SimCyberGrid - Simulator für Cyberangriffe auf verteilte elektrische Microgrids

Moritz Volkmann, Sascha Kaven, Prof. Dr. Volker Skwarek, Prof. Dr. Carsten Frank (HAW Hamburg FTZ CyberSec), Felix Scholl, Prof. Dr. Kolja Eger (HAW Hamburg, CC4E), Julian Behrensen, Prof. Dr. Milena Zachow (TH Lübeck)
felix.scholl@haw-hamburg.de

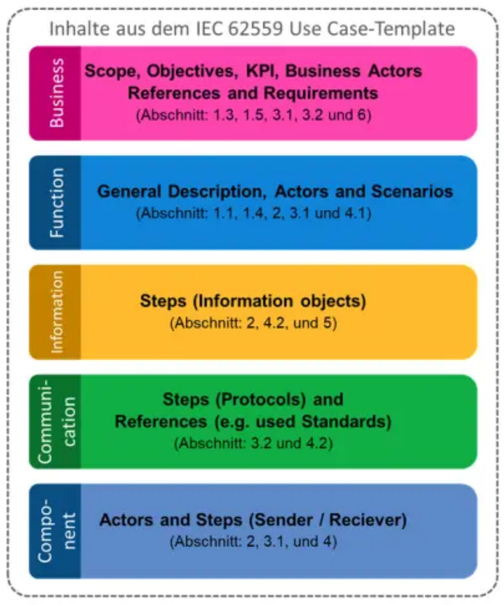
Tag der Energieforschung 2025

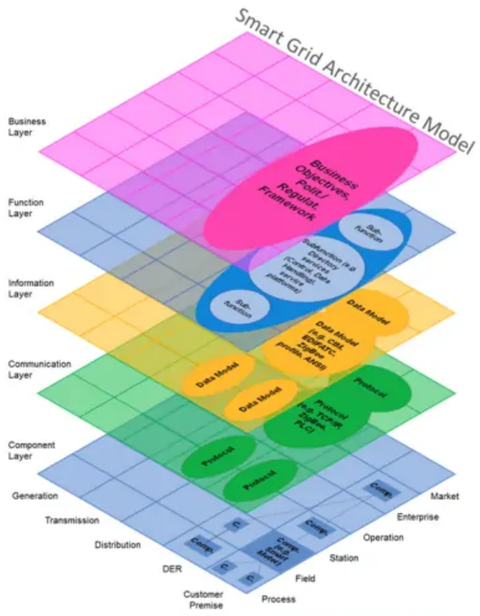
Motivation/Einführung/Konzept

Die Energiewende erfordert die weitgehende Integration erneuerbarer, also volatiler, Energiequellen ins Energiesystem, welche zumeist dezentral ans Netz angeschlossen werden. Eine besondere Herausforderung bieten die Dezentralität und der vergleichsweise hohe Kommunikationsaufwand: Es ist zu erwarten, dass die heutige Powerlan-ähnliche nicht mehr ausreichen wird und eine Kommunikation über das herkömmliche Internet oder drahtlose 5G/6G-Technologien erforderlich wird. Als Elemente der kritischen Infrastruktur müssen diese Microgrids besonders geschützt werden. Hierzu müssen erweiterte Überwachungs- und Absicherungsverfahren entwickelt werden. In diesem Projekt wird dazu auf der Meta-Ebene eine Co-Simulation aus einem elektrischen Netz, ähnlich wie es aus einer zukünftigen Netzleitstelle wahrgenommen würde, und dem Internet, das Cyberangriffen ausgesetzt ist, entwickelt.

Methodik

Durch ein Clustering von Use Cases nach dem Smart Grid Architecture Model (SGAM) werden die Grundlagen für Entwürfe von möglichen Angriffsszenarien gelegt und Bedrohungsanalysen erstellt. Anhand dieser werden Simulationen der Kommunikation- und Leistungspfade erstellt und durch einen Hardware-in-the-Loop-Teststand mit Smart-Meter-Gateways und Steuerboxen validiert. Das etablierte SGAM ermöglicht eine breite Verwendung der Use Cases nicht nur unter den Projektpartnern, sondern auch über Forschungsvorhaben hinaus.





Projektziele

Im Zuge des Projekts soll eine offene, softwarebasierte Co-Simulation aufgebaut werden, welche im Rahmen von Standardisierungsaktivitäten mit dem DKE – VDI e.V. weiterentwickelt wird. Diese Co-Simulation soll realitätsnah das Verhalten verteilter, prosumerbasierter Niederspannungsnetze abbilden, indem über internetbasierte Kommunikationsnetze per Smart-Meter-Gateways Informationen sowohl übermittelt als auch empfangen werden können. Es werden sowohl Front-of-the-Meter als auch Behind-the-Meter anhand der Use Cases Bedrohungsanalysen erstellt, welche verschiedenste Angriffe wie z.B. DoS, Man-in-the-middle, False Data Injection, Replay attack, Exploits, Port scanning (PortScan) oder Rank attacks auf unterschiedliche Assets wie Energiemanagementsysteme, Batteriespeicher oder Steuerboxen beinhalten. Durch eine umfangreiche Erprobung soll ein hoher Härtegrad der dezentralen Verteilnetze erreicht werden.

Zusammenfassung und Ausblick

Gefördert durch das Bundesministerium für Bildung und Forschung (BMBF) bringt das Projekt wissenschaftliche Akteure unter der Leitung des Forschung- und Transferzentrums CyberSec (FTZ Cybersec) der Hochschule für Angewandte Wissenschaften Hamburg (HAW) in Kooperation mit dem Competence Centre for Renewable Energies and Energy Efficiency (CC4E) und der Technischen Hochschule Lübeck (TH Lübeck) zusammen. Die Expertise der verschiedenen Forschungsgruppen soll einen wichtigen Beitrag für die Resilienz der Stromnetze von morgen erbringen und Netzbetreibern die Möglichkeit bieten, sich schon heute auf die virtuellen Gefahren der Zukunft vorzubereiten.