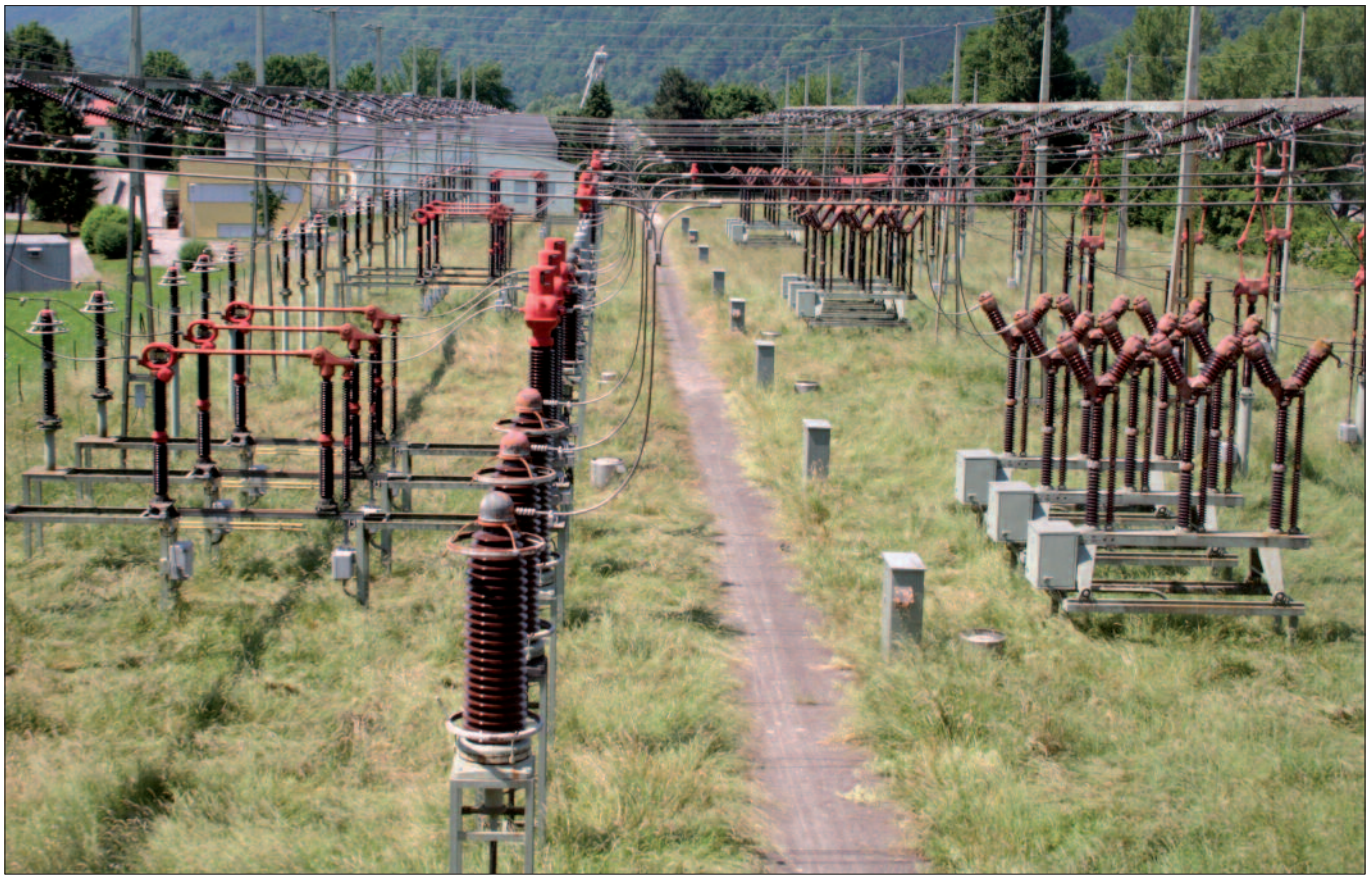

Ausfallsicherheit der Stromnetze: Zukünftig müssen auch Angriffe berücksichtigt werden, die durch die fortschreitende Vernetzung der IT-Komponenten innerhalb der Systeme sowie in Verbindung mit der IT anderer Energiedienstleister möglich sind.

Stromversorgung gewährleisten

Die Stromversorgung der Zukunft wird stärker computergesteuert sein als bisher. Damit werden Cyber-Angriffe auch zu einer Gefahr für die Energieversorgung.

Strom wurde früher ausschließlich in großen konventionellen Kraftwerken erzeugt, in das Übertragungsnetz eingespeist und über die Versorgungsnetze an den Endverbraucher geliefert. Dieses zentral gesteuerte Modell ermöglichte es, das Gleichgewicht zwischen Stromerzeugung und Stromverbrauch zu halten, um die Stabilität, Sicherheit und Versorgung zu gewährleisten.

Dieses klassische Elektrizitätsversorgungssystem ist jedoch aufgrund der zunehmenden Einspeisung von Elektrizität aus erneuerbaren Energiequellen im Wandel und Veränderungen ausgesetzt: Da die regenerativen Energiequellen vom Wetter abhängen, produzieren und speisen sie dann ein (je nach Größe der Stromerzeugungsanlage nunmehr auch in das Verteilernetz), wenn z. B. die Sonne scheint oder der Wind weht. Dies erschwert die Planung, auch wenn die Modelle immer besser werden, die unter anderem meteorologische Simulationen (z. B. von Windgeschwindigkeiten an Küstenzonen und Bewölkungsmodelle) beinhalten. Folglich wird der Aufwand für die Aufrechterhaltung der Versorgungssicherheit größer.

Im Fall einer großen Lastschwankung (z. B. einem Kraftwerksausfall oder anderen unvorhersehbaren Einspeise- oder Verbrauchsänderungen im europäischen Übertragungs- und Verbundnetz, dem *ENTSO-E-Netz)* sorgt der Regelzonenführer (die *Austrian Power Grid AG* für Österreich) in der gesamten österreichischen Regelzone mit der Beschaffung und Aktivierung der benötigten Regelleistung für den Ausgleich von Leistungsdefizit bzw. -überschuss.

Hinzu kam in den letzten Jahren durch die Liberalisierung, dass die Elektrizitätsversorgung (Erzeugung, Verteilung und Verkauf) nicht mehr durch ein einziges Unternehmen vorgenommen wird, sondern durch konkurrierende Marktteilnehmer, da sowohl die Erzeugung als auch der Handel und Vertrieb in den freien Markt überführt wurden, während die Elektrizitätsnetze zum Zwecke des Transports als natürliche Monopole erhalten blieben. Auch das liberalisierte System dürfte den Koordinationsaufwand zur Aufrechterhaltung der Versorgungssicherheit steigern.

Smart Grids. Eine technische Herausforderung ist es, bei stark schwankendem Stromverbrauch, zunehmender dezentralisierter Erzeugung und der nur begrenzten Speichermöglichkeit von Strom, die störungsfreie Stromversorgung auch in Zukunft zu gewährleisten. Smart-Grids, also „intelligente Netze“, sollen diese Herausforderungen bewältigen. Sie sollen die Effizienz

FOTO: WERNER SABITZER

Windenergie: Smart-Grids sollen die Effizienz der Stromversorgung gewährleisten, auch bei der Zunahme der Anzahl von alternativen Energiegewinnungsanlagen.

der Stromversorgung erhöhen, auch bei der zunehmenden Anzahl von Fotovoltaikanlagen, bei der Haushalte nicht nur Stromkonsumenten sind, sondern auch zu Stromproduzenten werden, bis hin zur Bedeckung von Lastspitzen der Akkus von Elektroautos.

Um die Versorgung zu stabilisieren, soll es den Kunden ermöglicht werden, ihren Stromverbrauch anzupassen, indem sie etwa in stromreichen Stunden Waschmaschine, Trockner und Spülmaschine anschalten oder das Elektroauto laden.

Herausforderungen an die IKT-Sicherheit. Bisher lag der Fokus von Netzbetreibern hauptsächlich auf der Ausfallsicherheit der Stromnetze. Künftig müssen zudem Angriffe berücksichtigt werden, die durch die fortschreitende Vernetzung der IKT-Komponenten innerhalb ihrer Systeme sowie in Verbindung mit der IT-Landschaft anderer Energiedienstleister leichter möglich sind. Computergesteuerte Verrechnungssysteme, Netzsteuerungssysteme, Power-Quality-Systeme u. a. sollen stärker automatisiert und in die IKT-Infrastruktur eingebunden und gegen physische Manipulation der *Smart-Meter* (digitale Zählgeräte), Softwaremanipulationen etc. geschützt werden. Verbrauchsdaten werden von *Smart-Metern* an Datenkonzentratoren weitergegeben, die mit Meter-Data-Management-Systemen, die noch aufgebaut werden müssen, kommunizieren. Mittels *M2M-Kommunikation (Machine-to-Machine)* können Lastverteiler, Netzsteuergeräte und Leitsysteme eingebunden werden und automatisiert handeln. Dadurch entsteht parallel zum Stromnetz ein IKT-Netz, das durch seine große Ausdehnung und vielen Teilnehmer und Zugangspunkte eine physische und datentechnische Absicherung benötigt.

Die Gefahren, denen Energieversorger als kritische Infrastruktur-Unternehmen ausgesetzt sind, reichen von Energiediebstahl, Stromzählermanipulation, Angriffen auf Kontrollelemente der Netzbetreiber zur Störung des Betriebes bis hin zu großräumigen Abschaltungen des nationalen Stromnetzes. Die Risiko- und Schwachstellenanalyse kritischer Infrastruktur erfordert einen standardisierten Ansatz.

KIRAS-Projekt. Mit dem Projekt $(SG)^2$, finanziert im Sicherheitsforschungs-Förderprogramm *KIRAS* vom Bundesministerium für Verkehr, Innovation und Technologie, wurden Maßnahmen für Verteilernetzbetreiber erforscht, die zur Erhöhung der Sicherheit der Computersysteme in der kritischen Infrastruktur „Energie“ der Zukunft dienen. Es wurde evaluiert, welchen Bedrohungen die Energiewirtschaft ausgesetzt ist, um Lösungsansätze für die Minimierung des Risikos zu finden, damit die Ausfallsicherheit und die Zuverlässigkeit von Systemen sichergestellt werden kann.

Aus über 500 Bedrohungen wurden 31 in einem Katalog zusammengefasst. Zu diesem wurde ein Risikokatalog mit den möglichen Gefahren entwickelt. Anschließend wurde ein Maßnahmenkatalog zur Minimierung der Risiken erstellt.

Smart-Grid-Komponenten wurden auf ihre Sicherheit gegenüber Hackerangriffen in ausgewählten Angriffsszenarien überprüft.

Österreichs Energie befasst sich seit einigen Jahren mit dem Schutz der kritischen Infrastruktur vor Cyber-Angriffen. Dazu wurden Projektgruppen eingerichtet mit Aufgaben wie sicherheitstechnische Anforderungen an Smart-Meter, sicherheitstechnische Anforderungen an Leitsysteme, Integration eines Informations-Sicherheits-Management-Systems, Risikoanalyse des Stromnetzes, Risikoanalyse des Gasnetzes.

Aus den Ergebnissen wurden Maßnahmen zur Risikoreduktion getroffen. Die Energieversorger setzen seit Jahren Maßnahmen zum Schutz vor Cyber-Angriffen zum sicheren Betrieb der Energienetze. Der im $(SG)^2$-Projekt erhobene Bedrohungskatalog wurde durch die im Projekt beteiligten Energieversorger mit den in anderen Projekten erhobenen Bedrohungskatalogen verglichen und ergänzt.

Mehrere von der *E-Control* und *Österreichs Energie* initiierte Projekte befassten sich mit der Risikoanalyse von Informationssystemen der Energieinfrastruktur (Stromnetz, Gasnetz). Ziel der Projekte ist die Erhöhung der Sicherheit in der Energiewirtschaft durch gemeinschaftlich, abgestimmte Sicherheitsmaßnahmen und Selbstverpflichtungen zur Erhöhung der Sicherheit der Strom- und Gasnetze. Die in den Projekten durchgeführten Risikoanalysen und daraus abgeleiteten Maßnahmen werden in regelmäßigen Abständen Reviews unterzogen. *A. M./R. G.*

FOTO: WERNER SABITZER