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

European Cluster for Securing Critical Infrastructures Virtual Workshop 24th – 25th June 2020

Gabriele Giunta

DEFENDER Project Coordinator

Engineering Ingegneria Informatica Spa

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

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**: *40 months (Closing Date: 31/8/2020)*
- **EU Contribution**: 6.790.837,50 €
- **Partners**: **20** (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

- E.ON Energy Research Center | RWTH AACHEN UNIVERSITY
- JSI
- ICS
- ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ Εθνικόν και Καποδιστριακόν Πανεπιστήμιον Αθηνών ΙΔΡΥΘΕΝ ΤΟ 1837

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

CEI Landscape

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

Fragmented landscape of innovative solutions for CEIs

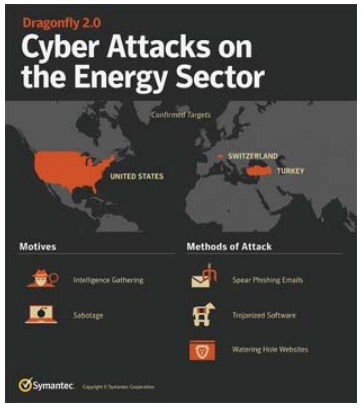
- Limits in the **threat scope** (e.g. either cyber or physical threats)
- Limits in the **coverage of the energy value chain** (from generation to consumer, from operation to market)
- Limits within the **organisation, silos** (e.g. technical, operations, business)
- Rarely involving **human dimension** (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)** still challenging at both **governance and technological levels**

Examples of attacks on smart grid infrastructures

Ukrainian grid cyber attack (2015)

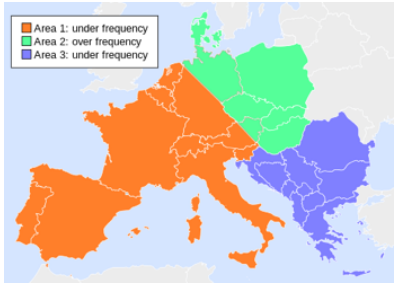
Access to the company system(s) via **emails infected to stole credentials for controlling SCADAs**. Destruction of files stored on servers and workstations causing **27** substations outage affecting about **225,000** customers

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

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**

Human and drone attacks (2013; 2019)

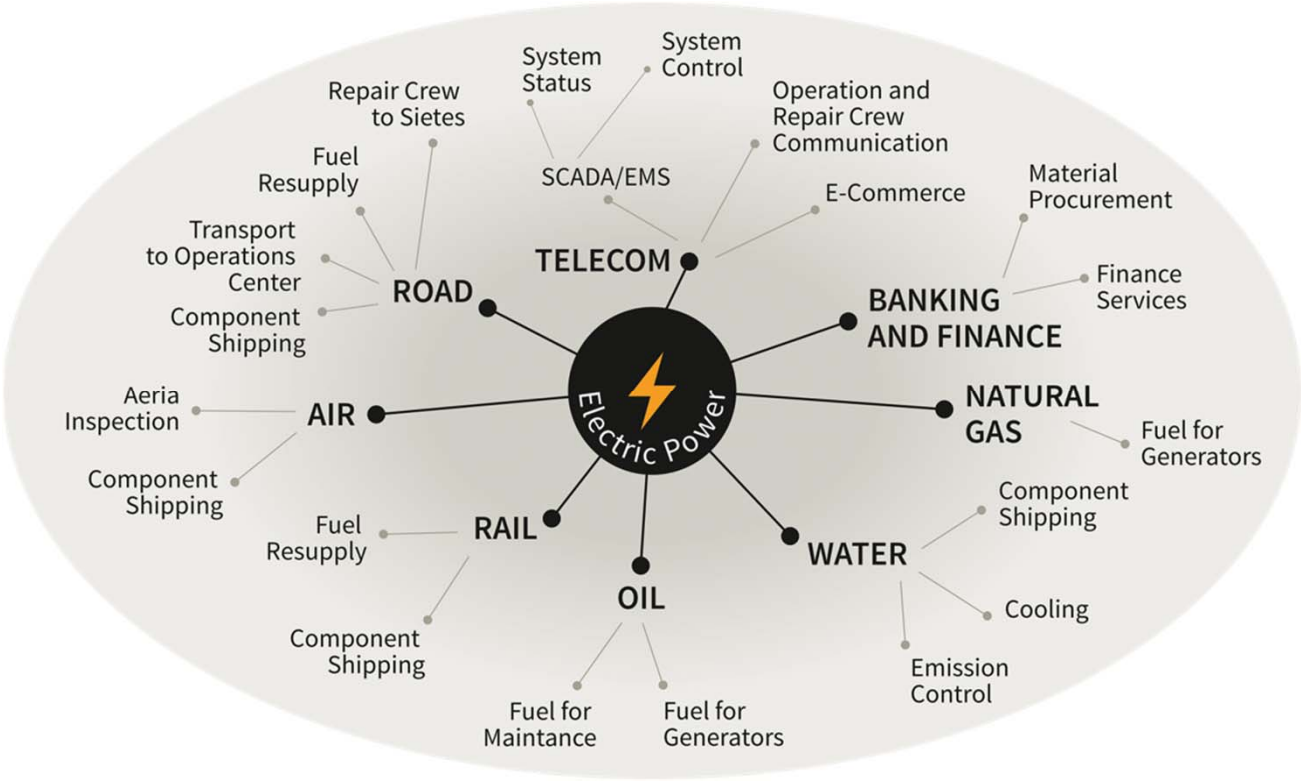
Gunmen fired on 17 Metcalf electrical transformers, causing **more than $15 million** of equipment damages.

The Yemeni Shiite rebels launched about **ten drones** against the largest Saudi oil extraction.

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…

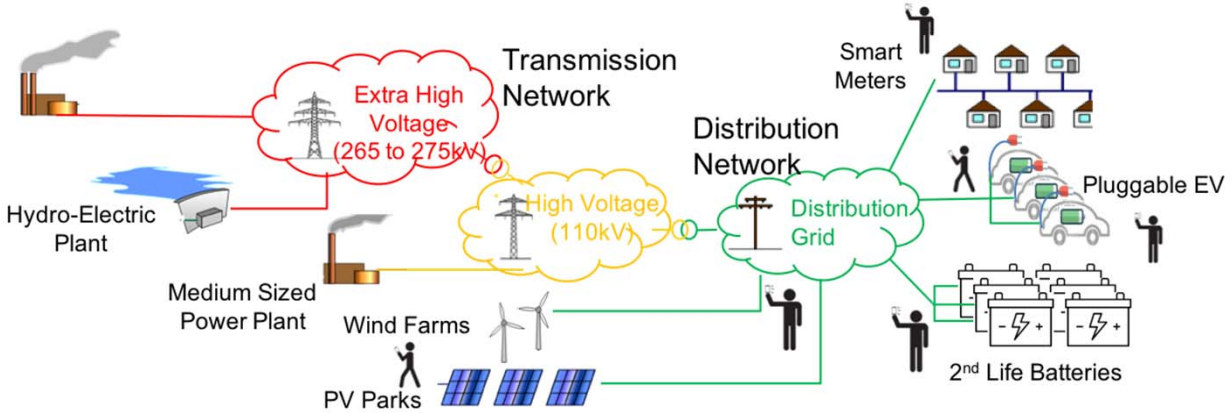
… all the other critical infrastructures have a **strong dependency from Critical Energy Infrastructures**



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]

DEFENDER Scope

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 resource optimization, 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

CEI threat (towards trials) modelling and analysis

Analysis, classification and modelling of the existing and unknown CEI threats through **attack trees notation**

CEI **threat scenario categories**

1. (T) Transmission
2. (R) Renewables
3. (D) Distribution and
4. (G) Generation

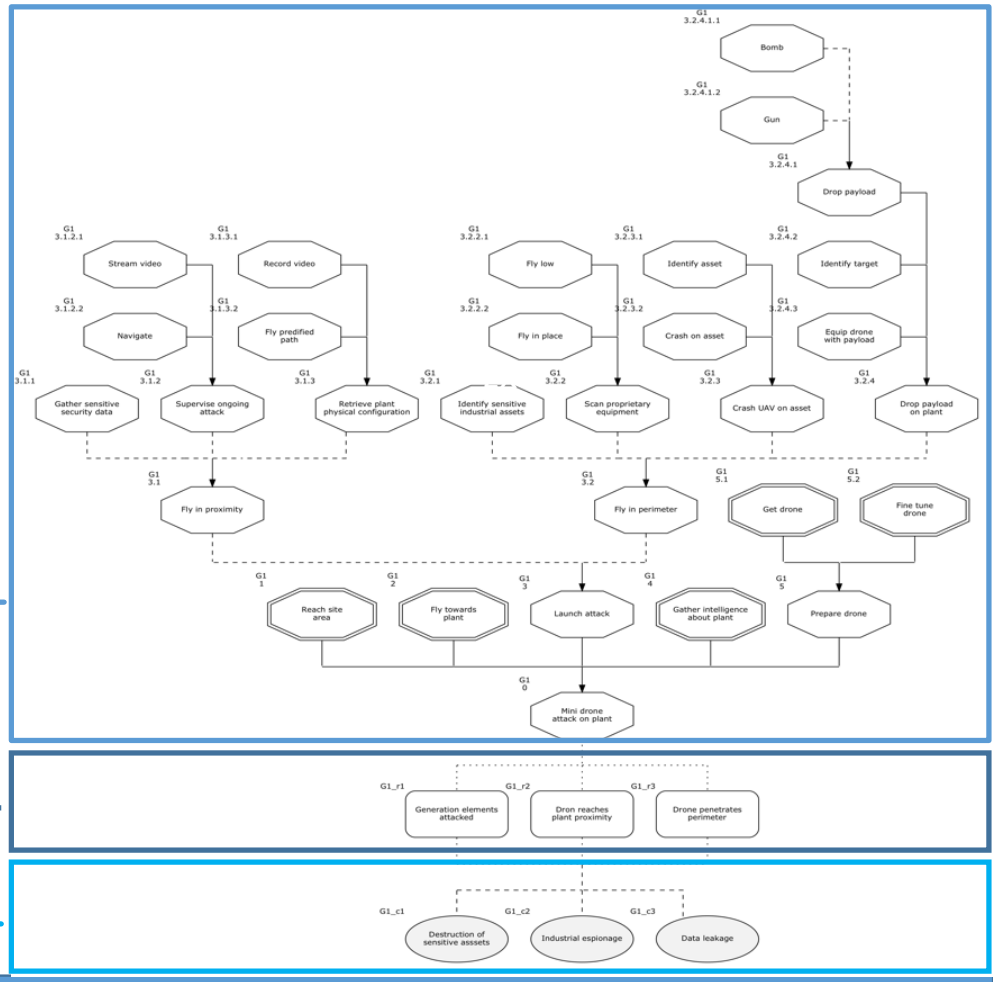
Threats and Attacks

System Response

Result

Table 42: G1 scenario attack tree summary table

Node	Explanation	Design mitigation	Detection	Run-time mitigation
G10	Mini drone attack on plant	Control plant access and proximity. Install drone detection and mitigation systems. Hide, camouflage and mechanically protect sensitive or critical assets.	Use short, mid and long range drone detection mechanisms within plant area and access to critical assets. HITL.	Alarm security team, if needed first responders. Use soft and hard drone neutralization mechanisms. Fuse sensor data and enrich situation awareness.



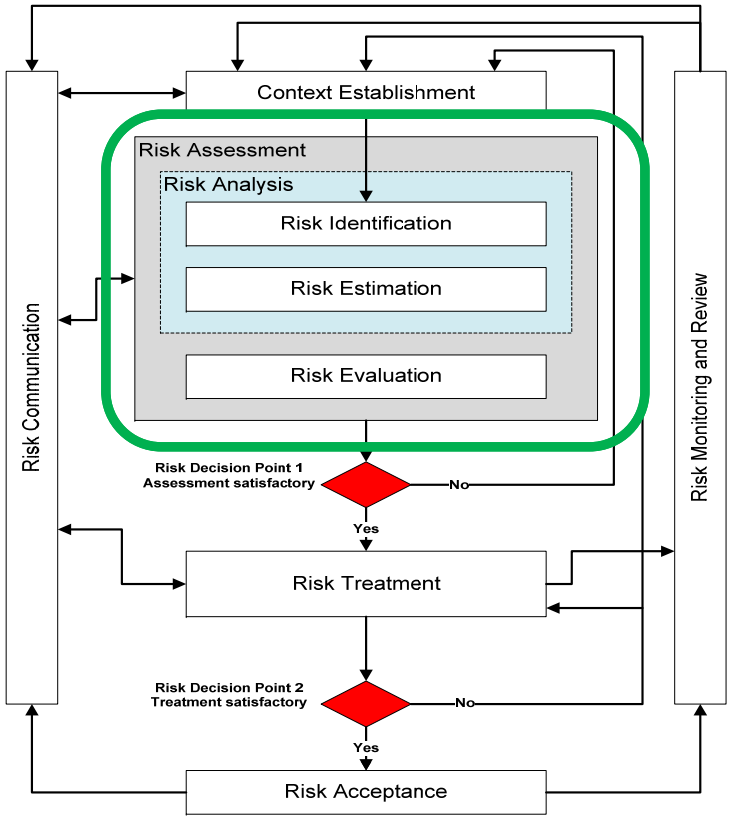
DEFENDER (up to date) achieved results #2

Risk Rate = Risk Impact X Risk Likelihood

CEI Secure Tiers Classification

- **Minimal**, green, 1 to 3, leave out
- **Small**, yellow, 4 to 6, monitor and re-evaluate
- **Medium**, orange, 8 to 12, schedule a mitigation plan
- **High**, red, 15 to 25, immediate attention and mitigation plan

Human Risk Rating Matrix		Risk Impact				
		Minimal	Small	Medium	High	Severe
Risk Likelihood	Almost certain	5	10	15	20	25
	Likely	4	8	12	16	20
	Possible	3	6	9	12	15
	Unlikely	2	4	6	8	10
	Rare	1	2	3	4	5



ISO/IEC 27005	JRC 70046	JRC 96623
Information technology – Security techniques -- Information security risk management	Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art	Risk assessment methodologies for Critical Infrastructure Protection. Part II: A new approach

DEFENDER (up to date) achieved results #3

Tools and components to reduce risk “by design”

Four DEFENDER “design objectives”:

1. Optimize resource allocation to **maximize cyber-physical security** with limited budget **(Long-term Security Lifecycle Assessment)**
2. Increase the resilience of distributed electronic systems, **enabling flexible migration between available devices** in case of failures (**Resilience by design**)
3. Analyse vulnerabilities and critical components of the electrical networks to **quickly identify the location of failures and to repair them** (**Self-healing by design**)
4. Recommendations to **privacy protection** during the development **(Privacy by design)**

DEFENDER (up to date) achieved results #4

CEI Monitoring and Detection of cyber-physical-human threats

Build on real-time multi-aspect monitoring to ensure that:

- CEI security state is known at every given moment
- The future CEI security state is predictable
- The CEI security guaranteed at all times

Physical Sensors

- Thermal/PMZ cameras, RF radars, LIDARs
- Fibre optics, Taut wires, Buried geophones

Cyber Sensors

- Logs, Firewall status, SCADA systems
- Co-simulator and ML at local and pan-European level

Human Sensors

- Acting as first-responders on possibly CEI incidents


(a) Surveillance Camera


(b) Laser Fence Sensor (LFS)


(c) 360° Perimeter Laser Sensor


(d) Efficient Doppler detector


(e) Wireless seismic & IR sensor


(f) Laser Radar Sensor (LRS)


Drone Visual Detection

Physical Detectors

1) **Human and Drone Intrusion**: Perimeter Laser Sensor (PLS) and Laser Fence Sensor (LFS) for human intrusion detection. Using PTZ Camera, these sensors are the only sensors able of smooth tracking by Pan, Tilt and Zoom, without any need for external PC. 3D MND for drone detection.
2) **Person Detection and Tracking**: As the first cordon of security, perimeter intrusion detection solution offers quick and reliable detection of any unauthorized entry or exit from CEI premises, ensuring an appropriate response could be deployed to mitigate the threat.
3) **Drone Detection**: Is a novel architecture that integrates a Region-based Fully Convolutional Network (RFCN) model for drone detection complemented by the low-cost sensing equipment powered by Raspberry Pi for visually tracking and locking upon the trajectory of the drone.
4) **Facial Biometric Access Control**: The facial biometric solution leverages the advancements of Multi-task Cascaded Convolutional Networks (MTCNN). The product also includes the facial detection and alignment for seamless deployment for restricted access control to sensitive areas of the CEI.
5) **Wind Turbine Blade Detector**: The use of UAVs offer an alternate solution to visual assessments of structures (currently carried out manually by engineers) while eliminating the need for manual inspections

DEFENDER (up to date) achieved results #5

DEFENDER Platform - CEI situation perception, comprehension and awareness:

1. **Perception of the current state of the environment** through the processing of all the data and information coming from the integrated cyber-physical and human sources
2. **Simulation of the current situation** in order to understand how it might evolve and identification of the potential attack categories as well as the related impact
3. **Prevention against the identified physical-cyber threat/attack**, prioritizing the most relevant countermeasures to secure CEIs, minimizing the effects in the network.

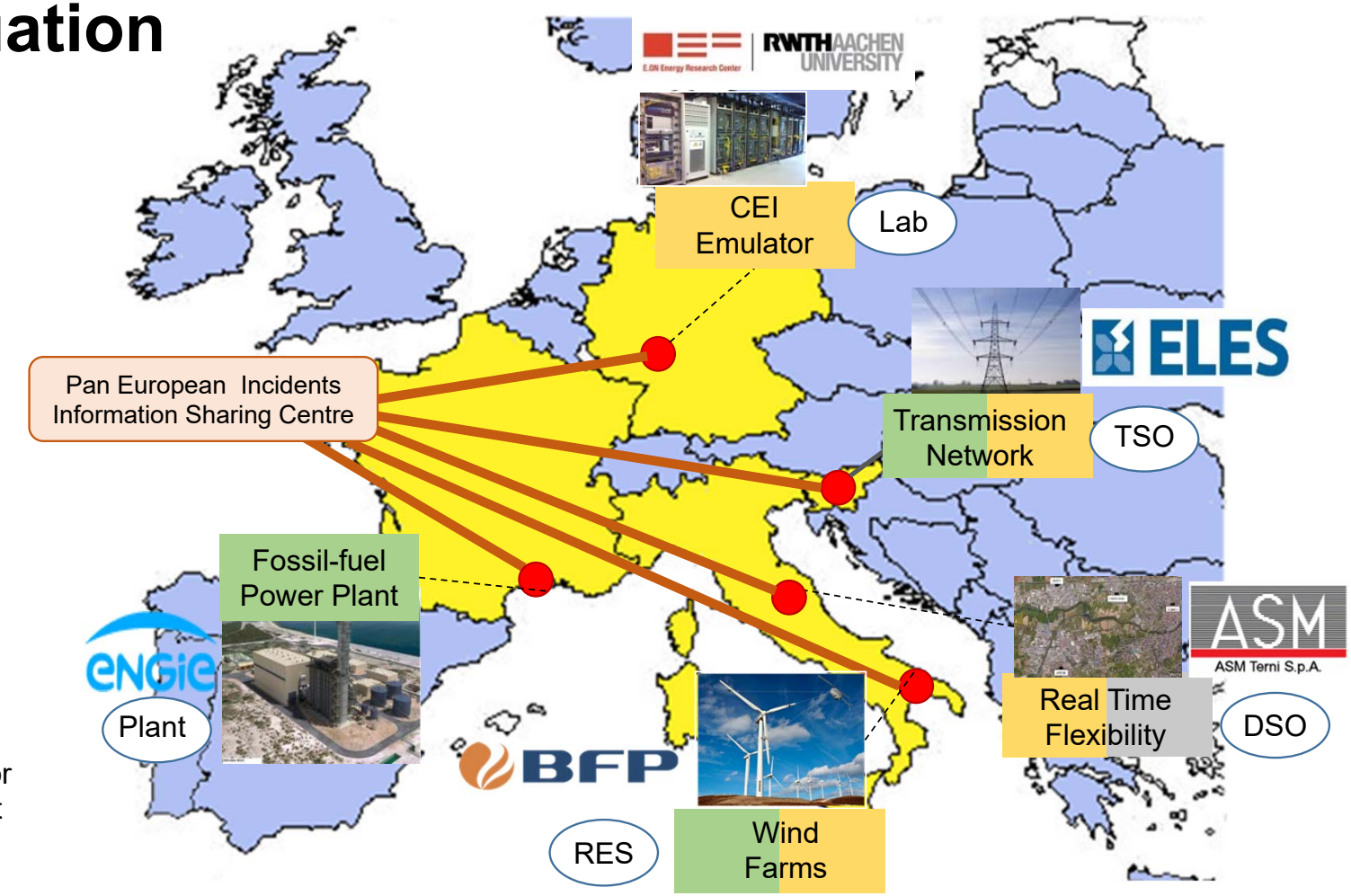
Human Sensor (as know as "Human-In-The-Loop") tool and application for innovative, trusted, traceable and bidirectional information flows, enabling efficient

a) **Communication from CEI Security Control Centre to Human Sensors** (information on incidents and instructions to humans (employees or citizens in the vicinity) and
b) **Communication from Human Sensors to CEI Security Control Centre** (humans acting as front line responders to collect and send relevant data for the emergency management).

Pilots Evaluation

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

Pilots Evaluation

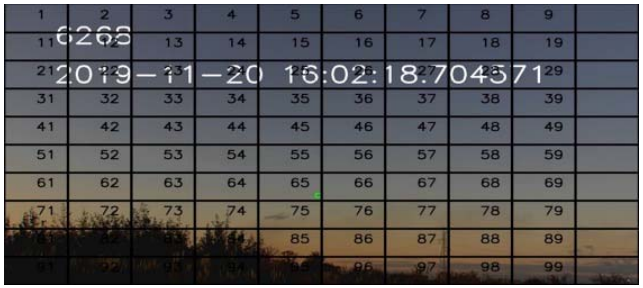


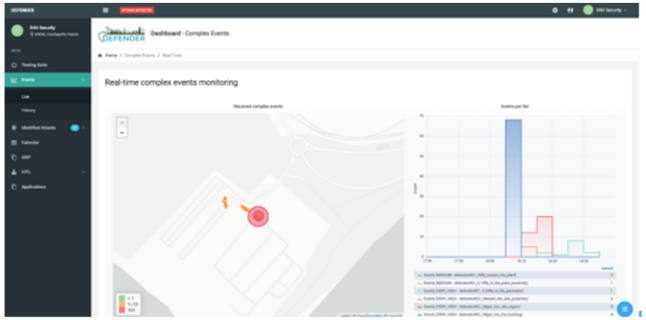
- Physical Protection
- Cyber Protection
- Human in the Loop

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

Bulk Energy Generation pilot

- **Pilot site:** Combigolfe plant at Fos-sur-Mer, France
- **Plant specifications :**
  - 424 MW NG power plant for electricity production
  - Located in prohibited airspace → flight protocol with French Air Force
  - 22 fixed camera all around fences for intrusion detection, manned surveillance patrol
- **Main focus:**
  - Human malicious attack via drone fleet
  - Drone fleet neutralization
- **Two threats scenario :**
  - G1 : Mini-drone attack & neutralization
  - G2 : Physical attack to gain network access
- **Evaluated technologies**
  - Autonomous drone coupled to GENETEC
  - Surveillance tour + doubt removal
  - 2D Laser Fence (PLS, LFS)
  - Video drone detection
  - DEFENDER Platform
- **Trial took place in November 2019**

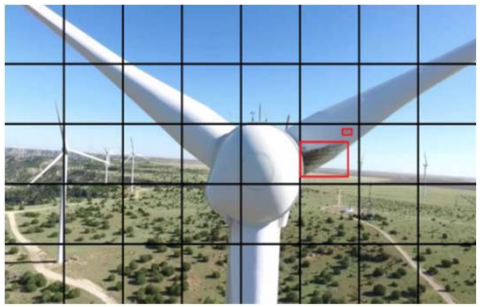


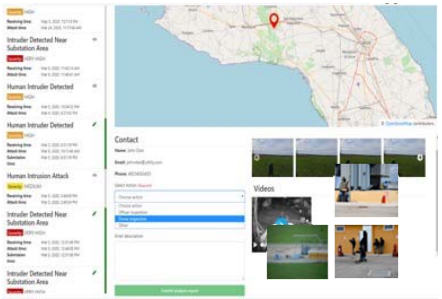


(*) RES: Renewable Energy Systems

Decentralized RES* Generation pilot

- **Pilot site:** Erchie wind farm, Italy
- **Main focus:**
  - Infrastructure Aging (structural collapse of wind tower) or natural hazard – Stop time reduction
  - Unauthorized access to substation and wind towers
  - Security gap between Renewable Energy System and Distribution System Operator
- **Four threat scenarios:**
  - R1: Unauthorized access to the electrical substation
  - R2: Unauthorized access to the wind turbines
  - R3: Drone attack
  - R6: Stop time reduction
- **Evaluated technologies:** Human/Drone Intrusion Detection Based on Video Analytics, Drone Intrusion Detection based on 3D Mini Drone Detection Drone-based surveillance, Flying Hunter, DEFENDER Platform, Video Analytics for Preventive Maintenance
- **Involvement of Italian Police (Polizia di Stato)**
- **Trial took place in December 2019**

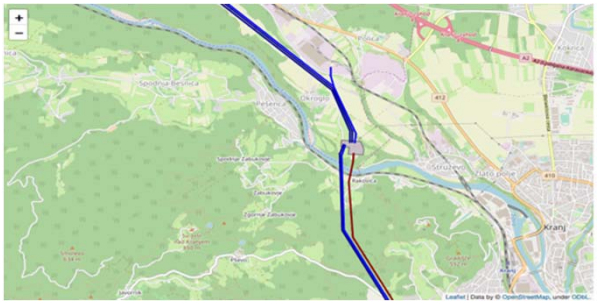


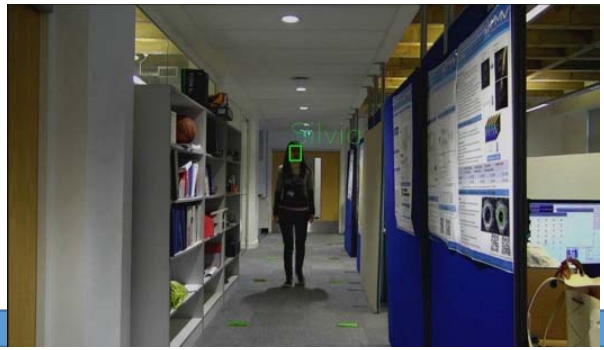


TSO* Network pilot

(*) TSO: Transmission System Operator

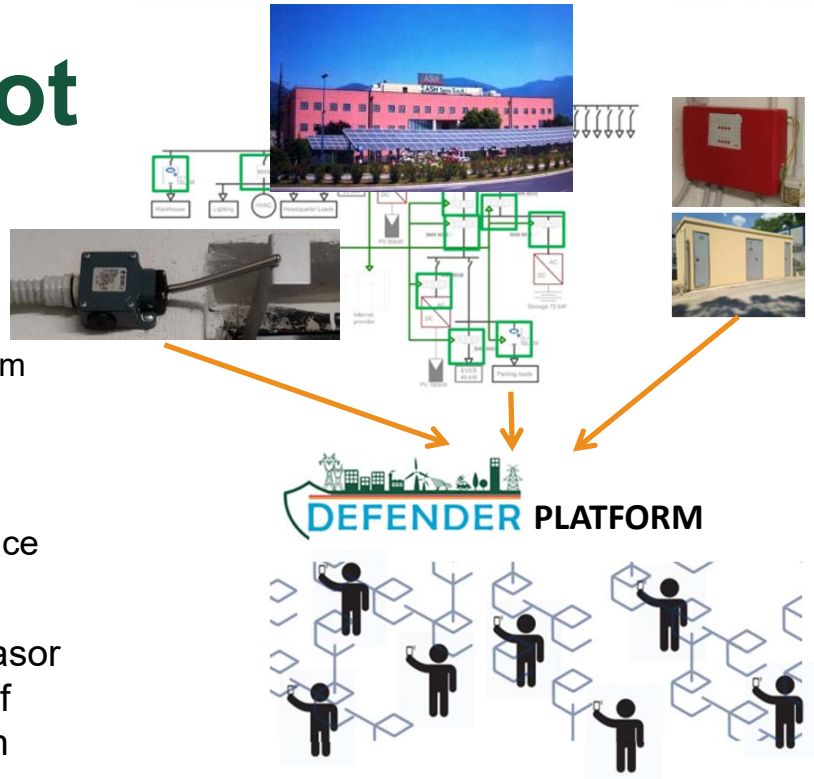
- **Pilot site:** Okroglo switching station, Slovenia
- **Main focus:**
  - Power line fault isolation and restore
  - Lack of coordination among different security platforms
  - Swarm of drones equipped with camera for lifecycle assets management
- **Three threat scenarios:**
  - T1: Power line fault isolation and restore based on optical and communication network observations
  - T2: Lack of coordination between different access control systems, physical access control and SCADA network access control
  - T3: Implant monitoring and control element in the system, SCADA network centre
- **Evaluated technologies:** Network Fault Detectors, Face Recognition, People Detection and Counting, 2D Laser Fence (PLS, LFS), DEFENDER platform, Human In The Loop Detector, Glaze Ice, Physical Access Control, Cyber Access Control, Double Authorization
- **Additional effort:**
  - Organisational improvements (all scenarios)
  - Swarm of drones evaluation for preventive maintenance
- **Due to COVID-19 limitation trial will take place in July 2020**





DSO* Network & Prosumer pilot

- **Pilot site:** ASM Terni, Italy
- **Main focus:**
  - Physical threat to network assets
  - Security gap between Distribution System Operator and Renewable Energy System
- **Two threat scenarios:**
  - D1: Fault Isolation and smart-grid self-recovery
    - D1a scenario – physical attack to the secondary substation
    - D1b scenario – Man-in-the-middle attack for generation of grid unbalance
  - D2: Human-In-The-Loop for CEI cyber-physical security and resilience
- **Evaluated technologies:** Fault Detection and Localisation based on the Phasor Measurement Unit (PMU), HITL Mobile App for Incidents Report, Detection of Electrical Anomalies based on Cyber Detectors, Intrusion Detection based on Smart Locks (SL)

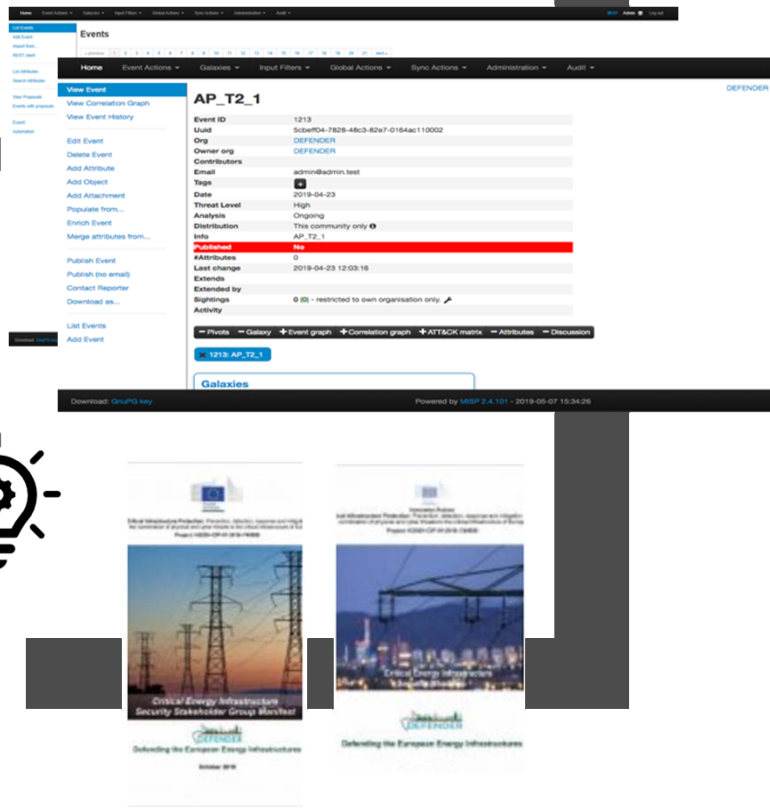


- **Continuous D2 trials since March 2019**
- **Continuous D1 trials since October 2019**

(*) DSO: Distribution System Operator

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**.



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

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