ENERGY SHIELD

ENERGYSHIELD PROJECT

Introducing the project and the collaboration strategy

Facilitators: Otilia Bularca (SIMAVI)
Anna Georgiadou (NTUA)

8/7/2020

SU-DS04-2018-2020 – SISTER PROJECTS AGENDA

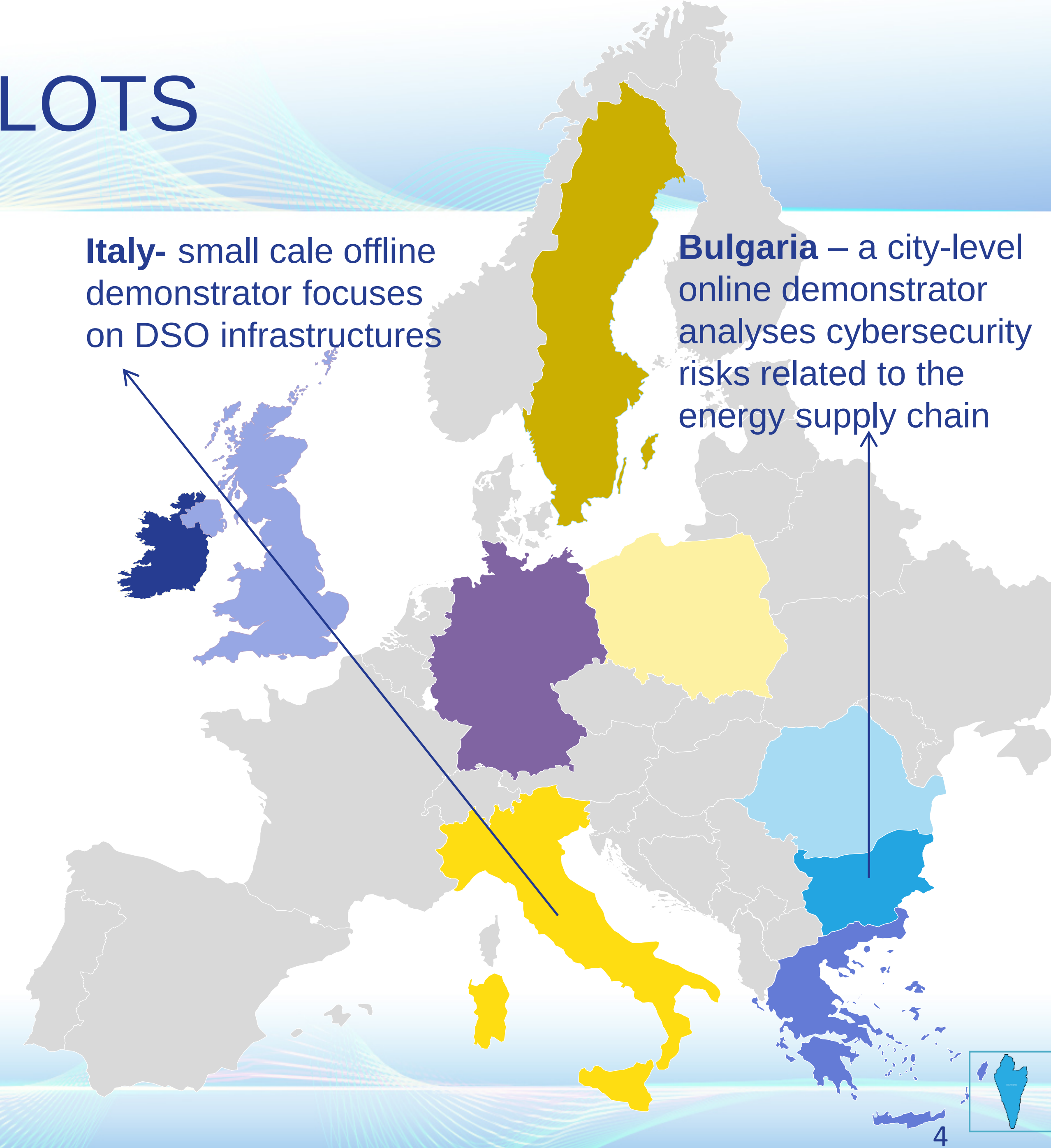
- Introducing the projects
  - Energy Shield – GA 832907 - https://energy-shield.eu/
  - PHOENIX – GA 832989 - https://phoenix-h2020.eu/
  - SDN-microSENSE – GA 833955 - https://www.sdnmicrosense.eu/
- Collaboration strategy
- Open discussion
- Way forward

ENERGYSHIELD PROJECT IN A NUTSHELL

- Title: Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring and Protection of Critical Energy Infrastructures
- Type of Action: Innovation Action
- Topic: SU-DS04-2018-2020
  - Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches
- Goal
  - EnergyShield captures the needs of Electrical Power and Energy System (EPES) operators and combines the latest technologies for vulnerability assessment, supervision and protection to draft a defensive toolkit.
- Start date: 1st of July 2019
- Duration: 36 months
- Grant: € 7,421,437.38

CONSORTIUM AND PILOTS

Romania:	Software Imagination & Vision
Germany:	PSI Software AG
Israel :	SI-GA Data Security (2014) LTD
Luxemburg	L7 Defense Luxembourg SARL
Sweden:	foreseeti AB
	Kungliga Tekniska Hoegskolan
UK:	Tech Inspire LTD
	City University Of London
Ireland:	Konnekt Able Technologies
Greece:	National Technical University Of Athens
Bulgaria:	Software Company EOOD
	Kogen Zagore EOOD
	MVETS Lenishta OOD
	Elektroenergien Sistemen Operator EAD
	CEZ Distribution Bulgaria AD
	MIG 23 LTD
	DIL DIEL
Italy	IREN SPA



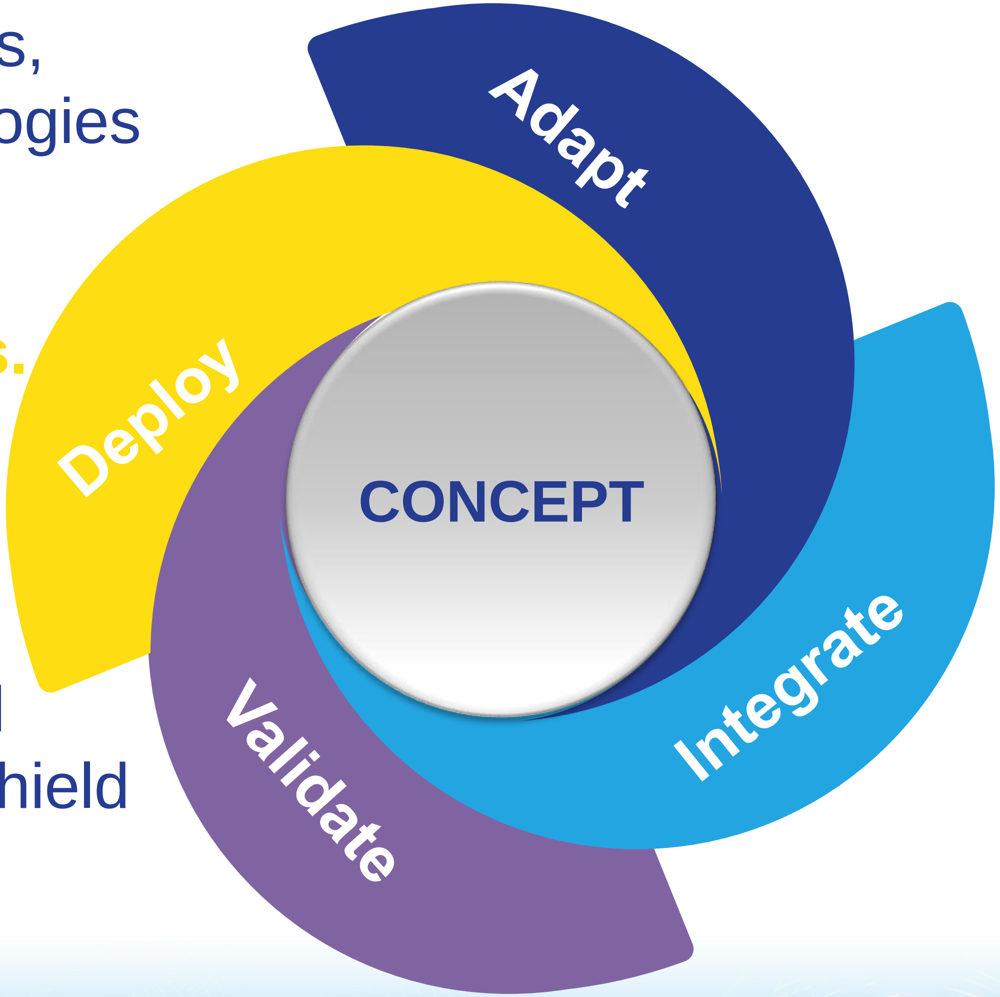
Italy- small cale offline demonstrator focuses on DSO infrastructures

Bulgaria – a city-level online demonstrator analyses cybersecurity risks related to the energy supply chain

CONCEPT AND OBJECTIVES

Deploy best practices, guidelines, methodologies and encourage the adoption of EnergyShield **results.**

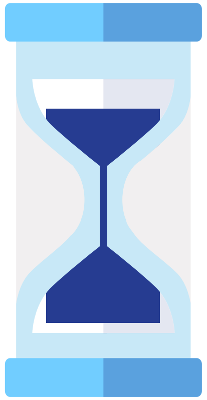
Adapt and improve available **tools** to support Electrical Power and Energy System (EPES) in fighting against cyber attacks.



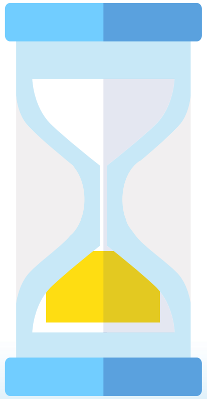
Validate the practical value of the EnergyShield **toolkit** with EPES stakeholders.

Integrate the cybersecurity tools in **a holistic solution** with assessment, monitoring, protection and learning capabilities.

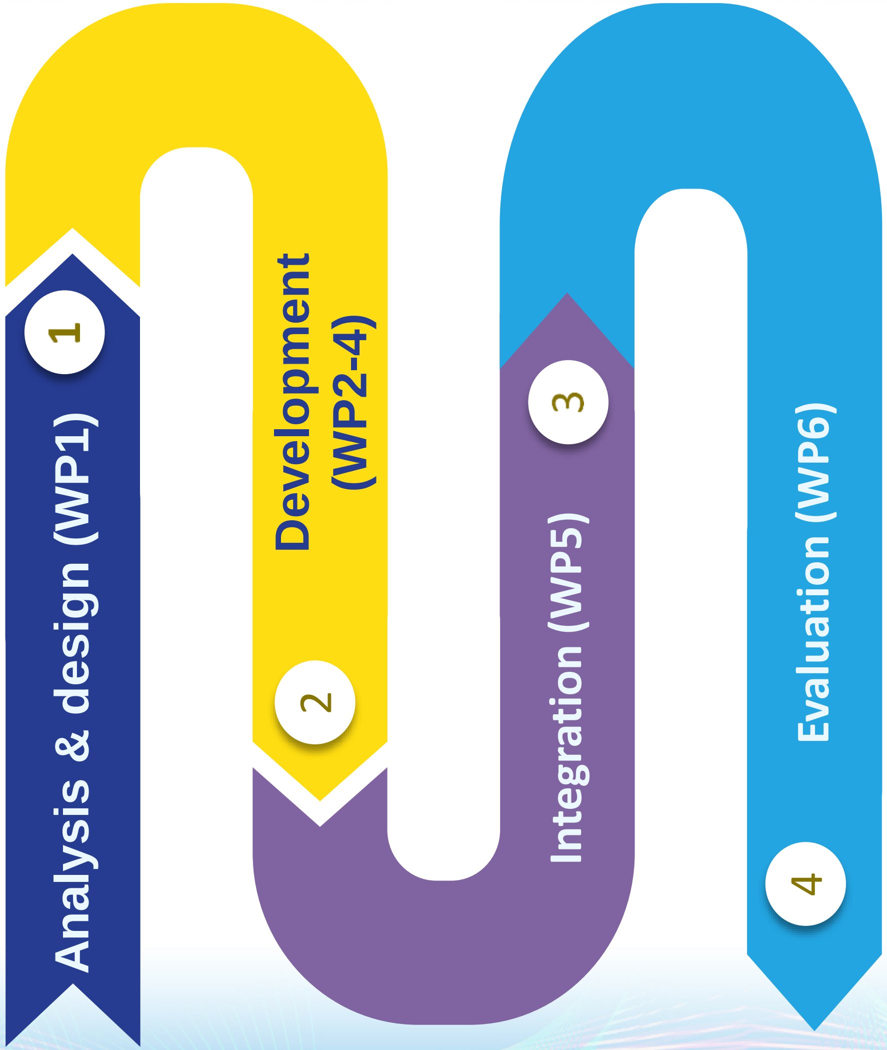
TECHNICAL ACTIVITIES PROGRESS



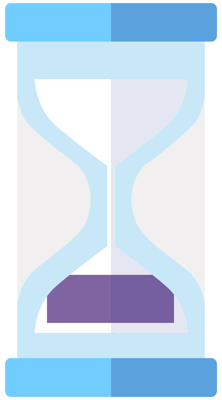
- Analysis
- Architecture
- FRs
- NFRs



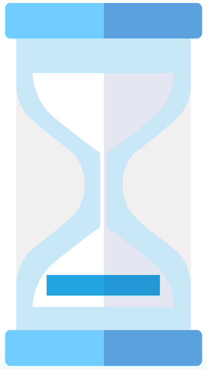
- Tools roadmap
- Tools release plan
- Demonstrators timeplan



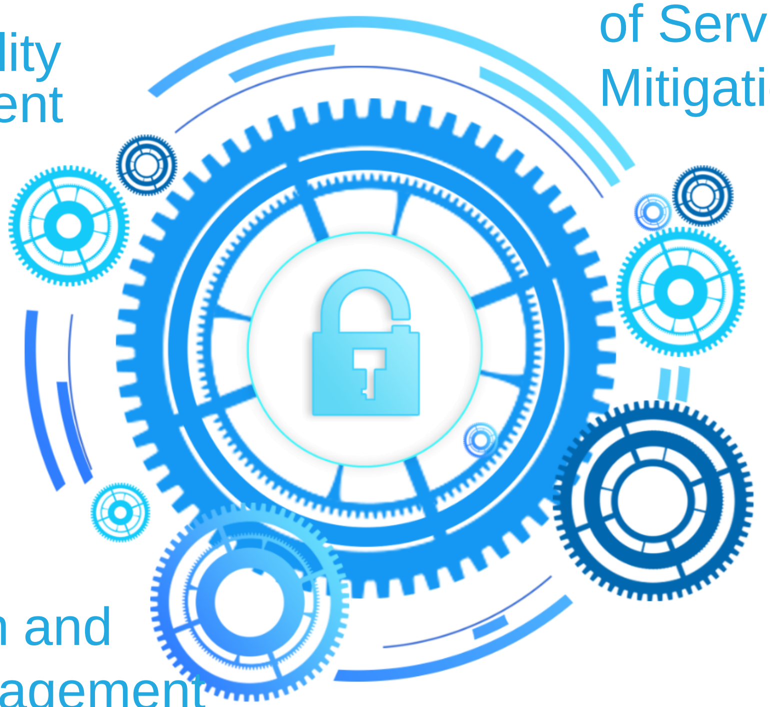
- Integration plan
- Deployment plans
- Test plan
- Toolkit demo release timeline



- User needs
- Tools evaluation
- On-site deployment
- Piloting
- Evaluation



ENERGYSHIELD TOOLKIT



Vulnerability Assessment

Distributed Denial of Service Mitigation

Security Behaviour Analysis

Anomaly Detection

Security Information and Event Management

Small scale attacks

- Targeting specific organization
- Meant to prevent them from conducting business normally
- *e.g. Distributed Denial of Service, ransomware*

Large scale attacks

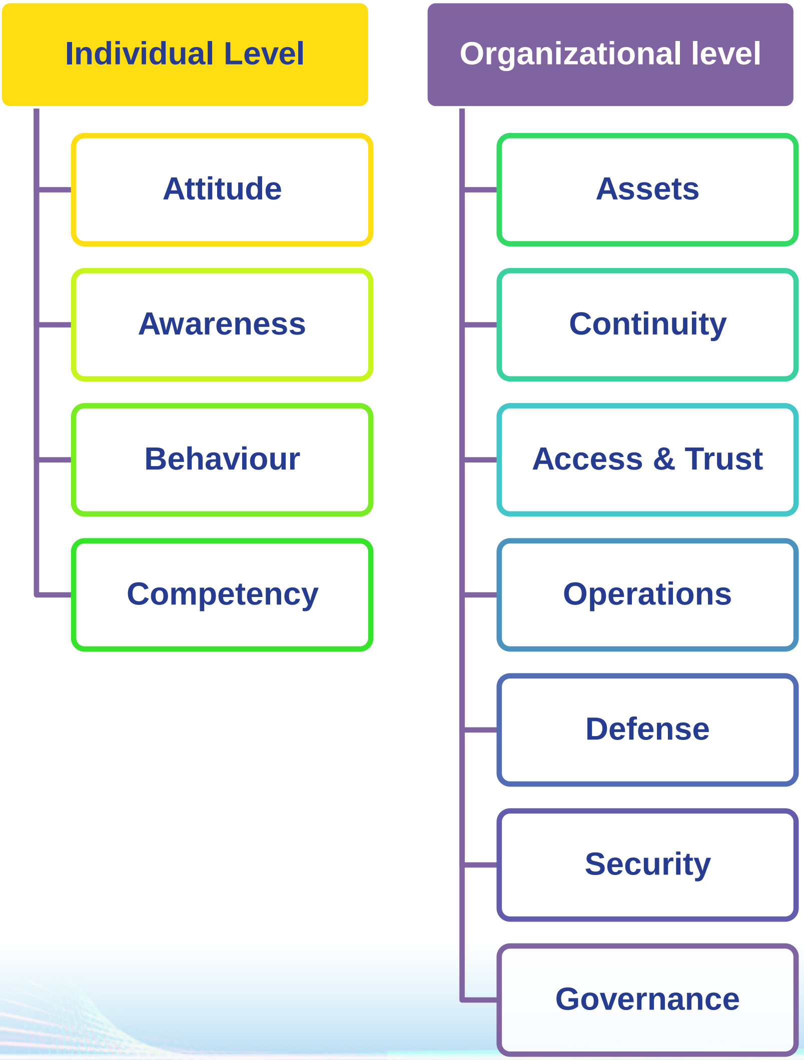
- Targeting the entire EPES value chain
- Meant to take down the energy supply services at regional or country level
- *e.g. malware deployment, man-in-the-middle*

VULNERABILITY ASSESSMENT TOOL

- Tool contributors
  - Leading partner: FOR
  - Contributing partners: **KTH**, PSI, SIMAVI
- Tool features
  - *Threat modelling & Attack Simulations*
    - Analyze cyber resilience in complex systems
    - Bayesian probability networks, Monte Carlo simulations and k-means clustering
  - *Operates on a model – a cyber “digital twin”*
    - Non-intrusive, risk-free
    - Exactness determined by the threat modelling “language” and quality of model
    - Cyber threats are automatically derived from the structural system model
  - *“The language” epesLang*
    - Codifies the cyber-characteristics of ICS and the electrical energy sector systems
    - Based on Meta Attack Language (https://mal-lang.org)
- TRL – Started on 7, targeting 8 (9 after project end)

SECURITY BEHAVIOR ANALYSIS TOOL

- Tool contributors
  - Leading partner: NTUA
  - Contributing partners: FOR, KTH, SC, IREN
- Tool features
  - Founded on a cyber-security culture model: **levels, dimensions** and **domains**
  - Evaluation methodology: **campaigns** and **self-assessment** possibilities
  - Socio-cultural behaviour mapping to specific **cyber-threats**
  - Decision-making insights and **recommendations** towards security culture improvement
  - Assistance into planning and implementing **security culture training programs**
  - Open, highly **customizable** and **interoperable** with third-party components
- TRL 4 → TRL 8



SIEM TOOL

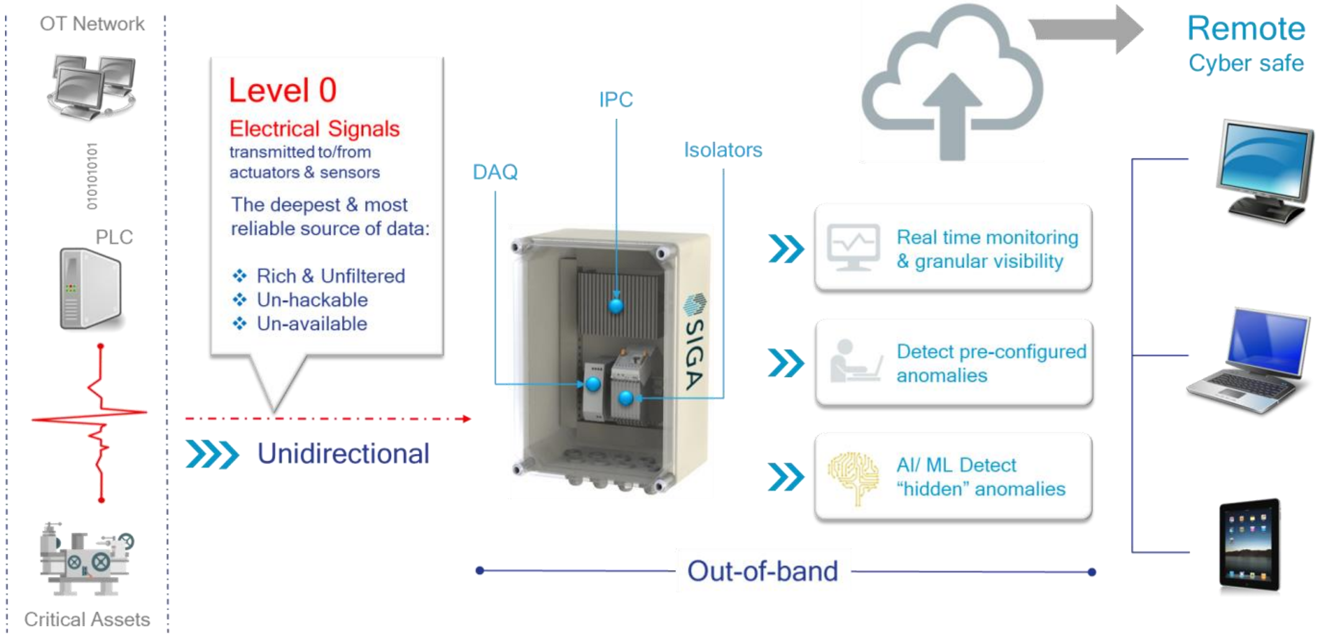
- Tool contributors
  - Leading partner: KT
  - Contributing partners: SIGA, FOR, L7D, TEC, NTUA, SC
- Objective
  - implement a customized SIEM tool able to interact with the other EnergyShield tools and components
- TRL 6 → TRL 8
- Concept to be integrated within SIEM
  - Homomorphic encryption
  - Automated forensic tool

SIEM features

- Event Logging
- Data Storage
- Secure Authorization
- Monitoring
- Alerting
- Visualization
- System Diagnostics

ANOMALY DETECTION TOOL

- Tool contributors
  - Leading partner: SIGA,
  - Contributing partners: IREN, SC (at the pilot's phase)
- Tool features
  - SIGA’s topology & architecture
  - Improved anomaly detection algorithms
  - Extended user’s understanding of anomalies
  - Extended variety of sources of process data



Level 0

Electrical Signals transmitted to/from actuators & sensors

The deepest & most reliable source of data:

- Rich & Unfiltered
- Un-hackable
- Un-available

OT Network
0101010101
PLC
Critical Assets
Unidirectional
DAQ
IPC
Isolators
SIGA
Real time monitoring & granular visibility
Detect pre-configured anomalies
AI/ ML Detect “hidden” anomalies
Out-of-band
Remote
Cyber safe

DISTRIBUTED DENIAL OF SERVICE MITIGATION TOOL

- Tool contributors
  - Leading partner: L7 Defense
  - Contributing partners: CITY
- Objective
  - Improve the Real time DDoS mitigation for Energy IT
- TRL 6 → TRL 8

FROST & SULLIVAN

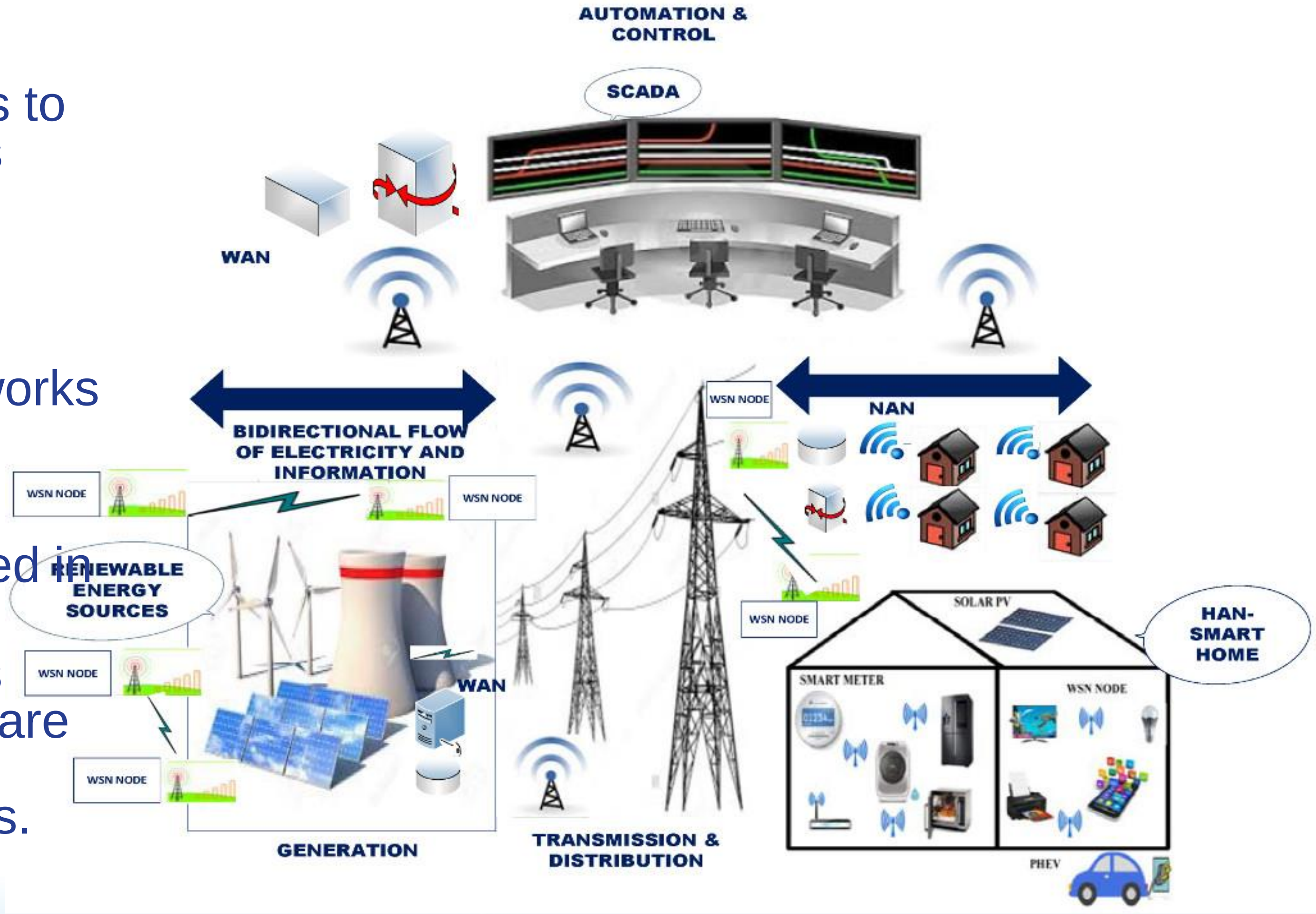
New Product Innovation Award

Anti-Distributed Denial of Service (DDoS) for Critical National Infrastructure

GLOBAL
DISRUPTIVE TECHNOLOGIES
INDUSTRY CONVERGENCE
GLOBAL MEGA TRENDS
CUSTOMER DYNAMICS
BEST PRACTICES
COMPETITIVE INTENSITY
EMERGING MARKETS
CEO

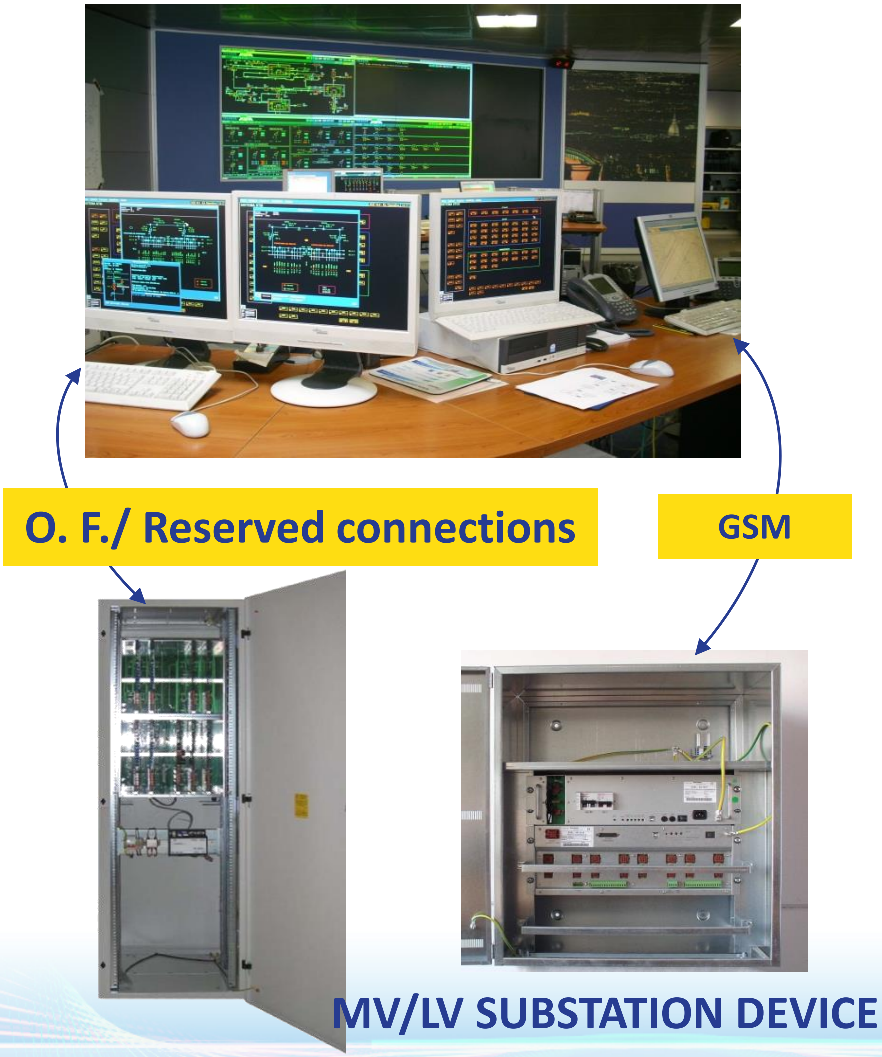
BULGARIAN PILOT

- Aim
  - to evaluate the most effective solutions to prevent, detect, and mitigate malicious cyber-attacks
- Scenarios
  - Attacks on Substation Infrastructure
  - Attacks on Consumer / Prosumer networks points
- Infrastructure
  - a SCADA system installed and operated in the various substations.
  - PLC/RTUs and measurement systems (energy meters, PMUs, DLR sensors) are interconnected by using the DNP3/IEC60870-5/IEC61850 protocols.



ITALIAN PILOT

- Aim
  - to evaluate the most effective solutions (hardware and software solutions, organizational approaches, changes in the procedures and qualified the staff in this field) to face malicious cyber-attacks.
- Scenarios
  - Testing the Security Behaviour Analysis tool on – **AMM** (Automatic Meter Management) and **ST Siemens** – Network remote control system
  - Perform a feasibility study on integration of the Anomaly detection tool on its specific SCADA (Supervisory Control and Data Acquisition) system – **ST Siemens**.
- Infrastructure
  - HV/MV Remote control system and SCADA
    - Network monitoring
    - Fault/outage detection
    - Emergency operations
    - Limited impacts (in terms of outages) on Clients



O. F./ Reserved connections

GSM

MV/LV SUBSTATION DEVICE

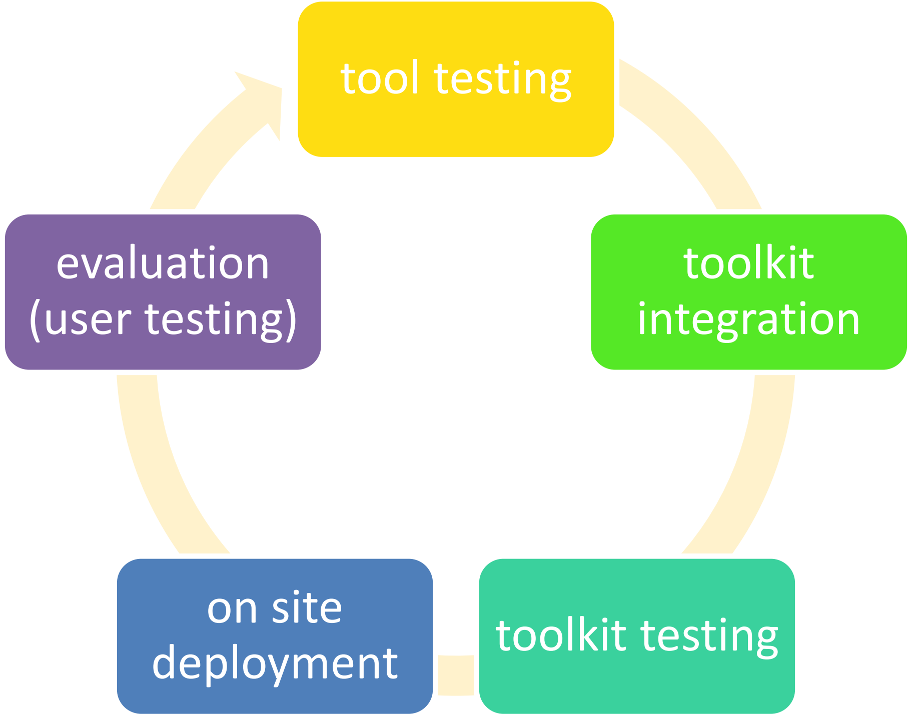
HV/MV SUBSTATION DEVICE

ENERGYSHIELD PILOTS COMPARATIVE APPROACH

	Bulgarian Pilot	Italian Pilot
Location	District of Sofia and Pernik, Kyustendil, Blagoevgrad, Vidin, Montana, Vratsa, Pleven and Lovech districts.	DSO network of the city of Turin, Italy
Aim	Study the **cascading effects** of cyberattacks throughout the value chain and analyse cybersecurity risks related to the cyber supply chain	The **feasibility study** (and possible offline trial on a dedicated, simulation area of the networks control systems, if feasible) will be set on Turin DSO network.
Innovation	**Mitigate** cyber attacks and data breaches taking into account decentralised architecture and all stakeholders of the value chain,	Possibility to **test** an integrated suite of cyber security tools; Defining **evaluation** KPIs of the testes solutions with all stakeholders involved
Approach	**Involving several generators** including distributed power generation (hydro and solar PV) as well as several primary substations, secondary substations and end users.	Identifying the most relevant **threats** and **vulnerabilities** in each subsystem of the network; Identifying the most effective **measures** to protect the systems;
Outcome	Full end-to-end demonstrator involving all stakeholders of the EPES value chain **Online** trial	Evaluate the most effective solutions (hardware and software solutions, organizational approaches, changes in the procedures and qualified the staff in this field) for industrialization **Offline** trial

INTEGRATION APPROACH

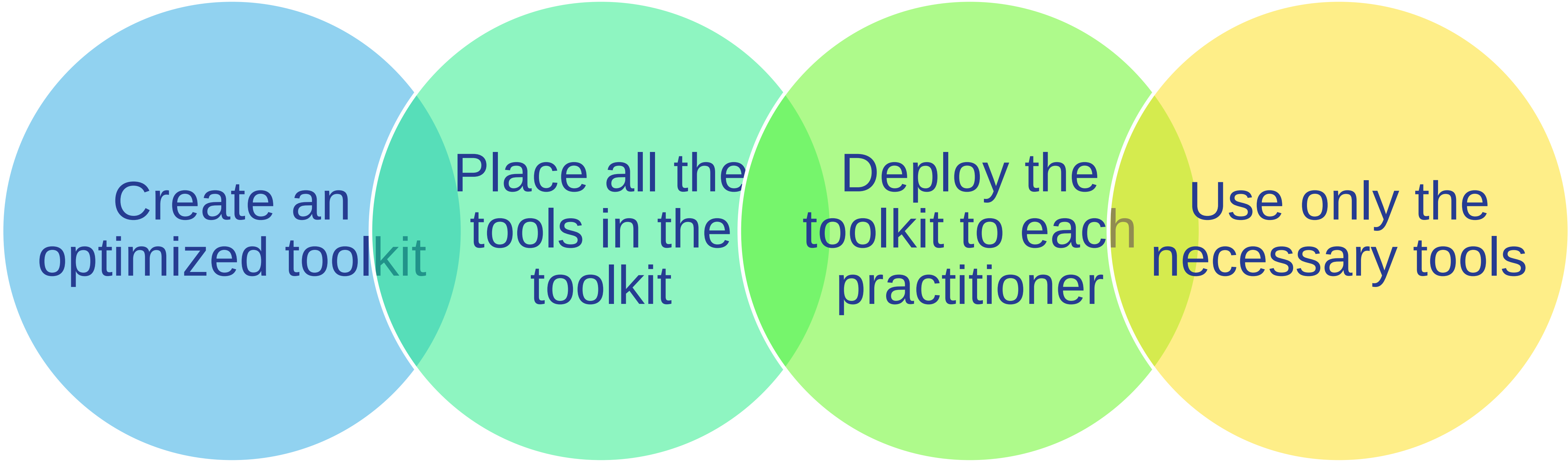
- Tools testing
  - available features and capabilities are tested and mapped against the needs of the pilot cases provisioned in EnergyShield project.
- Toolkit integration
  - EnergyShield multi-layered system covering operating systems, middleware, database and IoT harvesting methods.
- Toolkit testing
  - different testing from unit testing individual modules, integration testing an entire system to specialized forms of testing such as security and performance.
- On site deployment
  - operations to prepare EnergyShield system for assembly and transfer to the computer system(s) on which it will be run in production.



INTEGRATION PERSPECTIVES

- First stage of tests, focused on the whole toolkit, deployed at project (SIMAVI) level
- Second stage of tests, in pilot sites
  - Rent the toolkit and/or just some tools (Cloud SAAS)
  - Clone the toolkit and/or just some tools
- Integration prospects:
  - Development side focused on how to develop the different parts of the system (as a framework of tools) in a orchestrated way
  - Deployment side focused on how the final (integrated) system/solution will look like and how its specific parts will exchange and handle data and will trigger processes

INTEGRATION AND DEPLOYMENT FLOW OF ACTIVITIES



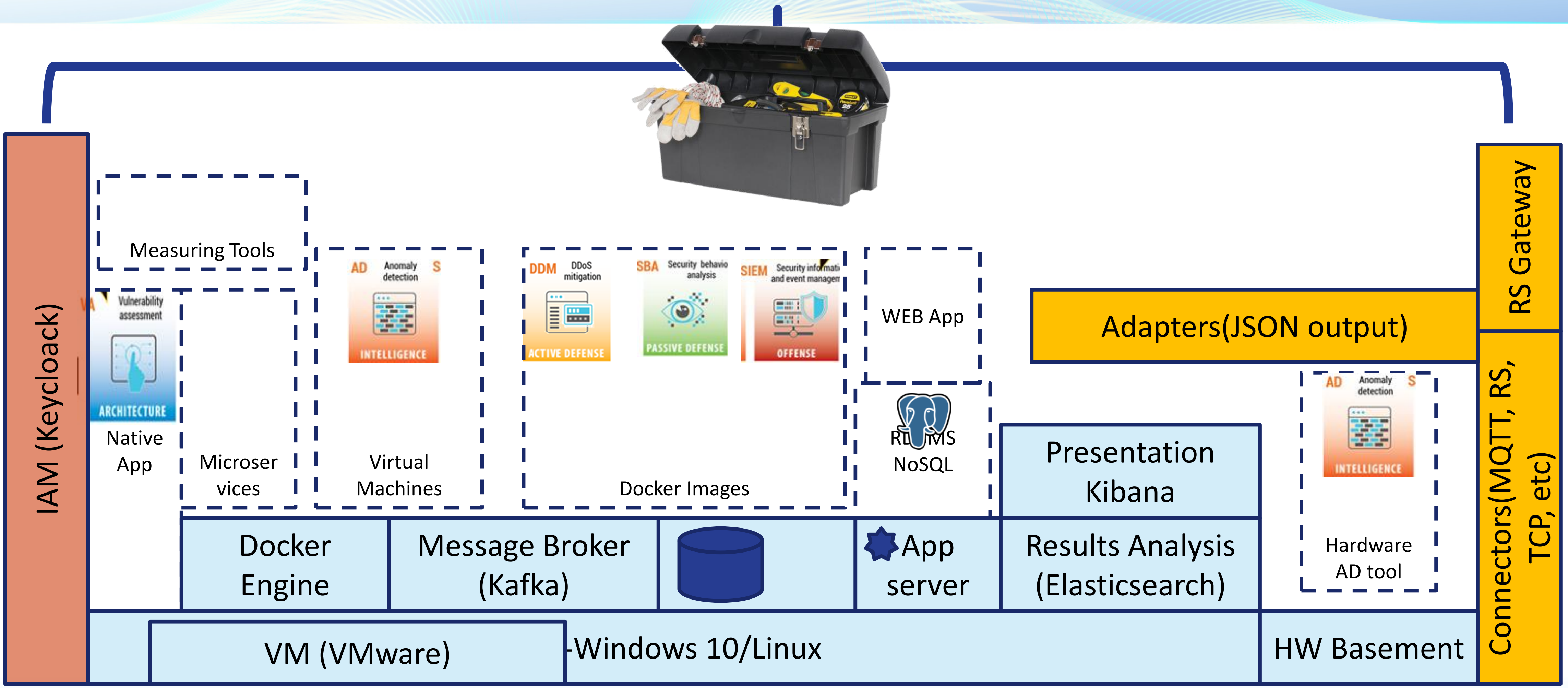
Create an optimized toolkit

Place all the tools in the toolkit

Deploy the toolkit to each practitioner

Use only the necessary tools

ENERGY SHIELD TOOLKIT ORGANIZATION



IAM (Keycloack)

Measuring Tools

Native App

Microser vices

Virtual Machines

Docker Images

WEB App

RDBMS NoSQL

Adapters(JSON output)

RS Gateway

Connectors(MQTT, RS, TCP, etc)

Presentation Kibana

Hardware AD tool

Docker Engine

Message Broker (Kafka)

App server

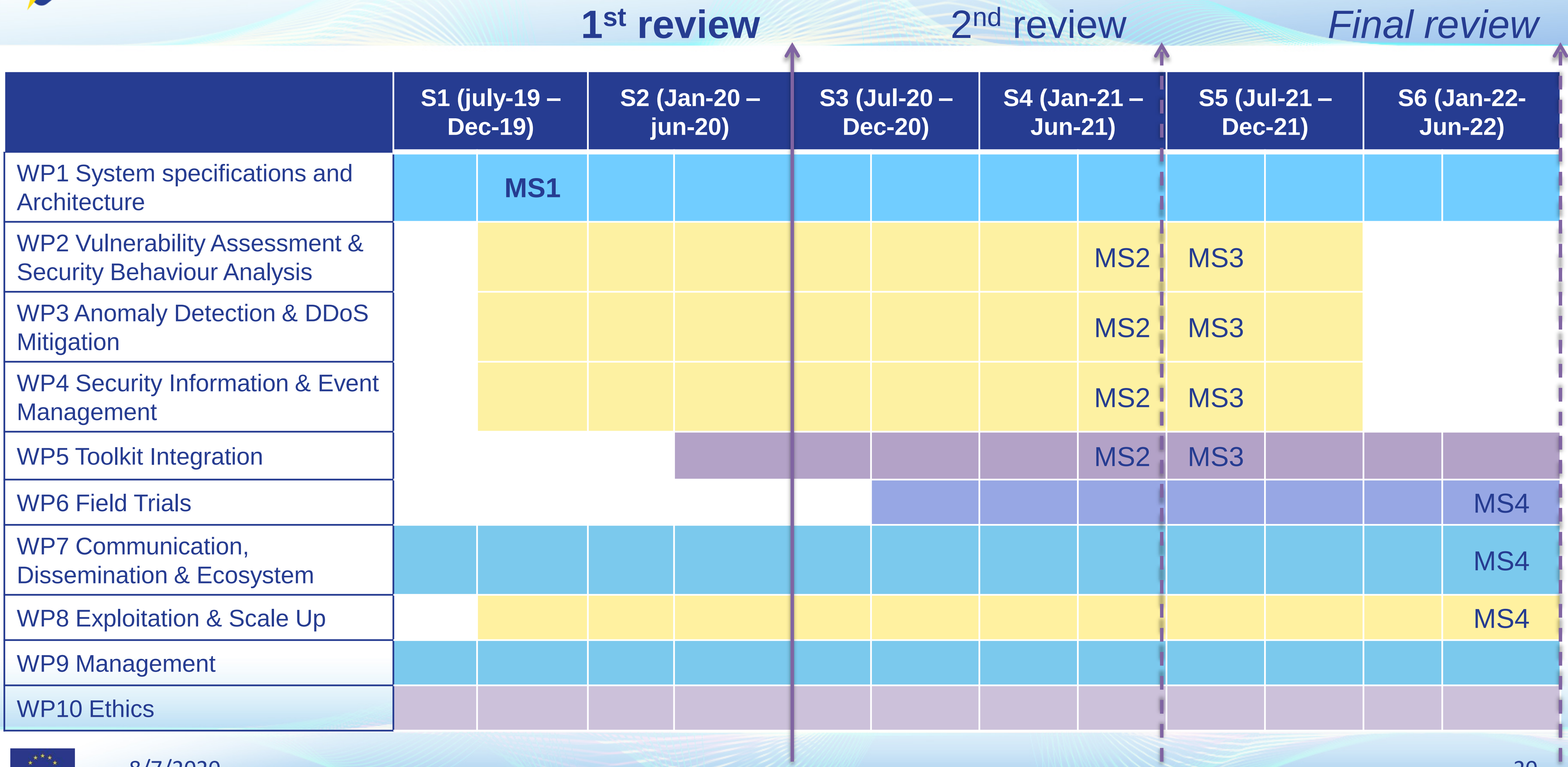
Results Analysis (Elasticsearch)

VM (VMware)

Windows 10/Linux

HW Basement

GANTT CHART



	S1 (july-19 – Dec-19)		S2 (Jan-20 – jun-20)		S3 (Jul-20 – Dec-20)		S4 (Jan-21 – Jun-21)		S5 (Jul-21 – Dec-21)		S6 (Jan-22-Jun-22)	
WP1 System specifications and Architecture	🟦	🟦 MS1	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
WP2 Vulnerability Assessment & Security Behaviour Analysis		🟨	🟨	🟨	🟨	🟨	🟨	🟨 MS2	🟨 MS3	🟨		
WP3 Anomaly Detection & DDoS Mitigation		🟨	🟨	🟨	🟨	🟨	🟨	🟨 MS2	🟨 MS3	🟨		
WP4 Security Information & Event Management		🟨	🟨	🟨	🟨	🟨	🟨	🟨 MS2	🟨 MS3	🟨		
WP5 Toolkit Integration				🟪	🟪	🟪	🟪	🟪 MS2	🟪 MS3	🟪	🟪	🟪
WP6 Field Trials						🟦	🟦	🟦	🟦	🟦	🟦	🟦 MS4
WP7 Communication, Dissemination & Ecosystem	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦 MS4
WP8 Exploitation & Scale Up		🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨 MS4
WP9 Management	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
WP10 Ethics	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪

PROGRESS TOWARDS OBJECTIVES

O1	O2	O3	O4
Adapt and improve available building tools (assessment, monitoring & protection, remediation) to support EPES needs	Integrate the improved cyber security tools in a holistic solution with assessment, monitoring and learning capabilities	Validate the practical value of the EnergyShield toolkit in demonstrations involving EPES stakeholders	Develop best practices, guidelines and methodologies supporting the deployment and adoption of results in the EPES
50%	15%	20%	30%

MILESTONES

4

PILOTS COMPLETED (SC)

[M34] – WP6, 7, 8 - All pilots and evaluation reports completed. All dissemination activities completed. All exploitation activities completed

3

TOOLKIT READY (SIGA)

[M26] WP2,3,4,5 - All components ready for trials. Full solution integration complete. Solution ready for trial deployment

2

CORE MODULES READY (FOR)

[M19] WP2,3,4,5 - All components released. Early solution integration completed Pre-pilot completed.

1

USE CASES READY (SIMAVI)

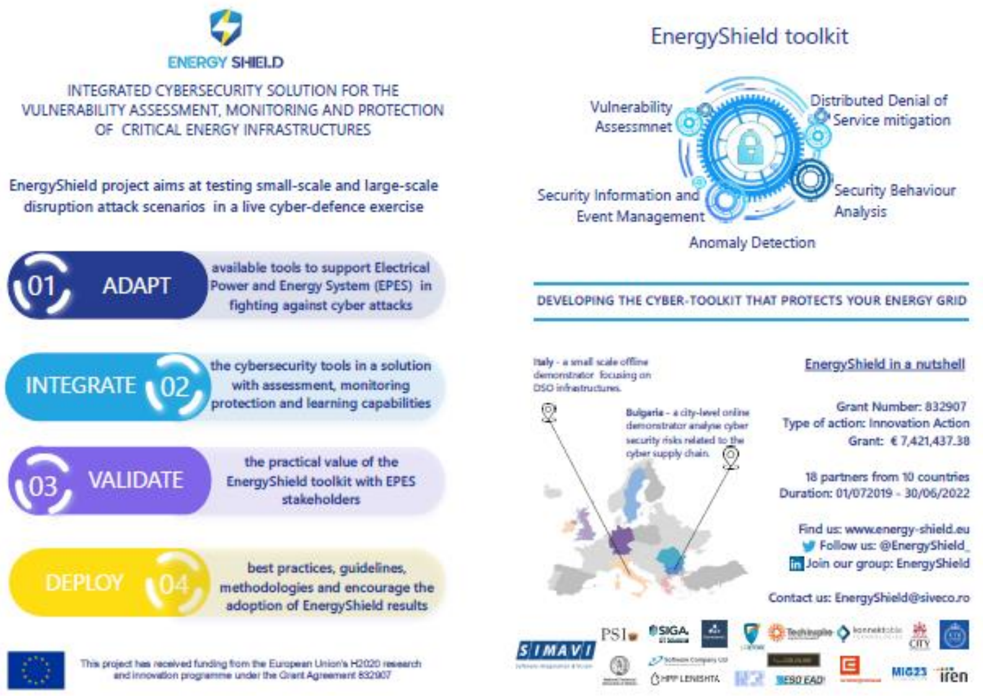
[M6] WP1 - All use cases documented. Technical, commercial and regulatory specifications ready.

TECHNICAL WORK AHEAD

Tools and system releases	M12	M15	M19	M20	M26	M30	M34	M36
1st Iteration of tools	■							
Toolkit concept release		■						
Evaluation framework		■	■					
2nd Iteration of tools			■					
Toolkit release v1				■				
1st round of field trial				■	■			
Toolkit release v2					■			
WP6 - 2nd round of field trial						■		
3rd iteration of tools						■		
Toolkit release v3 + QA						■		
Final version of toolkit							■	■
WP6 -final round of field trial							■	■

REACH OUT THE PROJECT

- Find us: www.energy-shield.eu
- Subscribe for Newsletter
- Follow us: @EnergyShield_
- Join our LinkedIn group: EnergyShield
- Contact us: EnergyShield@siveco.ro
- Video presentation: https://www.youtube.com/watch?v=AtSUnkrp1Dw
- Project Coordinator: SIMAVI
  - Otilia Bularca, Project Manager
  - E-mail: otilia.bularca@simavi.ro
  - Phone: 0040731202178



ENERGY SHIELD

INTEGRATED CYBERSECURITY SOLUTION FOR THE VULNERABILITY ASSESSMENT, MONITORING AND PROTECTION OF CRITICAL ENERGY INFRASTRUCTURES

EnergyShield project aims at testing small-scale and large-scale disruption attack scenarios in a live cyber-defence exercise

01 ADAPT available tools to support Electrical Power and Energy System (EPES) in fighting against cyber attacks

INTEGRATE 02 the cybersecurity tools in a solution with assessment, monitoring protection and learning capabilities

03 VALIDATE the practical value of the EnergyShield toolkit with EPES stakeholders

DEPLOY 04 best practices, guidelines, methodologies and encourage the adoption of EnergyShield results

This project has received funding from the European Union's H2020 research and innovation programme under the Grant Agreement 832907

EnergyShield toolkit

Vulnerability Assessmnet

Distributed Denial of Service mitigation

Security Information and Event Management

Security Behaviour Analysis

Anomaly Detection

DEVELOPING THE CYBER-TOOLKIT THAT PROTECTS YOUR ENERGY GRID

Italy - a small scale offline demonstrator focusing on DSO infrastructures.

Bulgaria - a city-level online demonstrator analyse cyber security risks related to the cyber supply chain.

EnergyShield in a nutshell

Grant Number: 832907
Type of action: Innovation Action
Grant: € 7,421,437.38

18 partners from 10 countries
Duration: 01/072019 - 30/06/2022

Find us: www.energy-shield.eu
Follow us: @EnergyShield_
Join our group: EnergyShield

Contact us: EnergyShield@siveco.ro

ENERGY SHIELD

COLLABORATION STRATEGY

COLLABORATION APPROACH

- Sister projects (funded in the same call SU-DS04-2018-2020)
  - PHOENIX – GA 832989 - https://phoenix-h2020.eu/
  - SDN-microSENSE – GA 833955 - https://www.sdnmicrosense.eu/
  - Energy Shield – GA 832907 - https://energy-shield.eu
- Meeting each other (this workshop)
  - Presentation duration
  - Presentation details, e.g. project presentation (objectives, progress, challenges, etc.), framework/tools demo, etc.
  - Project mailing list (to be used for workshop invitation emails)

WAY FORWARD - SYNERGIES

- Overall discussion and further light synergies suggestions
  - Share / Join forces on social media communication channels / networking boost
  - Include on project websites a section “sister projects” with information about this related projects
  - Online workshop to share technical achievements where BRIDGE leaders could be invited to endorse the event
  - Online end-user workshop

ENERGY SHIELD

THANK YOU | QUESTIONS

DEVELOPING THE CYBER-TOOLKIT THAT PROTECTS YOUR ENERGY GRID

SIMAVI
Software Imagination & Vision

PSI

SIGA
OT Solutions

foreseeti

ESO EAD

РАЗПРЕДЕЛЕНИЕ

CITY
UNIVERSITY OF LONDON
EST 1894

KTH
VETENSKAP
OCH KONST

L7 DEFENSE

ΕΘΝ. ΜΕΤΣΟΒ. ΠΟΛΥΤΕΧΝΕΙΟΝ

MIG23
turnkey engineering

TechInspire
Inspire for innovation

iren

K3

GOLDLINE

HPP LENISHTA

Software Company Ltd
Developing quality software solutions since 1996

konnektable
TECHNOLOGIES

This project has received funding from the European Union's H2020 research and innovation programme under the grant agreement No. 832907