Digitale Stromnetze

Sicherung von Automatisierung und Fernwirktechnik

Mit der Einführung von IP-basierter Kommunikation hat die Welle der Digitalisierung den Energieübertragungs- und -verteilungsmarkt erfasst. Mit der Zunahme von Urbanisierung und Energieverbrauch steigt auch der Bedarf an aktiver Netzsteuerung – von traditionellen Verteilungsnetzstationen in den Übertragungsnetzen bis zu modernen intelligenten Ortsnetzstationen in den Verteilungsnetzen, von der Integrierung dezentraler erneuerbarer Energiequellen wie Wind- und Solarparks über autarke Mikronetze für Inselbetrieb bis zum Energiemanagement in Industrieanlagen und auf dem Mobilitätsmarkt. Um diesem Bedarf gerecht zu werden, bietet die Energieautomatisierungstechnik heute Lösungen von hochmodernen Leitstellen bis zu kompakten Fernwirkgeräten. Welche Auswirkungen hat die schnell voranschreitende Digitalisierung auf die Sicherheit, die allgemeine Stabilität und die Zuverlässigkeit des Netzes?

Wie überall im digitalen Raum muss die Sicherheit schon im Vorfeld bei der Architektur und Auslegung des Netzes und seiner einzelnen technischen Komponenten, bei den Prozessen und Arbeitsweisen des Netzbetreibers und vor allen Dingen in der täglichen Arbeit des durchschnittlichen Bedieners vor Ort oder in der Lastverteilungszentrale als Grundanforderung berücksichtigt werden (*Bild 1*). Einige wichtige Sicherheitsaspekte der Überwachung und Steuerung durch Fernwirkgeräte (RTU) sollen hier behandelt werden:

- Sicherung der Prozesskommunikation
- Sicherung des lokalen und abgesetzten Parametrierzugangs
- sichere Speicherung sensibler Daten
- Überwachung der Geräte-, Nutzer- und Kommunikationsaktivitäten
- geeignete Entwicklungsprozesse, um die Herstellung sicherer Produkte über den gesamten Lebenszyklus zu garantieren
- Sicherstellen einer anbieter- und plattformübergreifenden Interoperabilität.

Sicherung der Prozesskommunikation

Die Hauptfunktion von RTU ist es, Netzleitstellen die Überwachung und Steuerung von Primärtechnik über Fernwirktechnik zu ermöglichen. Dazu wirken RTU auf Feldebene als Sensoren/Aktoren und auf Stationsebene als Kommunikationspartner zur Leitstelle, wobei sie mit der entfernten Leitstelle über Fernwirkprotokolle kommunizieren (*Bild 2*). Bei heutigen Anlagen geschieht die Prozesskommunikation vorwiegend über IP-basierte Protokolle wie IEC 60870-5-104 und DNP 3. Dabei muss darauf geachtet werden, dass die Kommunikation der RTU zur Leitstelle nicht kompromittiert wird, da dies zu Schäden sowohl an den Primärtechnik auf Feldebene als auch in der Leitstelle führen kann.

Unterstationen auf der Hoch- und Mittelspannungsebene sind normalerweise durch physische Sicherungsmaßnahmen wie Gebäudesicherung geschützt. Die in diesen Unterstationen eingesetzten RTU und sonstigen Sekundärgeräte sind normalerweise mit einem Prozessnetzwerk verbunden, das nur vom Standort des Leitstellennetzes und manchmal vom Standort des benachbarten Partnerprozessnetzwerks aus zugänglich ist.

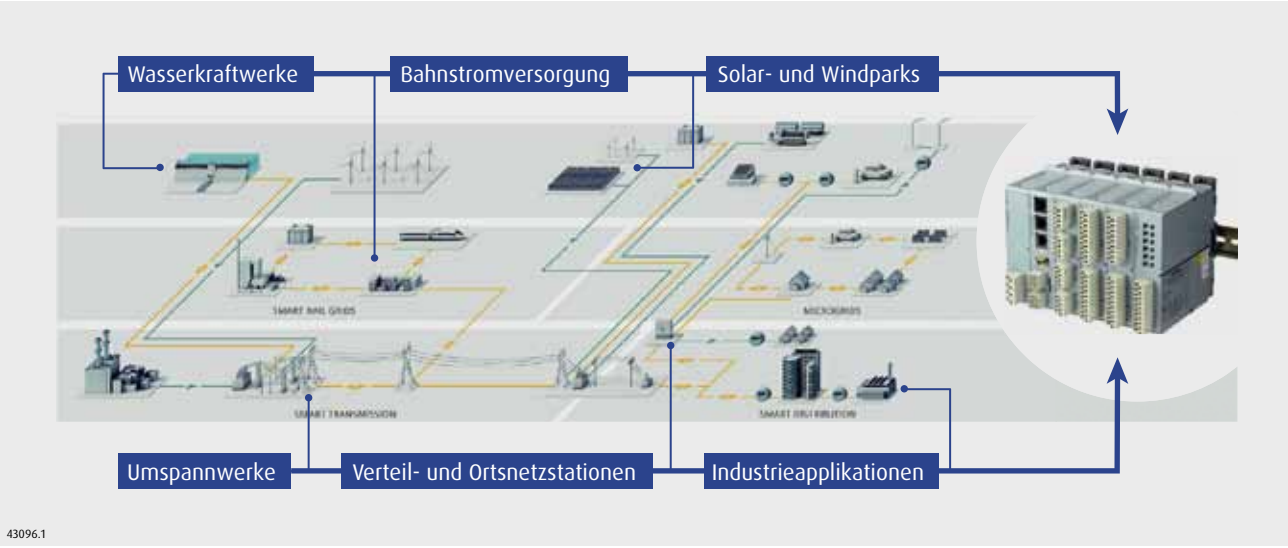

Bild 1. Einsatz RTU-basierter Energieautomatisierung in digitalen Stromnetzen heute

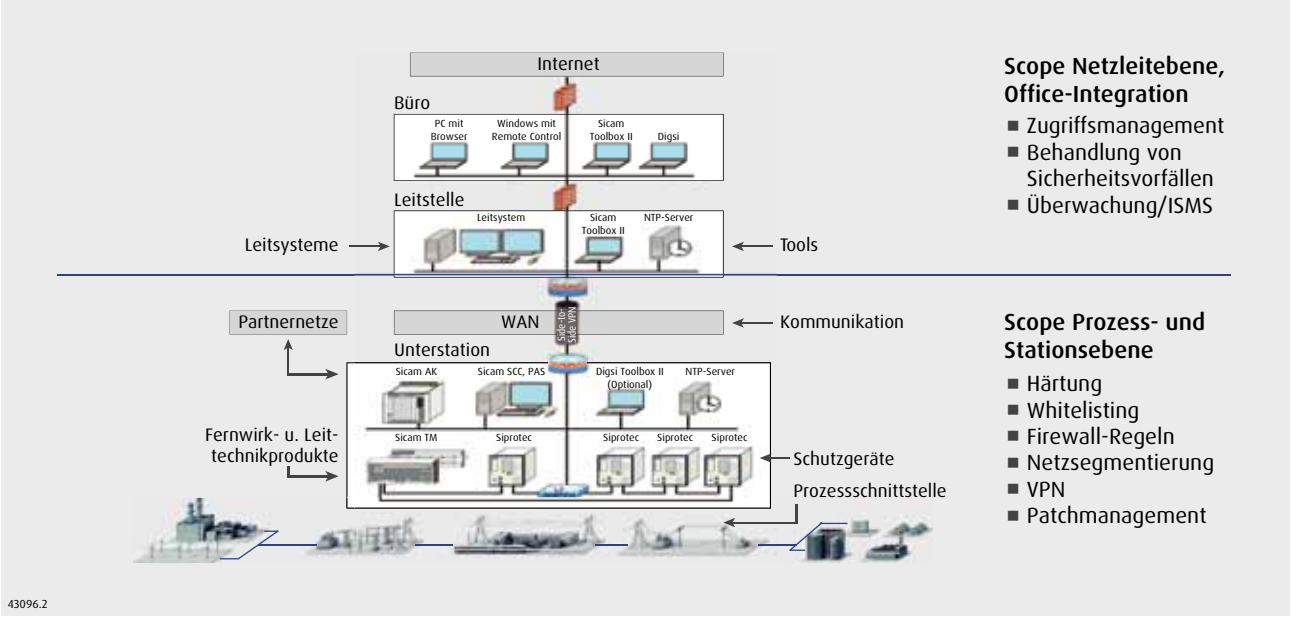

Bild 2. Typisches Beispiel einer ebenenübergreifenden Konfiguration von Netzautomatisierung und Netzführung

Ein Angreifer, der potenzielle Schwächen in der Prozesskommunikation zwischen Leitstelle und RTU ausnutzen oder die Kommunikation manipulieren oder behindern will, muss entweder die physischen Sicherungsmaßnahmen in der Unterstation überwinden, das Kommunikationsnetzwerk zwischen Stationsebene und Leitstellenebene angreifen oder eventuelle Partnernetzwerke kompromittieren (*Bild 3*). Zur Abwehr netzwerkbasierter Angriffe werden folgende Gegenmaßnahmen empfohlen:

- Sicherung der Kommunikation zwischen den Standorten durch VPN-Tunnel (Virtual-Private-Network) zwischen Unterstation und entfernten Standorten
- Netzwerkhärtungsmaßnahmen, um durch den Einsatz von Firewalls und entsprechenden Regeln die Zahl der von außen adressierbaren Schnittstellen und Dienste auf ein Minimum zu beschränken
- Einsatz von RTU mit eingebauten Firewalls in der Anwendungsschicht, mit denen bewusst verstümmelte, semantisch falsche oder anderweitig fehlerhafte Fernwirktelegramme ausgefiltert werden
- Definition maximaler Datenmengen an RTU und Schaltgeräte, um Denial-of-Service-Angriffe durch gezielte Ressourcenüberlastung zu verhindern.

Bei Unterstationen im Verteilungsnetz dagegen besteht ein erhöhtes Bedrohungsrisiko für die Prozesskommunikation, weil sie keine angemessene physische Zugangssicherung haben. So kann ein entschlossener Hacker relativ einfach die Sicherung durch ein Schloss an der Schalttafel mit der RTU und dem GPRS-Modem in einer entfernten Photovoltaikanlage überwinden. Sobald der Angreifer physischen Zugang zu den Geräten hat, kann er die IP-Verbindung zwischen RTU und Router intelligent kapern und sich statt der RTU mit der Leitstelle verbinden. Da der Standort der Leitstelle eine Verbindung mit dem entfernten Router und nicht mit der RTU als Endpunkt herstellt, genügt es nicht, dass ein Modem eine VPN-Verbindung zum Standort der Leitstelle herstellen kann. Für den Angreifer wäre es dadurch ein Leichtes, von der entfernten Station aus eine sichere Verbindung mit der Leitstelle herzustellen. Die Leitstelle würde lediglich während der Übernahme eine vorübergehende Verbindungsunterbrechung zur RTU feststellen. Nach der Übernahme kann der Angreifer Schadprogramme ausführen, die die RTU imitieren und komplexe Angriffe auf Leitstelle oder Primärtechnik ausführen.

Um solche Angriffe bei der Verteilungsnetzautomatisierung abzuwehren, ist es empfehlenswert, RTU einzusetzen, deren integrierte VPN-Funktion mit gängigen Verschlüsselungstechnologien wie IPSec ausgestattet ist. Eine solche IPSec-fähige RTU kann so konfiguriert werden, dass sie den Aufbau eines sicheren VPN-Tunnels zur Leitstelle einleitet, wobei skalierbare Edge-Router auf Leitstellenseite den Abschluss der IPSec-Verbindungen bilden. Wenn die RTU die gesicherte Verbindung mit der Leitstelle einleiten, ist es für Angreifer unmöglich, die IP-Verbindung zwischen RTU und Router im Feld zu kapern. Bei einem entsprechenden Versuch wird die gesicherte VPN-Verbindung zwischen RTU und Leitstelle unterbrochen, und damit geht auch die sicher durch die IPSec-VPN-Verbindung getunnelte Verbindung verloren. Damit hat der Angreifer keine einfache Möglichkeit, sich böswillig über kompromittierte Knoten im Verteilungsnetz Zugang zur Leitstellenanwendung zu verschaffen.

Um eine RTU vorzutäuschen und damit eine gesicherte Kommunikation mit der Leitstelle aufbauen zu können, müsste der Angreifer auf die IPSec-Parameter zugreifen. Dazu könnte er versuchen, während eines Remote-Engineering-Eingriffs an einer RTU das Netzwerk abzuhören oder die Parametrierung aus dem eingebauten persistenten Speicher der RTU auszulesen. Diese Möglichkeit wird im Folgenden behandelt.

Sicherung des interaktiven Parametrierzugangs

Um die Vertraulichkeit und Integrität bei der Inbetriebsetzung und Wartung vor allem bei einem Fernzugriff über IP-basierte Verbindungen sicherzustellen, sollten die Fernbedienungsterminals (RTU) eine geräteseitig integrierte gesicherte Parametriermöglichkeit haben. Dabei handelt es sich um eine webbasierte Parametrierung, bei der die RTU einen gesicherten Webserver bereitstellt und dem Anwender dadurch die Parametrierung über eine gesicherte HTTPS-Verbindung zur Verfügung stellt.

Mit dem HTTPS-Protokoll kann das Abhören einer Klartextkommunikation verhindert werden. Wenn eine desktop-

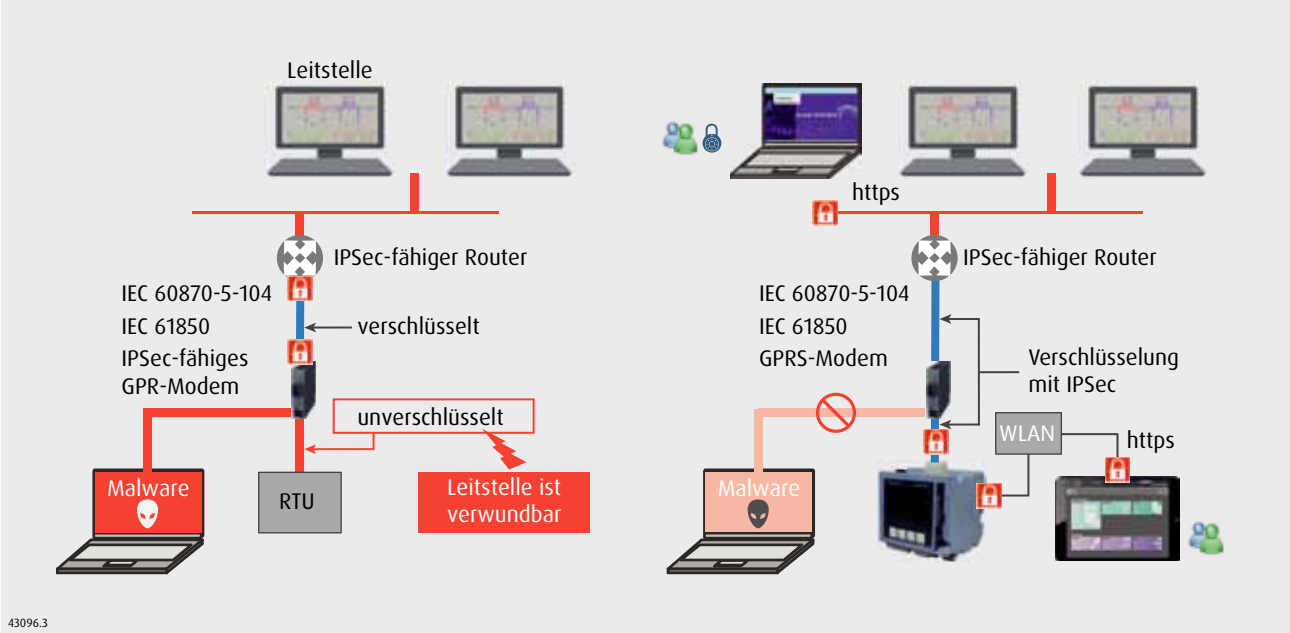

Bild 3. Sicherung der Kommunikation und des Betriebs in automatisierter Verteilung

basierte Parametriersoftware eine Fernverbindung mit den RTU herstellt, sollte die RTU in der Lage sein, die Richtigkeit der zugreifenden Software respektive der Verbindung zu überprüfen. Dazu wird das vom Hersteller oder Kunden vergebene digitale Zertifikat der Software beim Verbindungsaufbau geprüft – ebenso prüft umgekehrt die Parametrierungssoftware das digitale Zertifikat der RTU –, um den Aufbau einer gesicherten Verbindung mit einem Man-in-the-Middle oder einem unzulässigen Endpunkt zu verhindern (beiderseitige Authentisierung der Kommunikationspartner).

Des Weiteren ist auch die Fähigkeit der RTU zur Identifizierung von Engineering-Nutzern nach Name und zugewiesenen Rollen ein wichtiger Aspekt. Bei mittleren und großen Organisationen ist es unerlässlich, skalierbare, zentrale Nutzermanagementsysteme wie Radius und Microsoft Active Directory für die Verwaltung der Nutzer, ihrer Rollen (Berechtigungsstufen) und der entsprechenden Anmeldedaten wie Passwörtern einzusetzen. Daher ist es wünschenswert, dass die RTU standardmäßig zentrale Nutzermanagementsysteme und damit die Authentifizierung und Berechtigung von Nutzern unterstützen.

Sichere Speicherung sensibler Daten

Außer der Sicherung der Engineering-Kommunikation ist die Sicherung sensibler, in der RTU gespeicherter Daten ein wichtiger Punkt. Sensible Daten und Informationen sind zum Beispiel:

- lokal verwaltete Anmeldedaten von Nutzern
- Parameter für die gesicherte Kommunikation – zum Beispiel Pre-shared-Keys für IPSec
- kryptografische Schlüssel zur Sicherung der Authentizität der Verbindungsendpunkte und zur Integritätsprüfung der Firmware.

Können diese Daten von Angreifern manipuliert oder kompromittiert werden, können Angreifer eingerichtete Sicherheitsmechanismen umgehen. Um dies zu verhindern, muss die Fähigkeit der RTU zur Speicherung sensibler Informationen betrachtet werden. Die Möglichkeiten reichen von der teilweisen oder vollständigen Verschlüsselung der Parameter im persistenten inter-

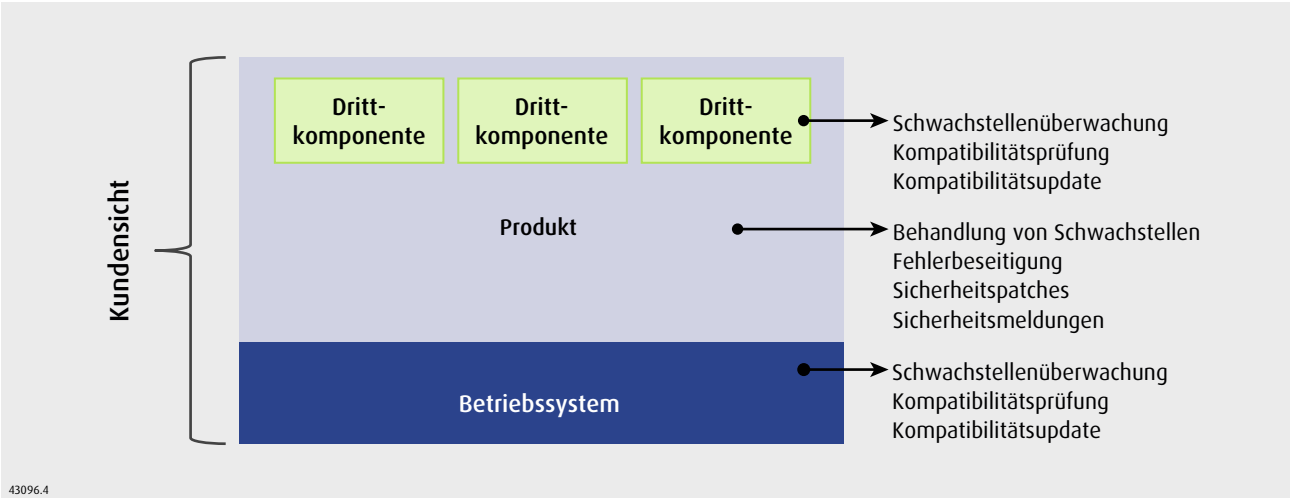

Bild 4. Management der Sicherheitspatches im Lebenszyklus eines Produkts

nen Speicher der RTU über die Verwendung dedizierter kryptografischer Prozessoren – auch als Krypto-Chips bezeichnet – und die manipulationssichere Speicherung sensibler Informationen wie kryptografischer Schlüssel bis zu hybriden Ansätzen, bei denen sich die obigen Methoden ergänzen, zum Beispiel sichere Speicherung privater Schlüssel im Krypto-Chip und Verschlüsselung sensibler Parameter über asymmetrische Schlüsselverfahren. Zusätzlich übernehmen in RTU integrierte Krypto-Chips einen Teil der rechenintensiven kryptografischen Berechnungen, so dass der RTU-Zentralprozessor für die funktionalen Anforderungen der Energieautomatisierung entlastet wird.

Überwachung der Geräte-, Nutzer- und Kommunikationsaktivitäten

Wenn im Prozessnetzwerk eine große Zahl IP-fähiger Geräte eingesetzt wird, ist es eine Herausforderung, Anomalien im Netzwerkverkehr festzustellen, die ein Hinweis auf bösartige Aktivitäten von Angreifern sein könnten. Um bösartige Aktivitäten im ganzen System mit zu erkennen, sollten RTU und ähnliche Geräte die Fähigkeit zum Audit sicherheitsrelevanter Ereignisse – erlaubte Aktionen und Aktivitäten – und Alarme – potenziell bösartige Aktionen und Aktivitäten – haben. Die RTU sollten fähig sein, diese Aktivitäten lokal und online in einem zentralen Protokollserver über gängige IP-basierte Protokolle wie Syslog aufzuzeichnen, so dass die Bediener die chronologische Reihenfolge von Ereignissen und Alarmen analysieren und bösartige Versuche zur Kompromittierung des Systems aufspüren können. Zusätzlich sollten die RTU die Ereignisse und Alarme über Fernwirk- und Netzwerkmanagementprotokolle an die Überwachungssysteme weiterleiten können.

Entwicklungsprozesse für die Herstellung sicherer Produkte über den gesamten Lebenszyklus

Ein wichtiger Aspekt bei der Betrachtung der RTU-Sicherheit ist der Patch-Management-Prozess des Herstellers (*Bild 4*):

- Sicherheitspatches werden von Drittkomponentenanbietern während der Lebensdauer der RTU geliefert
- Sicherheitspatches werden vom Anbieter des verwendeten Betriebssystems während der Lebensdauer der RTU geliefert
- Sicherheitspatches für RTU-interne Schwachstellen werden von den Anbietern der RTU während ihrer Lebensdauer entwickelt.

Die Anbieter von RTU sollten einen transparenten Ansatz beim Management von Sicherheitspatches mit schnellen Reaktionszeiten und eingeführten internen Prozessen für die Handhabung der Informationen und Aktivitäten in Forschung und Entwicklung zu den Patches wählen. Des Weiteren sollten sie die Netzbetreiber proaktiv unterstützen, damit diese die Anforderungen an das Patch Management entsprechend eines Informationssicherheitsmanagementsystems (ISMS) erfüllen. Ziel ist dabei, die Verfügbarkeit der kritischen Infrastruktur zu erhalten.

Eingeführte sichere Vorgehensweisen in der Forschung und Entwicklung beim RTU-Anbieter sind eine unabdingbare Voraussetzung dafür, dass die eingesetzten Produkte tatsächlich die Ziele für Sicherheit und Zuverlässigkeit im Betrieb erfüllen. Von der Erhebung der Sicherheitsanforderungen aus dem Markt bis zur Sicherung der Fertigungsschritte – in der individuelle digitale Schlüssel und Zertifikate in die RTU geladen werden – kann nur eine F&E-Organisation mit hohem

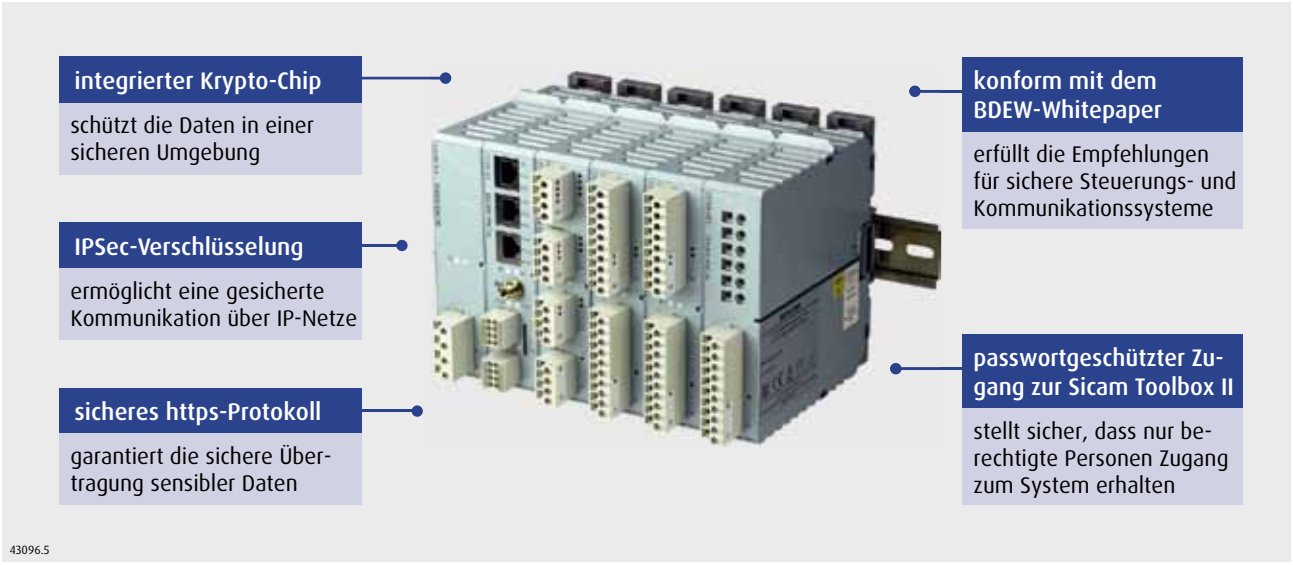

Bild 5. Einige der in RTU zu erwartenden integrierten Sicherheitsmerkmale und -fähigkeiten

Reifegrad die Sicherheitsanforderungen erfüllen, um gegen heutige Bedrohungen zu bestehen. Dazu gehören unter anderem:

- geschulte F&E-Mitarbeiter, die Sicherheitslücken bewerten können und die entsprechende Praktiken bei der Codierung kennen, um die Gefahr der Implementierung potenzieller Sicherheitslücken zu minimieren
- eingeführte Prozesse, mit denen die Validierung und Verifizierung von Bedrohungen und Risiken in der Architektur-, Design- und Implementierungsphase gewährleistet wird
- Management der Sicherheitspatches von Drittkomponenten und -systemen in der Entwicklungsphase und während des gesamten Lebenszyklus
- Validierung der Softwarefreigabe auf bekannte Schwachstellen, Durchführung von Penetrationstests
- Validierung der Softwarefreigabe für die Kompatibilität mit Antivirussoftware
- sichere Implementierung kryptografischen Schlüsselmaterials in Krypto-Chips
- digitale Signierung der RTU-Firmware.

Außerdem sollten die Anbieter von RTU – ebenso wie es die Behörden von den Netzbetreibern erwarten – ein eingeführtes Informationssicherheitsmanagementsystem haben, das die Vertraulichkeit, Integrität und Verfügbarkeit sensibler Informationsbestände wie Quellcode und Designartefakten durch Prozesse und Kontrollen schützt, die den Empfehlungen internationaler Standards wie ISO 27001 entsprechen.

Sicherstellen einer anbieter- und plattformübergreifenden Interoperabilität

Mit Blick auf die Zukunft mit immer mehr IP-basierter Automatisierung in der Energielandschaft wird die Interoperabilität im Betrieb – sowohl unter Funktions- als auch unter Sicherheitsaspekten – für Anbieter und Netzbetreiber ein wichtiges Thema werden. Die Unterstützung des sicheren Betriebs entsprechend der Definition in der IEC-62351-Normenreihe für Netzmanagement und der dazu gehörende Informationsaustausch ist dazu notwendig. Beispiele aus der Norm sind (*Bild 5*):

- sichere Kommunikation entsprechend der Normen IEC 62351-3 bis -6 und den dazu gehörigen Erweiterungen der Normen wie IEC 60870-5-7 auf Grundlage von IEC 62351-5 und IEC 62351-3 für die Sicherheit von IEC 104
- rollenbasierte Zugriffskontrolle entsprechend IEC 62351-8
- digitales Schlüsselmanagement entsprechend IEC 62351-9.

Unter dem Aspekt der Systemintegration sind die Standardisierungsanforderungen von IEC 62443-2-4 und IEC 62443-3-3 zu berücksichtigen.

Die sorgfältige und systematische Abdeckung dieser Aspekte bei der Entwicklung und dem Einsatz von RTU ermöglicht es Netzbetreibern, digitale Verbundnetze sicher, stabil, interoperabel und zuverlässig zu betreiben.

Dipl.-Inf. **Chaitanya Bisale**,
Product Manager,
Senior Key Expert Cyber Security, Energy Management Division, Digital Grid,
Siemens AG, Nürnberg

>> chaitanya.b@siemens.com

>> www.siemens.com/gridsecurity

43096