gefördert durch

Bundesministerium
für Forschung, Technologie
und Raumfahrt

Verbundprojekt „CyberStress – Modellbasierte Stresstests für cybersichere Energienetze“

Abschlussbericht zum Teilvorhaben der e-netz Südhessen AG: „Resilienz im Verteilnetz“ Laufzeit 01.05.2023 bis 30.04.2026

Zuwendungsempfänger

Organisation	Förderkennzeichen	Ansprechpartner	E-Mail
e-netz Südhessen AG	13N16628	Petermann, David	david.petermann@e-netz-suedhessen.de
Technische Universität Darmstadt*		Prof. Dr. Steinke, Florian	florian.steinke@eins.tu-darmstadt.de
Lehrstuhl Recht der Digitalisierung Institut für Digitalisierung		Prof. Dr. LL.M/ Spiecker genannt Döhmann, Indra	i.Spiecker@uni-koeln.de
QGroup GmbH		Schröfer, Ulfilas	u.schroeder@qgroup.de

*) Gesamtprojektleitung

Assoziierte Partner

Organisation	Ansprechpartner	E-Mail
Bundesnetzagentur	Haack-Stappel, Jonas	Jonas.Haack-Stappel@BNetzA.DE
Amprion GmbH	Rogge, Michael	michael.rogge@amprion.net

Liste der Autoren

Name	Organisation	E-Mail
Petermann, David	e-netz-Südhessen AG	david.petermann@e-netz-suedhessen.de
Hein, Christian	e-netz Südhessen AG	christian.hein@e-netz-suedhessen.de
Büchau, Nicole	e-netz Südhessen AG	nicole.buechau@netz-suedhessen.de
Lerchl-Mitsch, Kerstin	e-netz Südhessen AG	kerstin.lerchl-mitsch@e-netz-suedhessen.de
Chesi, Kirstin	e-netz Südhessen AG	kirstin.chesi@e-netz-suedhessen.de
Hayn, Karsten	e-netz Südhessen AG	karsten.hayn@e-netz-suedhessen.de

Für den Inhalt dieser Veröffentlichung haften die Autoren.

Projektkonsortium

Die Technischen Universität Darmstadt, Fachgebiet Energy Information Networks (EINS), war im Verbundprojekt „CyberStress – Modellbasierte Stresstests für cybersichere Energienetze“ Konsortialführer. Gemeinsam mit der e-netz Südhessen AG, der Q-Group GmbH sowie der Universität zu Köln (Lehrstuhl Recht der Digitalisierung, Institut für Digitalisierung) und den assoziierten Partnern Bundesnetzagentur und Amprion GmbH wurden vielversprechende Erkenntnisse erreicht. Insgesamt wurden im Teilvorhaben fundierte Ergebnisse erzielt, die wesentlich zum Verständnis der Bedrohungslage und möglicher Gegenmaßnahmen beitragen. Zugleich konnten nicht alle (rechtlichen) Fragestellungen abschließend beantwortet werden; teilweise haben sich im Projektverlauf zusätzliche Fragen ergeben, die nun in weiterführenden Arbeiten adressiert werden sollen.

Danksagung an Projektträger & Bundesministerium

Die e-netz Südhessen AG dankt dem Bundesministerium für Forschung, Technologie und Raumfahrt für die Förderung des Verbundprojekts „CyberStress“. Besonderer Dank gilt den Verbundpartnern und assoziierten Partnern für die konstruktive Zusammenarbeit und den intensiven fachlichen Austausch während der Projektlaufzeit.

Inhaltsverzeichnis

1. Kurzfassung 5
2. Ausgangslage und Zielsetzung 5
3. Projektverlauf und wesentliche Ereignisse 6
4. Wissenschaftlich-technische Ergebnisse 8
4.1 Definition eines Stresstests 8
4.2 Stresstestarchitektur 9
4.3 Szenario-Liste 9
4.3 Angriffsszenarien 10
4.3.1 Ankerszenario Missbrauch von Schutzmechanismen 10
4.3.2 Ankerszenario Fahrplanmanipulation 11
4.3.3 Ankerszenario Verteilte IoT-Attacke 12
4.4 Angriffs- und Schadensmodell für das Verteilnetz 13
4.5 Realdemonstrator in einer typischen Verteilnetzumgebung 13
4.5.1 Komponenten des Realdemonstrators 15
4.6 Anomalieerkennung 16
4.7 Gegenmaßnahmen 17
4.8 Ableitung technischer Empfehlungen 18
5. Vergleich mit Arbeits-, Zeit- und Kostenplanung 18
6. Erreichung der Projektziele und Änderungen der Zielsetzung 18
7. Relevante externe Forschungsergebnisse 19
8. Verwertung der Ergebnisse 19
8.1 Schutzrechte 19
8.2 Wirtschaftliche Erfolgsaussichten 19
8.3 Wissenschaftliche und technische Erfolgsaussichten 20
8.4 Wissenschaftliche und wirtschaftliche Anschlussfähigkeit 20
9. Zusammenarbeit im Verbund 20
10. Öffentlichkeitsarbeit 21
10.1 Publikationen/Veröffentlichungen 21
10.2. Veranstaltungen 23
10.3 Postersession 24
10.4 Microsite 25

11. Fazit 25

Abbildungsverzeichnis

Abbildung 1 Anomalieerkennung in der intelligenten Ortsnetzstation . Fehler! Textmarke nicht definiert.
Abbildung 2 Ablauf eines Stresstests 9
Abbildung 3 Fokusszenarien im Projekt CyberStress . Fehler! Textmarke nicht definiert.
Abbildung 4 Ankerszenarien mit Verantwortungsbereich ..... Fehler! Textmarke nicht definiert.
Abbildung 5 Missbrauch von Schutzmechanismen 11
Abbildung 7 Fahrplanmanupulation 11
Abbildung 8 Verteilte IoT-Attacke 12
Abbildung 9 Realdemonstrator im Projekt CyberStress 14
Abbildung 10 Ladepark bei e-netz Südhessen mit Realdemonstrator zur Anomalieerkennung 13
Abbildung 11 Ablauf Anomalieerkennung 16
Abbildung 12 Projektpartner der TU Darmstadt und e-netz im Gespräch mit Journalisten 24

Tabellenverzeichnis

Tabelle 1 Veröffentlichungen 22

1. Kurzfassung

Das vom Bundesministerium für Bildung und Forschung geförderte Verbundprojekt „CyberStress“ hatte das Ziel, eine modellbasierte Stresstestmethodik für Stromnetze zu entwickeln, mit der sich die Resilienz gegenüber Cyberangriffen systematisch bewerten und steigern lässt. Im Teilvorhaben der e-netz Südhessen AG stand dabei die Resilienz des Verteilnetzes im Mittelpunkt.

Ausgehend von einer umfassenden Analyse von Bedrohungsszenarien – insbesondere dem Szenario eines „verteilten IoT-Angriffs“ über zahlreiche steuerbare Verbrauchs- und Erzeugungsanlagen – wurden Angriffs- und Schadensmodelle für das Verteilnetz entwickelt, Gegenmaßnahmen konzipiert und in einem Realdemonstrator praktisch erprobt. Kern des Demonstrators ist eine typische Verteilnetzumgebung mit einem Ladepark für Elektrofahrzeuge und einer angebundenen Ortsnetzstation, in der ein Netzanalysator und ein Edge-Computing-System zur kontinuierlichen Messung, Analyse und Anomalieerkennung installiert wurden.

Die Ergebnisse zeigen, dass schon eine vergleichsweise geringe Anzahl synchron angesteuerter IoT-Geräte kritische Netzzustände verursachen kann. Gleichzeitig konnte nachgewiesen werden, dass eine Kombination aus lokaler, dezentraler Anomalieerkennung in der Ortsnetzstation, gezielten netzbetrieblichen Maßnahmen und der Nutzung vorhandener Steuerinfrastrukturen die Resilienz signifikant erhöhen kann. Die entwickelte Stresstestmethodik, die Erkenntnisse zur Anomalieerkennung sowie konkrete technische und organisatorische Empfehlungen sind frei nutzbar und können von anderen Netzbetreibern und Institutionen übernommen werden.

Die Arbeiten im Teilvorhaben von e-netz verliefen weitgehend planmäßig. Der Realdemonstrator wurde aufgebaut und in Betrieb genommen, die vorgesehenen Angriffsszenarien wurden durchgespielt und die Wirksamkeit von Gegenmaßnahmen bewertet. Die Projektziele wurden aus Sicht von e-netz erreicht, ohne dass sich grundlegende Änderungen der Zielsetzung ergeben hätten.

2. Ausgangslage und Zielsetzung

Die Energiewende führt zu einer fortschreitenden Dezentralisierung und Flexibilisierung der Energiebereitstellung. Mit dem starken Zubau verteilter, oft IoT-fähiger Erzeugungs- und Verbrauchsanlagen im Verteilnetz – etwa Photovoltaikanlagen, Heimspeicher, Wärmepumpen und Ladeinfrastruktur für Elektromobilität – steigt der Bedarf an Automatisierung und Digitalisierung der Netzbetriebsprozesse. Dies vergrößert die Angriffsfläche für Cyberangriffe auf kritische Infrastrukturen deutlich.

Die e-netz Südhessen AG betreibt Verteilnetze mit einer großen Anzahl an dezentralen Erzeugungsanlagen sowie vernetzter, schaltbarer Lasten. Neben klassischen IT-/OT-Systemen rücken damit zunehmend externe, vom Netzbetreiber nicht selbst betriebene IoT-Anlagen in den Fokus der IT-Sicherheit. Basierend auf der Ausgestaltung des § 14a

EnWG entstehen zusätzliche Angriffspunkte durch die steuerbare Ausgestaltung dieser Betriebsmittel.

Vor diesem Hintergrund verfolgte das Projekt CyberStress im Verbund das Gesamtziel, die Idee von Stresstests – wie sie etwa aus dem Finanzsektor bekannt sind – auf Stromnetze zu übertragen. Im Teilvorhaben von e-netz („Resilienz im Verteilnetz“) standen insbesondere folgende Ziele im Fokus:

Identifikation und Bewertung neuer Bedrohungen für das Verteilnetz, insbesondere durch koordinierte Angriffe auf verteilte IoT-Geräte.

Entwicklung von Angriffs- und Schadensmodellen für das Szenario „verteilter IoT-Angriff“ im Verantwortungsbereich eines Verteilnetzbetreibers.

Erarbeitung und Modellierung technischer Gegenmaßnahmen im Verteilnetz, inklusive eines Konzepts für ein dezentrales Edge-Frühwarnsystem zur Anomalieerkennung.

Aufbau und Betrieb eines Realdemonstrators in einer typischen Verteilnetzumgebung zur praktischen Erprobung von Detektions- und Gegenmaßnahmen.

Ableitung technischer Empfehlungen zur Erhöhung der Resilienz im Verteilnetz sowie Vorbereitung einer breit anwendbaren Stresstestmethodik.

Flankierend sollten die gewonnenen Erkenntnisse in Forschung und Lehre eingebracht, in Fachgremien diskutiert und in die Weiterentwicklung interner Prozesse und Sicherheitskonzepte von e-netz integriert werden.

3. Projektverlauf und wesentliche Ereignisse

Die Projektlaufzeit im Verbund begann im Mai 2023. Im Folgenden wird der Verlauf des Teilvorhabens e-netz entlang der wesentlichen Meilensteine zusammengefasst.

Zu Projektbeginn fand im Juli 2023 das gemeinsame Kick-off-Treffen an der Technischen Universität Darmstadt statt. In mehreren Abstimmungsrunden wurde der Kooperationsvertrag zwischen den Partnern finalisiert und fristgerecht abgeschlossen. Innerhalb der e-netz wurde Ende 2023 die neue Stabsstelle „Unternehmenssicherheit“ geschaffen, die sich speziell mit Cybersicherheit befasst und von Beginn an in das Projekt eingebunden wurde.

Im Jahr 2023 wurden zunächst die Anforderungen an eine allgemeine Stresstestmethodik im Energiesektor erarbeitet. In Workshops mit allen Projektpartnern, insbesondere dem Workshop am 22. Januar 2024 unter Leitung der TU Darmstadt, wurden aus Sicht des Verteilnetzbetreibers die relevanten Szenarien konsolidiert, die Akteure und Komponenten in Koordinationsdiagrammen abgebildet und Schadwirkungsketten diskutiert.

Als Fokusszenarien wurden die Folgenden festgelegt: Missbrauch von Schutzmechanismen, Fahrplanmanipulation und verteilte IoT-Attacke.

e-netz brachte in diesen Prozess seine Expertise in Bezug auf angreifbare und nicht angreifbare Betriebsmittel, Regelprozesse und Netzstrukturen ein.

Am 15. Februar 2024 fand das zweite Projekttreffen bei e-netz Südhessen statt, inklusive Besichtigung der Querverbundleitstelle und einer Umspannanlage. Diese Veranstaltung diente dazu, den Projektpartnern die reale Netz- und Leitstellenumgebung näherzubringen, die später auch für den Realdemonstrator relevant wurde.

In einer Telefonkonferenz am 16. April 2024 zwischen TU Darmstadt und e-netz wurden Aufbau und Konzeption des Realdemonstrators konkretisiert. e-netz stellte als Anwendungsfall eine Transformatorenstation sowie zwei Wallboxen auf dem Betriebsgelände im Dornheimer Weg in Darmstadt zur Verfügung. Das Mess- und Kommunikationskonzept wurde abgestimmt, mögliche Manipulationsszenarien wurden definiert und die dafür relevanten Messgrößen und Datenquellen festgelegt.

Im weiteren Verlauf bereitete e-netz Messdaten aus dem Verteilnetz auf, inklusive Transienten und Langzeitaufzeichnungen, und stellte diese der TU Darmstadt zur Entwicklung und Parametrisierung von Anomalieerkennungsverfahren zur Verfügung. Einen wichtigen Schritt bildete die Auswahl und Installation eines Netzanalysators in der Ortsnetzstation sowie die Zusammenstellung eines Industrie-PCs als lokale Edge-Computing-Plattform.

Die Algorithmusentwicklung erfolgte zunächst auf Messtechnik bei der TU Darmstadt, um die Sicherheit des produktiven Verteilnetzes zu gewährleisten. Anschließend wurde der Algorithmus auf den Industrie-PC in der Transformatorenstation bei e-netz übertragen.

Begleitend fanden Exkursionen und Abstimmungstermine statt, unter anderem eine Exkursion zur Hauptschaltleitung des Übertragungsnetzbetreibers Amprion in Brauweiler im Juli 2024

Bis Ende 2025 war der Realdemonstrator vollständig aufgebaut und in Betrieb. Es wurden koordiniert simulierte Angriffe auf verteilte IoT-Geräte durchgeführt, die Auswirkungen auf das Verteilnetz beobachtet und Gegenmaßnahmen getestet. Am 24. Oktober 2024 fand ein Meilensteintreffen an der TU Darmstadt statt, bei dem e-netz zu den Fortschritten im Teilvorhaben berichtete. Die im Realdemonstrator gewonnenen Ergebnisse bildeten die Grundlage für die abschließende Ableitung technischer Empfehlungen und Hinweispapiere.

Im Projekttreffen am 27.03.2025 wurden mehrere DER-basierte Angriffsszenarien mit ihren Schadwirkungsketten, Kennzahlen und Gegenmaßnahmen konkretisiert.

Am 7. Mai 2025 fand bei der e-netz Südhessen AG ein Workshop im Rahmen des Projekts CyberStress statt. Im Mittelpunkt standen neben dem Austausch zu möglichen Folgeprojekten die Vorstellung der Auswertung der „Datenkonserve“, die Abstimmung zu einer Veröffentlichung in EW-Medien über den Realdemonstrator beziehungsweise die Digitalisierung im Niederspannungsnetz, die Begehung des Realdemonstrators auf dem Betriebsgelände von e-netz sowie die Besprechung des weiteren Vorgehens zu Anwendungen und Stresstests im Realdemonstrator.

In der Projektsitzung vom 30.09.2025 wurden insbesondere technische und regulatorische Gegenmaßnahmen gegen cyberphysische Schadwirkungen im Stromsystem diskutiert. Schwerpunkte waren Leitungsüberlastungen durch kompromittierte Ladepunktbetreiber, mögliche Schnelltests einzelner Unternehmen sowie Ansätze zur Unterbrechung von Schadwirkungsketten, etwa durch Segmentierung und Plausibilitätsprüfungen

Am 13.04.2026 fand das interne Abschlusstreffen zum Projekt statt. Der Projektstatus wurde vorgestellt und die Folien für den offiziellen Abschluss in Bonn besprochen. Der Projektträger informierte das Konsortium umfassend zu den Abschlussarbeiten.

Die Sitzung vom 27.04.2026 diente dem Projektabschluss und bündelte die zentralen Ergebnisse zu Konzept, Ablauf und rechtlicher Einordnung von Cybersicherheits-Stresstests für das Stromsystem. Darüber hinaus wurden DER-basierte Angriffsszenarien, geeignete Gegenmaßnahmen sowie der Realdemonstrator zur Anomaliedetektion am E-Ladepark von e-netz vorgestellt und diskutiert.

Am 22.05.2026 führte e-netz gemeinsam mit der TUD eine Informationsveranstaltung für die Presse sowohl im Anschluss auch für die internen Mitarbeiter der e-netz statt. Nähere Informationen siehe Kapitel 10.2.

Über die gesamte Projektlaufzeit fanden regelmäßig stattfindende Jour-fixe-Telefonkonferenzen des Konsortiums statt, bei dem sich Wissenschaft und Praxis immer eng abstimmt haben.

4. Wissenschaftlich-technische Ergebnisse

4.1 Definition eines Stresstests

Im Rahmen des Projektes wurde unter Federführung des Lehrstuhls für Recht der Digitalisierung der Universtiät zu Köln eine Definition des Stresstests erarbeitet. Diese Definition war erforderlich, um ein gemeinsames Verständnis über Inhalt, Zielsetzung und wesentliche Merkmale des Instruments sicherzustellen, diente gleichzeitig dazu die passende Rechtsgrundlage bestimmen zu können und den Stresstest gegenüber Dritten nachvollziehbar und vergleichbar zu beschreiben.

Die im Projekt abgestimmte Definition lautet: Instrument der Analyse, das zu Prognosezwecken mittels der Simulation von Szenarien Informationen über das Verhalten von Systemen oder Systemkomponenten generiert.

Die Auswahl der konkreten Rechtsgrundlage hängt jedoch von der jeweiligen Ausgestaltung des Stresstests ab. Eine ausdrückliche gesetzliche Grundlage für Cybersicherheits-Stresstests im Energiesektor besteht bislang nicht.

4.2 Stresstestarchitektur

Gemeinsam mit den Verbundpartnern wurde eine formale Stresstestarchitektur in Anlehnung an den Bankensektor für Stromnetze erarbeitet. Die Stresstestarchitektur beschreibt dabei das Vorgehen, um aus den Ankerszenarien die Ergebnisse zu erhalten. Unter Ankerszenarien werden die konzeptionellen Ausgangsszenarien des Stresstests verstanden. Sie strukturieren die Betrachtung relevanter Angriffspfade und bilden die Grundlage für die Ableitung konkreter Subszenarien, anhand derer Schadenswirkungen, Modellannahmen und KPIs systematisch untersucht werden.

Der Ablauf eines Stresstests wurde in der nachfolgenden Abbildung 1 dargestellt.

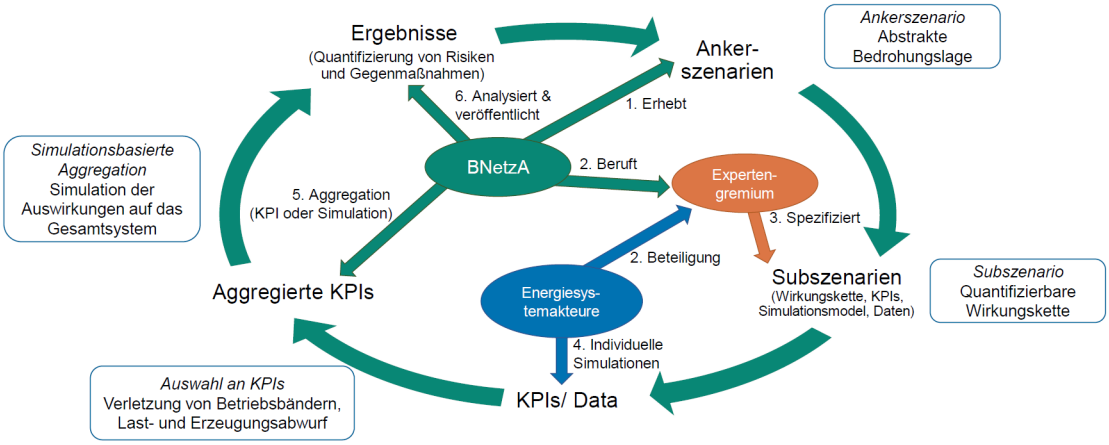


Abbildung.7.Ablauf.eines.Stresstests

Die Anforderungen an einen Stresstest wurden dabei wie folgt definiert:
1. Transparenz
2. Eindeutigkeit
3. Aufwand, Skalierbarkeit und Flexibilität,
4. Rechtliche Grundlagen/Umsetzbarkeit.

4.3 Szenario-Liste

Insgesamt wurden verschiedene Bedrohungsszenarien gemeinsam im Konsortium erarbeitet. Als Grundlage der weiteren Untersuchungen wurde eine Szenario-Liste mit sechs übergeordneten Angriffsszenarien erstellt. Diese sind nachfolgend aufgelistet:

1. Schwachstelle bei OT-Komponenten
2. Kompromittierte Komponenten in Stationen

3. Angreifer in Netzwerk aber nicht in der Leittechnik
4. Missbrauch von Schutzmechanismen
5. Marktmanipulation
6. Verteilte IoT-Attacke

Diese Szenarien fungieren als Ankerszenarien für den Stresstest und bündeln die aus fachlicher Sicht wesentlichen Angriffspfade auf das Stromsystem. Sie schaffen einen einheitlichen Bezugsrahmen für die systematische Analyse potenzieller Schadensmechanismen, die Quantifizierung der Auswirkungen anhand geeigneter Kennzahlen sowie die Ableitung technischer und organisatorischer Gegenmaßnahmen.

In einem gemeinsamen Workshop mit der TU Darmstadt bei der e-netz wurden die Szenarien „Missbrauch von Schutzmechanismen“, „Fahrplanmanipulation“ und insbesondere „verteilter IoT-Angriff“ im Detail analysiert und als Grundlage für weitere Arbeiten im Realdemonstrator genutzt.

4.3 Angriffsszenarien

Im Folgenden werden die identifizierten Angriffsszenarien aus Sicht des Verteilnetzbetreibers systematisch eingeordnet und hinsichtlich ihrer potenziellen Auswirkungen auf den Netzbetrieb bewertet. Die Betrachtung umfasst sowohl die möglichen Entstehungswege von Schäden als auch geeignete Kennzahlen zur Quantifizierung der Schadwirkung sowie Maßnahmen zur Prävention und operativen Schadensbegrenzung. Besonderes Augenmerk liegt dabei auf Beeinträchtigungen der Leistungs- und Transport Adäquanz, Überlastungen von Betriebsmitteln und Spannungsverletzungen.

Für den Verteilnetzbereich wurden von e-netz insbesondere folgende Elemente konkretisiert:

- Definition relevanter Szenarien mit Fokus auf Cyberbedrohungen.
- Ableitung von Kennzahlen zur Quantifizierung von Schadwirkungen, zum Beispiel Spannungsbandverletzungen, Oberwellenanteile, Auslastungsgrade von Betriebsmitteln und Auswirkungen auf die Spannungsqualität.
- Beschreibung der Wirkungsketten von Angriffen und Gegenmaßnahmen aus Sicht des Verteilnetzbetreibers, einschließlich prozessualer Abläufe und Meldewege.

4.3.1 Ankerszenario Missbrauch von Schutzmechanismen

Im Szenario „Missbrauch von Schutzmechanismen“ gelingt es einem Angreifer, Zugriff auf steuerbare Anlagen zu erlangen und diese gezielt zur Manipulation von Leistungsflüssen einzusetzen. Betroffen sind dabei insbesondere Komponenten wie Rundsteueranlagen oder Systeme des Einspeisemanagements. Das Szenario ist vor allem in der Domäne dezentraler Erzeugung sowie bei nachgelagerten Endkunden mit steuerbaren Ressourcen verortet. Im Unterschied zur verteilten IoT-Attacke liegt die

Besonderheit hier darin, dass der Netzbetreiber keinen direkten Zugriff auf die betroffenen steuerbaren Ressourcen hat. Dadurch entstehen zusätzliche Herausforderungen für die Erkennung, Begrenzung und Beherrschung möglicher Schadwirkungen im Netzbetrieb.

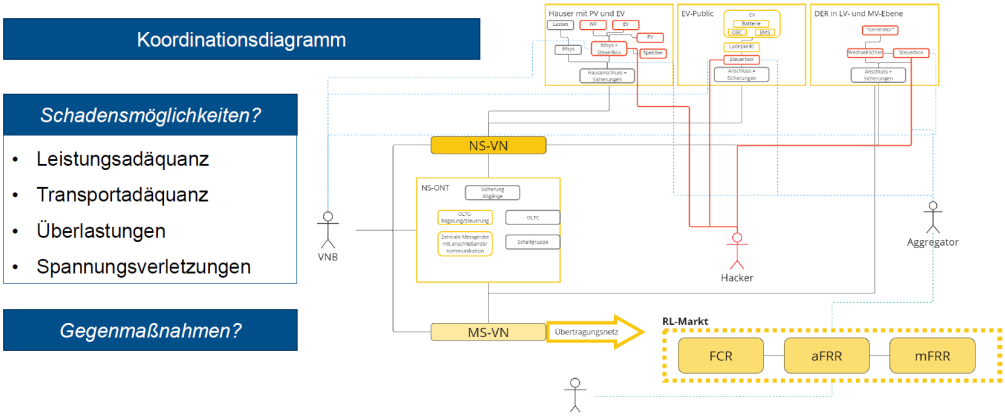


Abbildung.8.Missbrauch.von.Schutzmechanismen

Die Abbildung 2 veranschaulicht das Koordinationsdiagramm zum Szenario „Missbrauch von Schutzmechanismen“ sowie die wesentlichen Schadensrisiken im Verteilnetz. Besonders relevant sind Überlastungen, Spannungsverletzungen und mögliche Kaskadierungseffekte. Als Gegenmaßnahmen werden insbesondere intelligente Schutzmechanismen, Abregelung und technische Reserven betrachtet.

4.3.2 Ankerszenario Fahrplanmanipulation

Im Szenario „Fahrplanmanipulation“ werden Fahrpläne beziehungsweise fahrplanrelevante Steuerungs- und Koordinationsinformationen gezielt verändert, wodurch netzbetriebliche Fehlsteuerungen verursacht werden können. Besonders relevant ist dabei, dass sich die Auswirkungen aus Sicht des Verteilnetzbetreibers vor allem in Transportproblemen äußern. Im Zusammenhang mit dem Szenario ist zudem zu prüfen, inwieweit Plattformen für Redispatch die Koordination der Akteure verändern und welche Rolle die Häufigkeit von Redispatch-Maßnahmen im Verteilnetz spielt.

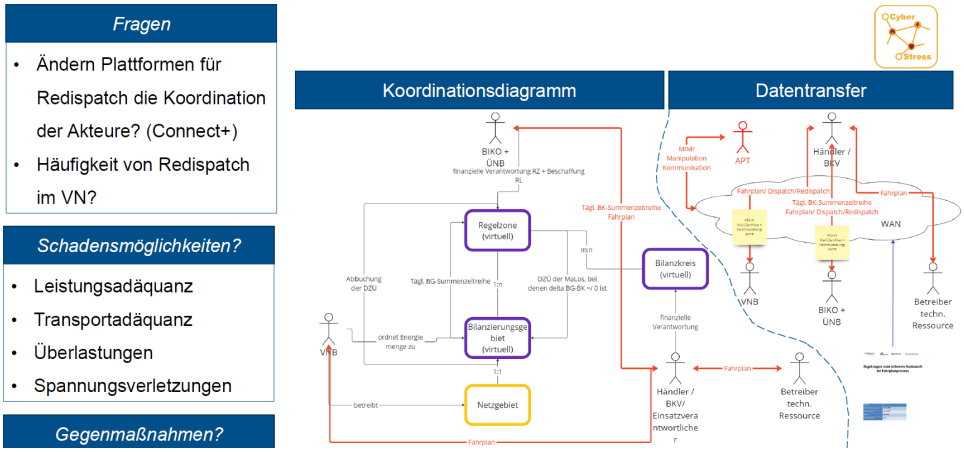


Abbildung.9.Fahrplanmanupulation

Die Abbildung 3 zeigt das Koordinationsdiagramm zum Szenario „Fahrplanmanipulation“ und verdeutlicht die möglichen Schadenswirkungen innerhalb des Netzbetriebs. Im Mittelpunkt stehen insbesondere Beeinträchtigungen der Leistungs- und Transport Adäquanz sowie potenzielle Überlastungen und Spannungsverletzungen. Für die Quantifizierung der Schadwirkung sind unter anderem eine mögliche „Ermüdung“ von Bauteilen, nicht versorgte Lasten sowie finanzielle Schäden durch einen übermäßigen Abruf von Regelenergie zu berücksichtigen. Kritisch ist zudem, dass eine Plausibilisierung der Fahrpläne nicht durchgeführt wird, wodurch Manipulationen unter Umständen unentdeckt bleiben können

4.3.3 Ankerszenario Verteilte IoT-Attacke

Im Szenario „Verteilte IoT-Attacke“ gelingt es einem Angreifer, die Kontrolle über eine große Anzahl dezentraler Verbraucher und IoT-Geräte wie Wärmepumpen, Ladepunkte oder Haushaltsgroßgeräte zu übernehmen und diese gezielt zur Beeinflussung der Leistungsflüsse einzusetzen. Das Szenario ist in der Domäne der Endkunden mit nicht steuerbaren Ressourcen verortet. Im Unterschied zum Szenario „Missbrauch von Schutzmechanismen“ besteht hier die Besonderheit darin, dass der Netzbetreiber grundsätzlich Zugriff auf die steuerbaren Ressourcen hat, was zusätzliche Möglichkeiten zur operativen Reaktion eröffnet

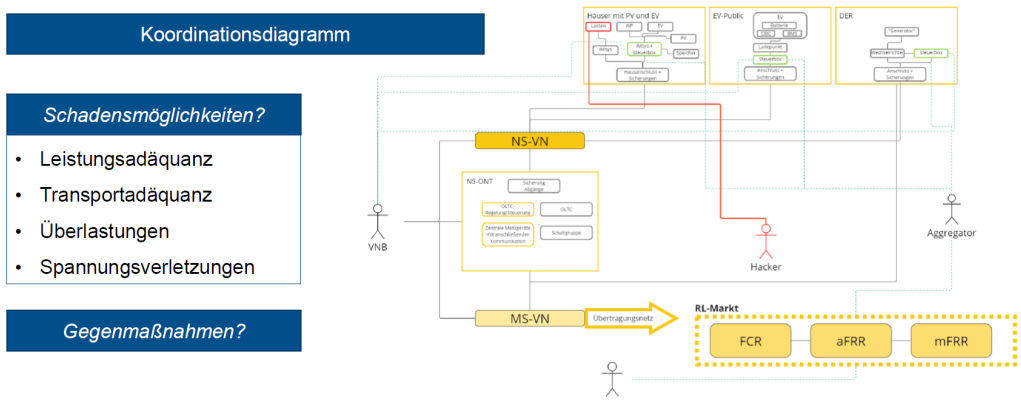


Abbildung.0.Verteilte.IoT_Attacke

Abbildung 4 veranschaulicht das Szenario „Verteilte IoT-Attacke“ und die daraus resultierenden potenziellen Auswirkungen auf den Netzbetrieb. Besonders relevant sind Beeinträchtigungen der Leistungs- und Transportadäquanz, Überlastungen sowie Spannungsverletzungen. Als Gegenmaßnahmen kommen insbesondere technische Überdimensionierung, das Erkennen manipulierten Verhaltens auf Strangebene sowie intelligente Primärtechnik zur selektiven Begrenzung betroffener Netzbereiche in Betracht; zusätzlich kann ein regelbarer Ortsnetztransformator (rONT) dazu beitragen, Spannungsprobleme lokal einzugrenzen

4.4 Angriffs- und Schadensmodell für das Verteilnetz

Im Arbeitspaket Angriffs- und Schadensmodellierung für das Verteilnetz wurde herausgearbeitet, durch welche Wirkungsketten Cyberangriffe Schäden und Störungen im Verantwortungsbereich eines Verteilnetzbetreibers hervorrufen können. Im Fokus standen steuerbare Verbrauchs- und Einspeiseanlagen mit größerer Anschlussleistung, etwa Erneuerbare-Energien-Anlagen, KWK-Anlagen, Ladeinfrastruktur für Elektromobilität und Wärmepumpen, insbesondere im Kontext von § 14a EnWG.

Es wurde gezeigt, dass koordinierte, synchrone Laständerungen bei einer Vielzahl dezentraler IoT-Geräte zu Spannungsbandverletzungen, ausgeprägten Oberwellen und einer generell schlechten Spannungsqualität führen können. Diese verschlechterte Spannungsqualität kann wiederum Abschaltungen nicht kompromittierter Anlagen auslösen und so eine Kaskade von Schadwirkungen erzeugen. Die Modelle berücksichtigen zudem potenzielle Rückwirkungen auf das Übertragungsnetz, etwa die Belastung von Leitungen und die Inanspruchnahme von Regelreserven. Auf Basis dieser Analysen wurde ein Konzept für ein dezentrales Edge-Frühwarnsystem zur Anomalieerkennung entwickelt. Dieses basiert auf der kontinuierlichen Beobachtung der Netzgrößen in der Ortsnetzstation und der Detektion charakteristischer Abweichungsmuster, die auf koordinierte Angriffe hindeuten.

4.5 Realdemonstrator in einer typischen Verteilnetzumgebung

Ein zentrales Ergebnis des Projekts ist der Aufbau und Betrieb eines Realdemonstrators in einer typischen Verteilnetzumgebung der e-netz Südhessen AG.

Abbildung 1 Ladepark bei e_netz Südhessen mit Realdemonstrator zur Anomalieerkennung

Dieser umfasst einen E-Auto-Ladepark (siehe Abbildung 5) mit einer Vielzahl von IoT-fähigen Verbrauchsanlagen, die an eine Ortsnetzstation angeschlossen sind. In der Ortsnetzstation wurde ein Netzanalysator installiert, der den Leistungsfluss und die

Spannungsqualität kontinuierlich misst. Die Messdaten werden an einen lokalen Industrie-PC weitergeleitet, auf dem die entwickelten Anomalieerkennungsverfahren ausgeführt werden. Die nachfolgende Abbildung 6 zeigt den Aufbau des Realdemonstrators im Projekt CyberStress. Aufgrund von sicherheitsrelevanten Aspekten wurde der Algorithmus zunächst in einem genau gleichen realen Aufbau bei der TU Darmstadt getestet.

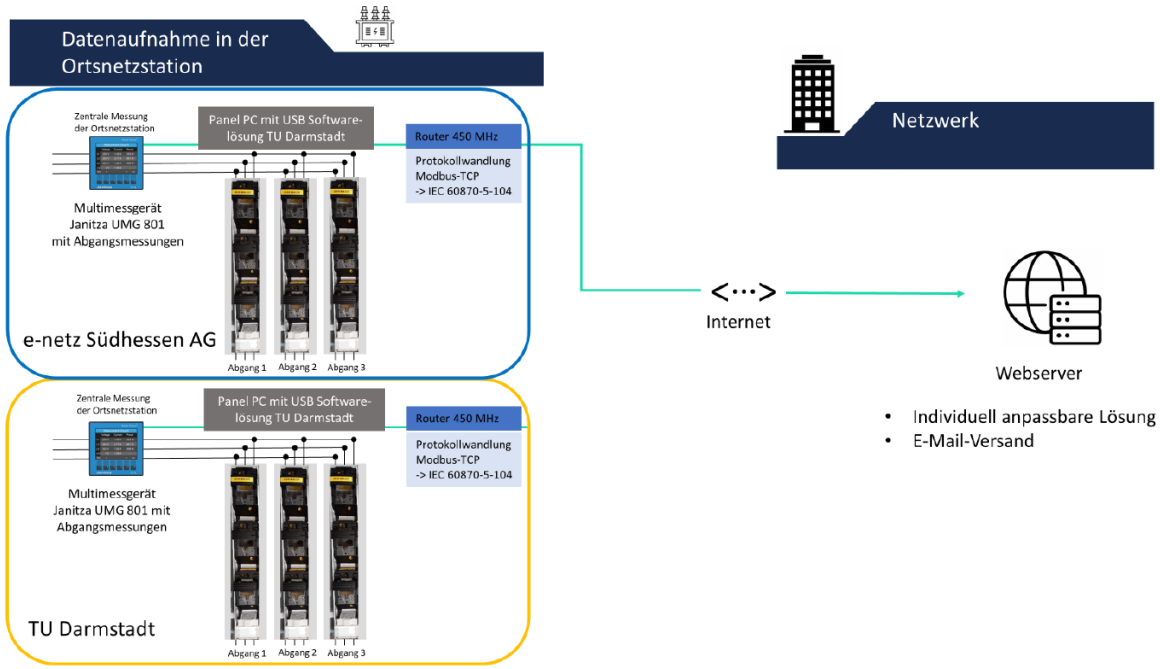


Abbildung 2 Realdemonstrator im Projekt CyberStress

Im Demonstrator wurde insbesondere das Szenario eines koordinierten Cyberangriffs auf verteilte IoT-Geräte umgesetzt. Angreifer könnten hierbei beispielsweise durch die Kompromittierung der Ladeinfrastruktur oder von PV-Anlagen, Wallboxen und Wärmepumpen eine synchrone Laständerung im Netz bewirken. Im Realdemonstrator wurden entsprechende Verhaltensmuster nachgebildet und die Auswirkungen auf die Netzstabilität und Spannungsqualität untersucht.

Die Untersuchungen haben gezeigt, dass bereits eine relativ geringe Anzahl synchron agierender Geräte ausreicht, um kritische Schwellenwerte zu überschreiten, die Spannungsqualität zu verschlechtern und Netzressourcen stark zu belasten. Damit wurde die im Antrag formulierte Hypothese eines signifikanten Angriffspotenzials durch verteilte IoT-Geräte empirisch bestätigt.

4.5.1 Komponenten des Realdemonstrators

Als Realdemonstrator wurde eine Ortsnetztransformatorenstation auf dem Firmengelände der e-netz ausgewählt, siehe Abbildung 7.

Abbildung 7: Ortsnetztransformatorenstation der e-netz

Diese wurde erweitert um zusätzliche Messtechnik von Janitza (UMG801 mit Strangmessung), einem Custom Panel PC von Siemens und einem 450 MHz Router, wie auf Abbildung 9 dargestellt. Als Entwicklungsplattform stand der TU Darmstadt ein eigener Aufbau mit einem baugleichen Messgerät und Panel PC zur Verfügung.

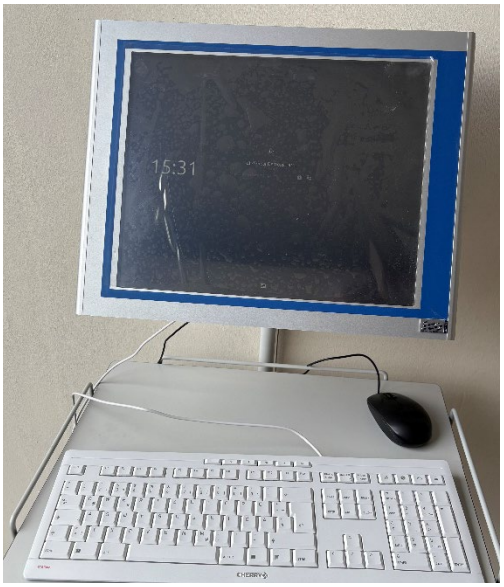


Abbildung 8: Komponenten des Realdemonstrators

4.6 Anomalieerkennung

Auf Basis der im Realdemonstrator gewonnenen Messdaten entwickelte die TU Darmstadt in enger Abstimmung mit e-netz ein Anomalieerkennungsverfahren, das im Edge-System in der Ortsnetzstation implementiert wurden. Der genaue Aufbau ist in Abbildung 9 dargestellt. e-netz stellte hierfür Messreihen aus dem realen Verteilnetz, einschließlich transienter Ereignisse, zur Verfügung und begleitete die Parametrisierung und Validierung der Algorithmen.

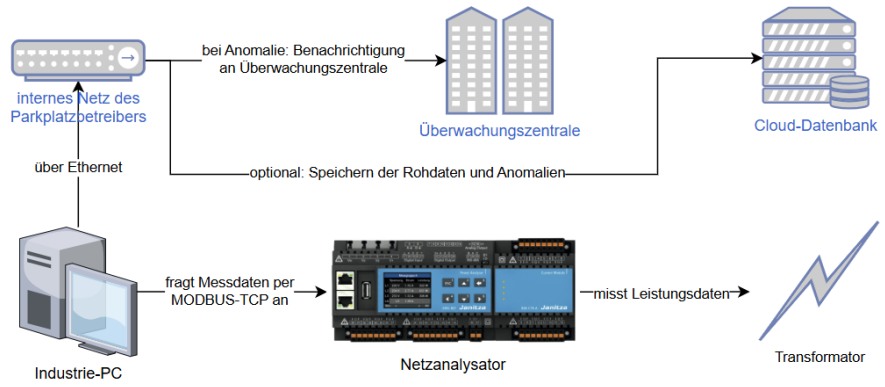


Abbildung 8 Messaufbau und Datengewinnung

Die TU Darmstadt erstellte verschiedene Datenanalysen, auf Wochen- und Tagesebene sowie bei Einschaltvorgängen. Ergänzend wurde eine Funktionsweise der Anomaliedetektion angefertigt, zum einen für den Ablauf der Echtzeit-Anomalieerkennung und zum anderen für den Ablauf des Modelltrainings und der Evaluierung. Hierfür stellte e-netz der TU Darmstadt Testdaten mit Anomalien zur Verfügung, aus denen verschiedene Anomalietypen abgeleitet wurden, siehe Abbildung 10.

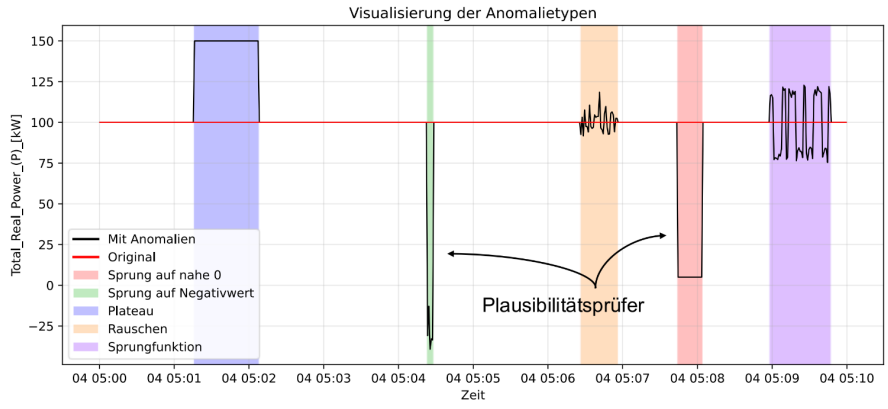


Abbildung 76 betrachtete Anomalietypen

Auf Basis der Datenauswertung wurden 12 unterschiedliche Feature-Matritzen getestet und dann ein Threshold ausgewählt. Die Umsetzung erfolgte als Docker-Container mit zwei Betriebsmodi.

Der Batch-Modus analysiert und wertet dabei eine bereitgestellte CSV-Datei aus, der Streaming-Modus erstellt eine Live-Auswertung einer PSQL-Datenbank (im Projekt aufgrund von KRITIS-Datenschutzrichtlinien nicht genutzt). Bei Erkennung einer Anomalie wird das Ergebnis unmittelbar auf der Konsole ausgegeben und der Datenausschnitt als CSV-Datei gespeichert.

Im Projekt konnte nachgewiesen werden, dass die entwickelte Anomalieerkennung verschiedene Anomalietypen mit hoher Präzision erkennt.

4.7 Gegenmaßnahmen

Die im Projekt identifizierten Gegenmaßnahmen lassen sich in drei Ebenen gliedern: die Verringerung von Angriffsmöglichkeiten, die frühzeitige Erkennung von Angriffen sowie die wirksame Begrenzung von Schadwirkungen im Betrieb. Auf präventiver Ebene wurden insbesondere Segmentierung, abgesicherte Kommunikationswege, verzögerte beziehungsweise randomisierte Steuerung, Diversifizierung und Zertifizierung von Komponenten, Plausibilitätsprüfungen etwa bei Fahrplänen sowie Einschränkungen von Update- und Parametrierungsmöglichkeiten identifiziert. Ziel dieser Maßnahmen ist es, die Angriffsfläche zu reduzieren und koordinierte Manipulationen zu erschweren. Im Netzbetrieb wurden ergänzend robuste technische Auslegungen wie Überdimensionierung, zusätzliche Reserven sowie Betriebsmittel wie rONT, Blindleistungsmanagement oder Speicher als Möglichkeiten zur Erhöhung der Resilienz betrachtet.

Ein besonderer Schwerpunkt lag auf der Erkennung und operativen Beherrschung von Angriffen im Verteilnetz. Hierzu wurden intelligente Schutz- und Detektionsmechanismen konzipiert und im Realdemonstrator erprobt, insbesondere strangscharfe Messungen und eine lokale Anomaliedetektion in der Ortsnetzstation. Diese ermöglicht es, auffälliges Verhalten frühzeitig zu erkennen, betroffene Netzbereiche zu lokalisieren und im Bedarfsfall selektiv Stränge mit manipulierten DERs abzuschalten. Ergänzend wurden Meldeketten, forensische Zuordnungsmöglichkeiten und eine koordinierte Weitergabe relevanter Informationen an überlagerte Ebenen betrachtet. Insgesamt zeigen die Arbeiten, dass eine Kombination aus dezentraler Detektion, klaren Entscheidungs- und Meldeprozessen sowie technischen Eingriffsmöglichkeiten die Auswirkungen koordinierter Angriffe deutlich begrenzen kann.

Ein zentrales Projektergebnis ist darüber hinaus, dass Resilienz nicht allein von technischer Ausstattung abhängt. Ebenso wichtig sind organisatorische Vorbereitung, klare Zuständigkeiten, geeignete Prozesse sowie die Fähigkeit der Netzbetreiber, im Ereignisfall schnell und koordiniert zu reagieren. Die im Projekt entwickelten Gegenmaßnahmen sind daher nicht isoliert technisch zu verstehen, sondern als Zusammenspiel aus technischen, operativen und regulatorischen Bausteinen zur Unterbrechung von Schadwirkungsketten.

4.8 Ableitung technischer Empfehlungen

Zum Abschluss wurden die Ergebnisse aus den Simulationen und Feldversuchen aus Sicht des Verteilnetzbetriebs bewertet:

- Empfehlungen für die Ausstattung von Ortsnetzstationen mit Mess- und Analysetechnik (Netzanalysator, Edge-Computing, Anbindung an Leitstelle).
- Hinweise zur Integration von Anomalieerkennung und Alarmsystemen in bestehende IT-/OT- und ISMS-Strukturen von Verteilnetzbetreibern.
- Empfehlungen zur Nutzung der Smart-Meter-Gateway- und CLS-Infrastruktur als operative Gegenmaßnahme bei Cyberangriffen.
- Vorschläge für organisatorische Maßnahmen, wie etwa Notfallprozesse, Planspiele und Schulungen, um die Reaktionsfähigkeit im Ereignisfall zu erhöhen.

5. Vergleich mit Arbeits-, Zeit- und Kostenplanung

Das Teilvorhaben der e-netz Südhessen AG verlief insgesamt planmäßig. Die in der Teilvorhabenbeschreibung definierten Arbeitspakete von der Anforderungsanalyse (AP 1) über die Modellierung von Angriffen und Gegenmaßnahmen (AP 4 und AP 5) bis hin zur beispielhaften Stresstestdurchführung und Ergebnisableitung (AP 6) konnten inhaltlich umgesetzt werden.

Die Meilensteine, insbesondere die Durchführung der Schadenspotenzialanalyse gemäß AP 4.2 und der Aufbau sowie die Inbetriebnahme des Realdemonstrators, wurden erreicht. Es waren keine grundlegenden Umplanungen des Arbeitsprogramms erforderlich. Geringfügige Verschiebungen ergaben sich lediglich aus der Abstimmung der Mess- und Kommunikationskonzepte und dem Beschaffungsprozess der Messtechnik. Diese hatten jedoch keine relevanten Auswirkungen auf die Laufzeit des Teilvorhabens.

Hinsichtlich der Kostenplanung traten keine signifikanten Abweichungen vom bewilligten Budget auf. Innerhalb einzelner Kostenpositionen, insbesondere im Bereich der Reisekosten, kam es zu kleineren Umwidmungen, die jedoch im Rahmen der bewilligten Gesamtmittel verbleiben.

6. Erreichung der Projektziele und Änderungen der Zielsetzung

Die Aussichten auf Erreichung der Projektziele wurden im Verlauf des Projekts regelmäßig bewertet und blieben durchgehend sehr gut. Die wesentlichen Ziele des Teilvorhabens – Entwicklung eines Angriffs- und Schadensmodells für das Szenario „verteilter IoT-Angriff“, Konzeption und Erprobung eines Realdemonstrators, Entwicklung eines Edge-basierten Anomalieerkennungskonzepts sowie Ableitung technischer Empfehlungen – wurden erreicht.

Es ergaben sich keine grundlegenden Änderungen der ursprünglichen Zielsetzung. Vielmehr bestätigten die praktischen Ergebnisse im Realdemonstrator die Relevanz und Umsetzbarkeit der im Antrag formulierten Ansätze. Die Projektergebnisse unterstreichen die Notwendigkeit, die Thematik koordinierter IoT-Angriffe und Stresstests für Energiesysteme auch zukünftig weiter zu verfolgen und zu vertiefen.

7. Relevante externe Forschungsergebnisse

Während der Projektlaufzeit wurden seitens der Projektpartner die Entwicklungen im Bereich Cybersicherheit, Smart Grids und kritische Infrastrukturen kontinuierlich beobachtet. Es wurden jedoch keine externen Forschungs- und Entwicklungsergebnisse identifiziert, die eine grundlegende Anpassung des Arbeitsprogramms oder der Zielsetzung erforderlich gemacht hätten.

Die im Projekt entwickelten Konzepte bauen auf dem Stand von Wissenschaft und Technik auf und erweitern diesen insbesondere durch die interdisziplinäre Verknüpfung von IT-Sicherheit, Netzbetrieb, Rechtsforschung und praktischer Erprobung im Realdemonstrator.

8. Verwertung der Ergebnisse

8.1 Schutzrechte

Im Projektverlauf sind nach aktuellem Kenntnisstand keine Schutzrechte der e-netz Südhessen AG oder Dritter entstanden, die einer späteren Ergebnisverwertung entgegenstehen würden. Schutzrechtsanmeldungen sind nicht vorgesehen. Die entwickelten Methoden und Konzepte – etwa Stresstestmethodik, Anomalieerkennung und Gegenmaßnahmen – sind frei nutzbar und können von anderen Netzbetreibern, Forschungseinrichtungen und Institutionen übernommen werden.

8.2 Wirtschaftliche Erfolgsaussichten

Die vorgeschlagene Stresstestmethodik und das vertiefte Verständnis des Szenarios „verteilter IoT-Angriff“ sind sowohl während als auch nach der Projektlaufzeit ein wichtiges technisches Ergebnis. Sie tragen dazu bei, die IT-Sicherheit in Energienetzen zu verbessern und die Resilienz des Energiesystems mittel- bis langfristig zu erhöhen.

Für Netzbetreiber ergeben sich funktionale und wirtschaftliche Vorteile gegenüber einem rein reaktiven Umgang mit Cyberbedrohungen. Durch die Identifikation von Schwachstellen und die Umsetzung geeigneter Gegenmaßnahmen können Störungen und Ausfälle reduziert und potenzielle Schäden begrenzt werden.

Die Erkenntnisse sind für die gesamte Energiewirtschaft und die deutsche Wirtschaft von Bedeutung. Sie können als Grundlage für künftige regulatorische Vorgaben dienen und unterstützen die Bundesnetzagentur bei der Weiterentwicklung von Sicherheitsstandards.

8.3 Wissenschaftliche und technische Erfolgsaussichten

Die Projektergebnisse werden in Form von Fachpublikationen und Beiträgen auf Konferenzen veröffentlicht. Sie fließen in die Lehre und Ausbildung ein, zum Beispiel in Vorlesungen an der Hochschule Darmstadt sowie in Exkursionen und Fachvorträge. Damit leisten sie einen Beitrag zur Heranbildung von Nachwuchskräften im Bereich Energiewirtschaft und Cybersicherheit.

Die Ergebnisse werden darüber hinaus in Expertengremien und Netzwerken eingebracht und können dort weiterentwickelt und verbreitet werden. Es entstehen neue Forschungsfragen, die die gesellschaftliche Sicherheit in Zeiten der Digitalisierung langfristig verbessern können. Die entwickelten Konzepte dienen als Ausgangspunkt für Folgeinnovationen.

Die Bundesnetzagentur war als assoziierter Partner eingebunden und wird die wissenschaftlichen und technischen Erkenntnisse in die Weiterentwicklung von Sicherheitsstandards und regulatorischen Vorgaben einfließen lassen.

8.4 Wissenschaftliche und wirtschaftliche Anschlussfähigkeit

Die im Projekt validierten Cyberstresstestkonzepte bilden die Basis für weiterführende Innovationen und Anpassungsmaßnahmen in den internen Abläufen und Techniken der e-netz Südhessen AG.

Die Zusammenarbeit mit anderen Netzbetreibern und Forschungseinrichtungen soll fortgeführt werden, um die Ergebnisse in die Praxis zu transferieren und weiterzuentwickeln. Die Erkenntnisse werden in die zukünftige Systemlandschaft des Verteilnetzes und in die Entwicklung netzbetriebsspezifischer Software eingebracht.

Durch die Einbindung der Bundesnetzagentur ist die Anschlussfähigkeit für eine bundesweite Umsetzung sowie für weitere regulatorische und technische Entwicklungen sichergestellt. Folgeprojekte zu ganzheitlichen Energiesystemstresstests auf allen Netzebenen bieten sich an und können auf CyberStress aufbauen.

9. Zusammenarbeit im Verbund

Die Zusammenarbeit im Verbund zwischen der Technischen Universität Darmstadt (Projektleitung), der Goethe-Universität Frankfurt am Main, der e-netz Südhessen AG, der QGroup GmbH sowie den assoziierten Partnern Bundesnetzagentur und Amprion GmbH war über die gesamte Laufzeit hinweg eng und konstruktiv. Regelmäßige Projekttreffen, Jour-fixe-Telefonkonferenzen, Workshops und Exkursionen gewährleisteten eine kontinuierliche Abstimmung.

e-netz brachte insbesondere seine Praxisexpertise als Verteilnetzbetreiber, seine Erfahrungen mit kritischer Infrastruktur, ISMS-Zertifizierung und netzbetriebsspezifischer Softwareentwicklung ein und stellte reale Netzabschnitte für den Realdemonstrator zur Verfügung.

10. Öffentlichkeitsarbeit

Auf Basis der wissenschaftlichen Erkenntnisse des Projektes wurden verschiedene Öffentlichkeitsarbeiten durchgeführt. Neben der Veröffentlichung von Fach- und Presseartikeln wurden zum Projektabschluss Poster und ein Kurzfilm erstellt. Das Projekt CyberStress wurde darüber hinaus auf einer Projekthomepage und in Social Media Kanälen (LinkedIn und Instagram) beworben.

10.1 Publikationen/Veröffentlichungen

Im Rahmen des Forschungsprojektes „CyberStress“ wurde ein ausführlicher Fachartikel in einer Branchenzeitschrift, in dem der Realdemonstrator und die Projektergebnisse verständlich für eine breite Fachöffentlichkeit dargestellt wurden, veröffentlicht. Darüber hinaus erfolgten Vorträge und Beiträge in einschlägigen Fachkreisen sowie eine Pressemitteilung zum Projektabschluss.

Der Artikel „Stromnetze unter Stress – Projekt CyberStress forscht für mehr Resilienz gegen IT-Angriffe“ wurde in der Ausgabe 12/2025 des „ew Magazin für die Energiewirtschaft“ veröffentlicht. Beschrieben wird darin das Forschungsprojekt „CyberStress“, in dem TU Darmstadt, e-netz Südhessen und Partner eine modellbasierte Stresstest-Methodik entwickelten, um die Resilienz von Stromnetzen gegenüber Cyberangriffen – insbesondere über vernetzte IoT-Geräte wie Wallboxen, PV-Anlagen und Wärmepumpen – zu bewerten und zu verbessern. Kern ist ein Realdemonstrator in einem echten Verteilnetzabschnitt, an dem koordinierte Angriffe auf viele dezentrale Geräte simuliert, deren Auswirkungen auf Netzstabilität analysiert und technische wie organisatorische Gegenmaßnahmen für Netzbetreiber und Regulierung abgeleitet werden.

Für die CIGRE als internationale, gemeinnützige Fachorganisation für Hochspannungs-Energieübertragung und -verteilung hat die e-netz gemeinsam mit dem Konsortium ein CIGRE-Paper erstellt. Das Dokument stellt ein allgemeines Rahmenwerk für simulative Stresstests vor, mit dem sich die Resilienz von Stromsystemen gegen Cyberangriffe – insbesondere über internetverbundene dezentrale Energieressourcen – quantitativ bewerten und technische Gegenmaßnahmen testen lassen. Anhand zweier Beispiel-Szenarien (Inter-Area-Oszillationen im Übertragungsnetz als Systemrisiko und Spannungsbandverletzungen im Verteilnetz als Entity-Risiko) sowie einer Einbettung in EU-/deutsches Recht (NIS-2, EnWG, BSIG) wird gezeigt, wie solche Cyber-Stresstests technisch umgesetzt und regulatorisch verankert werden können.

In der nachfolgenden Tabelle sind die Veröffentlichungen tabellarisch aufgelistet.

Tabelle.7.Veröffentlichungen

Medium	Titel	Zeitpunkt der Veröffentlichung
CIGRE	Stress testing power systems' systemic resilience against cyber-attacks	Mai 2025
ew Magazin für die Energiewirtschaft	Stromnetze unter Stress – Projekt CyberStress forscht für mehr Resilienz gegen IT-Angriffe	12/2025
Power Point Folien	Projektabschluss bei BNetzA	April 2026
Pressemeldung	Stresstests für resilientere Stromnetze: Projekt CyberStress macht stark gegen IT-Angriffe	22. Mai 2026
Poster auf Microsite	Poster Allgemein	22. Mai 2026
Poster auf Microsite	Poster Realdemonstrator	22. Mai 2026
Poster auf Microsite	Poster Anomalieerkennung	22. Mai 2026
Kurzvideo bei LinkedIn	Abschluss CyberStress	22. Mai 2026
LinkedIn Beitrag	Abschluss CyberStress bei e-netz	Mai 2026
@entega Mitarbeiterzeitschrift	Stresstests für ein sicheres Stromnetz	August 2026

Die nachfolgenden Beiträge wurden im Rahmen der Abschlussveranstaltung bei der Bundesnetzagentur in Bonn am 27.04.2026 und im Rahmen der Abschlussveranstaltung in Darmstadt bei e-netz Südhessen auf LinkedIn veröffentlicht.

Die nachfolgende Pressemitteilung wurde am 22.05.2026, gemeinsam durch die TU Darmstadt und die e-netz Südhessen, veröffentlicht.

Stresstests für resilientere Stromnetze: Projekt CyberStress macht stark gegen IT-Angriffe

DARMSTADT – Die Energiewende macht Stromnetze moderner und digitaler. Das eröffnet neue Chancen: Erzeuger, Speicher und Verbraucher lassen sich intelligent vernetzen, die Versorgung wird effizienter und flexibler. Doch mit der Digitalisierung wächst auch die Angriffsfläche für Cyberkriminelle: Bei Kunden installierte, vernetzte Geräte können manipuliert werden. Etwa durch die feindliche Übernahme aller Ladesäulen eines Herstellers könnten Hacker das Stromnetz aus dem Gleichgewicht bringen. Obwohl diese Ladepunkte nicht im direkten Einflussbereich der Netzbetreiber liegen, kann ihr massenhaftes, normwidriges Verhalten die Netzstabilität gefährden.

Vor diesem Hintergrund entwickelte das Forschungsprojekt CyberStress eine Stresstest-Methodik für Stromnetze, vergleichbar mit bereits etablierten Verfahren im Bankensektor. Auf Basis der Projektergebnisse hat das Konsortium konkrete Empfehlungen für eine gesetzliche Verankerung von Stresstests an die Bundesnetzagentur als regulierende Behörde übergeben. Ziel ist es, die Versorgungssicherheit zu erhöhen und den gesellschaftlichen Schutz zu stärken, indem systematisch überprüft wird, wie robust Stromnetze gegenüber IT-Angriffen sind.

Heute präsentierten die Technische Universität Darmstadt und die e-netz Südhessen AG einen im Projekt entwickelten Realdemonstrator, der in einer Transformatorenstation des Verteilnetzbetreibers verbaut wurde. Ein von der TU Darmstadt entwickelter Algorithmus erkennt und warnt vor Anomalien im Stromnetz, zum Beispiel bei plötzlich auftretenden Laständerungen durch manipulierte Ladevorgänge von E-Autos, die die elektrische Leistung in kürzester Zeit stark ansteigen lassen.

„Der Realdemonstrator erlaubt uns, reale Angriffsszenarien nachzustellen und Detektions- sowie Abwehrstrategien unter realistischen Bedingungen zu erproben. So schaffen wir die Grundlagen, damit Netzbetreiber künftige Risiken frühzeitig erkennen und die Energieversorgung auch in einer zunehmend digitalen Welt zuverlässig sicherstellen können“, erklärt Prof. Florian Steinke vom Fachgebiet Energy Information Networks and Systems der TU Darmstadt.

Ines Schultze, kaufmännische Vorständin der e-netz Südhessen, betont: „CyberStress hilft uns dabei, unser Netz gezielt auf Cyberangriffe zu testen und Maßnahmen abzuleiten, um es noch widerstandsfähiger zu machen. Besonders wertvoll war die enge Zusammenarbeit mit der TU Darmstadt, den Projektpartnern und der Bundesnetzagentur als unsere Regulierungsbehörde. So fließen wissenschaftliche Expertise, praktische Betriebserfahrung und regulatorische Perspektive zusammen und stärken gemeinsam die Sicherheit der Energieversorgung.“

CyberStress ist ein gemeinsames Projekt der TU Darmstadt, der e-netz Südhessen AG, der Q-Group GmbH sowie der Universität zu Köln (Lehrstuhl Recht der Digitalisierung, Institut für Digitalisierung). Assoziierte Partner sind die Bundesnetzagentur und der Übertragungsnetzbetreiber Amprion. Gefördert wird das Projekt vom Bundesministerium für Forschung, Technologie und Raumfahrt unter dem Förderkennzeichen 13N16628, betreut wird es durch das VDI Technologiezentrum GmbH.

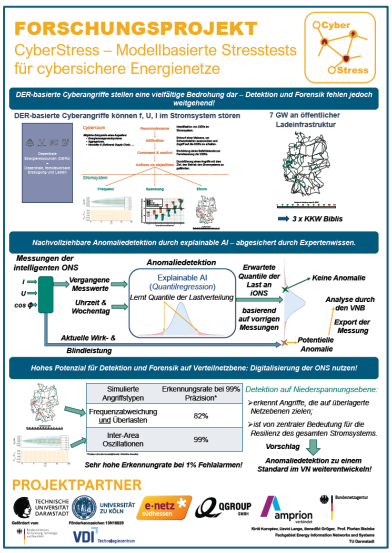
10.2. Veranstaltungen

Am 22. Mai 2026 wurden die Projektergebnisse einer Gruppe Journalisten auf dem Betriebsgelände der e-netz Südhessen in Darmstadt vorgestellt. Daraus resultierten fünf Beiträge in regionalen hessischen Medien (FAZ, Darmstadter Echo, Hitradio FFH, INDUSTR.com)

Abbildung.77.Projektpartner.der.TU.Darmstadt.und.e_netz.im.Gespräch.mit.Journalisten

Ebenfalls am 22. Mai 2026 fand, gemeinsam mit der TU Darmstadt, eine interne Abschlussveranstaltung zum Projekt bei e-netz Südhessen statt. Dabei stand die Vorstellung der Projektergebnisse im Vordergrund mit dem Ziel diese noch weiter in der Praxis zu nutzen und entsprechende Folgeprojekte voranzutreiben.

10.3 Postersession



10.4 Microsite

Für das Forschungsprojekt CyberStress wurde eine Microsite auf der Internetseite der e-netz Südhessen AG angelegt. Die Microsite bietet Interessierten, sowohl aus der Bevölkerung als auch der Industrie, die Möglichkeit, schnell und einfach Informationen über das Projekt zu erlangen. Auf der Seite sind Eckdaten des Projekts, beispielsweise Ziele, Laufzeit und Projektpartner hinterlegt. Auch die Förderung durch das BMWK ist, mit Logo und Link zur Website (https://www.e-netz-suedhessen.de/cyberstress), hinterlegt. Zudem finden sich hier ebenfalls die drei Poster, die den Projektablauf und die Ergebnisse beschreiben.

11. Fazit

Mit CyberStress wurde ein interdisziplinäres Projekt erfolgreich umgesetzt, das die Schnittstelle von Energiewirtschaft, IT-Sicherheit, Recht und Regulierung adressiert. Für das Teilvorhaben der e-netz Südhessen AG lässt sich festhalten:

Das Bedrohungsszenario eines koordinierten „verteilten IoT-Angriffs“ wurde realitätsnah analysiert und modelliert.

Die praktischen Untersuchungen im Realdemonstrator haben das erhebliche Schadenspotenzial solcher Angriffe aufgezeigt und gleichzeitig demonstriert, dass durch geeignete technische und organisatorische Maßnahmen eine deutliche Erhöhung der Resilienz möglich ist.

Die entwickelte Stresstestmethodik, die Konzepte zur Anomalieerkennung und die abgeleiteten Handlungsempfehlungen liefern eine belastbare Grundlage für andere Verteilnetzbetreiber und für die Weiterentwicklung von Sicherheitsstandards.

Die Projektziele wurden erreicht. CyberStress leistet damit einen wichtigen Beitrag zur Erhöhung der Cybersicherheit und Versorgungssicherheit im Zeitalter digitalisierter Energienetze.