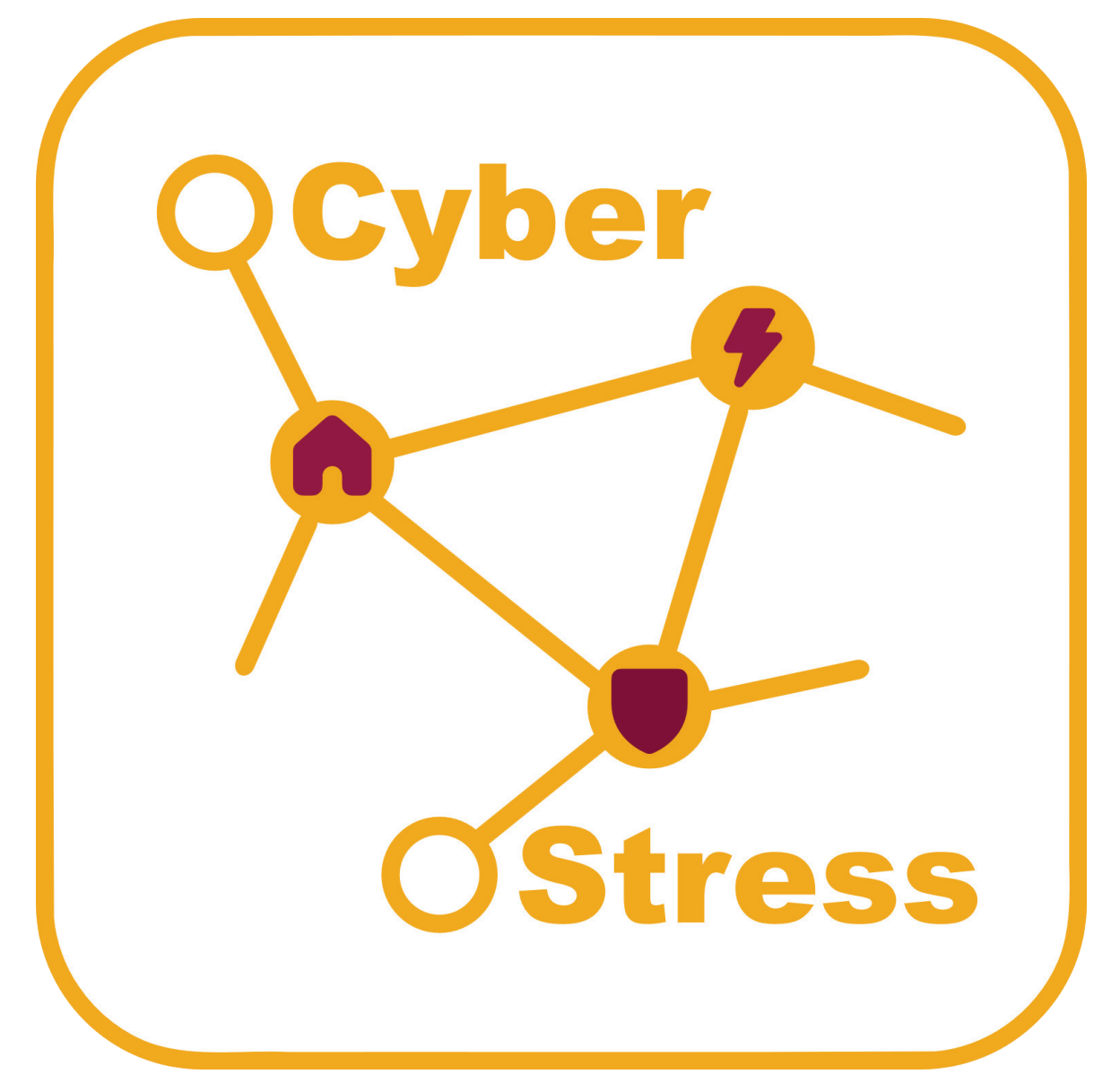


FORSCHUNGSPROJEKT

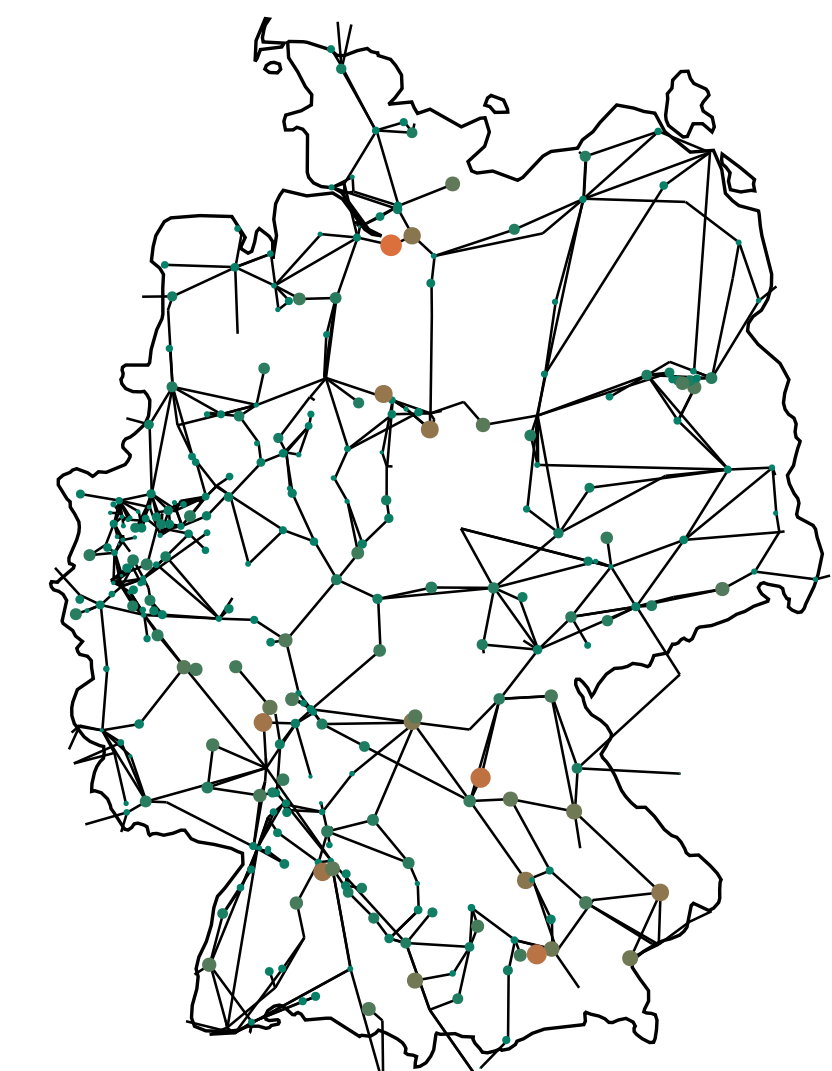
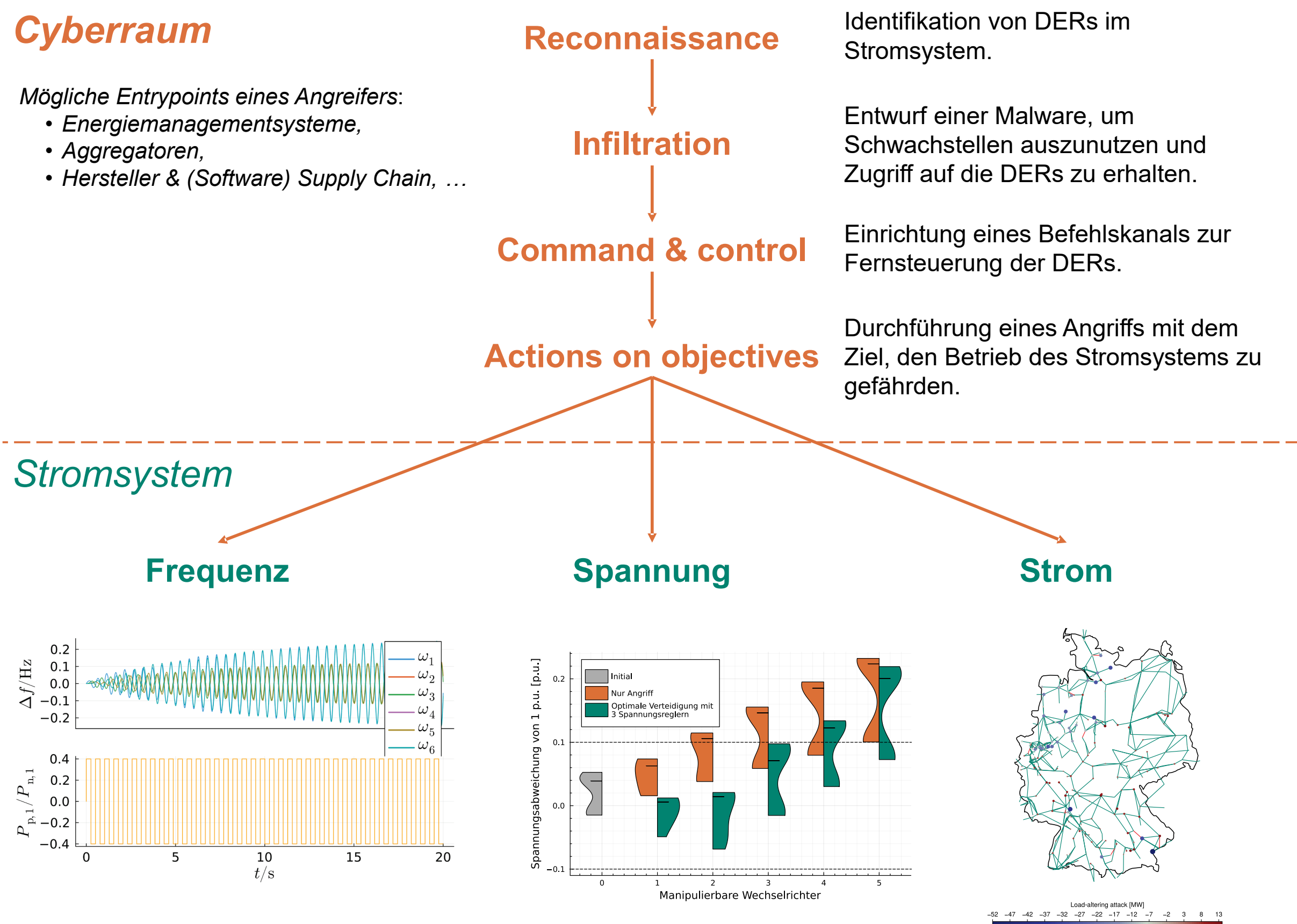
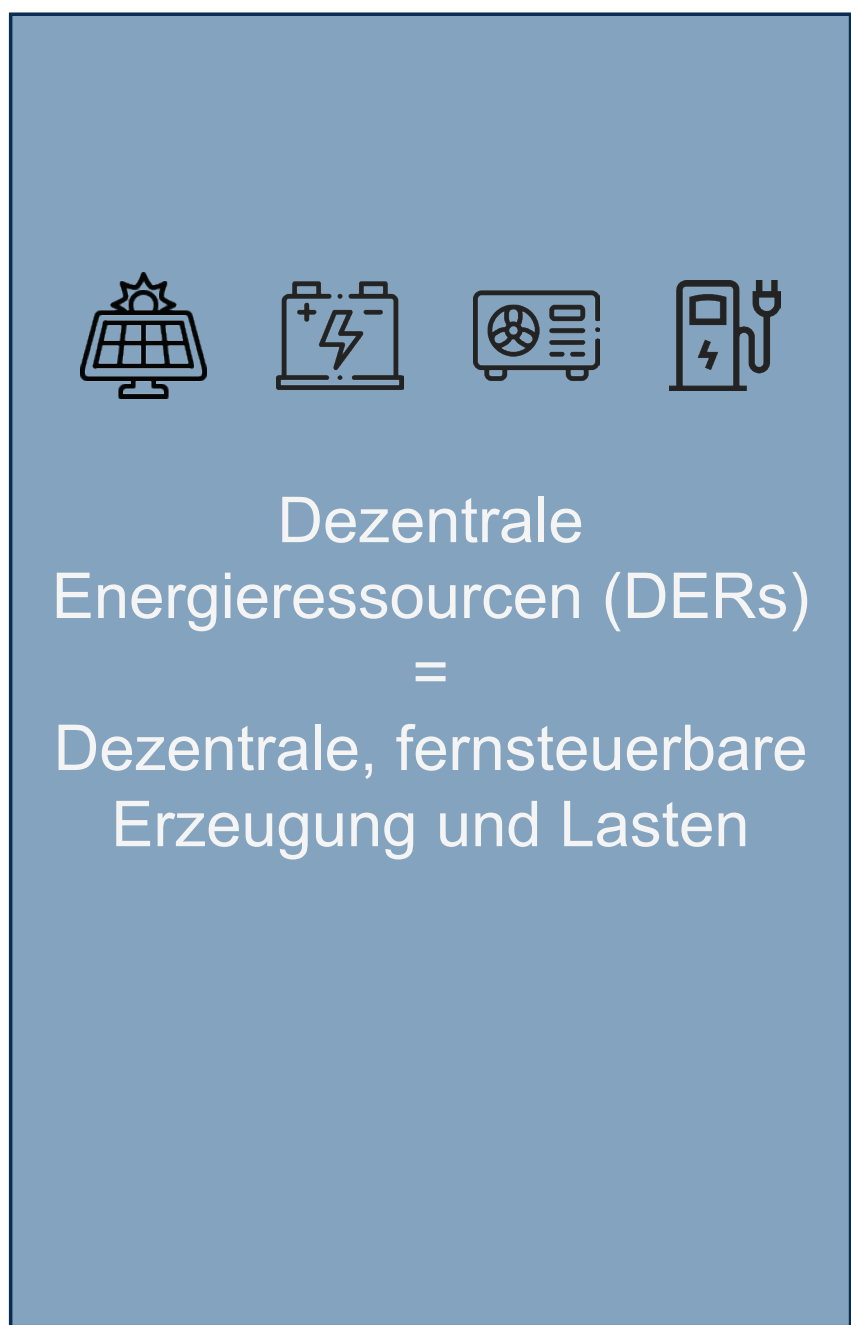
CyberStress – Modellbasierte Stresstests für cybersichere Energienetze



DER-basierte Cyberangriffe stellen eine vielfältige Bedrohung dar – Detektion und Forensik fehlen jedoch weitgehend!

DER-basierte Cyberangriffe können f , U , I im Stromsystem stören

7 GW an öffentlicher Ladeinfrastruktur

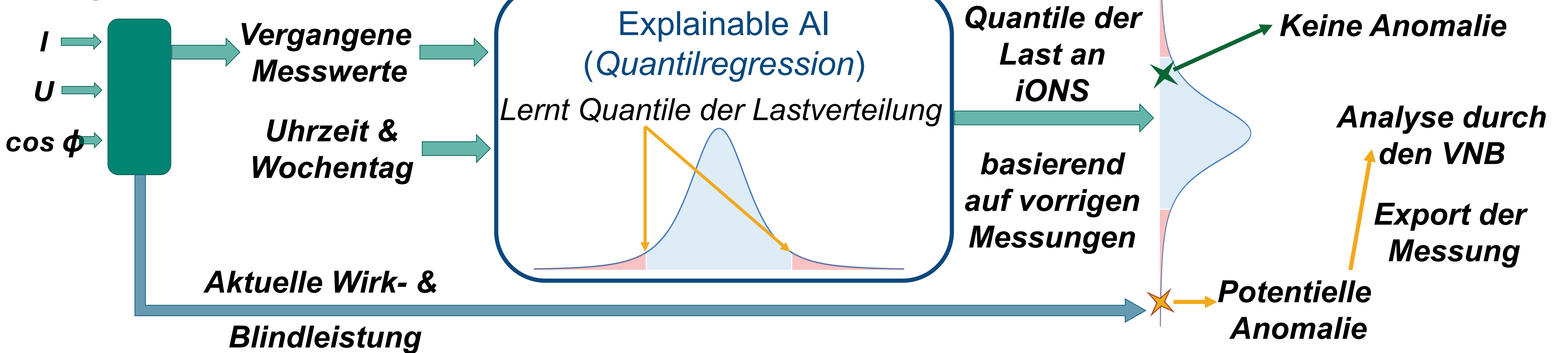


0 10 20 30 40 50 60 70 80 90 100 110

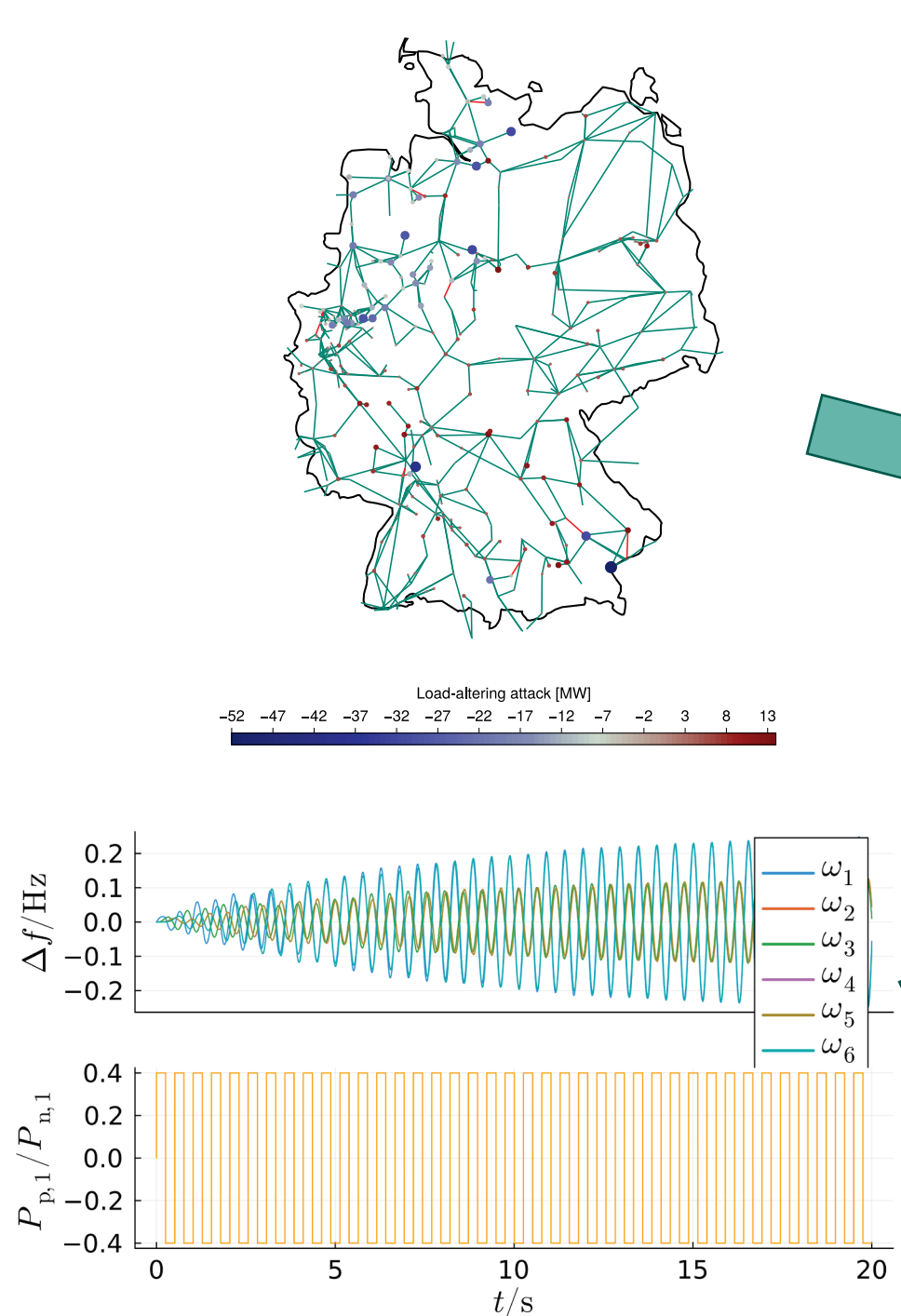
➔ 3 x KKW Biblis

Nachvollziehbare Anomaliedetektion durch explainable AI – abgesichert durch Expertenwissen.

Messungen der intelligenten ONS



Hohes Potenzial für Detektion und Forensik auf Verteilnetzebene: Digitalisierung der ONS nutzen!



Simulierte Angriffstypen	Erkennungsrate bei 99% Präzision*
Frequenzabweichung und Überlasten	82%
Inter-Area Oszillationen	99%

* Präzision = (Korrekte Anomalie) / (Korrekte + falsche Anomalien)

Sehr hohe Erkennungsrate bei 1% Fehlalarmen!

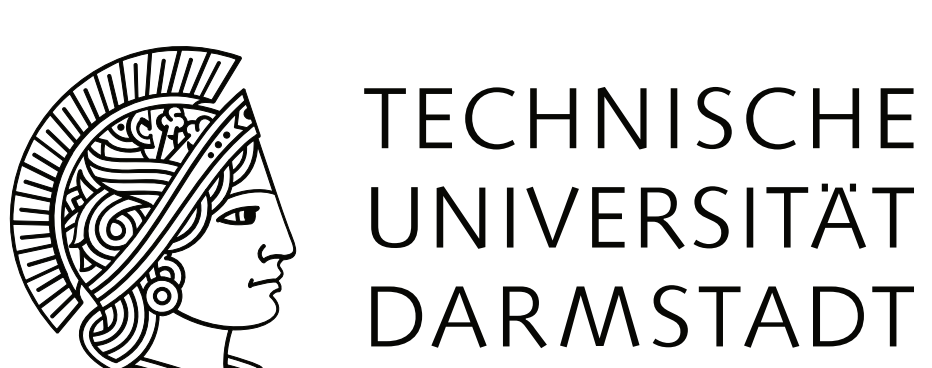
Detektion auf Niederspannungsebene:

- erkennt Angriffe, die auf überlagerte Netzebenen zielen;
- ist von zentraler Bedeutung für die Resilienz des gesamten Stromsystems.

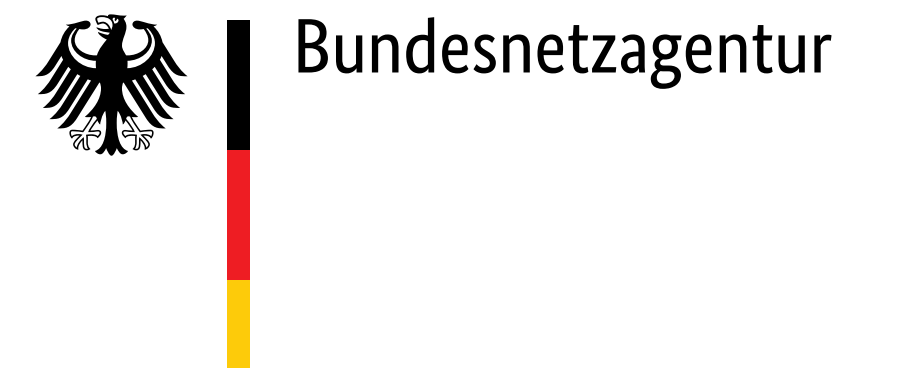
Vorschlag

Anomaliedetektion zu einem Standard im VN weiterentwickeln!

PROJEKTPARTNER



UNIVERSITÄT ZU KÖLN



Kirill Kuroptev, David Lange, Benedikt Grüger, Prof. Florian Steinke
Fachgebiet Energy Information Networks and Systems
TU Darmstadt