CyberSEAS

Cyber Securing Energy dAta Services

Fraunhofer
Fraunhofer-Zentrum Digitale Energie

Projektziele

Im Rahmen des von der Europäischen Union mit mehr als 7.9 Mio. geförderten Projektes CyberSEAS soll die Resilienz von Wertschöpfungsketten der Energieversorgung verbessert werden und diese vor schwerwiegenden Cyberangriffen geschützt werden.
Im Rahmen des Vorhabens werden mehrere Pilotinfrastrukturen und Testinfrastrukturen genutzt, um mehr als 100 IT-Sicherheitsszenarien zu erforschen. Das Konsortium aus 29 Partnern unter der Leitung von Engineering Ingegneria Informatica S.p.A analysiert hierzu komplexe Angriffe auf die eingesetzte Informationstechnik bei unterschiedlichen Akteuren der Energieversorgung. Dies geschieht sowohl unter Beachtung bestehender Systeme als auch neuer Technologien bei Energieinfrastrukturbetreiber als auch Dienstleistungsanbietern (Cloud, Datenspeicher,…). Neben der IT-Sicherheit wird auch der Datenschutz bestehender und zukünftiger IT-Lösungen analysiert.
Entwickelt wird ein offenes und erweiterbares Ökosystem von 30 anpassbaren Sicherheitslösungen, die wirksame Unterstützung bei zentralen Aktivitäten in der IT-Sicherheit bieten. Dazu zählen unter anderem Risikobewertung, Interaktion mit Endgeräten, sichere Entwicklung und Bereitstellung von IT-Lösungen, Sicherheitsüberwachung in Echtzeit, Verbesserung der Fähigkeiten und Sensibilisierung sowie Zertifizierung, Governance und Zusammenarbeit.
Die im Rahmen von CyberSEAS entwickelten Ansätze werden durch einen progressiven Pilotansatz validiert, der mit einem Laboreinsatz beginnt und in Vor-Ort-Einsätzen fortgesetzt wird.
Das Fraunhofer-Zentrum Digitale Energie wird im Rahmen des Vorhabens eine Laborinfrastruktur einbringen, welche die Analyse und Entwicklung von IT-Sicherheitslösungen im Bereich der Netzintegration dezentraler Erzeugungsanlagen als auch der Elektromobilität ermöglicht.

Nutzen

Basierend auf Simulations- als auch Emulationsansätzen werden aktuelle und zukünftige IT-Sicherheitsherausforderungen an die Primär- und Sekundärtechnik der Erzeugungsanlagen und Ladeinfrastrukturen in unterschiedlicher Detaillierung untersucht. Die Laborumgebung ermöglicht die Kopplung zwischen emulierten Anlagen und realen Hardwarekomponenten, wodurch eine cyber-physikalische Laborumgebung geschaffen wird. Dabei stehen reale Verteilungsnetze und Leitsysteme über Lade- und Messinfrastrukturen bis hin zu Smart Meter Meter Gateway Infrastrukturen zur Verfügung. Im Rahmen des Vorhabens werden so diverse IT-Sicherheitsvorfälle analysiert und die entwickelten IT-Sicherheitstechnologien entwickelt und getestet.

Konsortium

- Engineering SPA
- CINI
- AIRBUS
- Guardtime
- Ikerlan
- Informatika D.D.
- ICS
- EON ACS
- SIMAVI
- SQS
- STAM
- Synelixis
- WINGS ICT Solutions
- ZIV
- Comune di Berchidda
- Comune di Benetutti
- Operato
- PETROL
- SI CERT
- HOPS
- Enerim
- Elektrilevi
- Transelectrica
- CRE
- TIMELEX
- Enefit
- Eesti Energia
- ELES

Projektlaufzeit

10/2021 – 09/2024

Gefördert durch

Das Projekt wird von der Europäischen Union finanziert

Förderungsnummer 101020560

Fragen zum Projekt?

Schreiben Sie uns, oder besuchen Sie die Projekt-Webseite.