Schlüsselthemen für die Energieinfrastruktur

OT-Sicherheit in der Netzführung

Mit zunehmender Intelligenz in den Verteilnetzen rückt auch das Thema OT-Sicherheit immer stärker in den Fokus. Welche Aspekte dabei zu berücksichtigen sind und welche Lösungen die VIVAVIS AG dafür anbietet, beschreibt Ditmar Niederl.

Für Klimaschutz und Energieunabhängigkeit ist es unerlässlich, sich von fossilen Brennstoffen zu lösen und stattdessen auf den Ausbau erneuerbarer Energien zu setzen. Dies erfordert einen massiven Ausbau der regenerativen Stromerzeugung sowie der Elektromobilität und die verstärkte Nutzung von Wärmepumpen zur Wärmeerzeugung. Diese Maßnahmen haben erhebliche Auswirkungen auf die Mittel- und Niederspannungsnetze. Daher kommt der Automatisierung der Ortsnetzstation, als Verbindung zwischen Mittel- und Niederspannungsnetz, eine zentrale Bedeutung zu. Die Integration von Erzeugern und Verbrauchern, zum Beispiel Ladesäulen, Smart-Grid-Ready-Wärmepumpen und steuerbare Lasten, vervollständigt die umfassende Erfassung und Steuerungsmöglichkeit.

Quelle: VIVAVIS AG/Shutterstock

Die intelligente Ortsnetzstation als Bindeglied zwischen Energieerzeugung und -verbrauch

Datenerfassung und Steuerung

Erfassung: Informationen aus dem Mittel- und Niederspannungsnetz sind von essenzieller Bedeutung. Verbunden mit Daten von relevanten Erzeugern und Verbrauchern, beispielsweise über intelligente Messsysteme, ermöglichen sie die Beurteilung des Netzzustands, die Erkennung von Engpässen und Störungen sowie die Überwachung der Belastung von Betriebsmitteln. Statusinformationen und Messwerte können auf konventionelle Weise (digitale Eingänge, analoge Eingänge, Direktmessung auf Niederspannungsseite) über bereits in die Primärtechnik integrierte Sensorik (z. B. NH-Sicherungsleiste) erfasst werden. Die Erfassung erfolgt dabei über Standardschnittstellen (z. B. ModbusTCP) an der Primärtechnik.

Erfasste Informationen können nicht nur für die Netzführung, sondern auch für andere Teile der Organisation eine wichtige Entscheidungsbasis darstellen. Beispiele hierfür sind die strategische Netzplanung, die Netzanschlussplanung, die Investplanung, der Service und das Assetmanagement. Aus diesem Grund bietet die Erfassung immer die Möglichkeit, die Informationen nur an die Netzführung, nur an eine allgemein zugängliche Datenbank oder auch an beide zu übermitteln.

Steuerung: Die Steuerung in der Ortsnetzstation erfolgt ebenfalls konventionell über Kontakte oder serielle Schnittstellen. Dies umfasst die Lasttrennschalte auf der Mittelspannungsseite ebenso wie das Zurücksetzen von Kurz-/Erdschlussanzeigern oder die Regelung eines regelbaren Ortsnetztransformators nach erkannten Spannungsproblemen. Die Steuerung von Erzeugern (z. B. Leistungsreduktion) oder Verbrauchern (z. B. gemäß § 14a EnWG) kann sowohl über intelligente Messsysteme (Steuerbox am Smart-Meter-Gateway) als auch über dedizierte Technik am Gerät (FW-Technik, Rundsteuerung etc.) erfolgen.

Neben der Netztransparenz, der Steuerung gemäß § 14a, der schnellen Wiederversorgung, dem Engpassmanagement und der Resilienz ist zweifellos die Cyber-Sicherheit (NIS-2) das Top-Thema, das zwingend angegangen werden muss. Die Erfüllung der Anforderungen aus dem IT-Sicherheitskatalog der BNetzA, der auf das BDEW-Whitepaper in der jeweils aktuellen Fassung verweist, hat bereits entsprechende Schutzmaßnahmen im IT-Umfeld etabliert. Mit zunehmender Intelligenz in den Verteilnetzen rückt jedoch auch das Thema OT-Sicherheit immer stärker in den Fokus – vor allem dort, wo die meisten Prozesse noch manuell betrieben und die Geräte im Feld über den Lebenszyklus hinweg gewartet werden (tabellarisches/manuelles Assetmanagement).

Optimierung: Netzbetreibern bereiten nicht nur Personalengpässe Sorge, sondern auch die Bewältigung der damit verbundenen Komplexität bei der Umsetzung ihrer Aufgaben. Daher ist ein ganzheitlicher, skalierbarer Ansatz im Fernwirk- und Automatisierungsökosystem über alle Spannungsebenen hinweg sowie spartenübergreifend umso wichtiger.

Kernaufgaben im Bereich OT-Sicherheit

Die im Folgenden dargestellten Kernaufgaben müssen dabei etabliert werden.

Inventarisierung: Hierbei werden relevante Daten aller sekundärtechnischen Assets zentral erfasst und verwaltet. Dazu gehören gerätespezifische Informationen wie Name, Artikel- und Serien-

Quelle: Shutterstock

DIe Ortsnetzstation in ihrem klassischen Umfeld

nummern der einzelnen Komponenten, Hard- und Softwarestände sowie Parametrierstände oder Standortdaten. Ein großer Mehrwert entsteht durch die gleichzeitige Erfassung entsprechender Daten von den Netzwerkkomponenten, die oft noch manuell verwaltet werden. Die Netzdokumentation ist so immer auf dem aktuellen Stand, und ungewollte Änderungen können sofort erkannt werden.

Patchmanagement: Ein automatisiertes Patchmanagement lässt sich erst auf Basis der Inventarisierungsinformationen etablieren. Die Gerätehersteller sind verpflichtet, ihre Kunden über bekannte Sicherheitslücken in ihren Systemen zu informieren und entsprechende Patches bereitzustellen. Ein effizienter Rollout ist jedoch nur automatisiert möglich. Die Vorgehensweise variiert je nach Spannungsebene. Zur Risikominimierung unterliegt im Mittel- und Hochspannungsbereich die neue Firmware einer funktionalen Validierung vor einem operativen Rollout. Im Niederspannungsnetz, wo viele Geräte einen hohen Typisierungsgrad aufweisen, erfolgt eine Aktualisierung sukzessive in Gruppen. Die Geräte im Feld müssen die empfangene Firmware auf Integrität prüfen und bei einem fehlerhaften Update ein Rollback auf eine stabile Version durchführen können. In solchen Fällen sind eine remote Ausnahmebehandlung und gegebenenfalls eine Neuübertragung der Firmware erforderlich.

Konfigurations- und Parametermanagement: Typisierung und automatisierte Workflows zur Inbetriebsetzung sind entscheidend für einen effizienten Rollout. Die Geräte werden entsprechend vorkonfiguriert, sodass das Montagepersonal keine speziellen Fernwirk- oder Netzwerkkenntnisse benötigt. Eine elektronische Geräterfassung und Standortzuordnung ermöglicht einen Rollout des passenden Parametersatzes aus der Ferne und erleichtert so einen effizienten exemplarischen oder vollständigen Testlauf. Sowohl Patches als auch Parameteränderungen werden entsprechend verschlüsselt, signiert und validiert, um Manipulationen auszuschließen.

Zertifikatemanagement: Zertifikate sind Teil der Parametrierung und werden für den sicheren Datenaustausch zwischen Fernwirkgerät und Zentrale benötigt. Dabei kommen etablierte Technologien aus dem IT-Sicherheitsumfeld zum Einsatz, zum Beispiel EST (Enrollment over Secure Transport). Softwarekomponenten ermöglichen ein umfassendes Management, sowohl bei der Erstinbetriebnahme als auch beim regelmäßigen Austausch von Zertifikaten.

Mit dem VIVAVIS Device Manager bietet die VIVAVIS AG ihren Kunden ein entsprechendes Werkzeug, das zusammen mit dem Engineeringtool ACOS ET eine einfache, schnelle und sichere Inbetriebnahme sowie ein zentrales Gerätemanagement ermöglicht.

Es ist davon auszugehen, dass vor allem bei kritischen Infrastrukturen, trotz der getroffenen Vorkehrungen, Intrusionsversuche unternommen werden. Um diese rechtzeitig erkennen und abblocken zu können, ist die Überwachung aller Vorgänge sowohl auf Kommunikations- als auch auf Anwendungsebene zwingend erforderlich.

Logging und Logfile-Analyse: Alle Komponenten der VIVAVIS, aber auch Netzwerkkommunikationskomponenten, sind in der Lage, Logfiles mit zum Beispiel Hardware-Zuständen, Fehlern und Zugriffen zu generieren und an einen zentralen SysLog-Server zu senden. Anomalien können dort erkannt werden, sodass sich entsprechende Maßnahmen ableiten lassen.

Network Intrusion Detection (NID): Die verwendeten Protokolle können auf allen Ebenen des OSI-Protokollstacks (z. B. IP, IEC 104, NTP) überwacht werden.

Optimierung: Anomalien werden auf Basis eines konfigurierbaren Regelwerks erkannt, und es können entsprechende Maßnahmen abgeleitet werden, zum Beispiel das Sperren von Ports oder IP-Adressen.

Anomalie-Erkennung: Anomalien können auch aus der Korrelation von Daten aus unterschiedlichen Systemen (z. B. Logfiles, Network Intrusion, Anwendungen) übergeordnet erkannt werden.

Kundenspezifisches Betriebs- und Sicherheitskonzept

Vor allem beim Einsatz der Kleinfernwirkgeräte ACOS 730 oder der modularen ACOS 750 ist bei der sukzessiven fernwirktechnischen Ertüchtigung von Bestandsanlagen in Verteilnetzen oder bei Neubauprojekten ein effizientes Vorgehen unerlässlich. Zusammen mit dem Kunden wird zunächst ein Betriebs- und Sicherheitskonzept erarbeitet, das bei Bedarf eine Ertüchtigung/Erweiterung der bestehenden Anlage beinhaltet, sodass sie für künftige Anforderungen vorbereitet ist. Anschließend wird eine sekundärtechnische Typisierung unter Berücksichtigung der vorhandenen Stationstypen und Anforderungen aus dem Netzbetrieb durchgeführt. Die Bandbreite dieser Typisierung reicht von reinen Edge-Gateways, die Daten aus intelligenter Sensorik, zum Beispiel über Modbus RTU/TCP, auslesen und bedarfsgerecht in die Systeme der Mittelspannungs- und Niederspannungsnetzführung übertragen, bis hin zur vollständigen Automatisierung der Mittelspannungslasttrennschalter, einschließlich der sicherheitsrelevanten Anforderungen, die sich aus NIS-2 ergeben.

Ditmar Niederl,
Head of Products,
VIVAVIS AG, Ettlingen

>> info@vivavis.com

>> www.vivavis.com