

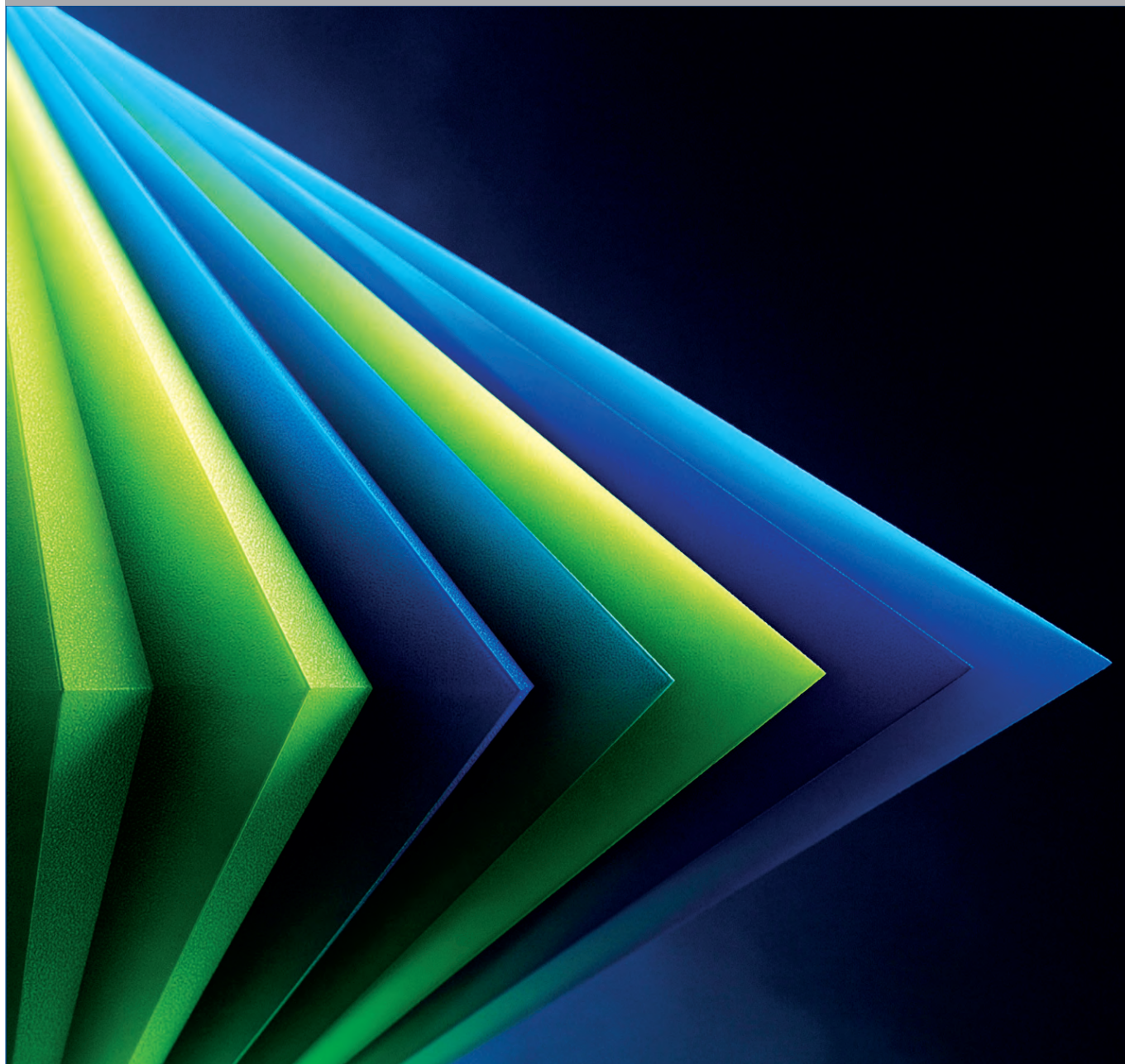


# ENERGIEWIRTSCHAFTLICHE TAGESFRAGEN

ZEITSCHRIFT FÜR ENERGIEWIRTSCHAFT · RECHT · TECHNIK UND UMWELT

10 · 2026

Inklusive H<sub>2</sub> compact – Magazin für Wasserstoffwirtschaft



## ENERGIEMARKT

IRANKRIEG UND  
KÜNFTIGE  
EU-ENERGIEPOLITIK

## DEZENTRALISIERUNG

VON DER KLEINEN  
SCHWACHSTELLE ZUM  
SYSTEMISCHEN RISIKO

## DEKARBONISIERUNG

BEDEUTUNG DES  
WASSERSTOFFS FÜR RESILIENZ  
UND WERTSCHÖPFUNG

# Vom Sicherheitskonzept zum sicheren Betrieb

Claus Schneeberger

*OT-Sicherheitsarchitekturen werden für einen definierten Sollzustand geplant. Energieinfrastrukturen bleiben über lange Betriebszeiträume jedoch nicht unverändert: Anlagen werden modernisiert, Komponenten ausgetauscht, Fernzugriffe eingerichtet und Kommunikationsbeziehungen angepasst. Der Beitrag zeigt, wie sich die Einhaltung definierter Sicherheitsgrenzen im laufenden Betrieb kontinuierlich überprüfen und Abweichungen frühzeitig erkennen und gezielt bearbeiten lassen.*

## Wenn Soll und Ist auseinanderdriften

Zonenkonzepte definieren die Sicherheitsgrenzen einer OT-Architektur und legen fest, welche Kommunikationsbeziehungen zwischen einzelnen Bereichen zulässig sind. Netzwerksegmentierung setzt diese Vorgaben technisch um. Wo Kommunikation vollständig unterbunden werden soll, können Netzbereiche physisch oder logisch voneinander getrennt werden. Dieser Sollzustand bildet die Referenz für den sicheren Betrieb.

Ob der tatsächliche Zustand diesem Soll entspricht, lässt sich aus der Planung allein jedoch nicht ableiten. Änderungen an Firewall-Regeln oder Kommunikationsbeziehungen können neue Verbindungen zwischen Sicherheitszonen ermöglichen oder vorgesehene Trennungen aufheben. Auch reguläre Eingriffe bei Wartung und Betrieb können dazu führen, dass temporäre Verbindungen bestehen bleiben. Solche Abweichungen fallen im laufenden Betrieb nicht zwangsläufig auf. Die betroffenen Systeme können weiterhin störungsfrei funktionieren. Betreiber müssen daher erkennen können, wenn der tatsächliche Zustand vom Soll abweicht.

## Von der Momentaufnahme zur kontinuierlichen Kontrolle

Projektanalysen, Audits, Penetrationstests und Compliance-Prüfungen liefern wichtige Erkenntnisse über den Zustand einer OT-Infrastruktur. Sie zeigen jedoch nur eine Momentaufnahme. Entwicklungen dazwischen werden nicht unmittelbar sichtbar. Kontinuierliche Validierung schließt diese zeitliche Lücke. Sie überwacht, ob die festgelegten Kommunikati-



Veränderungen im laufenden Betrieb können den Sicherheitszustand von OT-Infrastrukturen beeinflussen; eine kontinuierliche Validierung hilft, Abweichungen vom definierten Sollzustand frühzeitig sichtbar zu machen

Bild: stock.adobe.com

onsgrenzen eingehalten werden, und macht Abweichungen zeitnah sichtbar. Damit ergänzt sie die etablierten Verfahren um eine fortlaufende Kontrolle des tatsächlichen Zustands.

Besonders relevant ist dieser Soll-Ist-Abgleich bei sog. Air Gaps, also der vollständigen Trennung von Netzbereichen, zwischen denen keine Kommunikation stattfinden soll. Dass eine solche Trennung eingerichtet wurde, gibt allein noch keine Gewissheit darüber, ob sie im Betrieb tatsächlich besteht. Der fortlaufende Abgleich macht ihre Wirksamkeit überprüfbar.

## Relevanz für verteilte Energieinfrastrukturen

Die räumliche Verteilung energiewirtschaftlicher Infrastrukturen erhöht die Anforderungen. Netzbetreiber müssen Kommunikationsgrenzen bspw. über Umspannwerke und technische Standorte hinweg im Blick behalten. Bei Stadtwerken kommt häufig die Heterogenität der

Infrastruktur hinzu. Erzeugungsanlagen, Umspannwerke und Speicher sowie Anlagen zur Wassergewinnung und -aufbereitung können unterschiedliche Systemgenerationen und Betriebsanforderungen aufweisen. Nach Eingriffen muss nachvollziehbar sein, ob der vorgesehene Ausgangszustand wiederhergestellt wurde.

Für verteilte und heterogene Infrastrukturen liegt ein wesentlicher Nutzen in der standortübergreifenden Wirksamkeitskontrolle von Segmentierung, Firewall-Regeln oder Air Gaps. Zur technischen Umsetzung lässt sich bspw. die Lösung SensorFu Beacon einsetzen. Sie prüft automatisiert, ob vorgesehene Trennungen wirksam sind oder unerwartete Kommunikationswege bestehen. Dazu senden in den überwachten Netzsegmenten platzierte Beacons Testpakete über verschiedene Netzwerkpfade und Protokolle. Gelingt eine Verbindung über eine vorgesehene Isolationsgrenze hinweg, wird eine Meldung ausgelöst. Die Tests beeinträchtigen die produktiven OT-Systeme nicht.

## Aus einem Alarm wird ein Prozess

Mit der Meldung ist das zugrunde liegende Problem noch nicht gelöst. Ein Alarm muss eingeordnet werden: Handelt es sich um eine zulässige Veränderung, eine nicht dokumentierte betriebliche Anpassung, eine Fehlkonfiguration oder ein sicherheitsrelevantes Ereignis? Welche Systeme sind betroffen? Besteht unmittelbarer Handlungsbedarf? Damit wird aus der technischen Überwachung eine betriebliche und organisatorische Aufgabe. Erkannte Abweichungen müssen nach festgelegten Abläufen bewertet und bearbeitet werden. Dafür braucht es OT-spezifische Expertise, klare Zuständigkeiten und Eskalationswege.

SensorFu Beacon kann eigenständig eingesetzt oder als technisches Betriebsmodul in ein übergeordnetes Betriebsmodell eingebunden werden. Ein solches Modell ist bspw. der OT-Leitstand von Controlware zur externen Betriebsunterstützung. Technische Betriebsmodule, Servicemodule und bedarfsgerechte On-Demand-Leistungen werden dort mit strukturierten Abläufen und spezialisierter OT-Expertise verbunden. Bei integrierter Nutzung fließen Meldungen direkt in die weitere Bearbeitung ein. Bewertung und Maßnahmen werden dokumentiert und mit den Verantwortlichen auf Betreiberseite abgestimmt. Die Verantwortung für die OT-Infrastruktur bleibt beim Betreiber.

## Wirtschaftlicher Nutzen

Je früher Abweichungen erkannt und bewertet werden, desto schneller können Betreiber reagieren. Damit verkürzt sich der Zeitraum, in dem unbeabsichtigte Kommunikationswege unentdeckt bleiben und die Verfügbarkeit von Anlagen beeinträchtigen können. Das hilft, Ausfallrisiken und mögliche Folgekosten zu begrenzen. Die frühzeitige Erkennung unterstützt zugleich den Anlagen- und Investitionsschutz, wenn kritische Abweichungen sichtbar werden, bevor größere betriebliche Auswirkungen entstehen.

Hinzu kommt der effizientere Einsatz knapper personeller Ressourcen. OT-Expertise lässt sich gezielt dort einsetzen,

wo Handlungsbedarf besteht. Die dokumentierte Bearbeitung schafft zugleich Nachvollziehbarkeit für interne Kontrollen, Audits und regulatorische Nachweispflichten.

## Dauerhafte Wirksamkeit als Maßstab

Energieinfrastrukturen sind auf Betriebszeiten von mehreren Jahrzehnten ausgelegt. Die darin eingesetzte Steuerungs-, Kommunikations- und Sicherheitstechnik wird in deutlich kürzeren Abständen erneuert oder ersetzt. Damit verändern sich auch die Technologien und Instrumente, mit denen die Sicherheitsarchitektur umgesetzt und überprüft wird. Langfristig kommt es deshalb darauf an, die vorgesehenen Sicherheitsgrenzen auch bei technologischen und betrieblichen Veränderungen überprüfbar zu halten. Welche Werkzeuge dafür eingesetzt

werden, kann und wird sich im Laufe der Zeit ändern.

Für Energieunternehmen bedeutet das: Sicherheitsarchitektur und Betriebsprozesse müssen so angelegt sein, dass neue Technologien integriert und Komponenten ersetzt werden können, ohne den Sollzustand und seine Einhaltung aus dem Blick zu verlieren. Kontinuierliche Validierung lässt sich mit unterschiedlichen technischen Lösungen umsetzen. Entscheidend bleibt, ob die Sicherheitsarchitektur auch unter veränderten technischen und betrieblichen Rahmenbedingungen wirksam ist.

*C. Schneeberger, Senior Systems Engineer OT/ICS, Controlware GmbH, Dietzenbach  
ot@controlware.de*



## Alle Leistungen aus einer Hand

Wir unterstützen Energieversorger und Netzbetreiber beim Smart-Meter-Rollout. Mit TR-03109-6-konformer Infrastruktur, stabilem und skalierbarem Betrieb sowie nahtloser Integration in Abrechnungs- und Marktprozesse.

### IHRE VORTEILE

- Entlastung bei Betrieb und Administration
- M2M Simkarten Management
- ISO 27001 – konforme Sicherheit
- Zertifikatsmanagement inklusive Sub-CA

**Regulatorik erfüllen. Risiken minimieren. Rollout sicher betreiben.**



Jetzt kostenlose  
Beratung buchen!

Gestalten Sie mit uns  
die Zukunft der IT:

[www.rku-it.de](http://www.rku-it.de)