Defending the European Energy Infrastructures

Berichterstattung

Projektinformationen

DEFENDER

ID Finanzhilfevereinbarung: 740898

Projektwebsite

DOI
10.3030/740898

Projekt abgeschlossen

EK-Unterschriftsdatum
25 April 2017

Startdatum
1 Mai 2017

Enddatum
31 August 2020

Finanziert unter
Secure societies - Protecting freedom and security of Europe and its citizens

Gesamtkosten
€ 8 878 232,14

EU-Beitrag
€ 6 790 837,50

Koordiniert durch
ENGINEERING - INGEGNERIA INFORMATICA SPA
Italy

Periodic Reporting for period 2 - DEFENDER (Defending the European Energy Infrastructures)

Berichtszeitraum: 2018-11-01 bis 2020-08-31

Zusammenfassung vom Kontext und den Gesamtzielen des Projekts

Modern critical infrastructures, specifically Critical Energy Infrastructures (CEI), are increasingly turning into distributed, complex Cyber-Physical systems that need proactive protection and fast restoration to mitigate physical or cyber incidents or attacks, and most importantly combined cyber-

physical attacks, which are much more challenging and it is expected to become the most intrusive attack. As a result, a joint cyber-physical approach based on the following principles to manage CEI security becomes necessary to maximize security:

• CEI infrastructure needs to be treated as a distributed, large scale Cyber-Physical System (CPS) for combined physical and cyber security threat detection modelling and mitigation strategies;

• CEI security integrates human and social characteristics, moving towards a Cyber-Physical-Social System (CPSS) model of protection, including the Human-In-the-Loop (HITL) concept to build a Culture of CEI security;

• Each site and each segment of the CEI needs specialized attack prevention measures and incident mitigation to return to normal operation, especially if cost is taken into account.

Overall objectives are:

1. Analyse exiting CEI threats and risks and create a methodology for predicting new/yet unknown risks based on the development of key metrics to better identify and characterize threats and threat scenarios and to describe relative security posture before and after deployment of security solution. Moreover, create a methodology and a tool for the quantification of the trustworthiness and the categorization of CEI assets, systems and segments, and “system of systems” in to CEI Secure Tiers, taking into account availability, redundancy, resilience and survivability.

2. Study, analyse and validate key design objectives, namely CEI Security Lifecycle Assessment, Resilience, CEI Survivability and CEI Data Privacy during extensive evaluations and fine tuning, emulating real abnormal conditions and malicious incidents. The theoretical and analytical work contributes to define preventive measures to reduce risk by design and pave the way for next generation CEI security.

3. Develop methodologies and interfaces for gaining CEI situation awareness, perception and comprehension. APIs have been developed for interfacing and fusing information from state-of-the-art physical and cyber sensors as well as metering devices and specialised HITL applications.

4. Design and develop a Cyber Physical Social System co-simulator that models and simulates CEI situation environment and threats models.

5. Develop a dashboard and a mobile app for implementing innovative, trusted and traceable, bidirectional information flows, between CEI and HITL. The tools are based on blockchains technology and will be used by HITL, acting as front-line responders, to inform CEI operators on potential abnormal incidents and by CEI operators for informing humans in vicinity for potential de-escalation actions in case of an accident or attack.

6. Design and implement a dynamic countermeasures toolbox and a Decision Support System aimed at physical and cyber attack mitigation, including CEI infrastructure (self-) healing and drones’ neutralization.

7. Design and implement a CEI Incidents Information Sharing Platform as distributed repository of information sharing among CEI operators and countermeasures. The system starts from the SUCCESS Critical Infrastructures Security Operational Centre (CI-SOC), but it is extended to facilitate collaboration among various CEI operators throughout Europe.

Arbeit, die ab Beginn des Projekts bis zum Ende des durch den Bericht erfassten Berichtszeitraums geleistet wurde, und die wichtigsten bis dahin erzielten Ergebnisse

During the project a broad threat analysis and classification has been conducted, providing a holistic threat and threat agents taxonomy as a further basis for threat modelling and analysis of unknown threats. A final risk analysis and CEI assets, systems and segments classification according to their trustworthiness has been conducted and the Risk Analysis process has been elaborated. Moreover, the project released the DEFENDER System Architecture, characterized by a layered style that consists of five main logic layers, namely Source, Actuator, Data, Event, Situation, Service and Application Layer, able to flow the data from the physical level to the system applications and tools. Effort was also spent to define the Blockchain technology to ensure trusted by design, bi-directional information and communication flows tailored for use in CEI contexts in order to provide a platform allowing for the emergence of trusted, bi-directional information flows between Utilities, LEAs and HITL targets. The integration to the DEFENDER HITL framework has been performed in order to allow CEI operators to visually check in real-time the security reports of the HITL operators. Additionally, it has been developed a framework able to detect and mitigate threats, providing a clear set of models for manage incidents and countermeasures. The design and the development of a threat extraction tool module for the detection of attack and threats analysed by the Incidents Detection Support System has been started. The DEFENDER CEI Security Control Center allowing CEI operators to overview the security state of the CEI areas of their responsibilities and react, has been defined. Finally, DEFENDER intends to create a Pan-European CEI Security Stakeholders Group (CEIS-SG) to share information on CEI risks, incidents, threats and countermeasures, exchange reliability best practices. During the reporting period, CEIS-SG has been created along with the CIP roadmap with all the CEIS-SG activities related to the enhancement and finalization of the Security Roadmap.

Fortschritte, die über den aktuellen Stand der Technik hinausgehen und voraussichtliche potenzielle Auswirkungen (einschließlich der bis dato erzielten sozioökonomischen Auswirkungen und weiter gefassten gesellschaftlichen Auswirkungen des Projekts)

DEFENDER will produce a comprehensive framework protecting CEI expressed as:
• A set of design objectives exploiting security lifecycle management, resilience, survivability/self-healing and privacy in CEI in depth and by design,
• A holistic Cyber-Physical/human-enriched CEI co-simulator, incorporating energy assets and communications stochastic and uncertainty modelling, along with big-data techniques, virtual/human sensors and regulatory aspects,
• A range of prototypes and blueprints utilizing state of the art surveillance, security and intruder detection technologies for future energy and ICT sector products and services,
• Recommendations on countermeasures to address short, medium and long term threats along with business models to handle DS-SLAs,
• The DEFENDER platform applying countermeasures at TRL-7 level and validated in field trials,
• Built the Culture of CEI Security a) technologically via the implementation of a pan-European CEI Incidents Information Sharing Platform (I2SP) and b) politically via the formation of a pan-European

CEI Security Stakeholders Group,

DEFENDER partners share a common view on how security can impact the European Society and Economy contributing to EU integration. Specifically, European society will benefit from uninterrupted energy and from the boost of Renewable Energy Source penetration which has direct positive impact on the environment. Similarly, the EU economy will benefit through the active engagement of SMEs and Industries that will increase their competitiveness in the energy (possibly local) market economy. Finally, the development of the pan-European security platform envisioned by DEFENDER will allow for stronger standardization impact, also boosting the integration of energy markets across Europe.

ELES TSO Power Network

BFP Wind Farm Decentralized RES Generation

ASM DSO Power Network

Letzte Aktualisierung: 5 Mai 2021

Permalink: https://cordis.europa.eu/project/id/740898/reporting/de