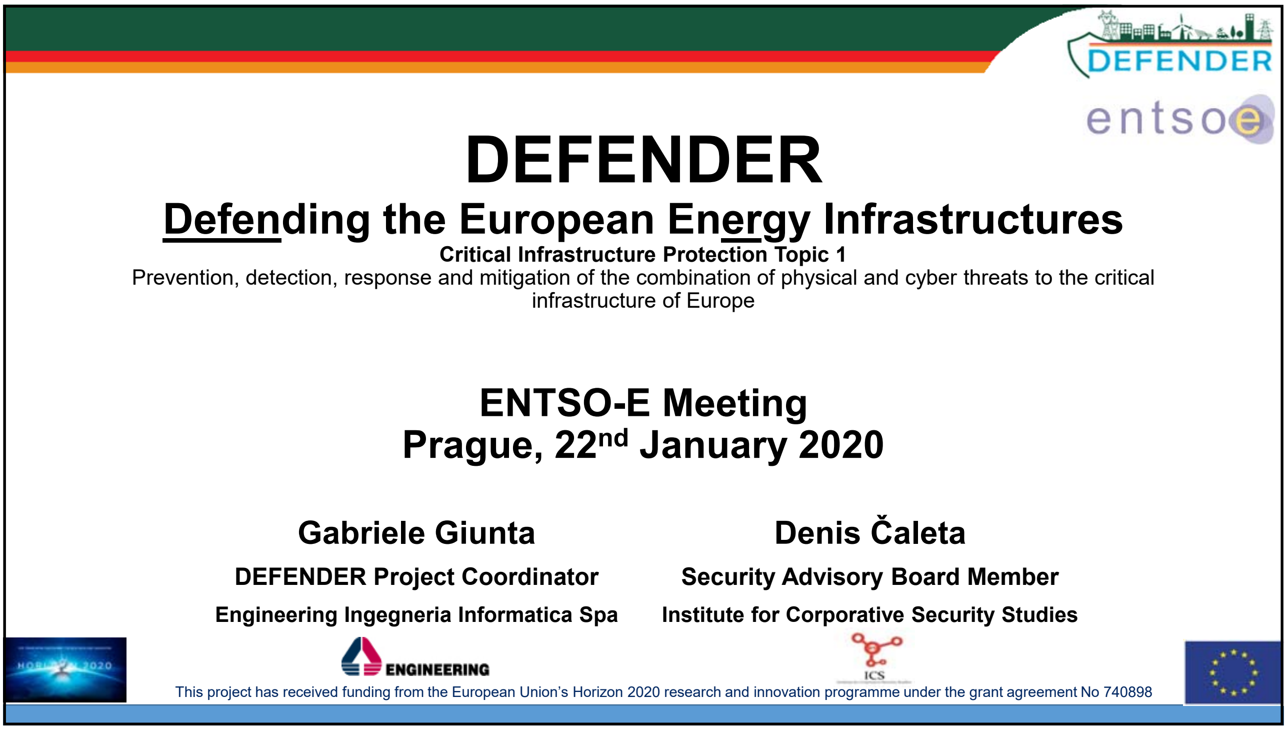


DEFENDER

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

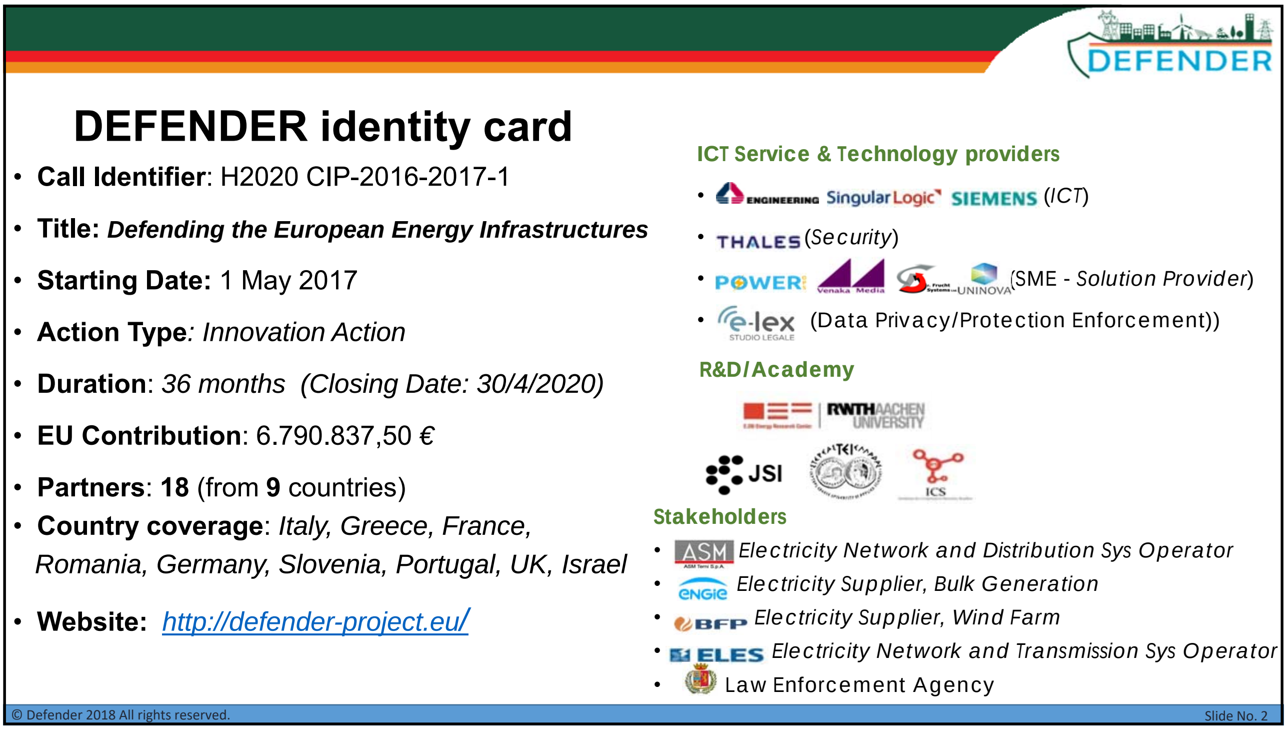
ENTSO-E Meeting
Prague, 22nd January 2020

Gabriele Giunta
DEFENDER Project Coordinator
Engineering Ingegneria Informatica Spa

Denis Čaleta
Security Advisory Board Member
Institute for Corporative Security Studies

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

- ENGINEERING SingularLogic SIEMENS (*ICT*)
- THALES (*Security*)
- POWER Venaka Media UNINOVA (SME - *Solution Provider*)
- e-lex STUDIO LEGALE (Data Privacy/Protection Enforcement))

R&D/Academy

RWTH AACHEN UNIVERSITY

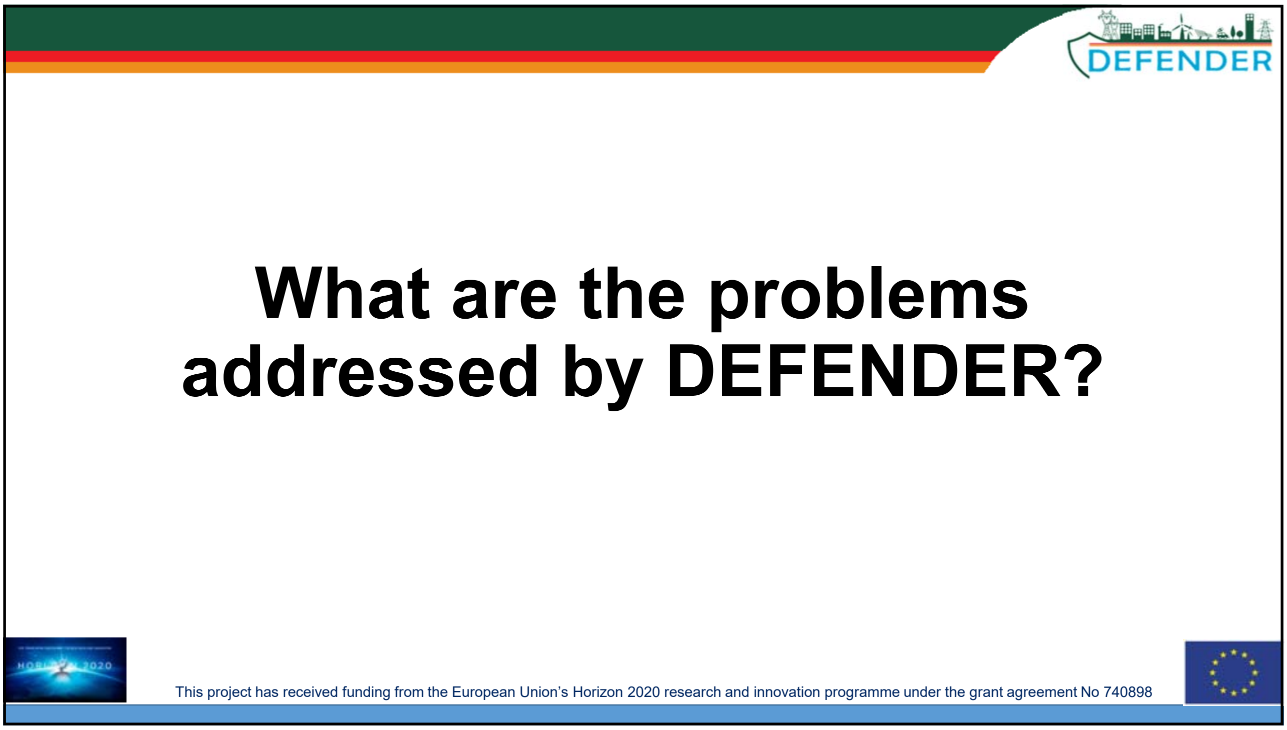
JSI

ICS

Stakeholders

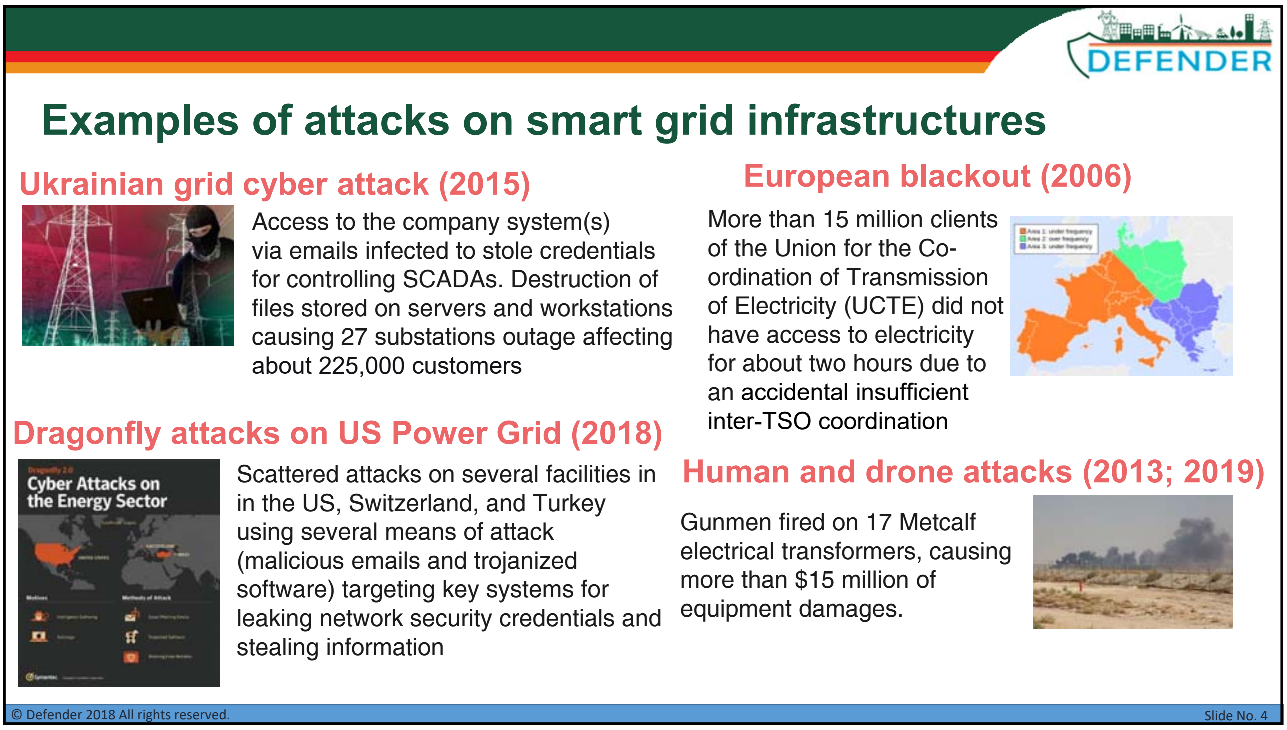
- ASM *Electricity Network and Distribution Sys Operator*
- ENGIE *Electricity Supplier, Bulk Generation*
- BFP *Electricity Supplier, Wind Farm*
- ELES *Electricity Network and Transmission Sys Operator*
- Law Enforcement Agency

2



What are the problems addressed by DEFENDER?

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



Examples of attacks on smart grid infrastructures

Ukrainian grid cyber attack (2015)

Access to the company system(s) via emails infected to stole credentials for controlling SCADAs. Destruction of files stored on servers and workstations causing 27 substations outage affecting about 225,000 customers

European blackout (2006)

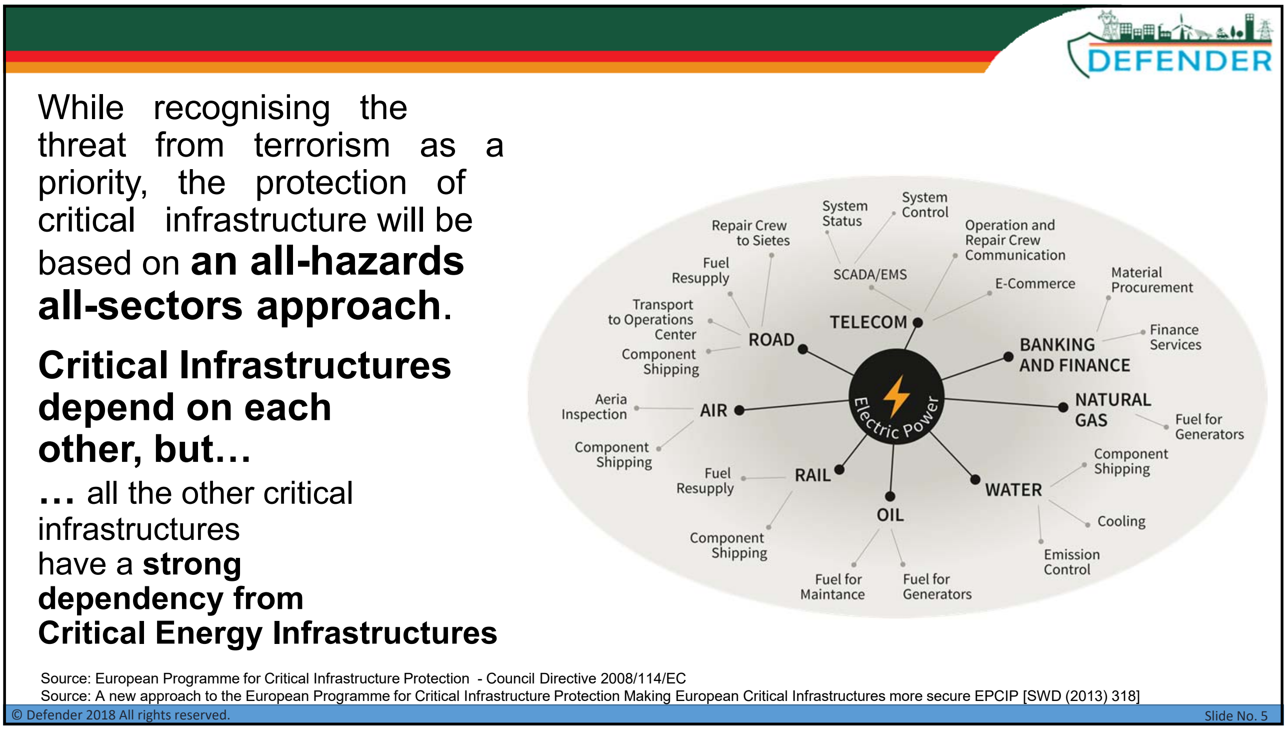
More than 15 million clients of the Union for the Co-ordination of Transmission of Electricity (UCTE) did not have access to electricity for about two hours due to an accidental insufficient inter-TSO coordination

Dragonfly attacks on US Power Grid (2018)

Scattered attacks on several facilities in in the US, Switzerland, and Turkey using several means of attack (malicious emails and trojanized software) targeting key systems for leaking network security credentials and stealing information

Human and drone attacks (2013; 2019)

Gunmen fired on 17 Metcalf electrical transformers, causing more than $15 million of equipment damages.

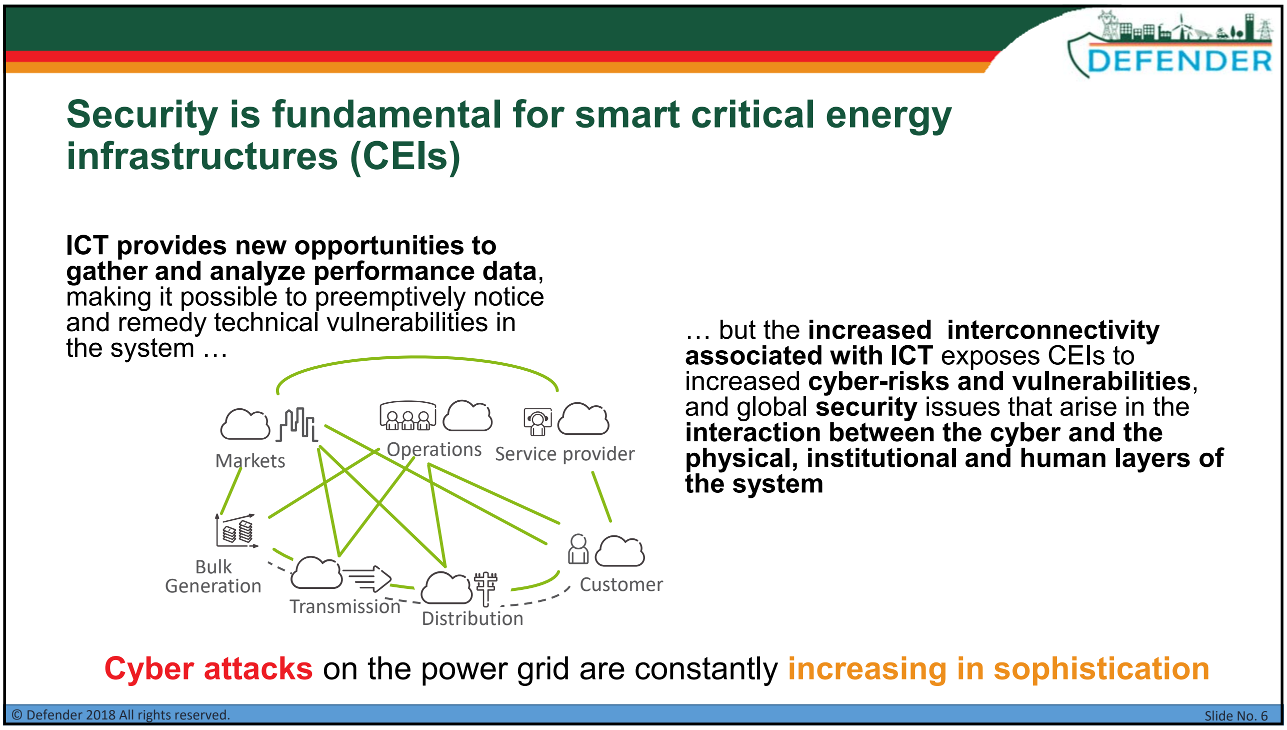


While recognising the threat from terrorism as a priority, the protection of critical infrastructure will be based on **an all-hazards all-sectors approach.**

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]



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**

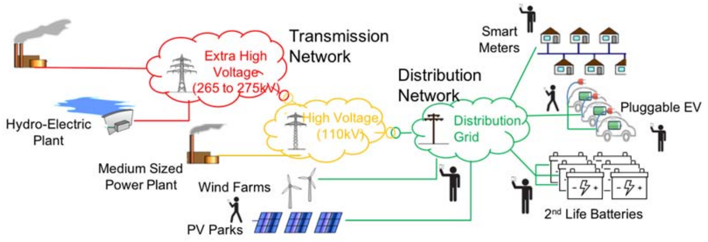
Fragmented landscape of innovative solutions for CEIs

- 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**

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



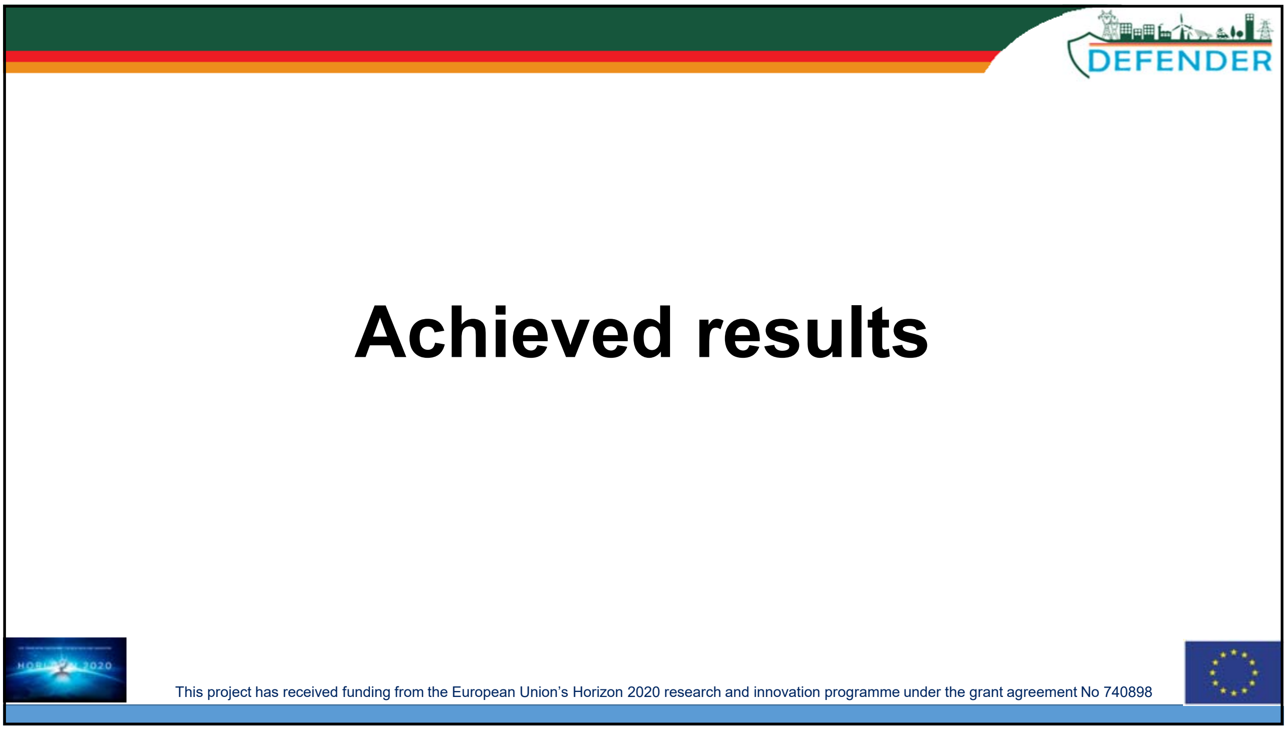
Physical Security

Natural Disasters

Aging Infrastructure

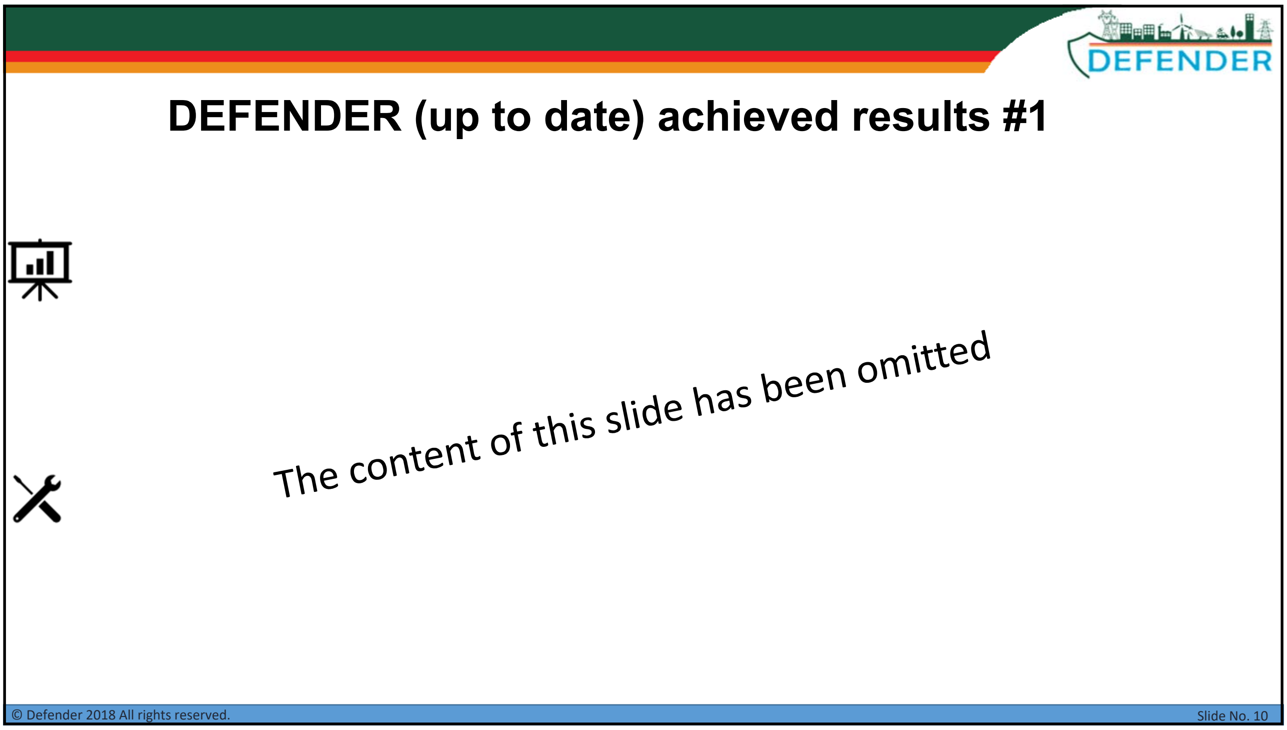
Cyber Security

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



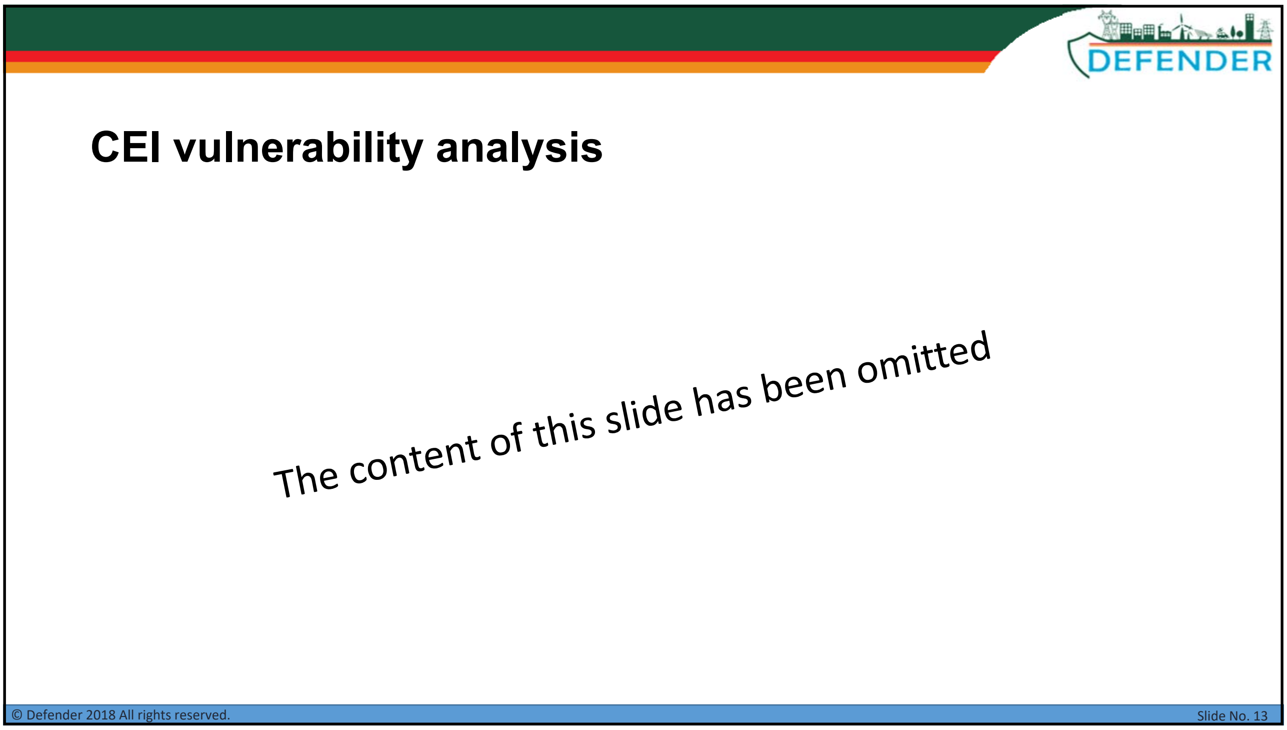
DEFENDER (up to date) achieved results #1

The content of this slide has been omitted

From CEI State of the Environment to Comprehension

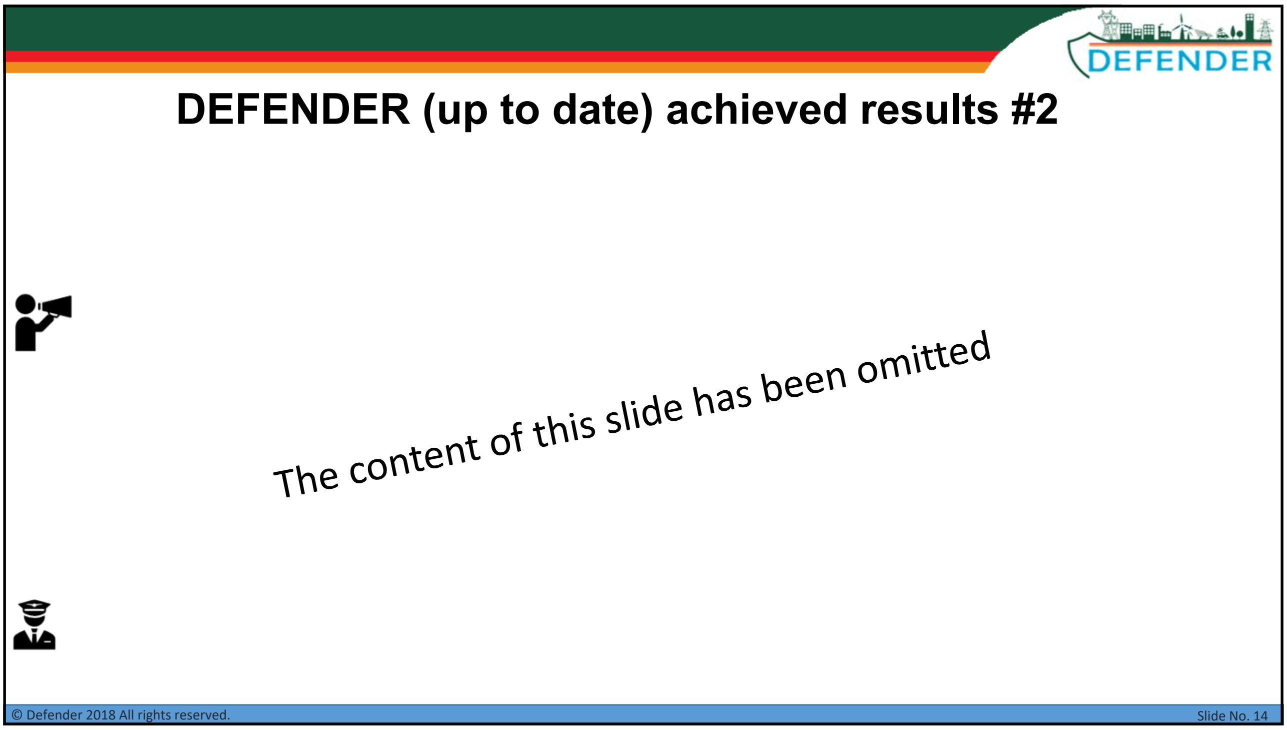
The content of this slide has been omitted

The content of this slide has been omitted



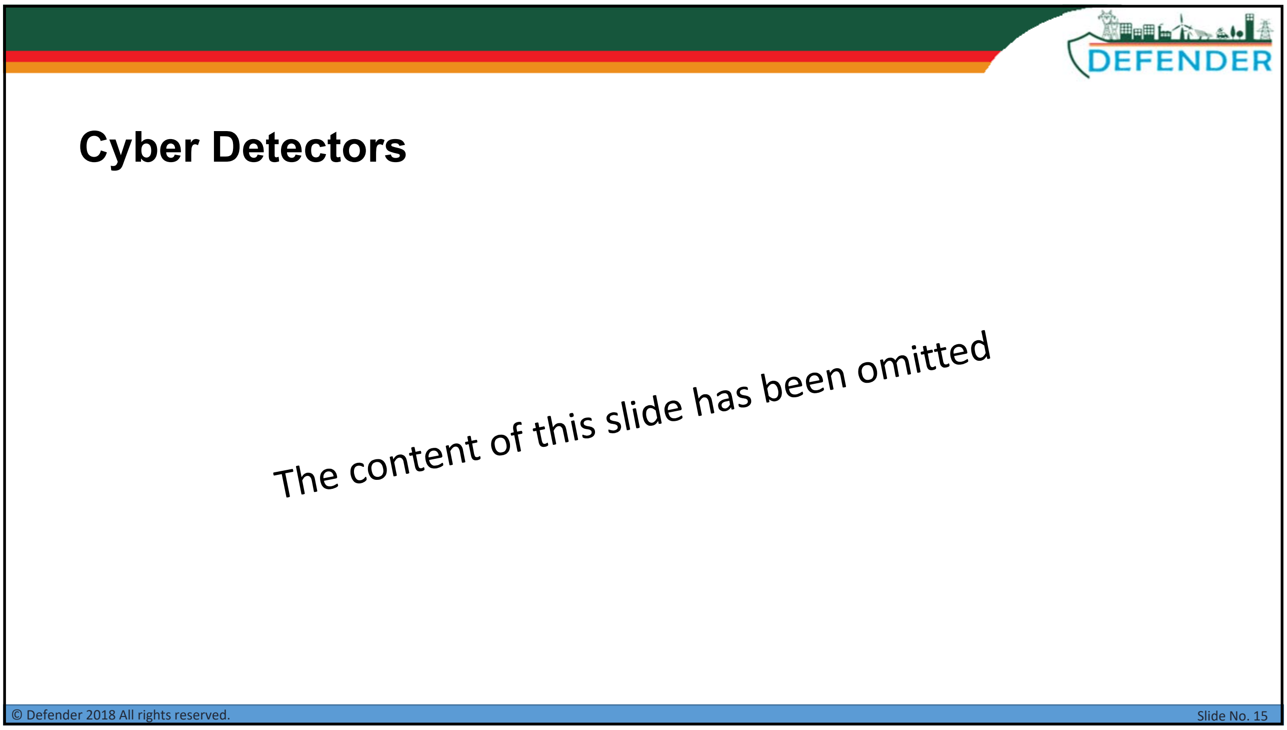
CEI vulnerability analysis

The content of this slide has been omitted



DEFENDER (up to date) achieved results #2

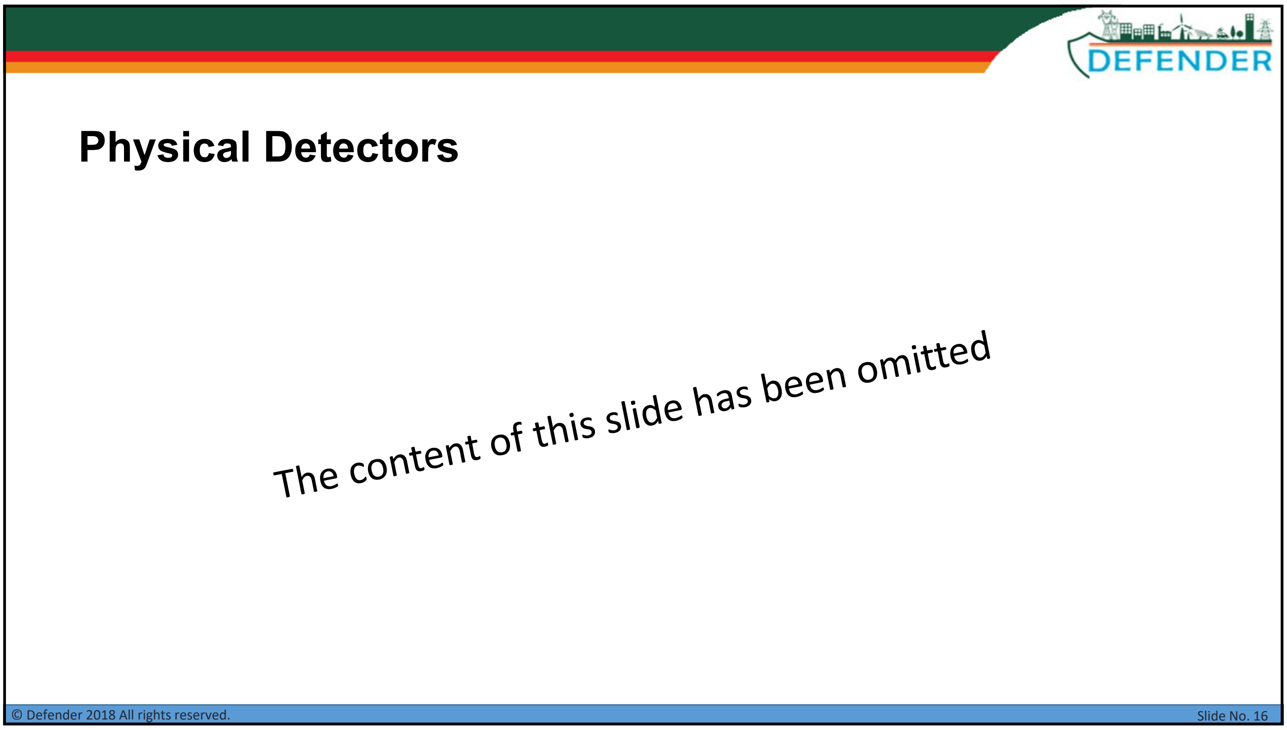
The content of this slide has been omitted



Cyber Detectors

The content of this slide has been omitted

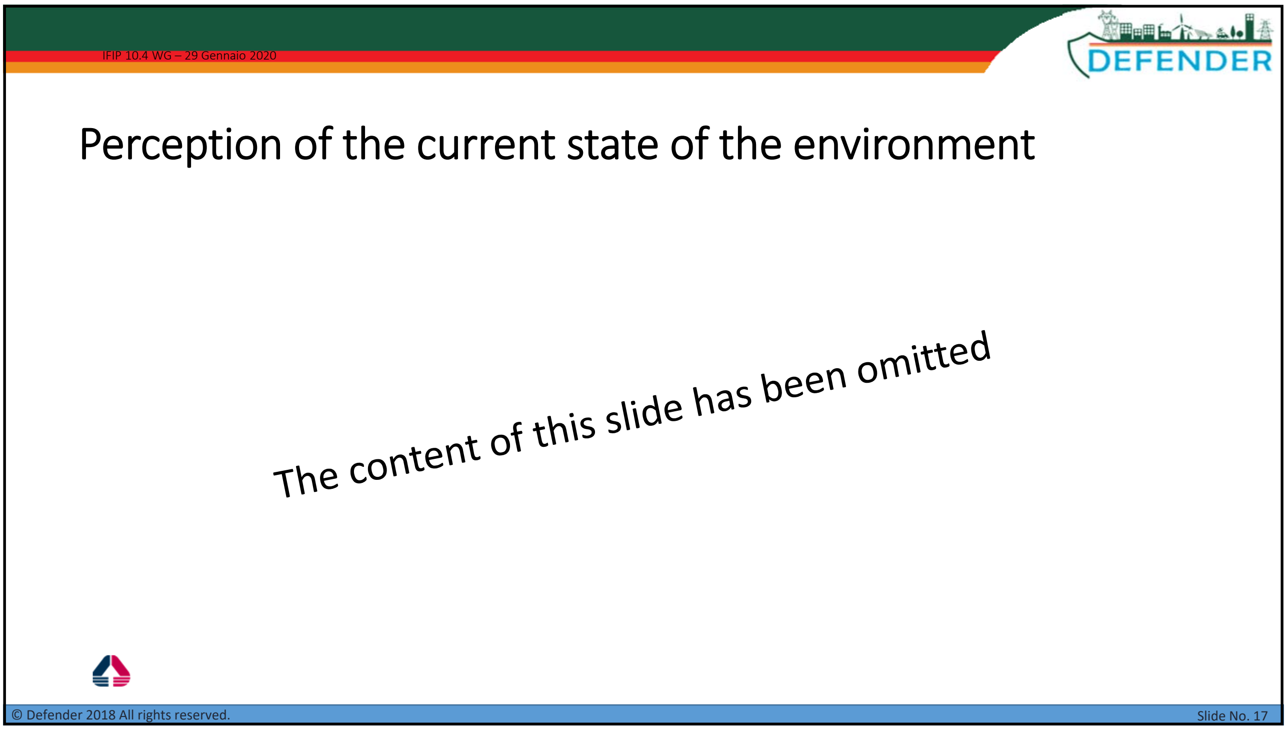
15



Physical Detectors

The content of this slide has been omitted

16



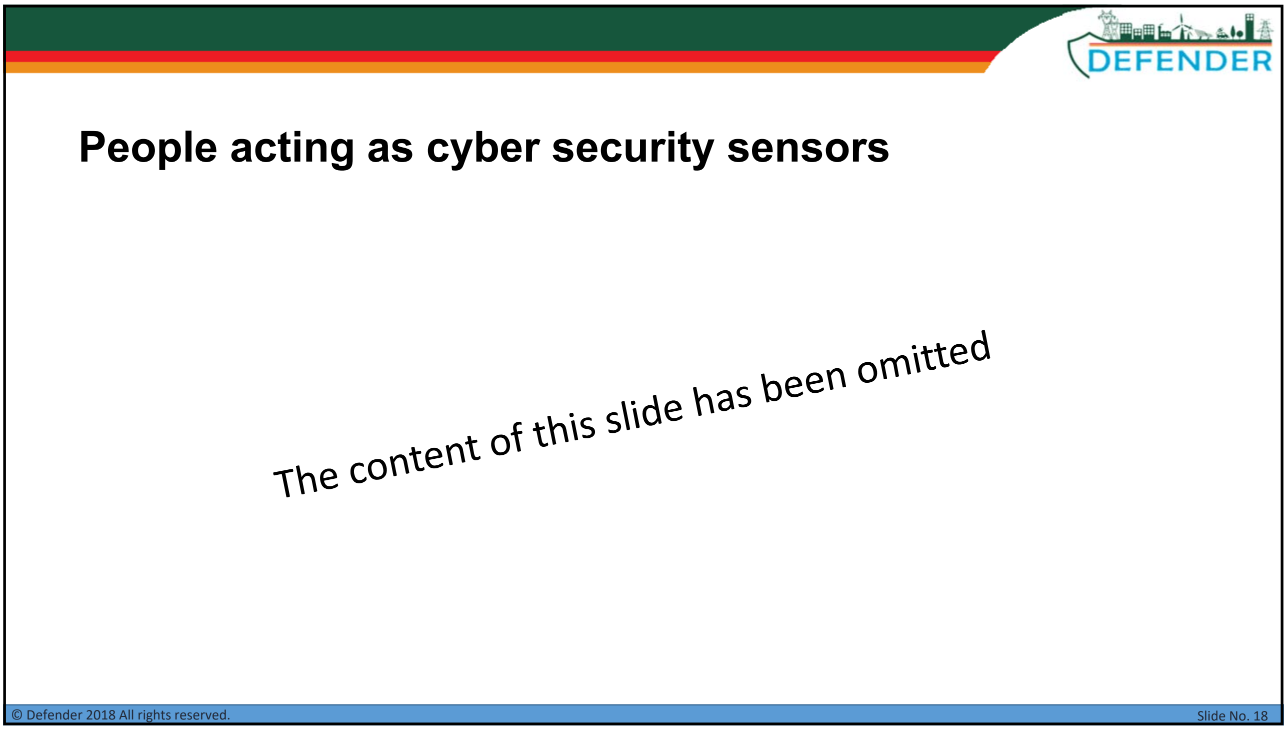
IFIP 10.4 WG – 29 Gennaio 2020

DEFENDER

Perception of the current state of the environment

The content of this slide has been omitted

17



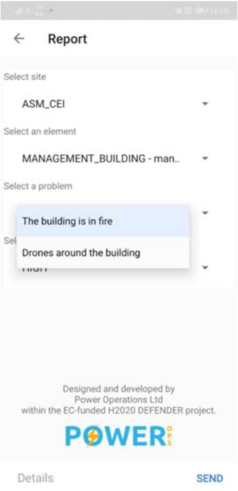
DEFENDER

People acting as cyber security sensors

The content of this slide has been omitted

18

Human-In-The-Loop (HITL) mobile app



Report

Select site

ASM_CEI

Select an element

MANAGEMENT_BUILDING - man..

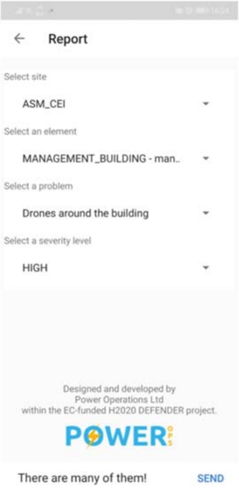
Select a problem

The building is in fire

Drones around the building

HIGH

Designed and developed by
Power Operations Ltd
within the EC-funded H2020 DEFENDER project.



Report

Select site

ASM_CEI

Select an element

MANAGEMENT_BUILDING - man..

Select a problem

Drones around the building

Select a severity level

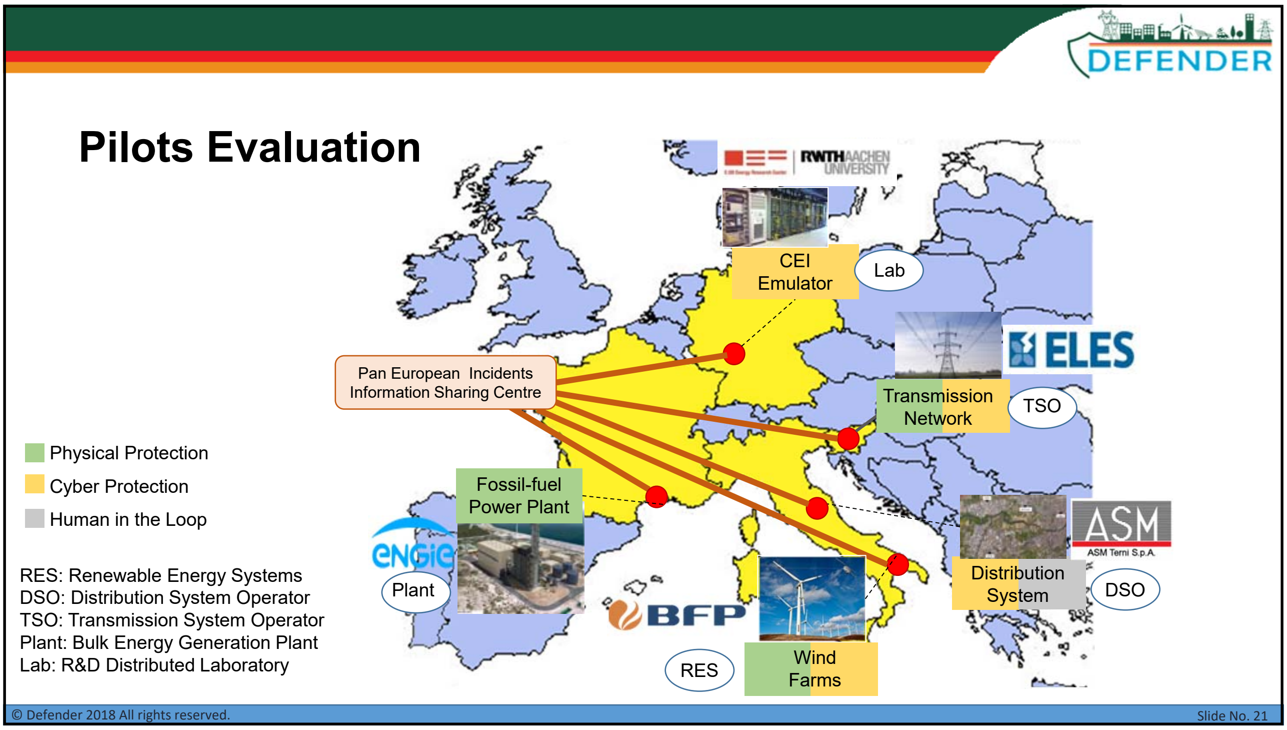
HIGH

Designed and developed by
Power Operations Ltd
within the EC-funded H2020 DEFENDER project.

There are many of them!

Ongoing activities

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



Pilots Evaluation

🟩 Physical Protection

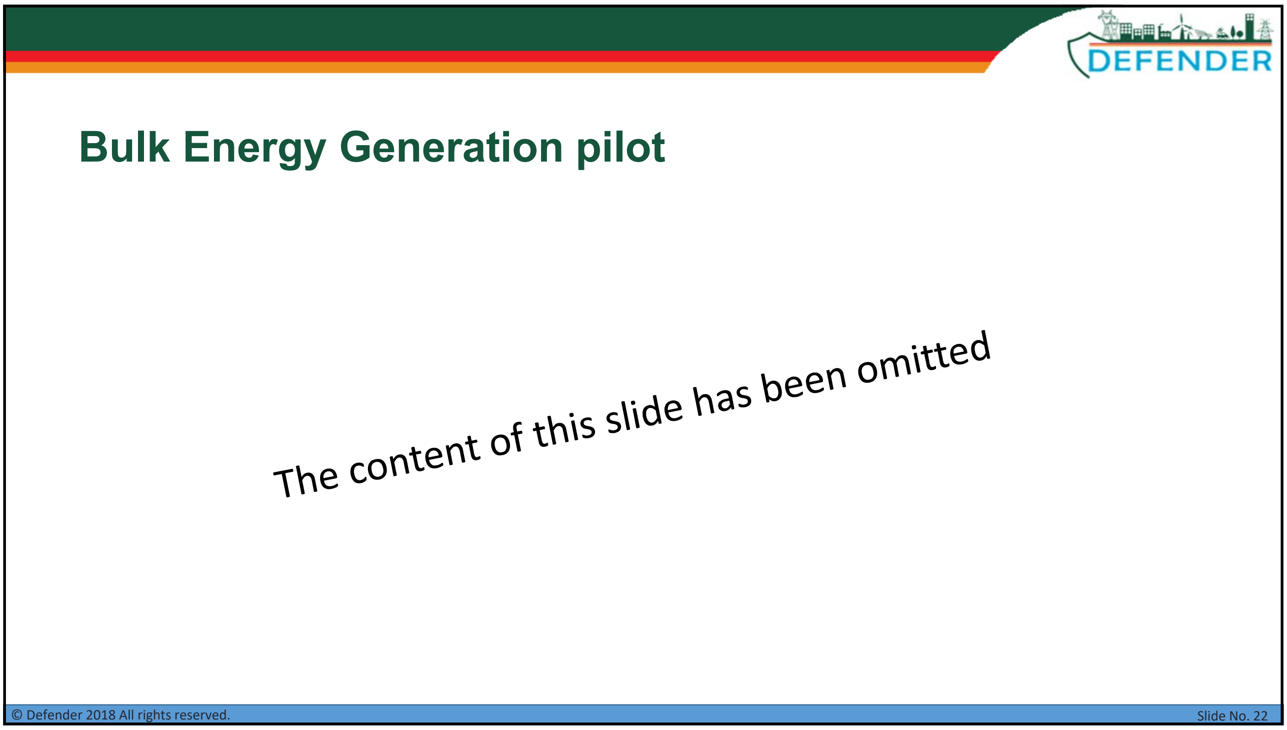
🟨 Cyber Protection

⬜ Human in the Loop

RES: Renewable Energy Systems
DSO: Distribution System Operator
TSO: Transmission System Operator
Plant: Bulk Energy Generation Plant
Lab: R&D Distributed Laboratory

© Defender 2018 All rights reserved.

Slide No. 21

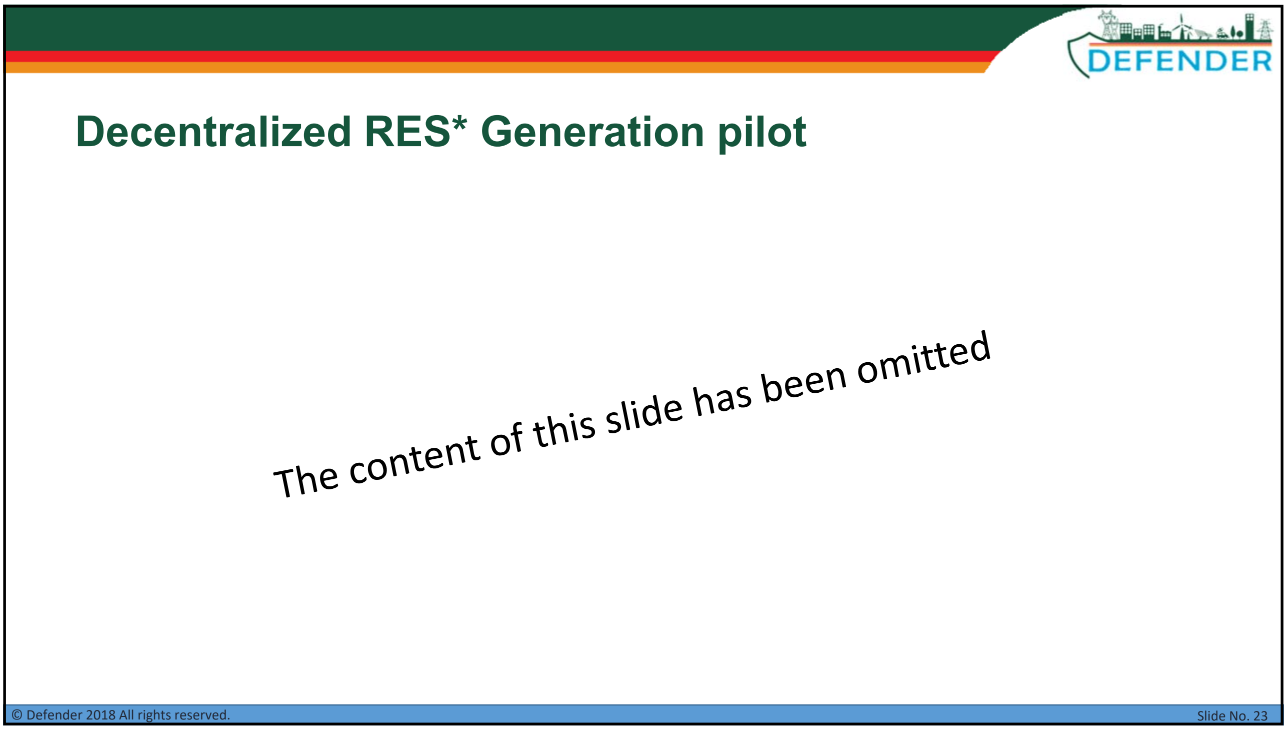


Bulk Energy Generation pilot

The content of this slide has been omitted

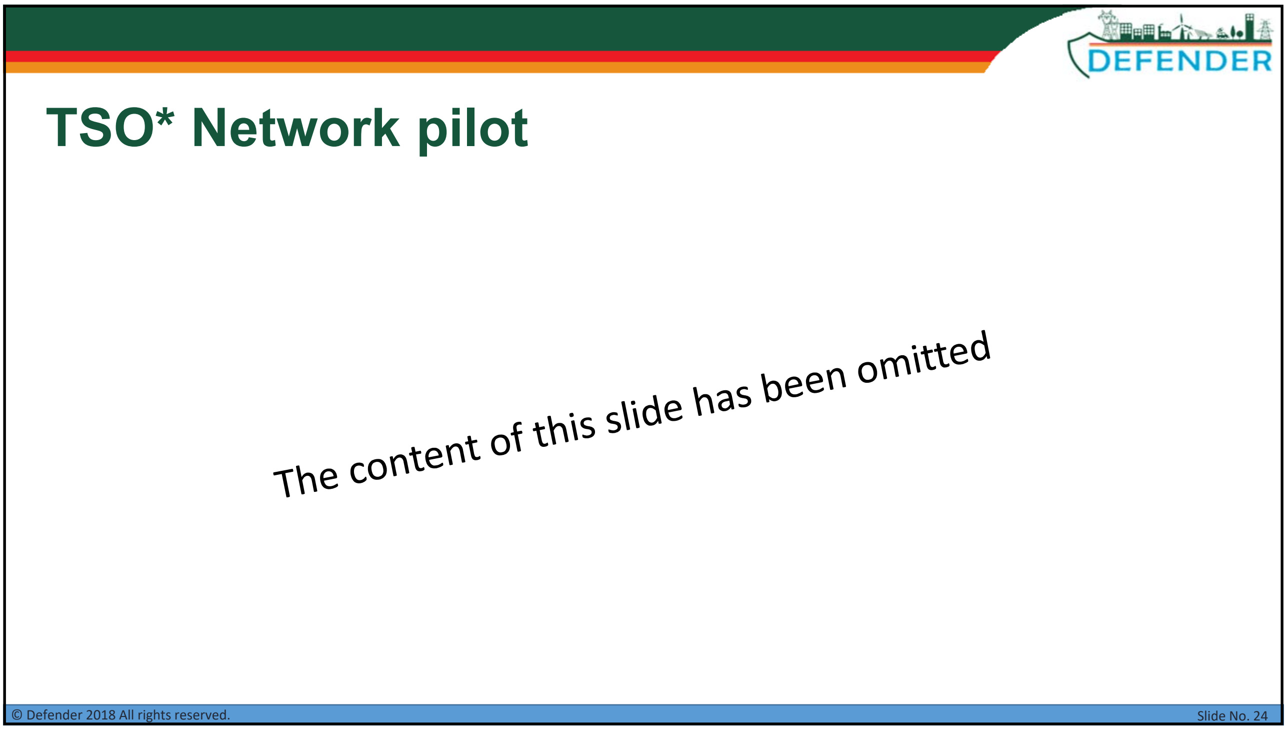
© Defender 2018 All rights reserved.

Slide No. 22



Decentralized RES* Generation pilot

The content of this slide has been omitted



TSO* Network pilot

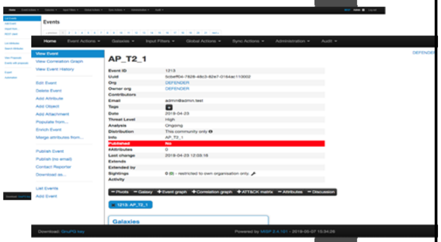
The content of this slide has been omitted

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 cyber 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.**

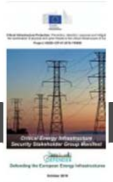


AP_T2_1

Event ID	1213
Uuid	5cbeff04-7828-48c3-82e7-0164ac110002
Org	DEFENDER
Owner org	DEFENDER
Contributors	
Email	admin@admin.test
Tags	+
Date	2019-04-23
Threat Level	High
Analysis	Ongoing
Distribution	This community only
Info	AP_T2_1
Published	No
#Attributes	0
Last change	2019-04-23 12:03:16
Extends	
Extended by	
Sightings	0 (0) - restricted to own organisation only.
Activity	

Galaxies

Download: GnuPG key Powered by MISP 2.4.101 - 2019-05-07 15:34:26


Critical Energy Infrastructure Security Stakeholder Group Booklet

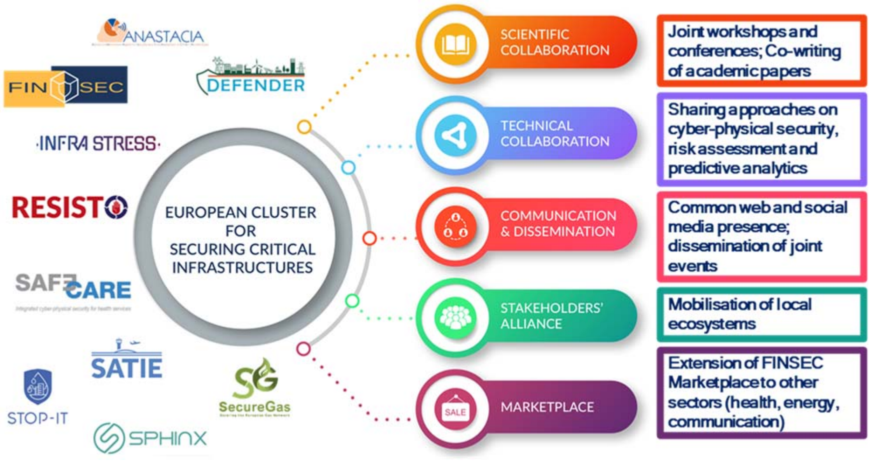
Defending the European Energy Infrastructures

October 2018

Critical Energy Infrastructure

Defending the European Energy Infrastructures

European Cluster for Securing Critical Infrastructures The First ECSCI Workshop, March 26-27, Brussels



Joint workshops and conferences; Co-writing of academic papers

Sharing approaches on cyber-physical security, risk assessment and predictive analytics

Common web and social media presence; dissemination of joint events

Mobilisation of local ecosystems

Extension of FINSEC Marketplace to other sectors (health, energy, communication)

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)

DEFENDER

Defending the European Critical Energy Infrastructure

Thank you for your attention

For further information do not hesitate to contact us at the following email:

gabriele.giunta@eng.it

denis.caleta@ics-institut.si

https://defender-project.eu/

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