4.4 Blaupause 8: Resilienz des elektrischen Energiesystems

Blaupause

Zielgruppen	KRITIS-Betreiber, ÜNB, VNB, VK-Betreiber, Komponenten-Entwickler
Ausgangslage und Problemstellung	Das Stromsystem muss in die Lage versetzt werden, auf unvorhergesehene Störungen so zu reagieren, dass es seine Grundfunktionalität dennoch aufrechterhalten oder zumindest selbstständig wiedererlangen kann. Für diese Selbstorganisation ist es unabdingbar, die IT als integralen Bestandteil des Stromsystems zu verstehen und die Potenziale der Digitalisierung zur Erhöhung der Resilienz des elektrischen Energiesystems voll auszuschöpfen. Durch die sogenannte IT/OT-Konvergenz im elektrischen Energiesystem verändert sich die Bedrohungsstruktur für die Energieversorgung in den kommenden Jahrzehnten aufgrund der zunehmenden Abhängigkeiten von IKT deutlich. Neue Risikofaktoren, die zu großen Blackouts führen können, kommen zu den Bestehenden hinzu. Der Systemwandel führt unter anderem dazu, dass die den Netzbetreibern heute zur Verfügung stehenden Mechanismen gegen große Blackouts nicht weiter ausreichen. So ist erkennbar, dass das bisher erfolgreich angewandte deterministische N-1-Prinzip aufgrund der Effekte einer zunehmenden Digitalisierung ergänzt werden muss.
Lösungsansatz	Schwerwiegende Unterbrechungen in der Stromversorgung lassen sich durch einzelne Maßnahmen nicht zuverlässig verhindern. Zu diesem Zweck wurden in SINTEG, im Sinne einer Resilienzstrategie, vielfältige Maßnahmen sowohl innerhalb der IT- als auch der Netzinfrastruktur auf verschiedenen Ebenen untersucht, entwickelt und erprobt. Essenziell bei allen Maßnahmen ist jedoch die fortlaufende Identifizierung von Schwachstellen und Risiken sowie die fortlaufende Entwicklung von Maßnahmen sowohl gegen erwartete als auch unerwartete Bedrohungsszenarien. Da ein vollständiger Schutz gegen bspw. Cyber-Angriffe oder auch Softwarefehler zu keinem Zeitpunkt garantiert werden kann, muss die OT darüber hinaus gegen ITFehler abgehärtet und so gestaltet werden, dass die OT auch bei einem Ausfall der IT operativ bleiben kann.
Einordnung der Blaupause	Blaupause in der Kategorie „IKT-Systemqualität von Smart Grids“
Technologiereifegrad (Spektrum der Detail-Blaupausen)	1 2 3 4 5 6 **7 8** 9 Das TRL befindet sich je nach konkreter Maßnahme zwischen 7 und 8. Prototyp mit systemrelevanten Eigenschaften existiert und wird im Betriebsumfeld getestet.
Eingeflossene SINTEG-Aktivitäten	**enera** ■ Schwarzfallfähigkeit und QoS unterschiedlicher Technologien zur digitalen Konnektivität (z. B. 450-MHz-Funknetz) **DESIGNETZ** ■ Kompositionelle Sicherheitsarchitektur als Enabler für ein sicheres Plug-and-Play von Diensten ■ • Aufbau und Untersuchung der Eignung des 450-MHz-Funknetzes im Schwarzfall **sells** ■ Untersuchung der Insel- bzw. Schwarzstartfähigkeit der Zellen ■ Konzeption und Entwicklung einer blauen Ampelphase als erweiterter Betriebsmodus der Abstimmungskaskade (Inselnetzbetrieb) **NEW 4.0** **WINDNODE** ■ Studie zur Digitalisierung in der Energiewirtschaft (IT-Sicherheit und Resilienz im Energiekontext als Schwerpunktthema)
Innovationsgehalt	In SINTEG wurden, im Sinne einer Resilienzstrategie, vielfältige bestehende, aber auch neuartige Maßnahmen sowohl innerhalb der IT- als auch der Netzinfrastruktur auf verschiedenen Ebenen untersucht, entwickelt und / oder erprobt.
Bedingungen für die Übertragbarkeit und Skalierbarkeit	Flexibilität sowohl im Energie- als auch im IKT-System ist essenziell, um die Resilienz zu erhöhen. Weitere Faktoren sind Interoperabilität, Standardisierung, und Security- bzw. Resilience-by-Design als Entwicklungsparadigma. Dabei ist auch die Aufnahme der IKT in eine Resilienzstrategie und die Verfügbarkeit von Flexibilität zur Ableitung von Gegenmaßnahmen ein entscheidender Aspekt.

HINTERGRUND UND PROBLEMSTELLUNG

Die wichtigste Anforderung an das Stromversorgungssystem als kritische Infrastruktur (KRITIS) ist die Versorgungs- bzw. Ausfallsicherheit. Fällt die elektrische Energieversorgung aus, wird dieses schnell zu einer Belastungsprobe für Gesellschaft und Wirtschaft, denn alle anderen KRITIS hängen von einer stabilen Stromversorgung ab. Ist sie gestört, folgen bald darauf Probleme in den Bereichen Wasserversorgung und -entsorgung, Transport, Gesundheitswesen oder IKT (vgl. Mayer et al., 2021). Bislang konnte diese Sicherheit unter Berücksichtigung des N-1-Prinzips durch eine redundante Auslegung der Systemlandschaft bzw. der elektrotechnischen Komponenten im Bereich von Stromnetzen, Umspannwerken oder Kraftwerken erreicht werden. Angesichts der Herausforderungen der Energiewende bzw. der zunehmenden Dezentralisierung sind erhebliche Anstrengungen erforderlich; die durch das N-1-Kriterium geschaffene Sicherheit stößt im Zuge der IT/OT-Konvergenz zunehmend an ihre Grenzen.

Während für die Resilienzstrategie des traditionellen Energiesystems bisher „lediglich“ Störereignisse des Energiesystems von Bedeutung waren, erzwingt die aus der aktuellen IT/OT-Konvergenz resultierende Transformation zu einem Cyber-physischen Energiesystem (CPES) neue Betrachtungsweisen. Aufgrund der wechselseitigen Abhängigkeiten zwischen der IT und der OT ist die zusätzliche Betrachtung der IKT ein entscheidender neuer Baustein für das CPES. Obwohl der Einsatz von IKT das Energiesystem in die Lage versetzt, autonom und in beinahe Echtzeit auf Störereignisse reagieren zu können, öffnet diese auch neue Gefahren, welche durch das klassische N-1-Prinzip nicht abgedeckt werden. Wie in Abbildung 19 dargestellt, kann der Ausfall der IKT zu einem Verlust der Überwachung sowie Steuerbarkeit führen; allerdings auch wieder entscheidend zur „System Restauration“ beitragen (vgl. WindNODE, 2021).

Basiert das Systemdesign der elektrotechnischen Komponenten auf der Annahme einer stetige Verfügbarkeit oder eines stetig korrekten Verhaltens der IKT, wird sich das Energiesystem ohne entsprechende Resilienzstrategie bzw. -maßnahmen nicht ausreichend gegen einen Ausfall, eine Manipulation oder ein Fehlverhalten schützen können. Aufgrund der unmittelbaren Wechselwirkung stoßen die in der Vergangenheit bewährten und vorrangig auf Robustheit setzenden Konzepte (»fail-safe«) zunehmend an ihre Grenzen, sodass der Cyber-Resilienz (»safe-to-fail«) eine Schlüsselrolle zukommt. So muss das elektrische Energiesystem in die Lage versetzt werden, auf unvorhergesehene Störungen so zu reagieren, dass es seine Grundfunktionalität stets aufrechterhalten bzw. selbstständig wiedererlangen kann, so dass sich die Folgen etwaiger Störungen auf einen Minimalschaden beschränken.

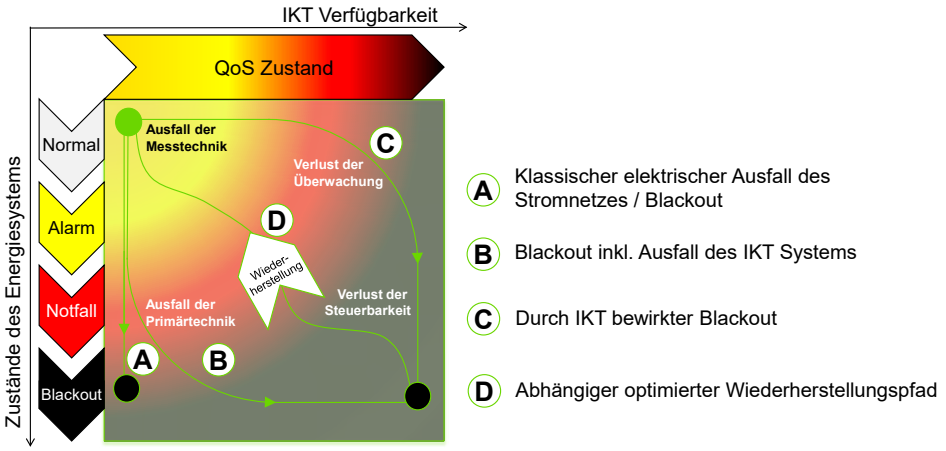

Abbildung 19 Resilienz und Cyber-Resilienz in der Stromversorgung (vgl. Fischer, 2018, WindNODE, 2021)

BISLANG ERREICHTER KENNTNIS- UND ENTWICKLUNGSSTAND

Schwerwiegende Unterbrechungen in der Stromversorgung lassen sich durch einzelne Maßnahmen nicht zuverlässig verhindern, sondern im Rahmen einer Resilienzstrategie nur durch ein Paket von vielfältigen Maßnahmen auf unterschiedlichen Ebenen. Bausteine einer solchen Strategie können sein:

1. Wechselwirkung IT und OT verstehen und lenken
2. Cyber-Sicherheit systemisch entwickeln
3. Technische Resilienz durch Netzbetreiber und Netznutzer stärken
4. IKT-Integration kleiner Anlagen netzdienlich gestalten

Unabhängig von den konkreten Maßnahmen ist jedoch - analog zum PDCA-Zyklus - eine fortlaufende Identifizierung von Schwachstellen und Risiken sowie Entwicklung von Maßnahmen sowohl gegen erwartete als auch unerwartete Bedrohungsszenarien essenziell. Dabei muss das Stromversorgungssystem in die Lage versetzt werden, auf unvorhergesehene Störungen so zu reagieren, dass es seine Grundfunktionalität aufrechterhalten oder zumindest selbstständig wiedererlangen kann, um die Folgen von Störungen so gering wie möglich zu halten. So sind zu diesem Zweck bspw. Maßnahmen für die Schwarzstartfähigkeit (vom Strom und IKT-Netz unabhängiges Hochfahren von Anlagen), für den Schwarzfall (vom Stromnetz unabhängig funktionierende IKT) sowie von der IT unabhängige Betriebsmodi (z. B. im Fehlerfall) der OT erforderlich. Die OT sollte so gestaltet sein, dass diese auch bei einem Ausfall der IT funktionsfähig bleiben kann – Resilience-By-Design.

Zu diesem Zweck ist es unabdingbar, die IKT als integralen Bestandteil des Stromsystems zu verstehen und die Potenziale der Digitalisierung zur Erhöhung der Resilienz voll auszuschöpfen.

IN SINTEG AUFGEZEIGTE LÖSUNGSANSÄTZE UND ERKENNTNISSE

Resilienz ist das Resultat vielfältiger Einzelmaßnahmen. Allgemein gefasst lässt sich die IKT-technische Erschließung von Flexibilitäten sowie alle dazugehörigen übergeordneten Aktivitäten der Referenzarchitekturentwicklung, IT-Sicherheit sowie Standardisierung und Interoperabilität als ein Aspekt der Resilienzstrategie bezeichnen – Resilienz ist ein inhärentes Ziel aller Maßnahmen der SINTEG-Aktivitäten. Dies bedeutet, dass bereits die IKT-technische Erschließung von Flexibilitätspotenzialen bzw. alle sektorkoppelnden Maßnahmen die Flexibilität und damit auch die Resilienz des elektrischen Energiesystems sowie damit einhergehend den Handlungsspielraum bei Engpässen erhöht. Über die (innerhalb der vorgelagerten Blaupausen und bereits genannten) Aktivitäten hinaus wurden in den Schaufenstern jedoch folgende weiterführende Aspekte als konkrete resilienzsichernde Maßnahmen beleuchtet:

- **DESIGNETZ:** Als ein Baustein einer Resilienzstrategie ermöglicht die Implementierung der DESIGNETZ-Datenkaskade bzw. deren Sicherheitsarchitektur mit SUCH, Sonata, IND2UCE und Separierungsmechanismen eine erstmalige kompositionelle Vorgehensweise in Bezug auf das Änderungsmanagement und die dazugehörige Zertifizierung (CC EAL 4) und somit ein Plug-and-Play von Diensten, ohne dass bei Änderungen jeweils eine erneute Zertifizierung der Gesamtplattform durchgeführt werden muss (vgl. DESIGNETZ,

2021a). Neben einer Kostenreduzierung, durch den Wegfall von zeitintensiven Zertifizierungsprozessen, wird durch die verkürzten Reaktions- bzw. die Fehlerbehebungszeiten der IKT zur Systemstabilität beigetragen. Des Weiteren nutzt die Sicherheitsarchitektur unter anderem ein innovatives Rollen- und Rechtemanagement und erlaubt eine übergeordnete Nutzungskontrolle als zusätzlichen Sicherheitsmechanismus für die Services.

- **enera:** Neben vielfältigen entwickelten Security-By-Design-Methoden bzw. sogenannten Lösungselementen, wie den „Anpassungen des Use Case-Templates hinsichtlich Security-by-Design“ als ein ganzheitliches ISMS-Konzept sowie „Assurance Cases als Leitfaden für die Use Case-Erhebung“ als eine weitere Erweiterung der IEC 62559-Methodik, wurde in enera die digitale Konnektivität unter Berücksichtigung unterschiedlicher Technologien, wie etwa LTE oder CDMA-450-MHz in Hinblick auf die Datenrate, Latenzzeiten, Abdeckung, Kosten sowie Schwarzfallfestigkeit, systematisch analysiert und zur Bestimmung des Technologie- und Hardwarebedarfs gegenübergestellt (vgl. enera, 2021b).

- **C/sells:** Analyse, Entwicklung und Demonstration von Ansätzen zur Erweiterung des Ampelkonzeptes, insbesondere hinsichtlich der roten Ampelphase, um die Systemstabilität und Versorgungssicherheit in zellulären Systemen stützen zu können. Dabei wurden (u. a.) Aspekte einer koordinierten Inselnetzbildung sowie Resynchronisation als Sonderfall der Subnetzsteuerung in der roten Ampelphase untersucht und eine sogenannte „blaue“ Ampelphase als ein erweiterter Betriebsmodus für die Abstimmungskaskade zum Zwecke der Systemrestrauration im Rahmen eines Inselnetzbetriebs eingeführt (vgl. C/sells, 2021a).

- **WindNODE:** Im Rahmen einer von WindNODE durchgeführten Digitalisierungsstudie (vgl. WindNODE, 2021) wurde Resilienz und deren Bedeutung im Rahmen der IT/OT-Konvergenz ausführlich beleuchtet. Weiterhin wurde analog zu enera eine IEC 62559-basierte Gesamtmethodik zur Analyse und Beschreibung von Gefährdungsszenarien sowie rechtlichen Rahmenbedingungen entwickelt, angewendet und ebenfalls im Rahmen der Digitalisierungsstudie veröffentlicht.