Electrical Power System's Shield against complex incidents and extensive cyber and privacy attacks

PHOENIX

Industrial Cybersecurity Testing Methodology on LSPs

2nd ECSCI (European Cluster for Securing Critical Infrastructures) virtual workshop presentation
29th April 2022

Ganesh Sauba
DNV-Netherlands

Overview – recent cyber attacks on windfarms

- Nov 2021 Vestas in Denmark partly hit by ransomware, hackers leak stolen personal data
- Mar 2022 China accused for long-term hacking on Indian power grid [not direct relation to windfarm]
- Mar-Apr 2022, In Germany, so far 3 attacks towards different windfarm operators since the Russian invasion of Ukraine

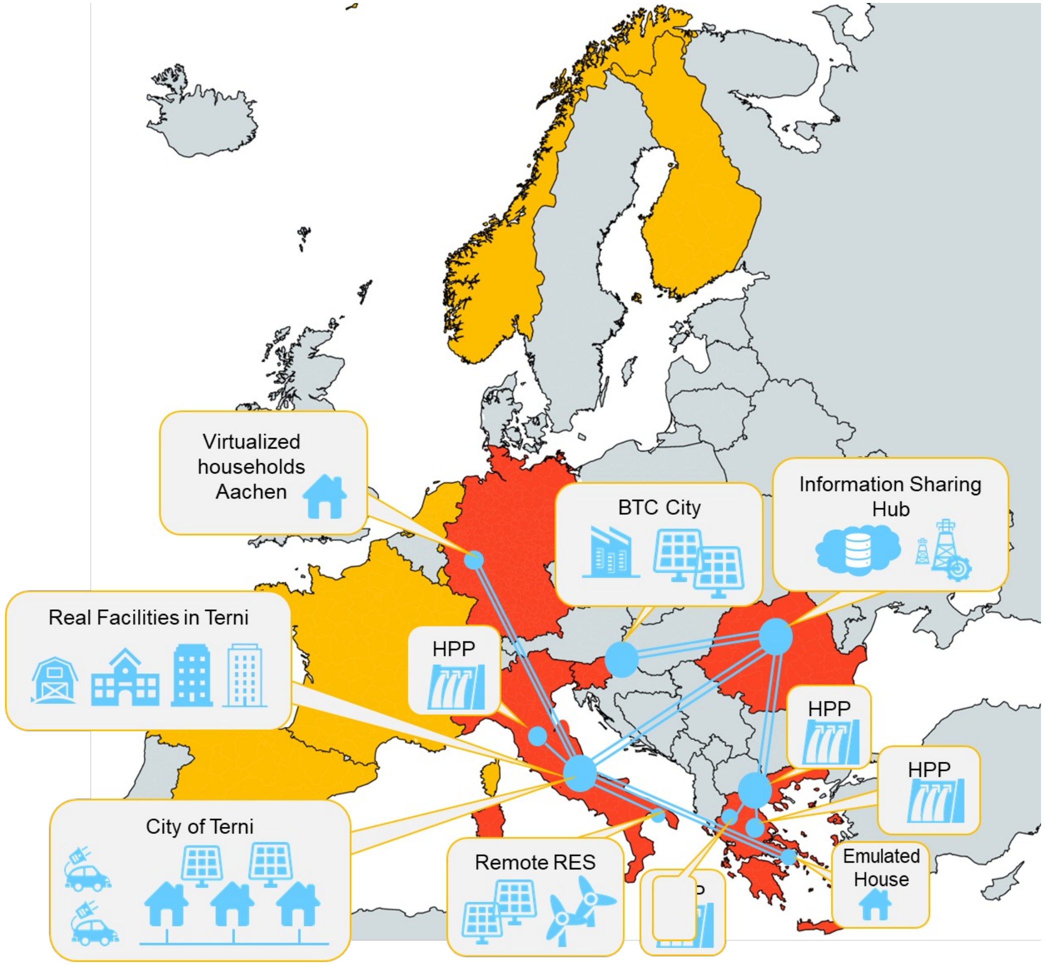
German attacks so far - Mar-Apr 2022

- 1st attack, March 22, Viasat KA-SATCOM terminals hacked causing cascading effects across Europe and knocks out remote communication of about 5800 German Enercon wind turbines. Malware “AcidRain”. Hardware must be replaced.
- 2nd attack, March 31, Nordex IT systems hit by ransomware attack named Conti APT. Turbines and third-party equipment unaffected, scope of impact is still unclear
- 3rd attack, April 11-12, Deutsche Windtechnik hit by cyber attack, but has already recovered
- Will there be a 4th ?

PHOENIX Pilots - Overview

5 diverse Large-Scale Pilots

- Multi-utility/Multi-owner RES cyberthreats and data breach detection (Italy)
- National-wide cooperative remotely controlled HPP (Greece)
- Collaborative Microgrid-enabled cyber risks mitigation (Slovenia)
- Collaborative / DSO flexibility vs cybersecurity and privacy (Italy, Germany, Greece)
- National vs Pan-European cooperative cyber threat information sharing (Romania)



Large Scale Pilots – Main Goals

- **LSP1 Multi-utility/Multi-owner RES cyberthreats and data breach detection (Italy)**
  - Securing MV/LV and generation asset and Preventing data breaches
  - Securing collaboration mechanisms among DSO, RES manager, eMobility and other critical infrastructures
- **LSP2 National-wide cooperative remotely controlled HPP (Greece)**
  - Preventing data breaches
  - Cybersecurity attack scenarios on HPP generation – transfer power grid
- **LSP3 Collaborative Microgrid-enabled cyber risks mitigation (Slovenia)**
  - Cybersecurity attacks on MV/LV EPES assets and AMI
  - Demonstration of on how can the microgrid contribute to the resiliency of the DSO network by utilizing the microgrid energy loads via appropriate power flow rerouting patterns.
- **LSP4 Collaborative / DSO flexibility vs cybersecurity and privacy (Italy, Germany, Greece)**
  - Securing sensing infrastructure and control modules
  - Securing Demand Response system
- **LSP5 National vs Pan-European cooperative cyber threat information sharing (Romania)**
  - Hosting I2SP platform to be used by all other PHOENIX LSPs .
  - Simulating a standard internet infrastructure of an EPES and getting data from real internet common cyberattacks for Phoenix tools

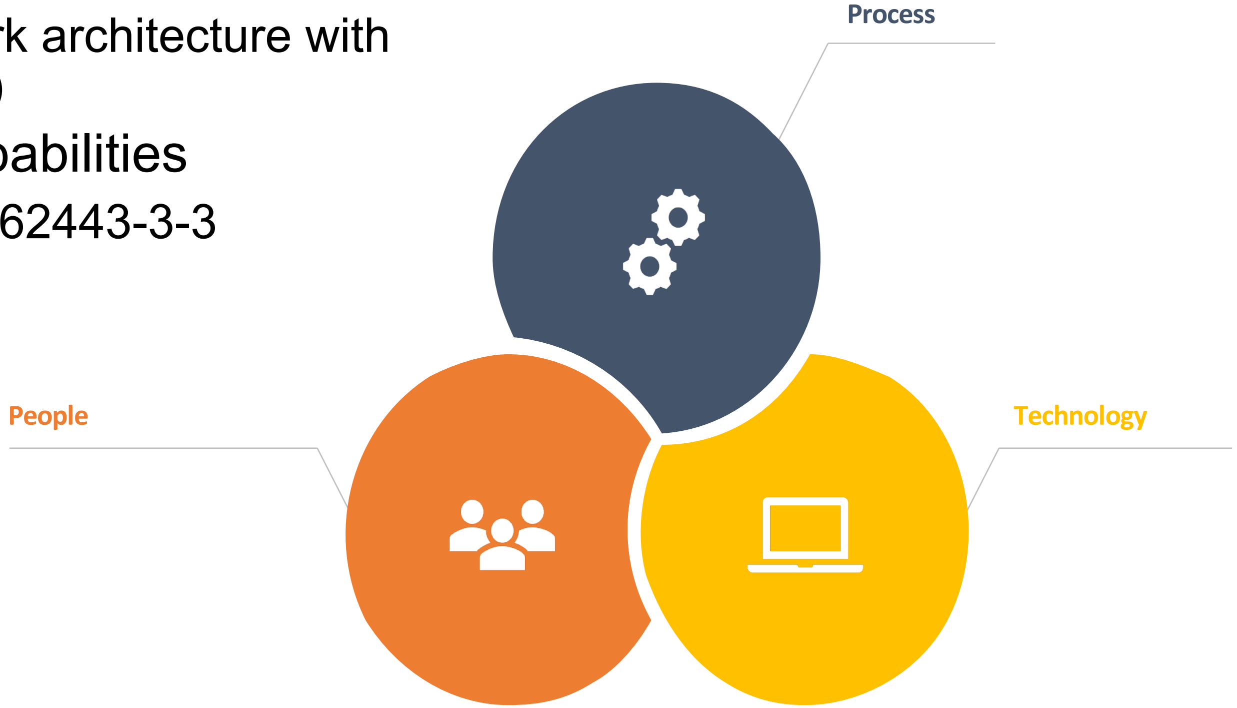
Addressing standard compliance

- A Certification of a EPES facility will be based on requirements from the ISA/IEC 62443 standard series
- How to address standard compliance

  I. Securing Zones & Conduits
  - ✓ Assessment and analysis of the current network architecture with respect to zones and conduits (IEC 62443-3-2)

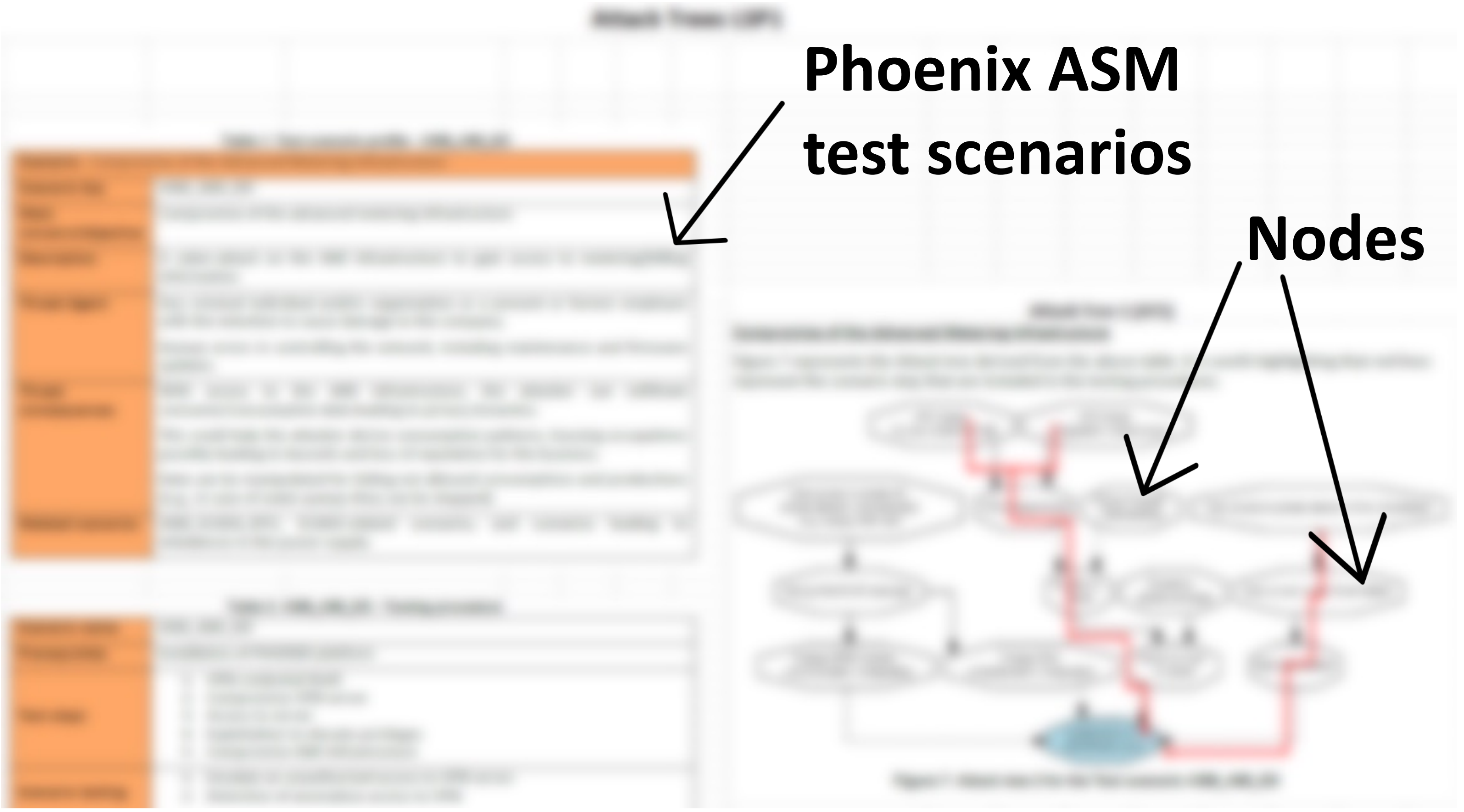
  II. Evaluation of Security Level targets & capabilities
  - ✓ Gap analysis towards the requirements in IEC 62443-3-3
  - ✓ Documentation review and test plan

  III. Attestation of Compliance
  - ✓ Physical testing of each requirement
  - ✓ Issue Attestation of Compliance to IEC 62443, and to Security Level achieved



Example of DNV test program for LSP1

- Mapping each attack tree **node** with applicable DNV security tests
- Main focus on the red line nodes
- Planning our pentest according to test scenarios depicted
- Team discussions on previous experience with the categories in the attack trees.



Phoenix ASM test scenarios

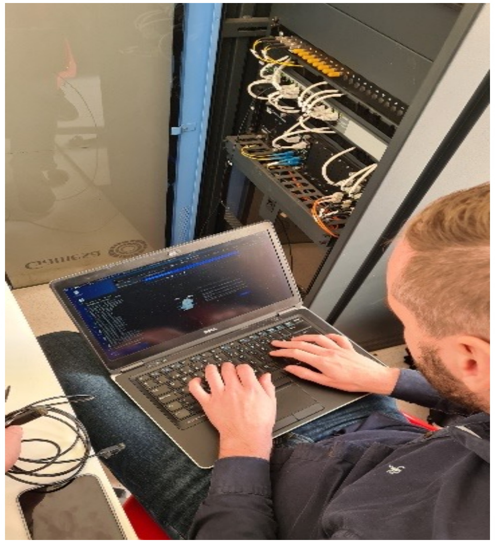
Nodes

PHOENIX LSP1 Results - Windfarm PenTesting

- Weak physical security of wind turbines; there is no cctv, may be possible for unauthorized personnel to enter turbine with some imagination and connect to the system
- Lack of segmentation between turbines in windfarm; its possible to reach all turbines from connecting to one, i.e. possible to see traffic, scan network and see each open service and ports, such as FTP, SSH, Telnet, etc.
- SCADA servers are running obsolete Windows XP with critical vulnerabilities that easily can be exploited if attacker somehow can reach it from external or internal network. Thereby impacting the entire windfarm.
- Violation of the principle of least privilege. E.g. User on SCADA server is running as Administrator.
- Leaked or default credentials were discovered, especially for the remote IP CCTV monitoring of the windfarm. This may be used to propagate further into the control systems.
- Overall weak password policy into different services

Windfarm Photos

Primary substation



Hacking SCADA

Turbines are interconnected by fiber-optic cables (no segmentation)

Thank you for your attention

PHOENIX

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No: **832989** with the management of the Innovation and Networks Executive Agency (INEA).

🌐 https://phoenix-h2020.eu

in company/phoenix-h2020/

@H2020Phoenix

Dr. Ganesh Sauba
Group Research & Development
Energy Systems & Renewables
DNV - Netherlands

DNV