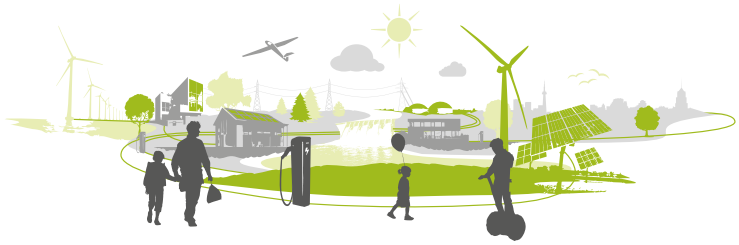
DIV | Deutschland intelligent vernetzt

Digital Gipfel

Intelligente Energienetze in Krisensituationen: Lessons learned und Handlungsempfehlungen für mehr Resilienz

Positionspapier der Expertengruppe Intelligente Energienetze



Digital-Gipfel
Plattform Innovative Digitalisierung der Wirtschaft
Fokusgruppe Intelligente Vernetzung

www.deutschland-intelligent-vernetzt.org

Die aktuelle Pandemie-Situation stellt eine bislang nicht gekannte Herausforderung für die Betreiber kritischer Infrastrukturen dar. Es gilt, die im internationalen Vergleich sehr hohe Zuverlässigkeit, Versorgungssicherheit und Qualität der Daseinsvorsorge auch weiterhin zu gewährleisten. All das unter Rahmenbedingungen, die den klassischen Betrieb deutlich erschweren. Vor diesem Hintergrund ergibt sich eine Fülle an Erkenntnissen und Erfahrungen, wie der Betrieb auch in Krisensituationen sichergestellt werden kann und welchen wachsenden Stellenwert das Thema Digitalisierung hierbei einnimmt. Es gilt, diese Erkenntnisse aus Sicht der intelligenten Energienetze zusammenzutragen, zu bewerten und daraus Handlungsempfehlungen abzuleiten. Insbesondere für die Digitalisierung der kritischen Infrastrukturen ergibt sich aus Sicht der Expertengruppe eine große Chance.

Verteilnetzbetreiber versorgen auch während der Pandemie zuverlässig mit Strom

Verteilnetzbetreiber müssen auch während der COVID-19-Pandemie den sicheren und zuverlässigen Betrieb der Netze gewährleisten und dabei gleichzeitig das Infektionsrisiko für Kund:innen und Mitarbeiter:innen minimieren. Als Betreiber kritischer Infrastruktur mit entsprechender gesellschaftlicher Verantwortung verfügen sie über ein etabliertes Störungs-, Notfall- und Krisenmanagement. Dennoch stellt die Pandemie auch sie vor massive Herausforderungen, wie etwa das Risiko des Ausfalls von betriebskritischem Personal sowie untypische Effekte in den Stromnetzen durch schwankende Produktionstätigkeiten in der Industrie oder vermehrte Heimarbeit. Durch das konsequente Umsetzen von angepassten Krisenplänen und neu entwickelten Maßnahmen konnten sich die Unternehmen diesen Herausforderungen bislang erfolgreich stellen.

So wurden etwa

- ein regelmäßiger Austausch zwischen allen relevanten Stakeholdern organisiert,
- die Kontakte durch weitgehend mobiles Arbeiten der Belegschaft aus dem Home-Office reduziert,
- die Teams in den Betriebsführungseinheiten verkleinert und Durchmischung verhindert, sodass komplette Ersatzteams auf Abruf bereitgehalten und eine unkontrollierte Verbreitung im Infektionsfall vermieden werden konnten und
- Konzepte zur „Kasernierung“ erarbeitet, um die Teams der Leitzentralen für den Fall einer erhöhten Infektions- und Gefährdungslage arbeitsfähig abzuschotten,
- die Voraussetzungen für das mobile Arbeiten verbessert, indem Kollaborationstools wie Office365, Zoom & Co. ergänzend eingeführt und die Mitarbeiter:innen in deren Anwendung geschult wurden,
- seitens der IT-Security der Unternehmen auf die geänderten Rahmenbedingungen reagiert und Vorgaben für das mobile Arbeiten sowie bestimmte Sicherheitsmaßnahmen angepasst (Anpassung von Prozessen, Freigabe neuer Hard-/Softwareprodukte, Einführung Multifaktorauthentifizierung, etc.)
- die IT-Infrastruktur wo nötig aufgerüstet, um eine hohe Performance für die Zugriffe der Mitarbeiter:innen aus dem Homeoffice sicherzustellen (VPN, SharePoint, energiewirtschaftliche Spezialanwendungen etc.)[1]

1 vgl. „Die Lage der IT-Sicherheit in Deutschland 2020“, Bundesamt für Sicherheit in der Informationstechnik (BSI) 2020, S.33 ff. Abgerufen am 30.09.2021 unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2#%5B%7B%22num%22%3A114%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22Fit%22%7D%5D

Lessons Learned: Digitalisierung stärkt Resilienz der Netze

Die vergangenen Monate zeigen, dass insbesondere die Digitalisierung einen wertvollen Beitrag leistet, die oben benannten Risiken zu beherrschen. Darüber hinaus ist zu erwarten, dass die Pandemie die Bereitschaft für digitale Zusammenarbeit sowie den routinierten Umgang mit digitaler Kundenkommunikation stärken wird und viele Aspekte der entwickelten digitalen Arbeitsabläufe zum „neuen Normal“ werden. Viele Netzbetreiber haben hierauf reagiert und in ihre IT-Infrastruktur sowie die IT-Ausstattung ihrer Mitarbeiter:innen investiert und gerade auch technische Mitarbeiter:innen hinsichtlich ihrer digitalen Kompetenzen konsequent weitergebildet.

In diesem Zusammenhang tritt immer deutlicher zutage, dass IKT und physikalische Netzinfrastrukturen nicht mehr getrennt voneinander gedacht werden dürfen. Beide verschmelzen zu einem integrierten Gesamtsystem, das erst in Summe die notwendigen Resilienzeigenschaften aufweist. Auf diesen Umstand hin ist auch die Betriebsüberwachung der Netze auszulegen: Sowohl der physikalische Netzzustand als auch der Zustand der Informations- und Kommunikationssysteme und -netze müssen gemeinsam gemonitort werden, sodass im Fall von Störungen im Bereich der IKT durch die Betriebsführung zeitnah reagiert werden kann.

Gerade durch den Anstieg des Anteils der Erneuerbaren Energien an der Stromerzeugung und der damit verbundenen Steigerung der Komplexität im Energiesystem haben sich die Herausforderungen im Netzbetrieb erhöht. Die Erfahrungen der Netzbetreiber mit diesem Szenario zeigen erneut, dass die Digitalisierung der kritischen Infrastruktur der Energieversorgung ein wichtiger Schlüssel zum Gelingen der Energiewende ist. Denn die hohe Versorgungssicherheit ist nicht selbstverständlich und gerade die aktuelle Situation erfordert große Anstrengungen und innovative Lösungen. Um diese Lösungen in den Netzen mit den erforderlichen Sicherheitsmechanismen umzusetzen, müssen zudem IT, IT-Security und OT (Operations Technology) eng zusammenarbeiten. Cyberangriffe wie der auf die Colonial Pipeline in den USA haben die Verwundbarkeit digital betriebener Infrastrukturen verdeutlicht. Konsistente, unternehmensübergreifende Sicherheitskonzepte für die Energienetze sind dabei genauso unerlässlich wie Systeme zur Angriffserkennung und -vermeidung.

Handlungsempfehlungen

- Die **Unterstützung durch die politischen Akteure** bei der Digitalisierung der Energienetze ist **auf unterschiedlichen Ebenen erforderlich**. Zum einen müssen die **rechtlich-/regulatorischen Rahmenbedingungen** eine **Refinanzierung** der oben genannten Anstrengungen ermöglichen.

- Darüber hinaus muss der Status quo in flankierenden Bereichen verbessert werden. So müssen durch **passende Gesetze** neue, **flexiblere Formen des Arbeitens ermöglicht** bzw. **noch stärker gefördert** werden.

- Daneben gilt es, allgemein anerkannte Problemfelder der Digitalisierung in Deutschland mit Nachdruck anzugehen. Als Beispiel seien hier der **Breitbandausbau im ländlichen Raum** und eine **flächendeckende Mobilfunkabdeckung** genannt. Die weiterhin unzureichende Umsetzung beider Themen führt zu teils erheblichen **Herausforderungen** seitens der Netzbetreiber zur **Absicherung der relevanten Betriebsprozesse** an den oft im ländlichen Raum gelegenen **Betriebsstandorten**.

- Die **Betriebsstandorte** sind auch gegen in der Zukunft verstärkt eintretende **extreme Umwelteinflüsse** (z. B. Starkregenereignisse wie im Ahrtal) noch **besser zu schützen**. In diesen Punkten muss Deutschland aufholen, wenn die notwendige Digitalisierung der Energienetze nicht ausgebremst werden soll.

- Die zunehmenden Herausforderungen und Chancen im Bereich der Digitalisierung, wie z. B. **mobiles Arbeiten, Fernsteuerung und -wartung von (Netz-) Infrastruktur und Cybersicherheit**, erfordern eine zunehmende **Weiterbildung der Mitarbeiter:innen**. Gleichzeitig sind entsprechende **Methoden, Werkzeuge und Schulungsinhalte** (weiter) zu entwickeln.

- Gemeinsame Aufgabe muss es sein, ein entsprechendes **Bewusstsein für die zunehmende Bedeutung** dieser Bereiche **in der Öffentlichkeit** zu schaffen bzw. noch stärker zu verstetigen.

- Zur Steigerung der **Resilienz der Energieversorgung** können stärker als bisher die **Vorteile von verteilten Energieerzeugungsanlagen aktiviert** werden. **Netzstützende und netzbildende Funktionalität** von **dezentralen Erzeugern und Speichern** erlauben bei Störungen des Gesamtsystems eine lokale Versorgung. Der operative Aufwand eines kleinteiligen Systems muss durch **Automatisierung** und eine **Stärkung der unteren Regelungshierarchien** kompensiert werden[2].

2 vgl. Resilienz digitalisierter Energiesysteme. Blackout-Risiken verstehen, Stromversorgung sicher gestalten. Ch. Mayer, G. Brunekreeft (Hrsg.), Acatech Schriftenreihe, Feb. 2021, abgerufen am 12.10.2021 unter https://www.acatech.de/publikation/rde-analyse/

Alle Dokumente
und Publikationen
kostenlos zum Download:

www.deutschland-intelligent-vernetzt.org

Digital Gipfel

Positionspapier der Expertengruppe
Intelligente Energienetze
Fokusgruppe Intelligente Vernetzung

November 2021

Herausgeber
Digital-Gipfel
Plattform Innovative Digitalisierung der Wirtschaft

Ansprechpartner
Dr. Andreas Breuer
Westnetz GmbH
andreas.breuer@westnetz.de

www.deutschland-intelligent-vernetzt.org