DIV | Deutschland intelligent vernetzt

Digital Gipfel

Dossier Ü-1

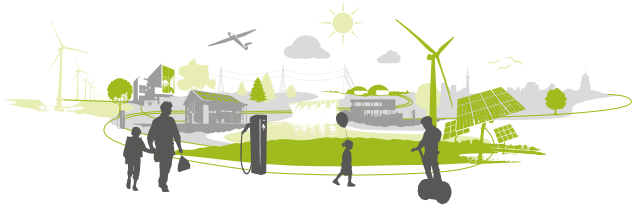
Digitalisierung des Energiesystems

Robust und Resilient

Nationaler Digital-Gipfel | Plattform Innovative Digitalisierung der Wirtschaft
Fokusgruppe Intelligente Vernetzung
Dossier der Expertengruppe Intelligente Energienetze

Digital-Gipfel
Plattform Innovative Digitalisierung der Wirtschaft
Fokusgruppe Intelligente Vernetzung

www.deutschland-intelligent-vernetzt.org



1. Zielbild

Jahr 2023
Die Digitalisierung des Energiesystems schreitet unaufhaltsam voran. Das Gesetz zur Digitalisierung der Energiewende und die Erweiterungen des Energiewirtschaftsgesetzes haben daran wesentlichen Anteil, aber auch viele Entwicklungen, die nicht durch Gesetzgebung oder Regulierung vorangetrieben werden. Dies hat viele Möglichkeiten der Effizienz geschaffen, aber auch dazu beigetragen, dass das zunehmend komplexe Energiesystem resilient, robust und zuverlässig bleibt. Damit die Verbesserungen durch die Digitalisierung die Risiken deutlich aufwiegen, wird ein Maßnahmenpaket umgesetzt, das deutlich über heutige eher unternehmensorientierte Security hinausgeht, und wirtschaftliche als auch technologische Effizienz wahrt.

Definitionen:
- Robust: Ein System heißt robust, wenn Störereignisse keinen Einfluss auf die Servicequalität haben.
- Resilienz: Ein System ist resilient, wenn Störauswirkungen unerwarteter Ereignisse gering bleiben und beseitigt werden.
- Zuverlässig: Zuverlässigkeit bedeutet, dass definierte Grenzwerte für die Servicequalität im Normalbetrieb nicht verletzt werden.

2. Kurzbeschreibung

Damit das Energiesystem den steigenden Herausforderungen gerecht werden kann, sind Ausbau und Optimierung der bisherigen Abstimmungs- und Steuerungsprozesse auch von IKT-Systemen erforderlich. Die Resilienz des zukünftigen Energiesystems steht und fällt mit der intensiven Digitalisierung der Funktionen zur Systemstabilisierung und der Erschließung zusätzlichen Potenzials zur Systemstabilisierung durch Digitalisierung. Zuvor unabhängige IT-Komponenten des Energiesystems müssen immer enger miteinander vernetzt werden.

Auf der anderen Seite steigt die Bedrohungslage im IT-Bereich, sei es durch neue und technologisch zunehmend anspruchsvollere Angriffe oder durch neue Akteure. Auch das „Internet of Things“, also eine Welt, in der allein in Europa viele Milliarden von Sensoren, Geräten und Gegenständen mit dem Internet verbunden sind[1], sowie völlig automatisierte Transaktionen (vgl. Blockchain) werden von vielen als mögliche Bedrohungen des Energiesystems angesehen.

Trotz dieser Einflüsse muss das Energiesystem resilient gehalten werden[2]. Die Störauswirkungen unerwarteter Ereignisse müssen gering bleiben und beseitigt werden. Gleichzeitig muss die *Robustheit* gewährleistet werden: Bekannte Störereignissen dürfen die Versorgungsqualität nicht beeinflussen.

Die Durchführung von Maßnahmen in intelligenten Energienetzen, etwa für einen Wiederaufbau des Stromsystems nach einer Großstörung[3], beruht auf vielen Einzelmaßnahmen, die über Kommunikationsnetze koordiniert werden müssen. Auch wenn die Kommunikationsanbindung verloren geht, muss die Digitalisierung etwa durch lokale Intelligenz noch in der Lage sein, stabilisierende Funktionen situationsangepasst auszuführen. Da die Richtlinien für einen

1 https://www.gartner.com/newsroom/id/3598917
2 https://energiesysteme-zukunft.de/fileadmin/user_upload/Publikationen/pdf/ESYS_Stellungnahme_Das_Energiesystem_resilient_gestalten.pdf
3 https://www.iee.uni-rostock.de/fileadmin/uni-rostock/Alle_IEF/IEE/Publikationen_EEV/Wiederaufbau_von_Uebertragungsnetzen_nach_Grossstoerungen.pdf

Systemwiederaufbau aus den dezentralen Systemen heraus heute noch unklar sind, ist es notwendig, IT-Security-Vorgaben so zu implementieren, dass die nötige Flexibilität gewahrt bleibt, um neue Anforderungen aus der Resilienz zügig umzusetzen.

Folgende Anforderungen an die IT-Security für die kritische Infrastruktur „digitalisierte Energieversorgung" werden auch im Kontext fehlertoleranten IKT-Systeme heute noch nicht ausreichend berücksichtigt:

- „Gehackte" IT-Systeme im Energiesystem müssen in Teilen kontinuierlich in Betrieb bleiben können. Dies erschwert Fehlerbehebung und Analyse.
- Exzellente Abwehrmechanismen reichen nicht aus. Auch erfolgreiche Angriffe dürfen das Energiesystem möglichst wenig beeinflussen.
- Das Energiesystem ist hochvernetzt. Daher sind bei Security-Maßnahmen immer auch die systemischen Auswirkungen zu berücksichtigen. Die Verantwortung kann daher nicht allein bei den einzelnen Akteuren wie etwa Netz- und Anlagenbetreibern liegen.
- Auch IT-Systeme, die auf den ersten Blick mit dem Netzbetrieb nichts zu tun haben (z. B. Markt- und Handelssysteme) können durch Manipulationen zu Versorgungsstörungen beitragen.
- Auch Fehlbedienungen, mangelnde Datenqualität oder Fehler bei der Softwareinstallation können zu Blackouts beitragen[4, 5].
- Security by Design muss schon im Produktentwicklungsprozess fest verankert sein
- End-to-End-Security ist zwingend beim Systemdesign zu berücksichtigen (z. B. ISMS).

3. Diskussionsperspektiven
Verringert oder erhöht Digitalisierung die Bedrohungslage?

Pro: Digitalisierung ist unverzichtbar für Resilienz

Die Resilienz des Energiesystems stützt sich schon heute ganz wesentlich auf die Digitalisierung. So benötigen Netzbetreiber eine genaue Kenntnis und Prognose des Netzzustandes, um in kritischen Situationen Maßnahmen untereinander abzustimmen. Ein zunehmender Automatisierungsgrad sorgt dafür, dass die Netzführung trotz steigender Komplexität sicher verläuft. Maßnahmen wie etwa das Einspeisemanagement sind ohne Digitalisierung nicht möglich. Da zunehmend die Dynamik in den Verteilnetzen das Systemverhalten bestimmt, müssen also auch Möglichkeiten geschaffen werden, den Systemzustand genau zu messen, zu prognostizieren und steuernd einzugreifen. Dies geht nur mit einem massiven Ausbau der Digitalisierung. Langfristig muss es sogar möglich sein, nach einem Blackout das Stromsystem aus den Verteilnetzen wieder hochzufahren. Dazu sind besonders viele Informationen notwendig, die dann IKT-Systeme für die Koordination der Netze und Anlagen nutzen müssen – diese IKT-Systeme müssen also auch bei Blackouts noch ausreichend funktionsfähig sein. Wie zentral oder dezentral ein Systemwiederaufbau zukünftig koordiniert sein wird und wie die Richtlinien dazu aussehen werden, ist heute noch unklar und braucht dementsprechende Forschungsprojekteund Rahmensetzung.

Diese neuen und IT-basierten Kommunikationsprozesse ermöglichen darüber hinaus neue Konzepte und Vorgehensweisen, um das Energiesystem der Zukunft noch widerstandsfähiger gegenüber externen Einflüssen (plötzliche Schwankungen auf der Erzeugungsseite oder im Verbrauch, Angriffe auf zentrale/vitale Komponenten) zu gestalten. Das Energiesystem der Zukunft sollte ohnehin im Vergleich zu heute ein höheres Maß an Resilienz aufweisen, um die steigende Anzahl an Akteuren sowie Abstimmungsvorgängen zu berücksichtigen.

4 https://www.computerworld.com/article/2573466/disaster-recovery/software-failure-cited-in-august-blackout-investigation.html
5 http://fm4v3.orf.at/stories/1717900/index.html

Contra: Digitalisierung schafft durch neue Risiken zu große Ungewissheit

Der Ukraine-Vorfall 2015[6] hat gezeigt, dass sich ein Energiesystem erfolgreich angreifen lässt. Die Hacker sorgten für einen mehrstündigen Stromausfall für mehrere hunderttausend Haushalte und Unternehmen. Vermutlich wäre es den Angreifern möglich gewesen, einen noch viel größeren Schaden zu produzieren. Viele Staaten, u. a. auch Deutschland planen, digitale Angriffswerkzeuge zu entwickeln oder versuchen gar, Hersteller von IKT-Systemen zum Einbau „Backdoors" zu verpflichten. Da diese in die Hände von böswilligen Angreifern gelangen können (wie bereits bei Wannacry passiert), wird dadurch ein bisher nicht absehbares Risiko für die kritische Energieinfrastruktur geschaffen.

Die erwartete umfangreiche Digitalisierung des Energiesystems schafft eine ganz neue Komplexität. Viele Angriffs-, Bedrohungs- und Fehlerszenarien sind heute noch gar nicht bekannt. Dies macht es schwer, die Risiken der Digitalisierung zuverlässig einzuschätzen. Viele Maßnahmen zur Gewährleistung der Resilienz müssen national oder gar supranational koordiniert und standardisiert werden, da in einem verbundenen Energiesystem und europaweiten Märkten Auswirkungen von Störungen nicht regional begrenzt sind. Nicht zuletzt wird neues und umfangreiches Know-How verlangt, dass in der Regel bei kleineren Akteuren (etwa Betreiber von Verteilnetzen, virtuellen Kraftwerken oder Windparks) nicht vorgehalten werden kann.

4. Handlungsempfehlungen

Um das Zielbild eines zunehmend digitalisierten und dennoch robusten sowie resilienten Energiesystems zu erreichen, sollten folgende Maßnahmen umgesetzt werden:

1. Es gilt Lösungsansätze für die anstehenden Herausforderungen zu erarbeiten und das Spektrum an negativen Seiteneffekten zu erschließen. Hierfür eignen sich F&E-Projekte, da Erprobungen in den Kritischen Infrastrukturen nicht möglich sind. Ebenfalls bieten Forschungsprojekte den Rahmen, um neue Ansätze und IKT-Systeme in die bestehenden Verfahren der Marktakteure zu integrieren, ohne dabei die Versorgungssicherheit zu gefährden. Ein erforderlicher Schwerpunkt ist die Bewertung von vorhandenen Systemen und Prozessen vor dem Hintergrund einer zunehmenden Digitalisierung, um die Robustheit in den kommenden Jahren sicherzustellen. Eine besondere Rolle spielen CyberResilienz-Labore, in der sich die Wechselwirkung von IKT und Energiesystem realitätsnah experimentell testen lässt. Diese Laborinfrastruktur ist vorrangig auf- und auszubauen.
2. Der IT-Fachkräftemangel verhindert flächendeckend die effektive Implementierung und Umsetzung von IT-Sicherheitsmaßnahmen. Deshalb müssen neue Ausbildungsinitiativen und zielgerichtete Lernmodule in Zusammenarbeit mit Bildungsträgern sowie der Industrie geschaffen werden.[7]
3. Da das Energiesystem supranational ist, können auch Angriffe durch Cybercrime, Cyberterrorismus und Cyberspionage nur international, fernab nationaler Grenzen bekämpft werden. Deshalb müssen zeitnah internationale, auf Freiwilligkeit basierende Netzwerke sowie Kooperationen mit allen Akteuren der staatlichen, wissenschaftlichen und industriellen Ebenen geschaffen werden.[8]

6 http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

7 Aus: Pressemitteilung Cyber-Sicherheitsrat Deutschland e. V. vom 26.1.2018

8 https://ec.europa.eu/energy/en/news/new-report-cyber-security-energy-sector-published

4. Für Politik und Regulierungsbehörden gilt es diese Prozesse zu unterstützen. Dies bedeutet vor allem auch bestehende Regelungen und regulatorische Vorgaben vor dem Hintergrund einer zunehmenden Digitalisierung zu bewerten.
5. Darüber hinaus ist die Förderung eines Bewusstseins aller Marktakteure für ein „digitalisiertes Energiesystem“ und den damit verbundenen IT-Risiken erforderlich. Möglich ist dies über einen Informations- und Wissensaustausch zwischen allen Akteuren, um ein hohes Verständnis für das Gesamtsystem auf allen Ebenen zu erhalten und damit einhergehend eine hohe Lösungskompetenz zu gewährleisten. Die bisherigen nationalen Abstimmungen in den unterschiedlichen Arbeitskreisen zu KRITIS sind um einen zusätzlichen, offenen und internationalen Informationsaustausch zu ergänzen. Hierbei ist zu prüfen, wie eine internationale Vernetzung durch z. B. supranationale Gremien umgesetzt werden kann. Schließlich sind andere Länder im Bereich digitalisierter Versorgungsnetze bereits weiter fortgeschritten. Deutschland könnte von den Erfahrungen profitieren.

Alle Dokumente
und Publikationen
kostenlos zum Download:

www.deutschland-intelligent-vernetzt.org

5. Referenzen

- acatech – Deutsche Akademie der Technikwissenschaften / Nationale Akademie der Wissenschaften Leopoldina / Union der deutschen Akademien der Wissenschaften (Hrsg.): Das Energiesystem resilient gestalten. Maßnahmen für eine robuste Versorgung (Schriften reihe zur wissenschaftsbasierten Politikberatung), 2017
- Krüger, M., H. Weber, W. Franke, R. Kirsch: Wiederaufbau von Übertragungsnetzen nach Großstörungen, VDI/VDE: 9. GMA/ETG-Fachtagung „Netzregelung und Systemführung“, 2008, München
- D. Verton: Software failure cited in August blackout investigation, 2003
- Blackout-Gefahr in Österreichs Stromnetzen
- E-ISAC/Sans: Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Grid, 2016
- Aus: Pressemitteilung Cyber-Sicherheitsrat Deutschland e. V. vom 26.1.2018
- EECSP Report: Cyber Security in the Energy Sector, 2017

Ansprechpartner

Christian Bruns (BTC)
Dr. Christoph Mayer (OFFIS)
Dr. Michael Stadler (BTC)

Herausgeber

Fokusgruppe Intelligente Vernetzung
im Nationalen Digital-Gipfel /
Expertengruppe Intelligente Energienetze