Schutzebenen der Kernenergieversorgung und Verteil- und Übertragungsnetzsysteme

- Abstrakt –

Ph. Lc. Thomas Riehl, 10.10.2025

Die Energieversorgung, insbesondere die Stromversorgung, ist ein komplexes Netzwerk aus Erzeugung, Transformation und Wandlung, das kontinuierlich abläuft und lediglich durch die natürlichen Ressourcen der jeweiligen Regionen begrenzt wird. In jüngerer Zeit rücken zentrale Energieerzeuger und ihre Transportwege verstärkt in den Fokus feindlich gesinnter Akteure, seien es Einzeltäter, Terrorgruppen oder Staaten mit gegensätzlichen Interessen. Die Verwundbarkeit souveräner Staaten wird durch aktuelle Konflikte besonders deutlich. Die gezielte Zerstörung von Energieanlagen kann als Druckmittel gegen die staatliche Souveränität, die notwendige Ökonomie und Wirtschaft sowie die Bevölkerung eingesetzt werden. Besonders kritisch ist die Bedrohung von Atomkraftwerken aber auch ihrer Infrastrukturwege, den sogenannten Übertragungs- und Verteilnetzen. Diese Anlagen gepaart mit der Verteilung der elektrischen Energie verursachen nicht nur gravierende Ausfallrisiken, sondern bergen durch atomare Sprengkraft und langfristige Verseuchung Gefahren mit einer Wirkung über Jahrhunderte. Etliche staatliche wie nicht staatliche Organisationen sind seit Jahrzehnten damit beschäftigt Konzepte zu entwickeln, welche die zentrale und dezentrale Versorgungsstrukturen intelligent koppeln können, um Ausfallraten in Krisen- und Kriegszeiten zu minimieren. Vor diesem Hintergrund stellt sich die Debatte oft in den Raum, das die Energieversorgung nicht ohne konkrete Sicherheits- und Investitionskonzepte dauerhaft sicherzustellen ist. Als Schlüsselfaktor für diese These, gelten Umspannwerke der Übertragungs- und Verteilnetzbetreiber in westlichen Staaten. Diese können derzeit zwar durch effiziente militärische Schutzmaßnahmen wie den Rheinmetall C-UAS Jammer (Rheinmetall, n.d.) physisch gesichert werden. Parallel dazu werden Cyber- und Automatisierungssicherheit auf IT- und OT-Ebene durch mehrschichtige Schutzmechanismen implementiert und gewährleisten einen sicheren Softwarebetrieb. (CNAS, 2025) Das erforderliche Schutzniveau richtet sich jedoch nach Art und Größe des Versorgungsgebiets sowie der ganzheitlichen Versorgungssicherheit eines Bundesstaates und seiner Landesintegrität.

Investitionen in die Energieinfrastruktur müssen sowohl aus Bundesmitteln, Steuergeldern und Gewerbeeinnahmen als auch durch private Investoren getragen werden. Die Rolle der Investierenden wird oftmals mittels eines induktiven, qualitativ interpretativen Forschungsansatzes untersucht, bei dem Fallstudien und die Delphi-Methode zum Einsatz kommen. (Wojciech, 2024) Ziel ist es, differenzierte Erkenntnisse zu komplexen Zusammenhängen zu gewinnen. Grundsätzlich führen Angriffe auf Instrumentierungs- und Kontrollsysteme (I&C) in Kernkraftwerken zu Systemfehlern außerhalb zulässiger Betriebsparameter. Daher muss ein mehrstufiges Schutzkonzept („Defence in Depth“, DiD) implementiert werden. (IAES, 2021) Dabei sind auch nicht-computerisierte Systeme zur Risikominderung bei Cyberangriffen zu berücksichtigen. Die Anwendung von Computer-Sicherheitsprinzipien auf I&C-Systeme dient der Erfüllung sicherheitsrelevanter Anforderungen und minimiert zukünftige Nachrüstungen – ein Aspekt mit erheblicher wirtschaftlicher Bedeutung. Das Sicherheits-DiD gliedert sich dabei in unabhängige Systemebenen mit unterschiedlichen Funktionen zur Verhinderung von Ausfallfortschritten. Physische Trennung und Unabhängigkeit sollen verhindern, dass einzelne Systemausfälle sicherheitsrelevant werden. Die Computer-Sicherheit fokussiert sich traditionell auf Vertraulichkeit, Integrität und Verfügbarkeit. Dabei wird häufig ein abgestuftes Sicherheitsniveau angewandt, wobei kritische Funktionen höhere Schutzmaßnahmen erhalten. Die Delphi-Methode dient als strukturiertes Verfahren zur systematischen Erhebung und Konsolidierung von Expertenmeinungen. Sie ermöglicht fundierte Einschätzungen zu zukünftigen Entwicklungen unter Berücksichtigung von Kosten-Nutzen-Erträgen sowie Unsicherheiten und unterschiedlichen Perspektiven. So können subjektive Sichtweisen und dynamische Prozesse innerhalb von Unternehmen präzise erfasst werden. Eine Investition von physikalischen Schutzmaßnahmen wie beispielweise nicht-staatliche Abwehrdrohnen und Raketenabwehrsystemen und präventive staatlich-militärische Überwachung werden somit in den Kotext zur wirtschaftlichen Netzendgeldanalyse der Betreiber gesetzt. Eindeutig wird

oftmals damit aufgezeigt, dass der integrative Schutz von Kernenergieanlagen sowie ihrer Netzbetriebe höherwertiger als nicht-staatliche wie auch staatliche Investitionsabfluss wiegt.

Im Kontext von IT/OT-Strukturen im Vergleich zu INPRO-Planungen (International Project on Innovative Nuclear Reactors and Fuel Cycles) und DCSA-Vorgaben (Defensive Computer Security Architecture) werden klar definierte technische sowie strategische Rahmenbedingungen für Kernenergieanlagen berücksichtigt. (IAEA, 2021) Diese sind gesetzlich vorgeschrieben und zielen zugleich auf wirtschaftliche Optimierung sowie ökologische Bilanzierung ab. Die Anwendung der Delphi-Methode im Kraftwerksschutz – sowohl für Cyber- als auch physikalische Sicherheit – kann zur wirtschaftlichen Optimierung beitragen. Durch strukturierte Expertenbefragungen sowie nationale Vorgaben wie jene des U.S. Department of Transportation lassen sich relevante Risiken fundiert einschätzen und Unsicherheiten reduzieren. Dies führt zu einer gezielteren Ressourcenzuteilung und vermeidet unnötige Investitionen. Ein Argument was viele Betreiber wie auch staatliche Haushaltplanung in ihre Betrachtung mit einbeziehen. Im Unterschied zur Krisen- und Kriegssimulation verfolgt der INPRO-Service jedoch lediglich einen strategisch-normativen Ansatz zur Unterstützung nationaler Planungsprozesse im Bereich nachhaltiger Kernenergiesysteme (NES). Langfristige Zielsetzungen sowie regulatorische Anforderungen werden durch strukturierte Prozesssysteme umgesetzt und dies ermöglicht präzise Abschätzungen für Instandhaltungs- und Reinvestitionskosten. Eine aktuelle Reaktion auf Krisenfälle wird innerhalb der INPRO-Planung durch die vorbereitenden Strukturgeberverfahren vorausgesetzt.

Insgesamt verdeutlicht dies eindrücklich das nur durch sorgfältig geplante Sicherheitskonzepte mit gezielten Investitionen die Versorgungssicherheit durch Kernenergieanlagen in Kombination mit ihren Netzsystemen nachhaltig gewährleistet werden kann. Der Schutz nuklearer Anlagen sowie der sichere Transport elektrischer Energie können aktuell nicht umfassend gewährleistet werden. Eine Herausforderung, deren Erkenntnis und

zugleich Bewältigung essenziell für den Schutz staatlicher Souveränität sowie ökonomischer Stabilität ist. Die Implementierung der beschriebenen Sicherheitsmaßnahmen erfordert zudem eine kontinuierliche Überwachung und Anpassung der Schutzsysteme an sich wandelnde Bedrohungslagen. Hierbei ist die Integration von Echtzeit-Datenanalysen und automatisierten Kontrollmechanismen unerlässlich, um potenzielle Risiken frühzeitig zu erkennen und adäquat reagieren zu können. Die Einbindung von Stochastik-Methoden ermöglicht darüber hinaus eine quantitative Bewertung der Ausfallwahrscheinlichkeiten und unterstützt so die Priorisierung von Investitionen in kritische Systemkomponenten. Eine ganzheitliche Betrachtung, welche physische und kybernetische Schutzsysteme gleichermaßen umfasst, trägt dazu bei, die Resilienz der Energieversorgung nachhaltig zu stärken und Eigentümerinteressen sowie Stakeholder-Anforderungen gleichermaßen zu berücksichtigen. Nur durch eine solche systematische und präzise Steuerung kann langfristig die Balance zwischen Sicherheit, wirtschaftlicher Optimierung und ökologischer Bilanz gewährleistet werden. Gleichzeitig ist eine vollständige Absicherung zentraler Energieversorgung weder generell noch vollständig möglich. Daraus ergibt sich die Notwendigkeit, verstärkt auf dezentrale Versorgungskonzepte mit Mehrteilbereichsnetzen zu setzen. Obwohl auch dieser Umbau hohe Kosten verursacht, erhöht er insbesondere in Krisensituationen die Versorgungssicherheit einzelner Gebiete signifikant. Zukünftig müssen verschiedene Ansätze zusammengeführt werden, um aussagekräftige Modellierungen zu gewährleisten.

Eine PSVBTR-Mastercom-System-Investitionsstrategie kann anhand folgender Beispielrechnung erfolgen. Die weltweite nukleare Erzeugung betrug 2024 rund 377 Gigawatt (Statista, 2025). Bei einem Preis von 0,182 US-Dollar pro Gigawattstunde ergeben sich Betriebskosten von etwa 69 US-Dollar pro Stunde pro Gigawatt, gemessen auf ein fokusiertes ökonomischen Betreibermodell. Ein Ausfall von nur 0,01 Prozent dieser Anlagen über 360 Tage verursacht hochgerechnet Kosten von circa 6.000 US-Dollar pro Stunde pro Gigawatt. Ein durchschnittliches Industriegebiet benötigt jährlich etwa 1,5 Terawattstunden (Janson, 2025), was Kosten von circa 287 US-Dollar pro Stunde entspricht. Im Falle eines Totalausfalls entstünden jedoch Ausfallkosten von rund 6.000 US-Dollar pro Stunde, der wirtschaftliche Schaden wäre vermutlich um ein Vielfaches höher. Demgegenüber stehen Investitionskosten von rund 100 Millionen US-Dollar wie zum Beispiel militärische Aufrüstung und Aufklärung, Schutzgeräte für militärische Cyber- und Spionageabwehr gemessen über drei Jahre. Diese könnten Ausfallkosten von etwa 52 Millionen US-Dollar durch den Stillstand von zwei Kernreaktoren sowie circa fünf Milliarden US-Dollar wirtschaftlichen Schaden pro Jahr signifikant reduzieren, eine Gegenüberstellung im Rahmen des Delphi- und Biba-Modells bestätigt dies. Wir erhalten somit einen durchschnittlichen Gewinn von über 50 Millionen US-Doller im Jahr, durch die Erhöhung der Schutzlevel und verstärkten Aufrüstung für Kernenergieanalagen sowie ihrer Verteil- und Übertragungsnetzbetriebe.

References

Drohnenabwehr Toolbox. (n.d.). Rheinmetall. https://www.rheinmetall.com/de/produkte/flugabwehr/flugabwehrsysteme/drohnenabwehr-toolbox

Center for a New American Security (CNAS). (2025, April 7). *AI and Autonomy in Future Warfare*. CNAS. https://www.cnas.org/research/defense/the-future-of-warfare

Wadhwani, P. (2024). Marktgröße für Drohnenabwehr – nach Komponenten (Hardware, Software), nach Plattformen (bodengestützt, Handheld, UAV), nach Abwehrtyp (destruktives System, zerstörungsfreies System), nach Anwendungen (Erkennung, Störung, Unterbrechung), nach Endbenutzer und Prognose, 2024 – 2032. In *Global Market Insights Inc.* https://www.gminsights.com/de/industry-analysis/anti-drone-market

Statista. (2025, September 15). *Installierte Leistung der Kernkraftwerke weltweit bis 2024*. https://de.statista.com/statistik/daten/studie/28692/umfrage/leistung-der-atomkraftwerke-weltweit/

Janson, M. (2025, May 2). Rechenzentren überholen Heizungen bei Stromhunger. *Statista Daily Data*. https://de.statista.com/infografik/34393/prognose-zum-anstieg-des-weltweiten-strombedarfs-nach-sektoren/

Wojciech Muras, & Katarzyna Szczepańska-Woszczyna. (2024). *Shareholders, Strategy and Value Creation : The Case of the IT Sector*. Routledge.

Iaea. (2021). *Computer Security Aspects of Design for Instrumentation and Control Systems at Nuclear Power Plants* (Vol. 00003). International Atomic Energy Agency.

Iaea. (2021). *Planning Enhanced Nuclear Energy Sustainability: Analysis Support for Enhanced Nuclear Energy Sustainability (ASENES) : An INPRO Service to Member States* (Vol. 00003). International Atomic Energy Agency.