CREIS

Cybersicherheit und Resilienz für systemkritische Energieinfrastruktur und deren Automatisierungssysteme

Programm / Ausschreibung	EW 24/26, EW 24/26, Energieforschung 2024 FTI - Fokusinitiativen	**Status**	laufend
Projektstart	01.10.2025	**Projektende**	30.09.2028
Zeitraum	2025 - 2028	**Projektlaufzeit**	36 Monate
Keywords	Digitalisierung des Energiesystems, System- und Versorgungssicherheit durch Cyberresilienz, Cyber Resilience Act, NIS-2, Systemsicherheit		

Projektbeschreibung

Die Digitalisierung des Energiesystems und die wachsende Vernetzung von Energieinfrastrukturen durch das Industrial Internet of Things (IIoT) bringt nicht nur verbesserte Monitoring- und Steuerungsmöglichkeiten mit sich, sondern birgt auch signifikante Sicherheitsrisiken und erfordert eine erhöhte Resilienz gegenüber Cyberangriffen. Sowohl direkte als auch indirekte Angriffe auf unser Energiesystem können schwerwiegende Auswirkungen auf die Energieversorgung und andere kritische Infrastruktur haben.

Das Forschungsprojekt CREIS (Cybersicherheit und Resilienz für systemkritische Energieinfrastruktur und deren Automatisierungssysteme) analysiert mögliche Angriffsflächen, von Software-Schwachstellen bis hin zu Side-Channel Angriffen, um ein ganzheitliches Verständnis der Bedrohungslage für die Energieautomatisierung zu schaffen und darauf aufbauend ganzheitliche, effiziente und langfristige Schutzmaßnahmen gegen Cyberangriffe für Energieautomatisierungsgeräte zu schaffen.

CREIS verfolgt vier Innovationsansätze: Zunächst werden die Angriffsflächen von Energiesystem-Komponenten unter neuen Angreifermodellen analysiert. Darauf aufbauend wird eine Co-Simulations-Umgebung erweitert, um moderne Cyberangriffe auf die Energieinfrastruktur realitätsnah abbilden zu können. Basierend auf den Erkenntnissen werden neue Schutzmaßnahmen gegen ganze Angriffsklassen entwickelt, die sowohl software-basiert als auch hardware-unterstützt umgesetzt werden. Außerdem zielt CREIS auf die Entwicklung neuartiger Update- und Attestierungskonzepte für IIoT Geräte, um deren Integrität und Validierung im Feld zu gewährleisten. Die Evaluierung der Methoden erfolgt mittels Co-Simulation um den Einfluss von Cyberattacken sowohl auf Geräte als auch auf Systemebene zu simulieren und analysieren zu können.

CREIS erarbeitet Konzepte und Prototypen, die eine effiziente Cybersicherheit aufweisen und damit auch eine langfristige Einhaltung der Cyberresilienz-Verordnung (CRA) und der NIS-2-Richtlinie ermöglichen. Zusätzlich zu wissenschaftlichen Publikationen zur Verbreitung von Projektergebnissen, werden die Ergebnisse am Ende des Projekts auch in einem Empfehlungsbericht für Entscheidungsträger und Bedarfsträger formuliert, wobei die im Projekt entwickelten Lösungen nicht

nur im Energiesektor, sondern auch in anderen Branchen der Industrieautomatisierung Einsatz finden können, um diese nachhaltig vor Cyberangriffen zu schützen.

Abstract

The digitalization of energy systems and the growing interconnectedness of energy infrastructures through the Industrial Internet of Things (IIoT) enables enhanced monitoring and control capabilities. However, this also introduces significant security risks that require improved resilience against cyberattacks. Direct and indirect attacks on an energy system have serious consequences for energy supply and other critical infrastructure.

The CREIS research project (Cybersecurity and Resilience for Critical Energy Infrastructure and their Automation Systems) analyzes potential attack surfaces, from software vulnerabilities to side-channel attacks, to create a comprehensive understanding of the threat landscape for energy automation and to develop holistic, efficient and long-term protective measures against cyberattacks for energy automation devices.

CREIS pursues four innovations: First, the attack surfaces of energy system components are analyzed under new attacker models. Building on this, a co-simulation environment is being expanded to realistically depict modern cyberattacks on energy infrastructure. Based on the findings, new protective measures against entire classes of attacks are being developed, which are both software-based and hardware-supported. In addition, CREIS aims to develop novel update and attestation concepts for IIoT devices to ensure their integrity and validation in the field. The evaluation of the methods is carried out using co-simulation to simulate and analyze the influence of cyberattacks on both device and system levels.

CREIS is developing concepts and prototypes that demonstrate efficient cybersecurity and thus enable long-term compliance with the Cyber Resilience Act (CRA) and the NIS 2 directive. In addition to scientific publications for dissemination, the project results will also be formulated in a recommendation report for authorities and stakeholders at the end of the project, whereby the solutions developed in the project can be used not only in the energy sector, but also in other industrial automation sectors to sustainably protect against cyberattacks.

Projektkoordinator

- Technische Universität Graz

Projektpartner

- Siemens Aktiengesellschaft Österreich