InnoSys 2030

Innovationen in der Systemführung bis 2030: Cybersicherheit für das Stromnetz von morgen

Fraunhofer
Fraunhofer-Zentrum Digitale Energie

Projektziele

Das Forschungsprojekt InnoSys 2030 untersucht neuartige Ansätze in der Systemführung für eine effizientere Ausnutzung des Stromnetzes, auch durch den Einsatz kurativer Maßnahmen. Dies bedeutet vor allem, dass der operative Netzbetrieb und die Netzführung stärker automatisiert werden müssen und folglich die Vernetzung mit Informations- und Kommunikationstechnologien (IKT) vorangetrieben werden muss.
An dieser Stelle kommt auf die Stromnetzbetreiber eine weitere, wichtige Herausforderung zu: Die IKT-Sicherheit des Stromnetzes. Die Cyberangriffe auf das ukrainische Stromnetz von 2015 und 2016 haben die wachsenden Bedrohungen für das Stromnetz als kritische Infrastruktur verdeutlicht. Daher adressiert das Fraunhofer-Zentrum Digitale Energie diese Entwicklung, indem es IKT-Sicherheit in InnoSys 2030 von Anfang an berücksichtigt und umsetzt.

Nutzen

Für die Stärkung der IKT-Sicherheit in InnoSys 2030 wurden einerseits die entwickelten Konzepte auf potenzielle Schwachstellen und neuartige Bedrohungen für den zuverlässigen und sicheren Systembetrieb untersucht. Die im Zuge der Untersuchung gewonnen Erkenntnisse bilden die Grundlage für eine spätere sichere Umsetzung der Konzepte. Andererseits wurden diese präventiven Maßnahmen aber auch durch die Entwicklung und Evaluation von Detektionsverfahren von Cyberangriffen innerhalb des IKT-Netzwerks ergänzt, wo sich eine Einbindung von Kontextwissen als besonders vielversprechend herausgestellt hat, um bei zukünftig unvermeidbaren Sicherheitsvorfällen schnell und zielgerichtet reagieren zu können.
Dieser Security-by-Design-Ansatz bedeutet, dass bereits bei der Entwicklung von neuen Konzepten in der Systemführung die IKT-Sicherheit mitgedacht werden muss. Weiterhin ist es zwingend notwendig, das Zusammenspiel der neuentwickelten Konzepte kontinuierlich im Hinblick auf die IKT-Sicherheit zu bewerten und gegebenenfalls Sicherheitsmaßnahmen frühzeitig nachzuschärfen.

Ergebnisse

Aus den Bewertungen und praktischen Evaluationen ergeben sich wichtige Erkenntnisse für die IKT-Sicherheit von zukünftigen Stromnetzen. Etwa dass auch zukünftige Entwurfs- und Umsetzungsentscheidungen einen maßgeblichen Einfluss auf die IKT-Sicherheit des resultierenden Gesamtsystems haben werden. Aus diesem Grund ist es unabdingbar, dass das Thema IKT-Sicherheit weiterhin kontinuierlich bei der Entwicklung und Umsetzung von neuen Maßnahmen und Konzepte mitberücksichtigt wird, um somit die Stromnetze der Zukunft auch gegen den wachsenden Raum der unbekannten Bedrohungen effektiv wappnen zu können.

Das Fraunhofer-Zentrum Digitale Energie wird die Stromnetzbetreiber bei den Umsetzungen der Konzepte, insbesondere im Rahmen des Fachbeirats von InnoSys 2030 dabei vertrauensvoll und wissenschaftlich begleiten.

Konsortium

- TenneT
- 50Hertz Transmission GmbH
- Amprion GmbH
- TransnetBW GmbH
- Avacon Netz GmbH
- EWE NETZ GmbH
- Mitteldeutsche Netzgesellschaft Strom mbH
- Westnetz GmbH
- Netze BW GmbH
- TU Dortmund
- TU Ilmenau
- Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)
- Institut für Elektrische Anlagen und Netze, Digitalisierung und Energiewirtschaft (IAEW), RWTH Aachen University
- Fraunhofer IEE
- Fraunhofer FKIE
- PSI Software AG
- Siemens AG

Projektlaufzeit

10/2018 – 12/2021

Gefördert durch

Das Bundesministerium für Wirtschaft und Klimaschutz - BMWK

Fragen zum Projekt?

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