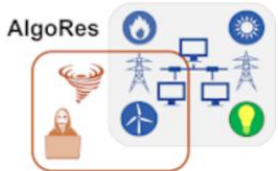


Resiliente Stromnetze: Reaktion in den Fokus stellen

Prof. Dr. Florian Steinke
www.eins.tu-darmstadt.de



Perfekter Schutz ist nicht möglich

- Physische Attacken auf weitverteilte, sichtbare Infrastruktur
- Cybersecurity ist problematisch, v.a. verteilte Energieanlagen (PV-Umrichter, E-Autos, ...)

Reaktion in den Fokus stellen (nicht nur Robustheit / „Verhindern“)

- ÜNB: schnelle Reaktion ermöglichen (Reparaturtrupps, Hardwarelager, ...)
- VNB: Notfall-Inselnetze einplanen (Diesel + EE + Batterien + KWK, kritische Lasten wie Handymasten)
- Alle: Detektion/Identifikation von Hacking verbessern (im IT- und Stromnetz)

Mentale Einstellung verändern

- Verteidigungsfall ernst nehmen: Art der Fehler, „20% besser als 0%“
- Preparedness-Kosten minimieren: bestehende Hardware nutzen, Finanzierung VNBs nötig

Dezentrale, digitale Systeme können resilienter sein als wenige Großanlagen