

Combining cyber and physical security management for critical energy infrastructure protection: the DEFENDER project

Massimo Bertoncini

*Senior Innovation Manager
for Smart Energy*

Engineering Ingegneria
Informatica (Italy)



Gabriele Giunta

DEFENDER Project Manager

Engineering Ingegneria
Informatica (Italy)



Denis Caleta

President of the Board

Institute for Corporate Security
Studies (Slovenia)



Engineering Ingegneria Informatica: who we are



IN ITALY



30/
cities



ABROAD

- USA: Wilmington
- BRAZIL: Belo Horizonte / Curitiba / São Paulo Santo André / Rio de Janeiro
- ARGENTINA: Buenos Aires
- GERMANY: Berlin / Düsseldorf / Hamburg / Hannover Munich / Stuttgart/ Wiesbaden
- BELGIUM: Brussels
- SPAIN: Madrid
- REP. OF SERBIA: Belgrade

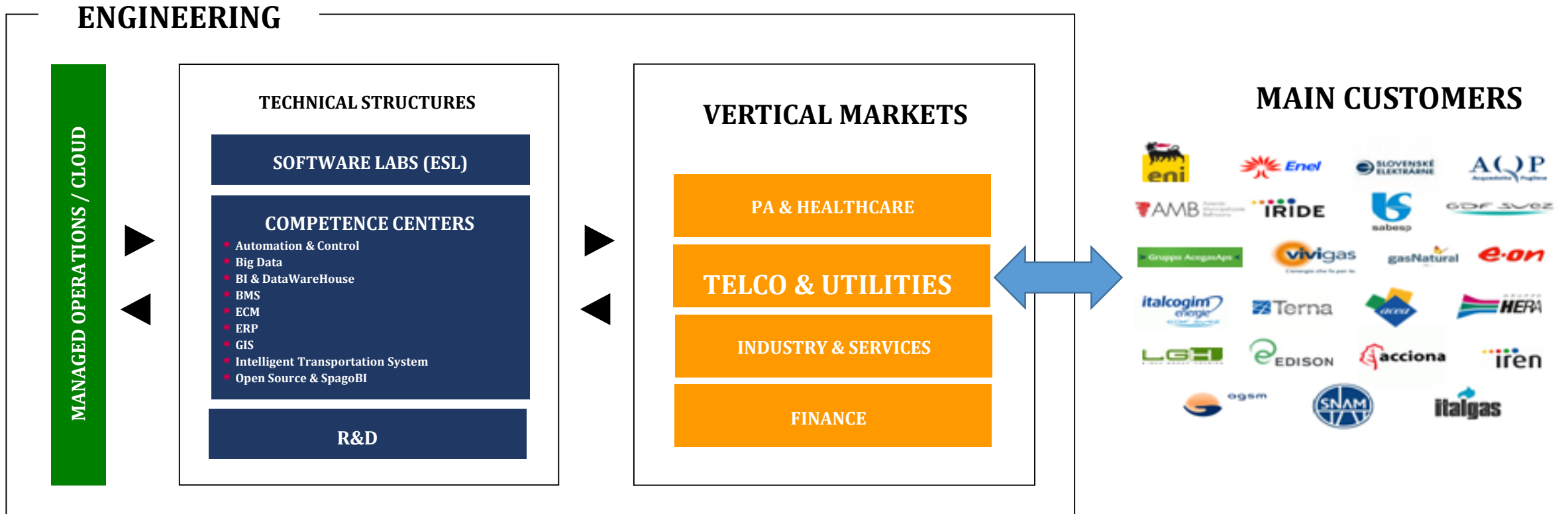
A global player
Business Integration
Consulting
Outsourcing
Products and solutions

8,500
professionals
+ 3,100
external resources

9%
market share
in Italy

1,000
large accounts

More than 1 M€ of
total revenues



6
R&D LABS

LABS

- ENG involvement in ongoing H2020 TSO-driven projects
 - H2020 **OSMOSE** (<https://www.osmose-h2020.eu/>)
 - H2020 **COORDINET** (<https://coordinet-project.eu/>)

PlatONE

250
RESEARCHERS

70
LIVE PROJECTS



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

R&D/Academy

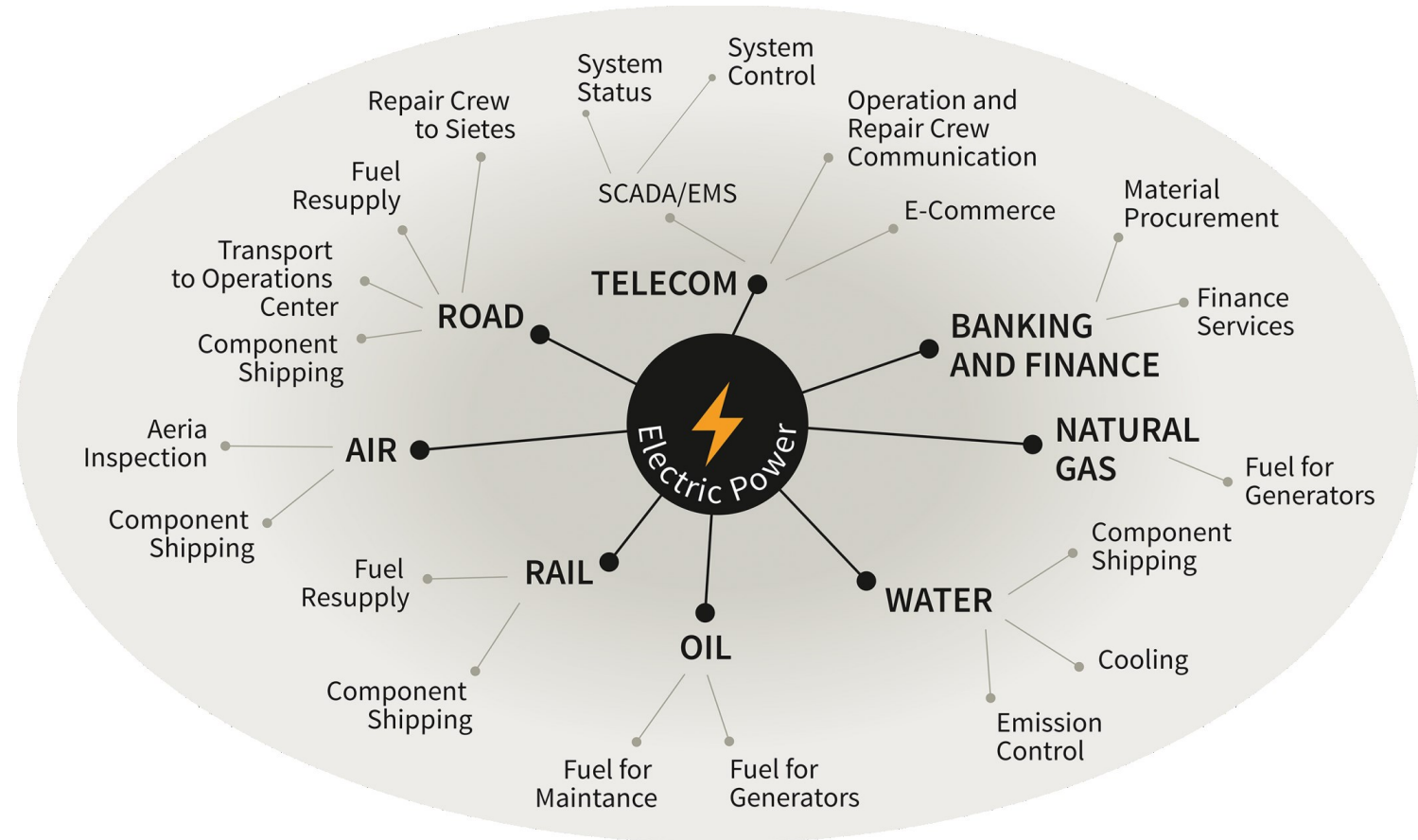


Stakeholders

-  **ASM** (Electricity Network Operator, DSO)
ASM Termi S.p.A.
-  **engie** (Electricity Supplier, Bulk generation)
-  **BFP** (Electricity Supplier, Wind farm)
-  **ELES** (Electricity Network Operator, TSO)
-  (Law Enforcement Agency)

Critical Infrastructures depend on each other, but...

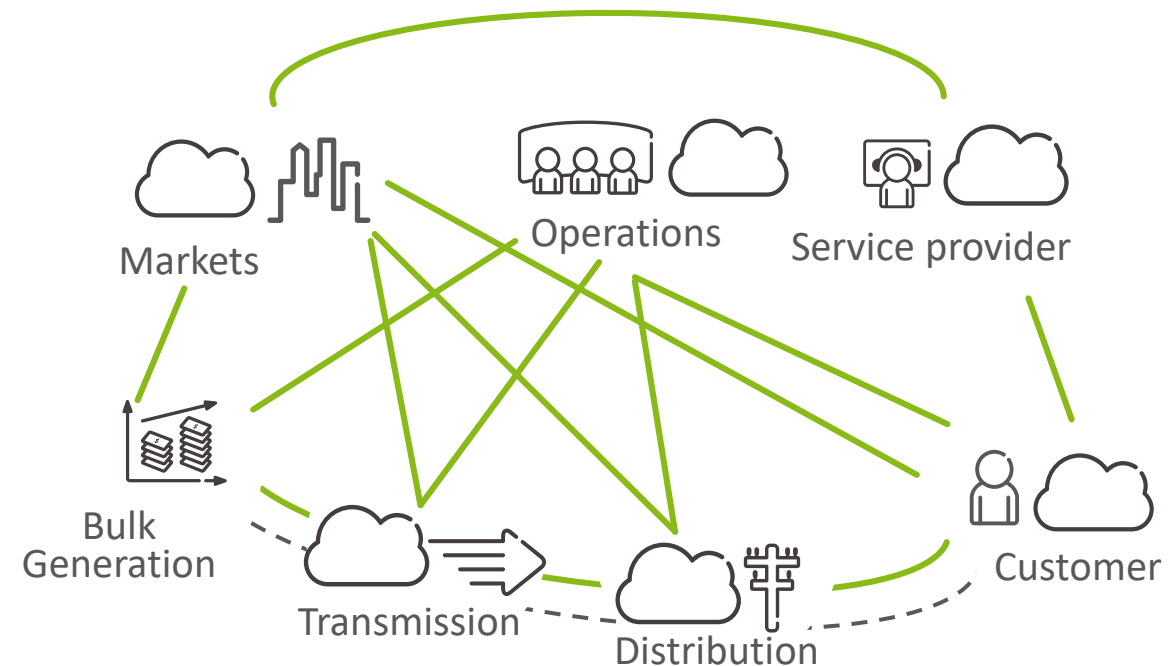
...All the other critical infrastructures have a **strong dependency from Critical Energy Infrastructures**



Source: A new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure EPCIP [SWD (2013) 318]

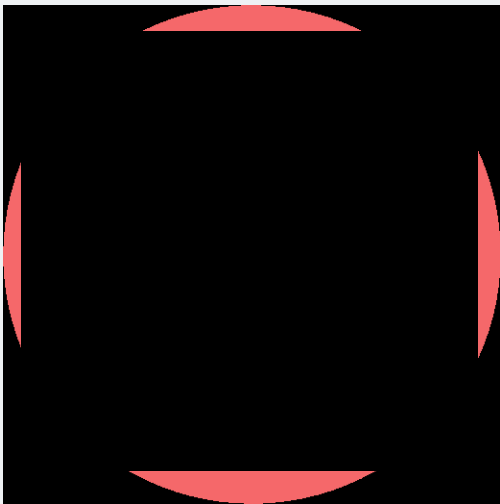
Security is fundamental for smart critical energy infrastructures (CEIs)

- The fast developing **ICT provides new opportunities to gather and analyze performance data**, making it possible to pre-emptively notice and remedy technical vulnerabilities in the system (e.g. aligning demand to supply)...
- ... but the **increased interconnectivity associated with ICT** brings in its own **vulnerabilities** and 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**

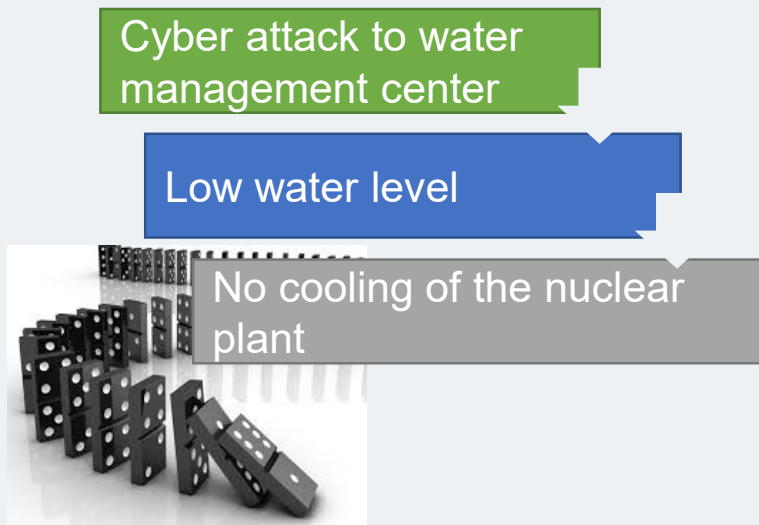


Multiple critical infrastructure attack types

Central/radiating attacks are targeting resources common to several CIs (e.g. control centre).

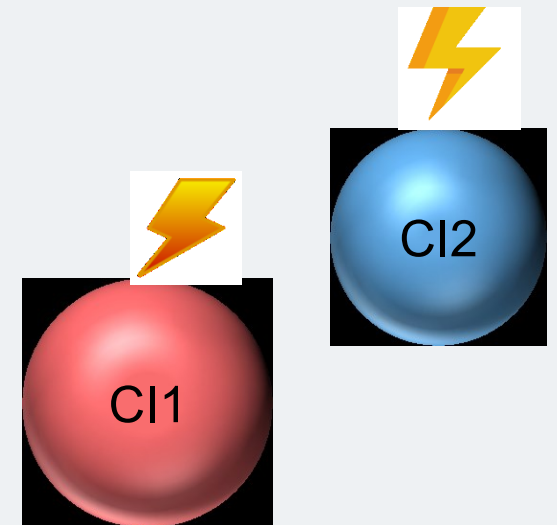


Attack to one CI sequentially causing **cascading** effect to another CI(s) because of CI interdependencies



Source: google

Parallel attacks of different types to several CIs

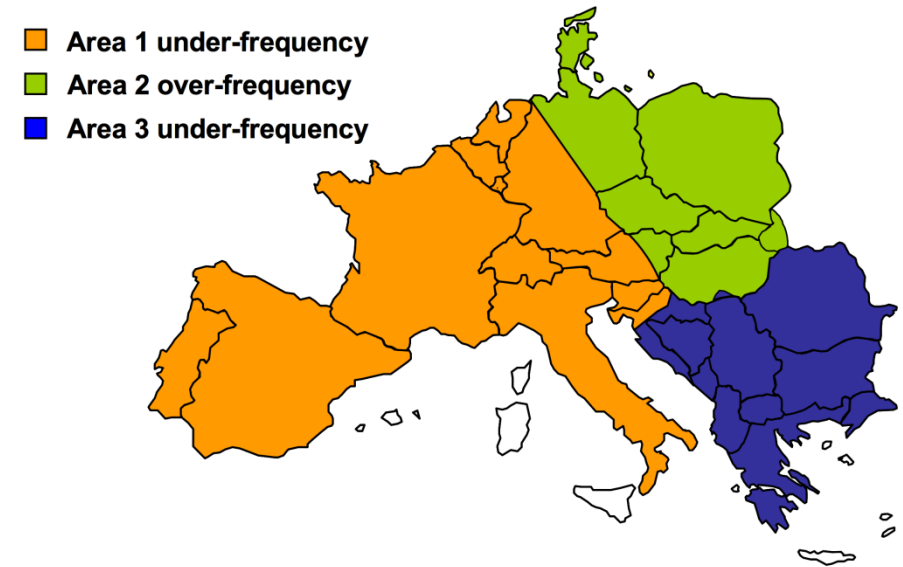


Examples of attacks on smart grid infrastructures

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 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)

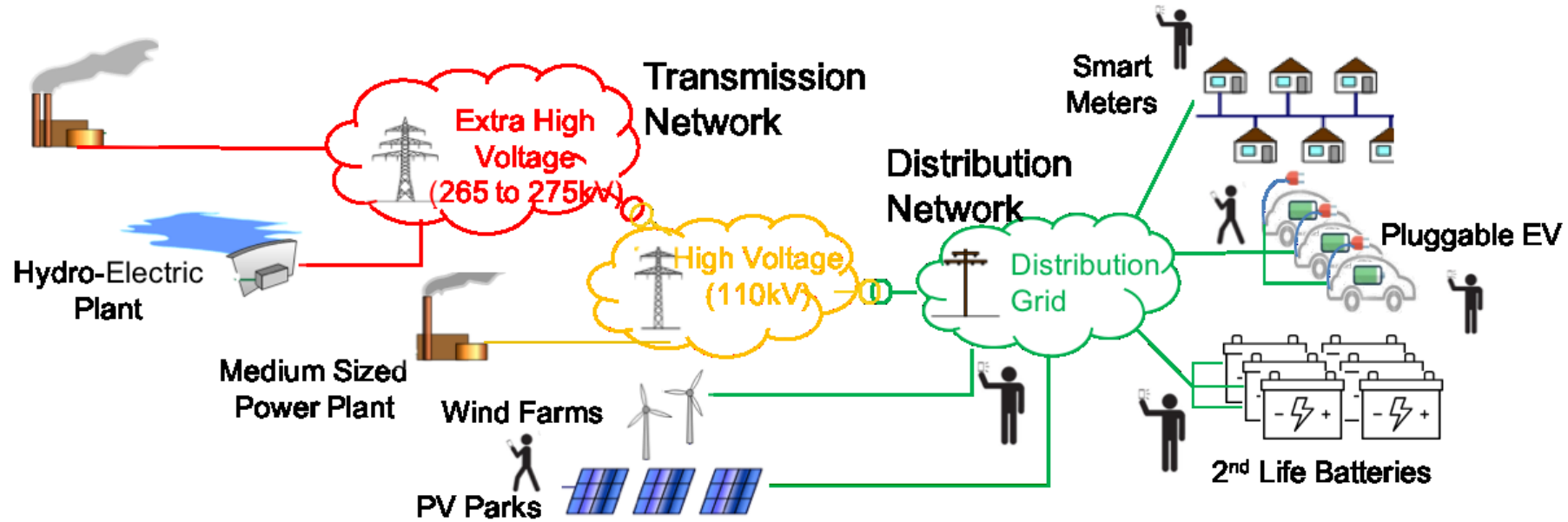


- Accidental
- Non fulfilment the N-1 criterion
- Insufficient inter-TSO co-ordination

Solutions for Critical Energy Infrastructures: SoTA

- Actually fragmented landscape of innovative solutions for Critical Energy Infrastructures
 - Limited in the **threat scope** (e.g. either cyber or physical threats)
 - Limited in the **coverage of the energy value chain** (e.g. Addressing smart metering, or network branches)
- Rarely involving **human dimension** (citizens or workers)
- No **systematic relationship between power network operators and security operators/service providers and/or Law Enforcement Agencies actually in place**
- Interaction and underlying procedures for linking **power network operators with CERTs and ISACs (EE-ISAC)** still challenging at both **governance and technological levels**

DEFENDER Scope



Physical Security



Natural Disasters



Aging Infrastructure



Cyber Security



Aging Workforce

DEFENDER Main Objectives

1. Analyse CEI **threats and risks**, create methodology for **predicting new/yet unknown risks**
Gain **CEI situation awareness, perception and comprehension** by interfacing **Physical, Cyber & Human/Virtual sensors** and metering devices and by utilising a Cyber-Physical Social System (CPSS) co-simulator
2. **Human/Virtual 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 sharing and exchange on physical and cyber attacks patterns and countermeasures, via a ***CEI Incidents Information Sharing Platform (I2SP)***
7. Coordinate the ***Critical Energy Infrastructure Security Stakeholders Group*** (CEIS-SG)

DEFENDER Multi-layered Innovation Streams

- Model CEIs as **distributed Cyber-Physical Systems** for managing the **potential reciprocal effects** of **cyber** and **physical** threats
- Deploy a **novel adaptive security governance model**, which leverages on **lifecycle assessment for cost-effective security management over the time (-> CI-SLAs)**
- To design and make it available a two-layered **intelligent cyber-physical security management framework**, which combines a **strategic-level “by-design” toolbox** stack with **operational near real time approaches** for **cyber-physical threats detection and mitigation** aimed to manage CEI security countermeasures performances against KPIs over the time
- Seamless integration of **finer-grained situational awareness, anticipated prediction and detection of cyber-physical threats and attacks** and appropriate **mitigation techniques** leveraging on **scalable big data intelligent processing technologies** and **AI-based situation perception**

DEFENDER Multi-layered Innovation Streams (2)

- To **scale up** to **pan-European P2P DLT/blockchain-based Incident Sharing Platform** tailored to CERTS or ISACs
- To **bring people at centre stage (building a culture of security)** via **Human in the Loop** approach, where **trusted identity** is managed in a decentralized way via novel **Blockchain** applications
- To design and validate novel “**sharing-economy**” **business models**, where **citizens, power network operators and LEAs** will mutually **cooperate** to achieve system-level CEI security
 - Setting up interoperability between power network operators AND LEAs

An End-to-End Closed-Loop Solution: From Monitoring to Optimized CEI Security Management

Feedback & Full Lifecycle Governance



Cyber sensors
Physical sensors
Human sensors

Thermal/PMZ cameras
RF radars, LIDARs,
Logs processing,
Antivirus/-malware
SCADA Firewall, HITL

Detect that **something is wrong**
(security incident,
accident, fault..)

Perceive the **near future state of the CEI**
(Consolidated view)

Understand **what** is
happening and **how**
to mitigate

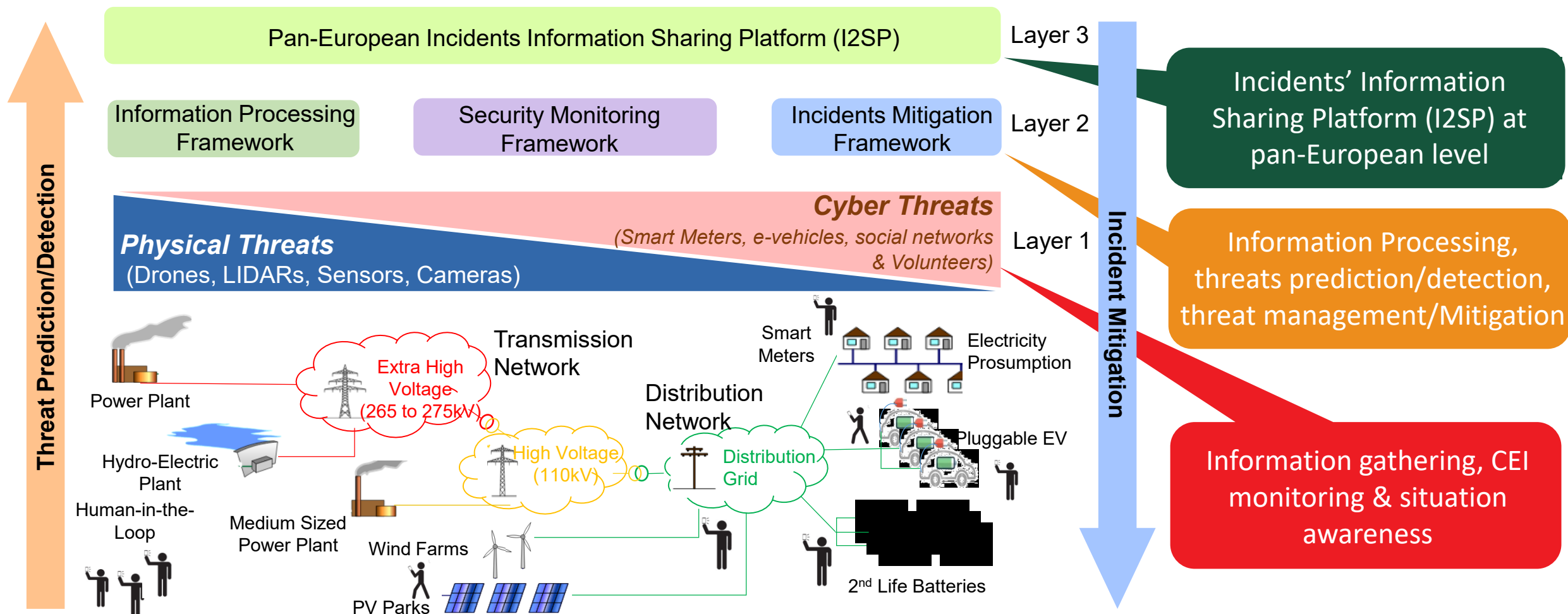
Apply the **mitigation plans** & prevent
cascading effects

CEI Security: Combining strategic-level with operational approaches



- **CEI Security “by-design”**
 - Self-healing (e.g. fault-location /restoration)
 - Data Protection (e.g. Cryptography/Blockchains)
 - Security Assessment Lifecycle Assessment
 - Risk Impact vs Threat Matrix
- **CEI Security at operational level**
 - Countermeasures toolbox for incident mitigation
 - Decision support systems to assist CEI security authorities when automated mitigation is not possible
 - Avoidance of cascading attacks by notification & “Human Sensors”

DEFENDER Overall Architecture



DEFENDER Monitoring

DEFENDER builds 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
- ✓ CEI cyber-physical security optimally managed any time

Physical

- Thermal/PMZ cameras, RF radars, LIDARs
- Strain sensitive cables, Fibre optics, Taut wires, Buried geophones
- Logs, Antivirus/Antimalware/Firewall status, SCADA systems

Cyber

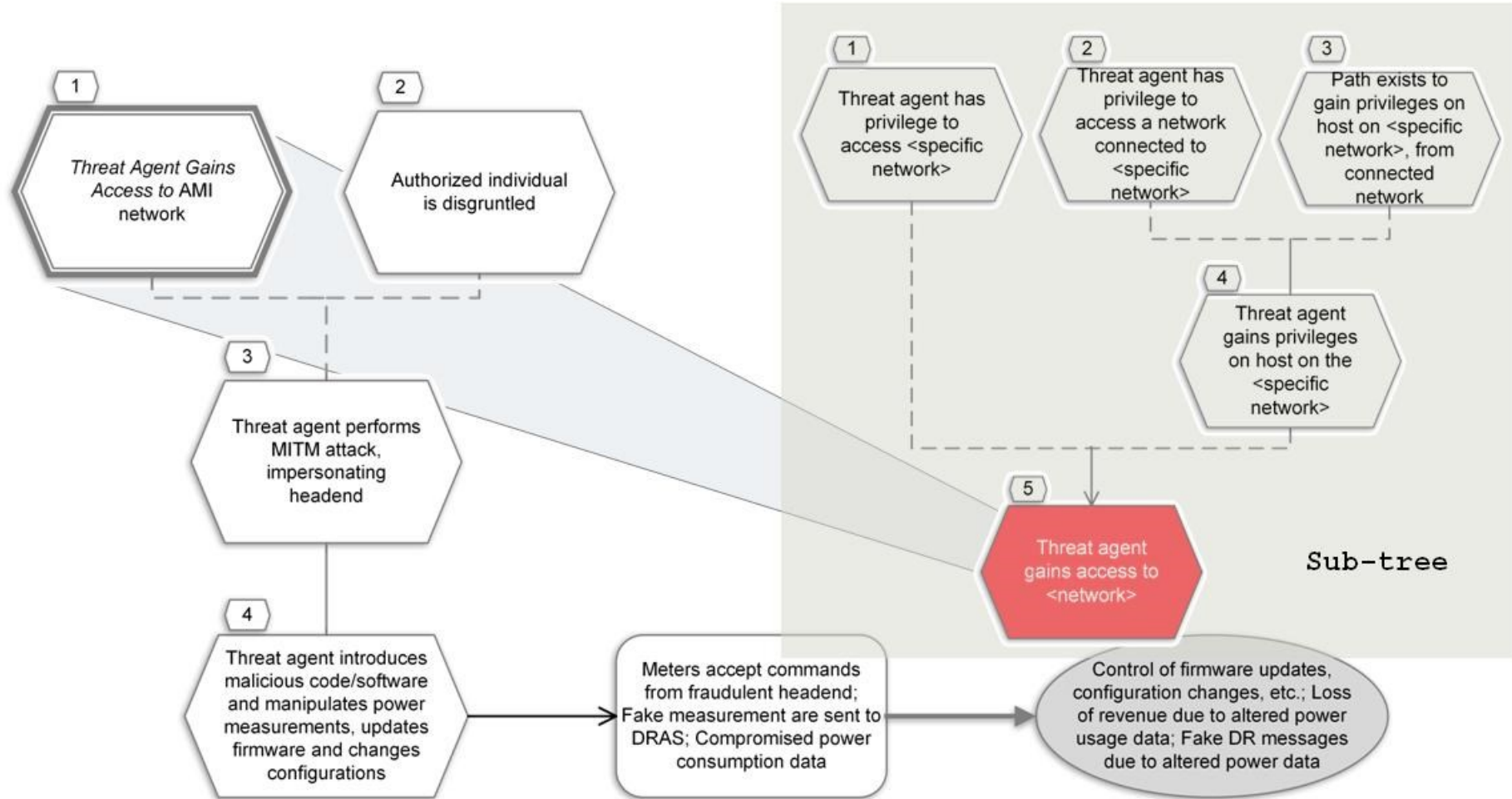
- Big Data Analytics and Machine Learning outputs at local and pan-European level

Human

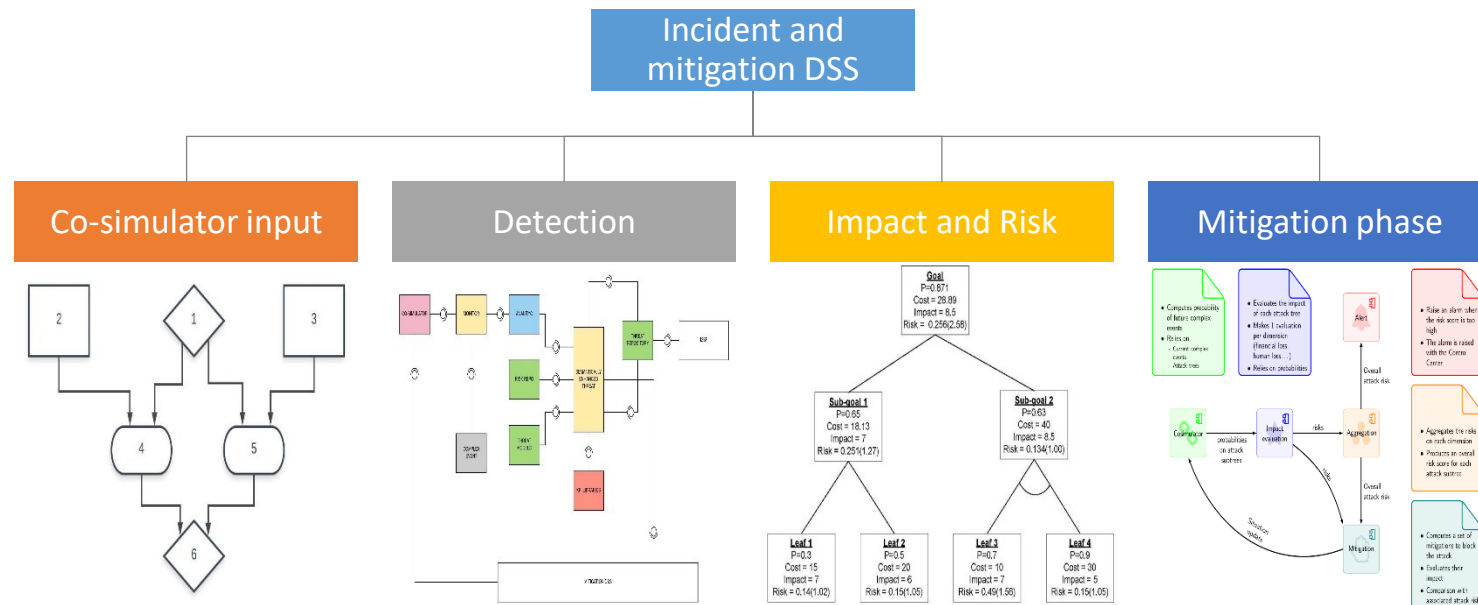
- Acting as first-responders, sharing text, photographs and videos from possibly perilous CEI incidents

From CEI security state Awareness to Comprehension

- Threats and attack **semantically enhanced**
- Extensive use and frameworks
 - Near real time
 - **Data mining** o
 - **Machine learn** Trees)
- Security compreh



From CEI security state Comprehension to Mitigation



People acting as cyber security sensors

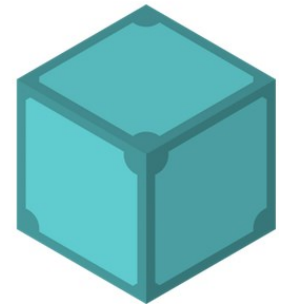
- Volunteers leaving in proximity of CEI acting as first responders (report via specialized applications possibly accidents or suspicious incidents)

- Short messages
- Photographs
- Videos



We need to ensure

**Trusted, Traceable, Private,
Bi-directional Communications**

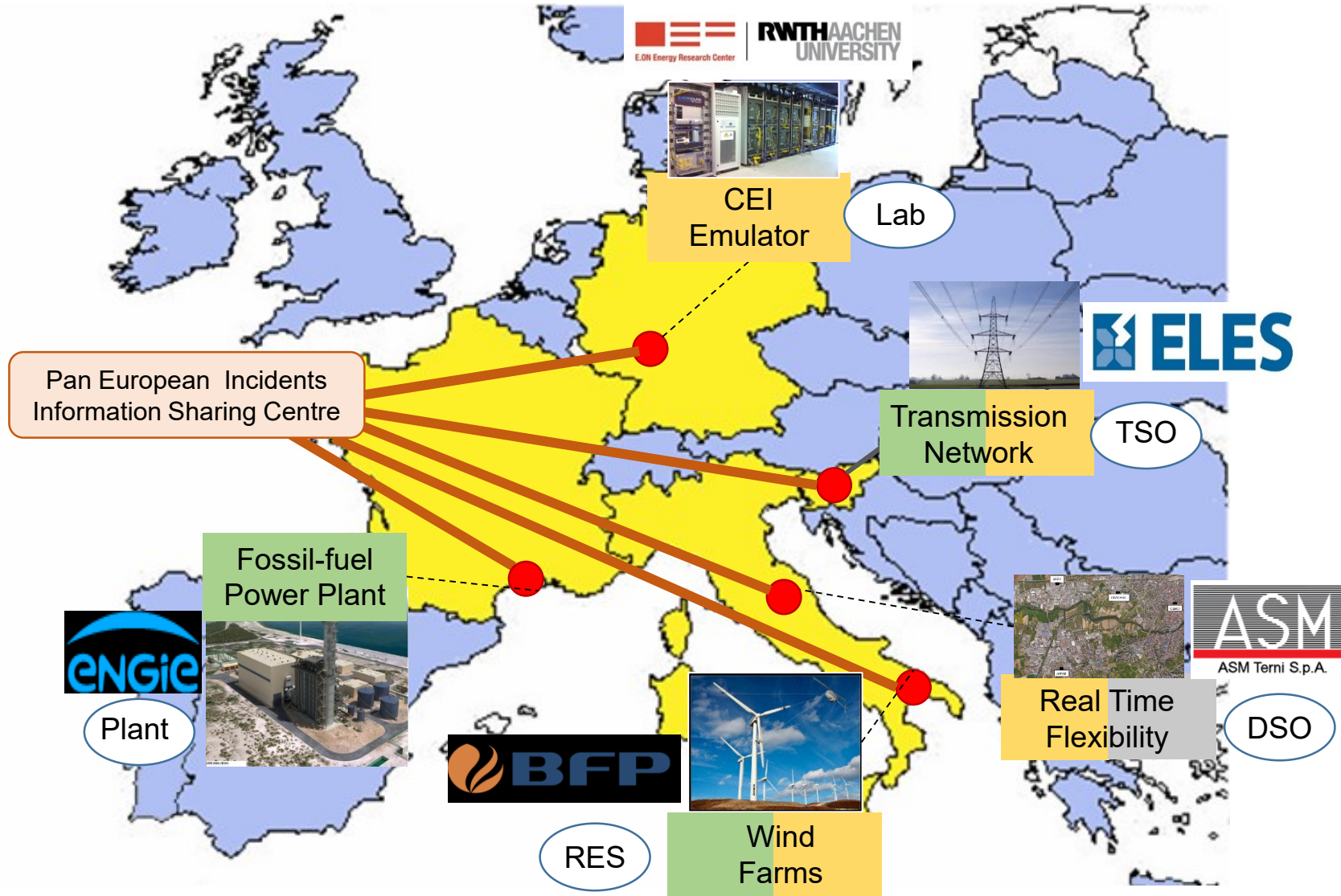


Ethereum as a Consortium
blockchain to store the identity

IPFS distributed,
encrypted file system

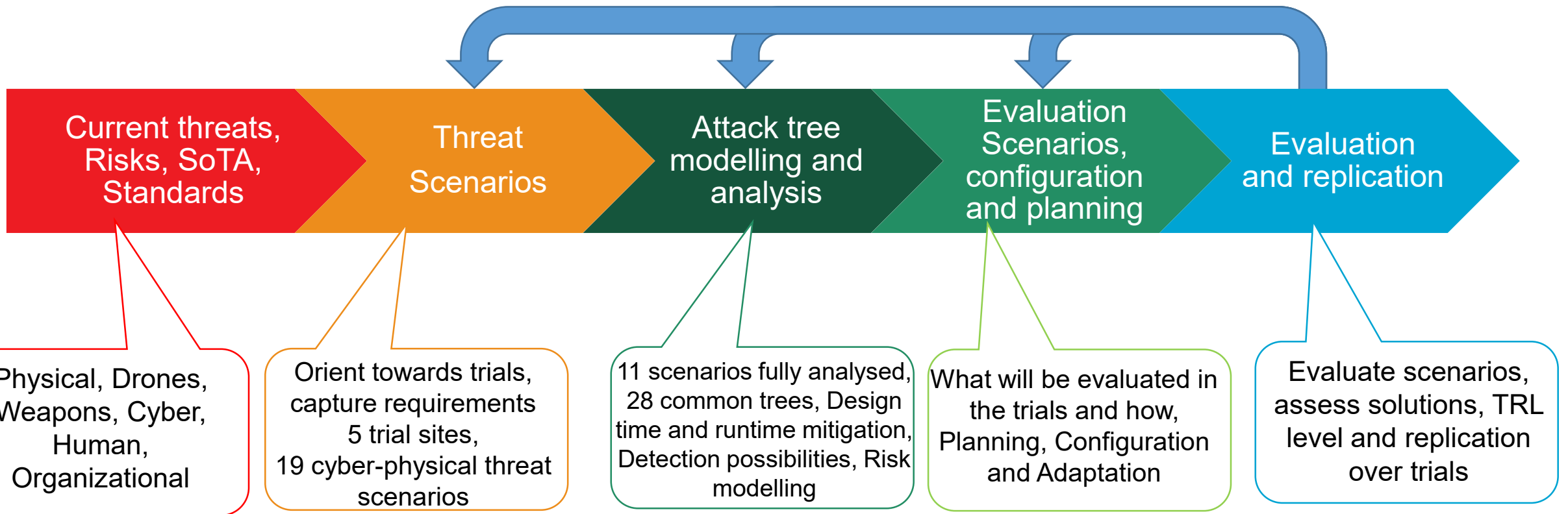
End-to-end encryption using open source technologies
(Open Whisper Signal)

Pilots Evaluation



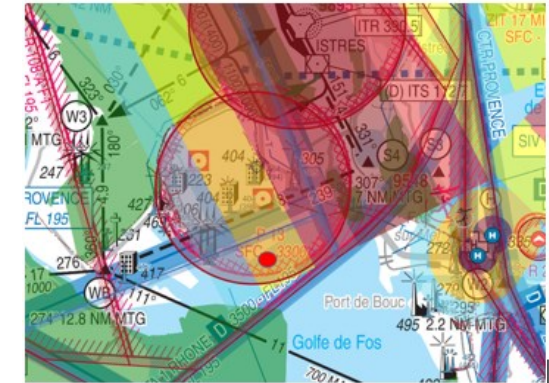
Methodology: From requirements to evaluation

Continuous feedback and improvements



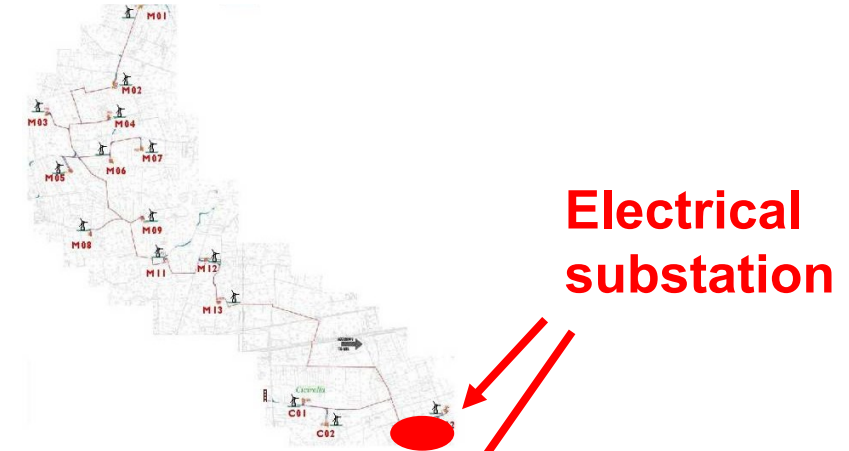
Bulk Energy Generation Trial

- **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
- **Threats scenario :**
 - R1 : Mini-drone attack & neutralization
 - R2 : Physical attack to gain network access
- **Surveillance proposal**
 - Autonomous drone coupled to GENETEC
 - Surveillance tour + doubt removal
 - 2D Laser Fence
- **Trials planned in November 2019**



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 RES generator and DSO
- **Four threat scenarios:**
 - R1: Unauthorized access to the electrical substation
 - R2: Unauthorized access to the wind turbines
 - R3: Drone attack
 - R6: Stop time reduction
- **Technology:** Human Intrusion Detection Based on Video Analytics, Drone-based surveillance, 3D LIDAR, Flying Hunter, Drone for inspection, Video Analytics for Preventive Maintenance
- **Involvement of Italian Police (Polizia di Stato)**
- **Trials planned in December 2019**



TSO Network Trial Pilot

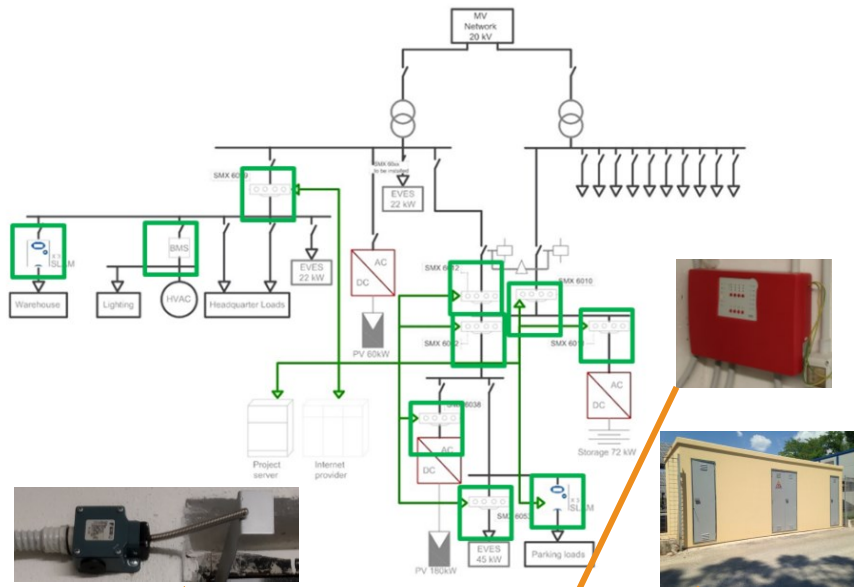
- **Pilot site:** Okroglo switching station, Slovenia
- **Main focus:**
 - Power line fault isolation and restore
 - Lack of coordination among different security platforms
 - Swarm of drones equipped with camera for lifecycle assets management
- **Three threat scenarios:**
 - T1: Power line fault isolation 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
- **Technology:** Network Fault Detectors, Face Recognition, People Detection and Counting
- **Additional effort:**
 - Organisational improvements (all scenarios)
 - Swarm of drones evaluation for preventive maintenance (T1 scenario)
- **Continuous trials from July 2019**

- The site
 - Two 400 kVA and 110 kVA transformers
 - Two-story station consists of building including a ICT control room
 - SCADA control room and offices
 - Secondary and backup powers systems
 - Warehouse
 - Switch yard
- The substation extends on 34.323,56 m²



DSO Network & Prosumer Trial – Terni (Italy)

D1 – a) Cyber-Physical attack



PLATFORM

- **Main focus:**
 - Physical threat to network assets
 - Security gap between DSO and RES

D1 – b) MV fault localization and Power flow re-routing

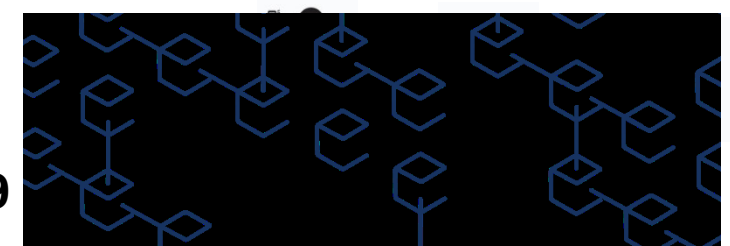
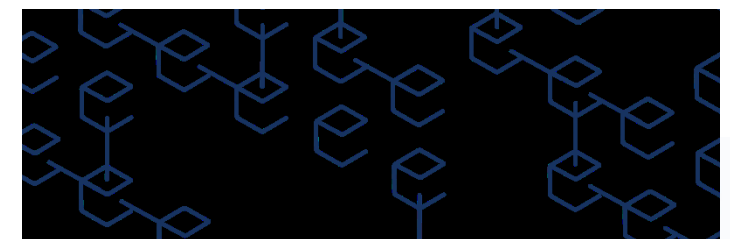


PMU-based algorithm for fault localization



- **Trials will begin in September 2019**

D2 - HITL



Achieved results and Ongoing activities

DEFENDER (up to date) achieved results #1

- CEI threats and risks:

1. Analysis and classification of the existing and unknown CEI threats through **attack trees modelling**,
2. **Risk assessment methodology and tool** to determine and visualize an **overall risk exposure/rate**
3. Criteria to assess the risk and classify the CEI assets, systems and segments (**CEI Secure Tiers**)

- Tools and components to reduce risk by design:

1. Short-term and long-term security aspects for **Security Lifecycle Assessment by design**
2. Double Virtualization and Network Function Virtualization for **Resilience by design**
3. Optimized Security Resource Allocation, Fault Localization and Service Restoration for **Self-healing by design**
4. Recommendations to privacy protection during the development to establish **Privacy by design**

DEFENDER (up to date) achieved results #2

- **CEI situation perception, comprehension and awareness:**
 1. **Cyber and Physical detectors** based on sensors, devices and tools for *anomaly detection*
 2. **Information Fusion and Event Processing** components for the *state of the environment* perception
 3. **CPSS co-simulator** that simulates how the CEI situation environment might evolve, mapping in a certain attack tree
 4. Novel **dynamic countermeasures toolbox** aims at physical and cyber threat/attack prevention, prioritizing the more relevant information and security objectives along with their effect in the network.
- **Human Sensors and HITL tools and application** for innovative, trusted, traceable and bidirectional information flows, enabling efficient
 - a) **CEI-to-HITL communication** (information from the CEI on incidents and instructions to employees or citizens in the vicinity) and
 - b) **HITL-to-CEI communication**, acting as front line responders.

DEFENDER ongoing activities

- Define **adaptable countermeasures and resiliency enhancing mitigation strategies** combining and integrating **threat and vulnerability analysis** as well as **historical attacks and applied mitigations** so as to trigger the most suitable response
- **CEI Incidents Information Sharing Platform (I2SP)** enabling information exchange on **physical and cyber attacks patterns and countermeasures at Pan-European level**
- **Heterogeneous and pan-European trials** to demonstrate and evaluate the **DEFENDER platform functionality** for physical-cyber proactive and reactive safeguarding behaviour.
- 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.**

Towards the Standardisation

Standardisation: ongoing Work and Potential Impact

- Impact on Standards focusing on **information security** (family of ISO 27000) guidelines and threats assessment for **industrial system control** (incl. SCADA) (IEC 62443, NIST 800-82) guidelines
 - incorporating **physical and human aspects/threats into combined threat assessment and vulnerability management (attack trees)** (Human in the loop) with a view to provide comprehensive approach for protection of CEI
 - Potential impact/liaison with ENTSO-e procedures (e.g. Network Code on Operational Security)
- Impact on Standards focusing on **communication protocols/data exchange for bulk power generation plants (IEC 62351)**
 - Potential extension to manage **Distributed Energy Resources (DERs)**
- Standards targeting **technical security systems** (cameras, sensors, security centres)
- Input to potential standards (communication protocols and data exchange)
 - among **power network operators and LEAs**
 - TSOs vs National-level CERTs (ENISA) and EE-ISAC
- **Links with** European Cyber Security organization (ECSSO), ENISA, EE-ISAC
- Drone's and preparation new EU regulative;

Conclusions

- DEFENDER as *First-of-this-kind EU-scale solution for cyber-physical protection and security fully tailored to cover the complete value chain of smart Critical Energy Infrastructures*
- Bringing citizens and CEI stakeholders workforce at a center stage, as key elements of the proposed solution (**human dimension**)
- One of the very first attempts to bring together in a systematic way **electrical energy network operators and Law Enforcement Agencies (LEAs)** at the same table

*Defending the European
Critical Energy Infrastructure*

Thank you!

For further information do not hesitate to contact us at :

massimo.bertoncini@eng.it,

gabriele.giunta@eng.it,

denis.caleta@ics-institut.si

**Defending the European
Critical Energy Infrastructure**

Backup