

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

Programme Committee Meeting Brussels, 18th October 2019

Gabriele Giunta

DEFENDER Project Coordinator
Engineering Ingegneria Informatica Spa

David Bernelle

Project Manager
ENGIE – R&D Center (CRIGEN) – Lab Robotics



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



1

DEFENDER identity card

- **Call Identifier:** H2020 CIP-2016-2017-1
- **Title:** *Defending the European Energy Infrastructures*
- **Starting Date:** 1 May 2017
- **Action Type:** *Innovation Action*
- **Duration:** 36 months (Closing Date: 30/4/2020)
- **EU Contribution:** 6.790.837,50 €
- **Partners:** 18 (from 9 countries)
- **Country coverage:** *Italy, Greece, France, Romania, Germany, Slovenia, Portugal, UK, Israel*
- **Website:** <http://defender-project.eu/>






ICT Service & Technology providers

-    (ICT)
-  (Security)
-     (SME - Solution Provider)
-  (Data Privacy/Protection Enforcement)

R&D/Academy



Stakeholders

-  Electricity Network and Distribution Sys Operator
-  Electricity Supplier, Bulk Generation
-  Electricity Supplier, Wind Farm
-  Electricity Network and Transmission Sys Operator
-  Law Enforcement Agency

2

Which are the problems DEFENDER address?



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

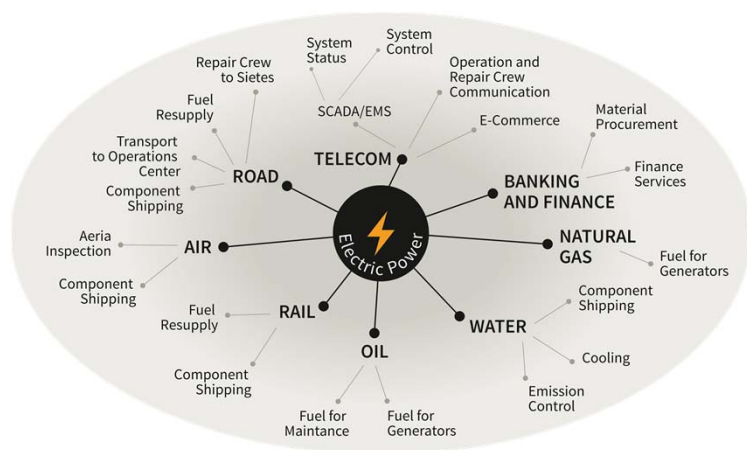


3

While recognising the threat from terrorism as a priority, the protection of critical infrastructure will be based on **an all-hazards all-sectors approach**.

Critical Infrastructures depend on each other, but...

... all the other critical infrastructures have a **strong dependency from Critical Energy Infrastructures**

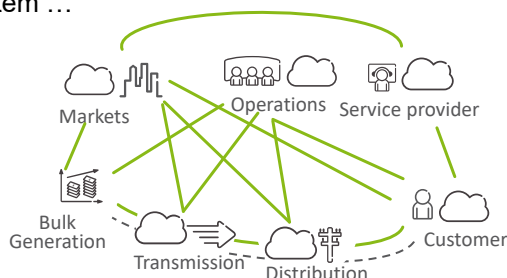


Source: European Programme for Critical Infrastructure Protection - Council Directive 2008/114/EC
 Source: A new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure EPCIP [SWD (2013) 318]

4

Security is fundamental for smart critical energy infrastructures (CEIs)


ICT provides new opportunities to gather and analyze performance data, making it possible to preemptively notice and remedy technical vulnerabilities in the system ...



... but the **increased interconnectivity associated with ICT** exposes CEIs to increased **cyber-risks and vulnerabilities**, and global **security** issues that arise in the **interaction between the cyber and the physical, institutional and human layers of the system**

Cyber attacks on the power grid are constantly **increasing in sophistication**

Fragmented landscape of innovative solutions for CEIs

- Limits in the **threat scope** (e.g. either cyber or physical threats)
- Limits in the **coverage of the energy value chain** (from generation to consumer, from operation to market) 
- Limits within the **organisation, silos** (e.g. technical, operations, business)
- Rarely involving **human dimension** (citizens or workers)
- **Little systematic relationship** between Power Network Operators and Security Operators/Service Providers and/or Law Enforcement Agencies
- Interaction and underlying procedures for linking **Power Network Operators** with **Computer Emergency Response Teams (CERTs)** and **Information Sharing & Analysis Centres (EE-ISAC)** still challenging at both **governance and technological levels**

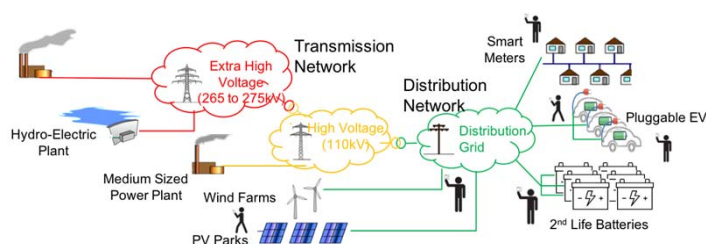
EU Policy Goals

- **Reducing the vulnerabilities of critical infrastructure and increasing their resilience is one of the major objectives of the EU !!!**
- Ongoing processes in EU Commission according to European Programme for Critical Infrastructure Protection are:
 - Collection of CIP related best practices, risk assessment tools and methodologies
 - Commissioning studies concerning interdependencies
 - Implementation of minimum protection measures
- Ongoing processes of collecting suggestion for updating COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructures and the assessment of the needs to improve their protection

DEFENDER Scope

MISSION

DEFENDER aims at safeguarding existing and future European CEI operation over **cyber-physical-social threats**, developing a **new approach** based on **novel protective concept for lifecycle assessment, resilience and self-healing** offering **Security-by-design**, and **advanced intruder inspection and incident mitigation systems**



Physical Security



Natural Disasters



Aging Infrastructure



Cyber Security



Aging Workforce

Achieved results



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



DEFENDER (up to date) achieved results #1



The content of this slide has been omitted

DEFENDER (up to date) achieved results #2



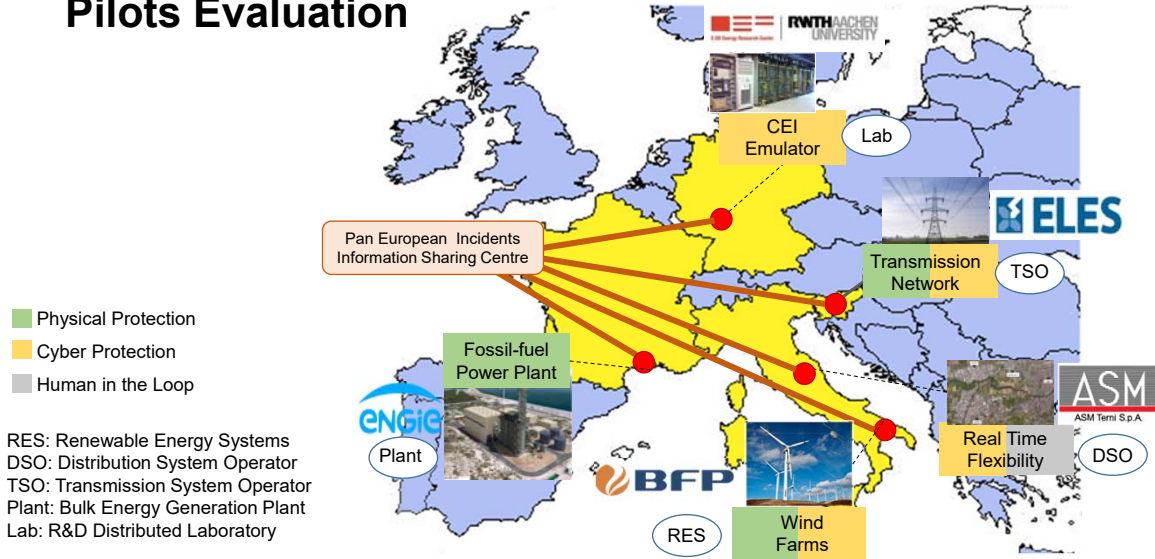
The content of this slide has been omitted



Ongoing activities



Pilots Evaluation



Bulk Energy Generation pilot

The content of this slide has been omitted

Decentralized RES* Generation pilot

The content of this slide has been omitted




TSO* Network pilot

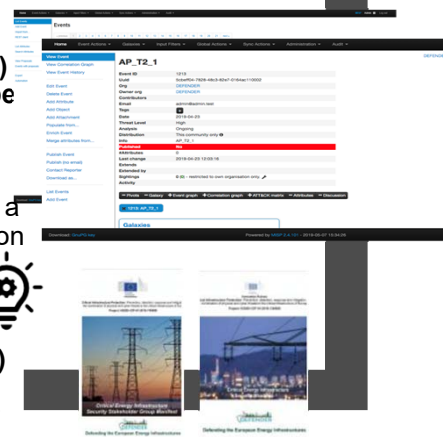
The content of this slide has been omitted

DSO* Network & Prosumer pilot

The content of this slide has been omitted

Other ongoing activities

- 
CEI Incidents Information Sharing Platform (I2SP) enabling information exchange on **physical and cybe attacks patterns and countermeasures** at Pan-European level
- 
 Promote learning and information exchange towards a **Culture of Security** via wide audience communication channels, targeted industrial or scientific events
- 
 Initiate and coordinating the Critical Energy Infrastructure Security Stakeholder Group (**CEIS-SG**) as a **pan-European stakeholders' eco-system** to define the roadmap for next generation **CEI security by design and by default.**



DEFENDER contribution to EU policy goals

- Analysis of **new and future** complex threats to CEI
- Analysis of **selected scenarios** of threats to CEI (attack tree method evaluation)
- Analyses of processes and procedures that address certain **security gaps** in the field of physical and cyber security including human in the loop approach)
- Analysis of **interdependency** between CEI and other CI sectors
- Establishment of DEFENDER Critical Energy Infrastructure Security Stakeholders Group (**CEIS-SG**) (exchanging best practices, new knowledge and developments)



*Defending the European
Critical Energy Infrastructure*

Thank you for your attention

For further information do not hesitate to contact me at the following email: gabriele.giunta@eng.it

