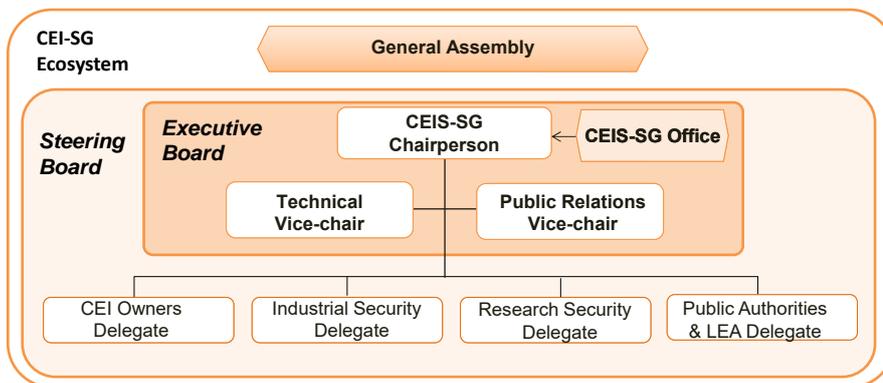
Goal: European CEIs are able to

Survive Large scale, combined, cyber-physical-social incidents and accidents

Guarantee Continuity of operations while minimizing the cascading effects.

Coordinate Safer CEI planning/roadmap

CEI-SG Participants & Structure



Thank you

Discussion