Cisco Digital Utilities Whitepaper: Prozesskommunikationsnetze in der Energieversorgung

Inhalt

Whitepaper Prozesskommunikationsnetze in der Energieversorgung

Welche Bedeutung haben Prozesskommunikationsnetze auf unsere Energieversorgung? Welche zusätzlichen Herausforderungen entstehen durch den Ausbau erneuerbarer Energien? Und wie werden diese durch den Einsatz von verfügbaren und sicheren Kommunikationsnetzen gemeistert?

Energiewende und Telekommunikation

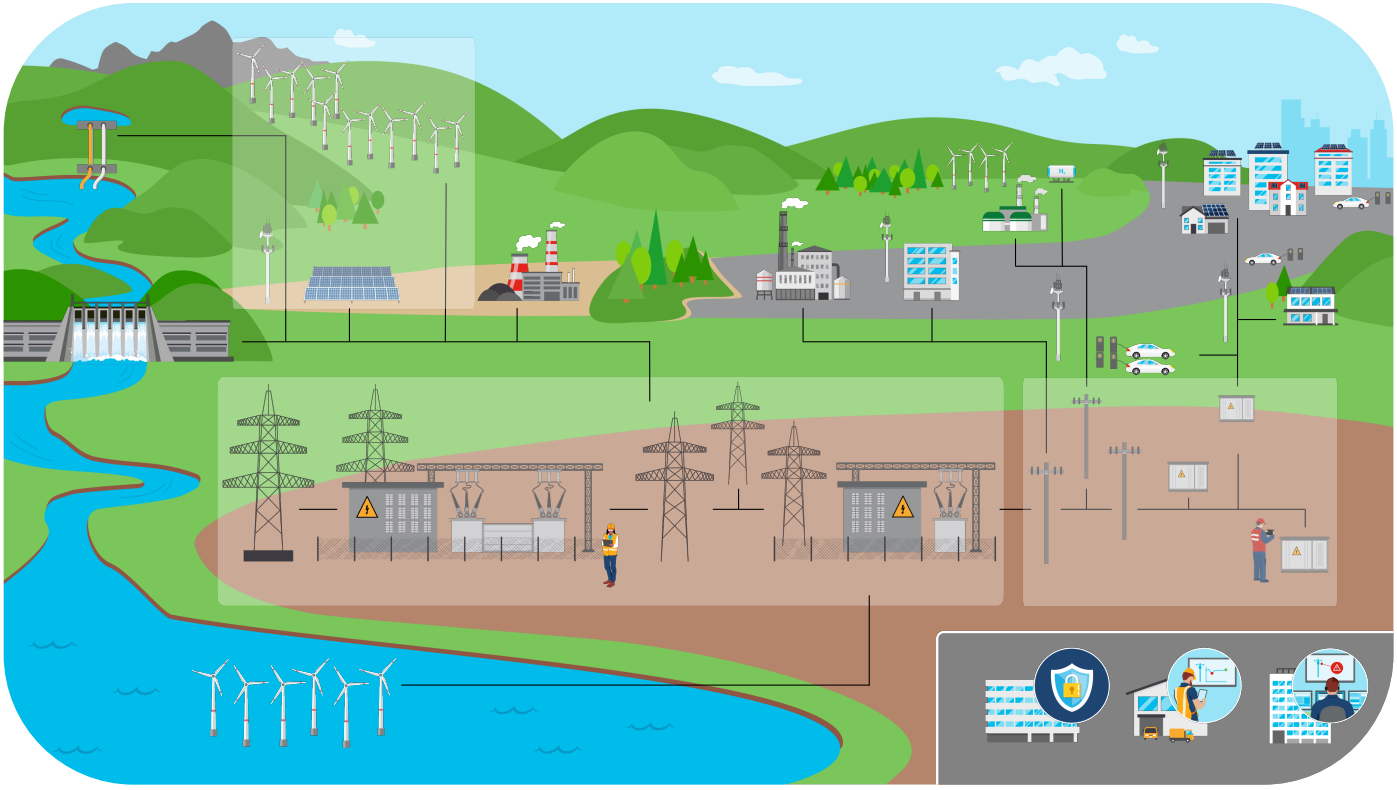
Erneuerbare Energiequellen eröffnen den Weg zur lang erwünschten Minimierung des CO2-Fußabdrucks und damit zu Nachhaltigkeit in der Energieversorgung. Allerdings erfordert der zuverlässige Einsatz von erneuerbaren Energien, dass unsere Stromnetze wesentlich besser überwacht und gesteuert werden müssen als heute. Das Ziel besteht in einer zunehmend automatisierten Systemsteuerung und einer nahezu vollständigen Beobachtbarkeit der Stromnetze. Dieses ist u.a. aufgrund der stark fluktuierenden Einspeisecharakteristik von erneuerbaren Energien wie Wind- und Sonne aber auch stark schwankenden Lasten wie Elektromobilität dringend erforderlich.

Denn durch die Erneuerbaren entsteht eine hohe Dynamik der Energieflüsse im Stromnetz: Mittags erfolgt bei wolkenlosem Himmel die Maximaleinspeisung durch Photovoltaikanlagen. Bei wolkigem Himmel hingegen wird weniger oder gar nicht eingespeist. Ähnliches gilt für die Windenergie, sie schwankt abhängig von der Windstärke. Auch auf der Lastseite steigen die Anforderungen, etwa durch den Ausbau der Elektromobilität und den vermehrten Einsatz von Speichern. Ein stabiler Betrieb unserer Stromnetze erfordert allerdings zu jedem Zeitpunkt ein Gleichgewicht zwischen eingespeister und abgenommener Energie. Kann dieses Gleichgewicht nicht mehr mit bestehenden Regelenergiemechanismen ausgeglichen werden, so kollabiert das Stromnetz. Die letztendliche Konsequenz ist dann ein Blackout (sog. Schwarzfall).

Vor 50 Jahren waren in Deutschland etwa 150 Großkraftwerke in Betrieb. Heute sind über eine Million Erzeugungsanlagen in das Stromnetz in Deutschland integriert. Diese extreme Komplexität lässt sich nur mit modernen Kommunikationstechnologien beherrschen, also mit paketbasierten Kommunikationssystemen. Sie basieren auf Technologien wie Ethernet, MPLS und Internet-Protokoll-basierten (IP-basierten) Übertragungstechniken.

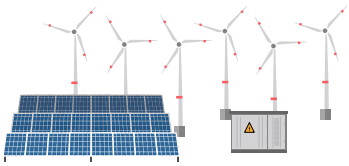
Die Vernetzung der Prozess-Kommunikationsnetze, mit der Außenwelt nimmt immer weiter zu. Denn für die Systemführung werden viele Informationen aus der Außenwelt benötigt. So sind beispielsweise für den Day-Ahead-Forecast zur Einspeisung der erneuerbaren Energien Wetterdaten erforderlich, die von externen Anbietern stammen. Die Steuerung von Windrädern oder Solarparks erfordert eine bidirektionale Kommunikation: Steuerbefehle, etwa um die Einspeiseleistung zu reduzieren, gehen von der Netzleitstelle zum Windrad. Die aktuell eingespeiste Leistung wird im Gegenzug als Messwert zum Leitsystem geschickt. Überdies erfolgt eine intensive Kommunikation zwischen den Energieversorgern untereinander zur Steuerung des Gesamtnetzverbundes in Deutschland und Europa. Wenn Prozessnetze aber keine Inselnetze mehr sind, sondern nach außen vernetzt, können sie auch Ziel von Cyberangriffen werden. Deshalb erfordert der Übergang zu einer offenen Kommunikationsinfrastruktur erhebliche Anstrengungen beim Thema Cybersicherheit. Vernetzung und gleichzeitige Absicherung

ziehen sich durch alle Bereiche der Energieversorgung: Die verschiedenen Spannungsebenen, die Umspannungsanlagen, die Sekundärtechnik oder das Weitverkehrsnetz.



Erneuerbaren Energien und Digitale Ortsnetzstationen

Wie werden erneuerbare Energien und digitale Ortsnetzstationen sicher integriert?



Betrachtet man die Einspeiseleistungen der erneuerbaren Energiequellen je Spannungsebene im Stromnetz in Deutschland, so wird deutlich, dass der überwiegende Teil in das Mittelspannungsnetz eingespeist wird. Danach folgen Hochspannungsebene, Höchstspannung und Niederspannung. Die Erneuerbaren in allen Spannungsebenen verlässlich zu steuern ist für die Netzstabilität unerlässlich. In der Höchstspannungsebene betreiben die Übertragungsnetzbetreiber ihre eigenen, vollständig schwarzfallfesten Glasfasernetze, um die Höchstspannungsnetze sicher zu managen.

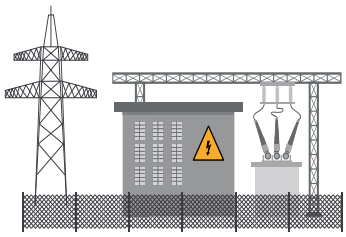
Ähnlich sieht es in der Hochspannungsebene aus. Die Verteilnetzbetreiber betreiben in der Regel auf eigener Glasfaser- oder Kupferinfrastruktur Telekommunikationsdienste – falls erforderlich sogar schwarzfallfest - , um Stromnetze und große erneuerbare Einspeiser sicher zu steuern.

Anders verhält es sich in der Mittel- und Niederspannungsebene: Hier kommen überwiegend Telekommunikationsdienste externer Anbieter zum Einsatz. Insbesondere im Schwarzfall stehen diese Dienste für die systemkritische Steuerung der erneuerbaren Energiequellen bei Netzwiederanlauf nicht zur Verfügung. Die Versorgung, insbesondere der Mittelspannungsebene, mit schwarzfallfesten Kommunikationsdiensten ist demnach eine Aufgabe mit höchster Priorität. Darüber hinaus benötigen im Schwarzfall alle Netzbetreiber zur Koordination von Netztechnikern und Netzführern die Möglichkeit zur Sprachkommunikation. Diese ist mit Satellitenkommunikation heute nur unzureichend möglich.

In der für die Einspeisung erneuerbarer Energien so wichtigen Mittelspannungsebene greifen die Energieversorger auf die Dienste externer Provider zurück, da ihnen eine eigene Kommunikationsinfrastruktur fehlt. Hier nutzen sie typischerweise Mobilfunkdienste wie 4G oder DSL-Verbindungen. Der entscheidende Nachteil dieses Ansatzes ist offensichtlich: Im möglichen Schwarzfall fallen diese Dienste aus und stehen dann – gerade für die in diesem Fall so notwendige Netzsteuerung – nicht zur Verfügung. Das gilt im Übrigen auch für die Niederspannungsebene: Folglich besteht in diesem Bereich aktuell eine Versorgungslücke, die sich jedoch durch die in Deutschland noch junge 450 MHz-LTE-Technik weitgehend schließen lässt. Diese wird dann auch einen schwarzfallfesten Sprachdienst beinhalten, welcher für die Bewältigung von Krisen- oder sogar Katastrophenszenarien dringend erforderlich ist. Im Falle eines Systemwiederanlaufes erfolgt die Sprachkommunikation zwischen Systemführer und den Netztechnikern im Feld dann über einen im Schwarzfall nutzbaren Mobilfunkdienst über das LTE 450-Netz.

Automatisierung von Umspannanlagen and Sekundärtechnik

Automatisierung von Umspannanalagen



Umspannanlagen im Bereich der Hoch- und Höchstspannung sind überwiegend durch Glasfaserkabel angebunden. Die in vielen Fällen eingesetzte Steuerungs- und Kommunikationstechnik nutzt das Potenzial der Glasfaser aber meist noch nicht aus. Steuerungen und Messwertabfragen erfolgen vielfach auf Basis eines seriellen Protokolls aus der IEC 60870 Normen-Familie.

Die neuen Protokolle im Bereich der Norm-Familie IEC 61850 bieten unter anderem Datenmodelle, die die Kommunikation von Geräten und Anlagen untereinander beschreiben. Sowohl IEC61850 als auch IEC 60870-5-104 nutzen paketbasierte Technologien, wie Ethernet und IP. Auf diese Weise kann auch im Bereich der Stationen eine standardisierte Netzwerkinfrastruktur aufgebaut werden. Zur Zeit wird allerdings immer noch ein großer Teil der Steuerungsaufgaben in den deutschen Stromnetzen über das IEC-Protokoll 60870-5-104 abgewickelt. Aspekte aus dem Bereich der Sicherheit, wie das Zonenkonzept nach IEC 62443 oder Security-Ansätze nach IEC 62351 (Standard für Sicherheit in Energiemanagementsystemen), müssen hierbei Berücksichtigung finden. Das ist aber nicht alles: Die Einführung eines Stationsbus- oder Prozessbus-Systems auf Basis von Ethernet ermöglicht zudem eine flexible Integration von neuen Diensten. Darüber hinaus lassen sich so erstmalig alle kommunikationsbasierten Ereignisse in einem Umspannwerk umfassend und transparent überwachen.

Alle Umsetzungen müssen dabei den Sicherheitsrichtlinien und funktionellen Anforderungen entsprechen. Segmentierungen von Datenströmen zur gezielten Isolation von Gruppen ermöglichen eine höhere Sicherheit. Netzwerktechnologien- und Infrastrukturen, basierend auf Hochverfügbarkeitsinfrastrukturen mit HSR (high seamless redundancy) oder PRP (parallel redundancy protocol) sind die Grundlage für die erforderliche hohe Verfügbarkeit.

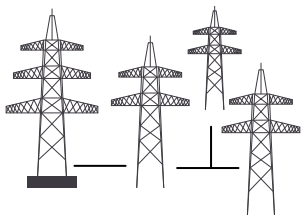
Neue Services, wie Zeitsynchronisierung über das WAN, Remote Administration, zentrales Logging, oder RBAC-basierte (Role based Access Control) Anmeldungen an Komponenten der Sekundärtechnik sind nur einige Beispiele der möglichen neuen Funktionen. Darüber hinaus setzt eine ganze Reihe von zukünftigen Anwendungen, wie zum Beispiel der Einsatz von digitalen Replikaten (digital twins), die neuen Kommunikationstechniken voraus.

Sekundärtechnik

Mit paketbasierten Infrastrukturen ergeben sich viele neue Möglichkeiten in Betrieb und Service von sekundärtechnischen Komponenten. Dieser Ansatz erfordert zwar einerseits die kurz- oder mittelfristige Änderung der Kommunikationsschnittstellen zu IP mit der Anschlusstechnik basierend auf Ethernet, auf der anderen Seite entstehen aber zusätzliche Funktionen, die einen deutlichen Mehrwert im Betrieb erbringen. Ein konkretes Beispiel wäre die zentrale Administration oder Parametrierung von Feldleit- und Schutzkomponenten, die durch den Einsatz von IP-Technologie möglich wird. Allerdings müssen entsprechenden Sicherheitsrichtlinien berücksichtigt werden. Besonders wichtig ist an dieser Stelle die bereichsübergreifende Zusammenarbeit: Die verantwortlichen Abteilungen sollten Anwendungsfälle gemeinsam planen und erstellen – dies ist ein zentraler Arbeitsschritt, wenn ein IP-basiertes Prozess-Kommunikationsnetz einschließlich der dazugehörigen Sicherheitsfunktionen implementiert wird.

Dies gilt insbesondere für den Einsatz von applikationsspezifischen Firewalls, welche Anwendungsprotokolle wie das IEC 60870-5-104 in den Firewall Regeln berücksichtigen und damit einen erheblichen Sicherheitsgewinn liefern.

Weitverkehrsnetz



Das Prozess-Kommunikationsnetz ist für die Steuerung der Stromnetze im Normalbetrieb unverzichtbar geworden. Insbesondere gilt dies für den Systemwiederanlauf im Falle eines Blackouts. Im Bereich der aktiven Komponenten erfolgt derzeit ein Technologiewandel von synchronen Zeitmultiplex-basierten Systemen hin zu paketorientierten Technologien, wie IP (Internet Protocol und MPLS (Multiprotocol Label Switching). Heute sind vielfach noch SDH- (Synchrone Digitale Hierarchie) und PDH-Systeme (Plesiochrone Digitale Hierarchie) im Einsatz. Diese sind allerdings von den Herstellern bereits abgekündigt und werden meist nicht mehr weiter unterstützt. Deshalb gilt es, in den kommenden Jahren zu handeln. Als Übertragungsmedium zu den Automatisierungsgeräten kommen paketbasierte Technologien zum Einsatz, die schon seit langem im Carrier- und Bürobereich verwendet werden.

Paketbasierte Technologien haben im Ursprung keine intrinsische Echtzeitfähigkeit wie die früheren Zeitmultiplexverfahren. Traffic-Engineering-Mechanismen schaffen hier jedoch auf der MPLS- und IP-Ebene die geforderte Echtzeitfähigkeit. So lassen sich dann unter anderem auch die hohen Anforderungen für den Anschluss von Schutzrelais erfüllen: Hier geht es um sehr hohe Standards hinsichtlich der Latenzzeiten und dem damit in Verbindung stehenden Jitter. Für gute Sprachübertragung gelten ähnliche, jedoch weniger strenge Echtzeitbedingungen.

Hinzu kommt die Forderung nach garantierter Übertragung, beispielsweise von Schaltbefehlen. Sie lässt sich durch Quittierungsmechanismen erreichen. Diese Maßnahmen sind allerdings für hochverfügbare Kommunikation in der Energieversorgung immer noch nicht ausreichend. Um die Verbindungen auch bei unterbrochenen Kommunikationsleitungen nutzen zu können, ist eine Redundanz in der Topologie erforderlich. Sie erfolgt – ähnlich wie im Stromnetz – etwa durch die Bildung von Ringen oder vermaschten Netzen, die immer zwei mögliche Kommunikationspfade zu kritischen Stationen bereitstellen. Zudem wird die gesamte aktive Kommunikationstechnik mit Batterien und Netzersatzanlagen ausgerüstet. Dies dient dazu, im Schwarzfall unabhängig von der Stromversorgung zu sein.

Mit den beschriebenen Maßnahmen wird die höchste Verfügbarkeit der Kommunikationsdienste sichergestellt – auch im Schwarzfall.

OT Security

Die paketbasierte Kommunikationstechnologie bietet einen entscheidenden Vorteil: die Skalierbarkeit. Zudem ist sie offen, sodass die Systeme herstellerübergreifend umgesetzt werden können. Darüber hinaus hat der Markt große Erfahrung mit paketbasierten Kommunikationssystemen aus dem Bereich der Carrier und der Bürokommunikation. Allerdings stellen vor allem die Offenheit und Kopplung von IP-Netzen eine der größten Herausforderungen dar: Wie schützt man die IP-Netze gegen Hackerangriffe von außen und innen? Hier lassen sich viele Lösungen und Konzepte aus dem Carrier-Geschäft und aus der Bürokommunikation nutzen – wenn auch in abgewandelter Form.

Maßnahmen für eine effektive und robuste Cybersicherheit

Paketbasierte Technologien haben sich im IT-Bereich als Standard etabliert – deren Offenheit jedoch bietet auch das Potenzial für Angriffe durch Hacker. Deshalb ist Cybersicherheit an dieser Stelle besonders wichtig. Insbesondere IP-basierte Kommunikationssysteme dürfen im Bereich Energienetze, beispielsweise kritische Infrastruktur, nur zusammen mit wirksamen Maßnahmen für Cybersicherheit eingesetzt werden. Anderenfalls ist das Angriffsrisiko und somit die Bedrohung für die Versorgungssicherheit eines Landes unkalkulierbar hoch. Energieversorgung ist nur dann gewährleistet, wenn es auch die Kommunikationsdienste sind, mit denen die Energienetze gesteuert werden. Sicherheit gemäß eines Zero-Trust-Ansatzes zu

gestalten, ist daher unerlässlich: Dieses Konzept beinhaltet, grundsätzlich keinem Gerät, Nutzer oder Dienst innerhalb oder außerhalb des eigenen Netzwerks ungeprüft zu vertrauen. Entsprechend umfangreich muss daher auch die Authentifizierung und Rechtevergabe gestaltet sein. Der Einsatz von PKI-Systemen (Public Key Infrastructure) liefert in Zeiten des durch die Digitalisierung der Stromnetze stark anwachsenden Einsatz von Mess- und Automatisierungsystemen die Sicherheit, nach Zertifikatsüberprüfung ein neues Gerät ohne Risiken in das Prozess-Kommunikationsnetz aufzunehmen. Darüber hinaus liefert die Schlüsselverteilung die Grundlage für eine hochgesicherte Datenübertragung.

Schutz der Steuerungs- und Kontrollsysteme

In der Praxis der Cybersicherheit ist der erste Schritt der Schutz der sogenannten Perimeter, also der Übergänge des Prozess-Kommunikationsnetzes zur Außenwelt. Die offensichtliche Lösung ist hier der Einsatz von Nextgeneration Firewalls, welche auf der Anwendungsebene fungieren, die bereits in der Bürokommunikationswelt erfolgreich zur Anwendung kommen. Hier kommt die erste Herausforderung: Die in Energienetzen eingesetzten Kommunikationsprotokolle unterscheiden sich deutlich von denen im Bürobereich. Identisch sind lediglich die Ethernet-Technologie, das Internet-Protokoll auf der Ebene 3 des OSI-Schichtenmodells sowie TCP (Transmission Control Protocol) und UDP (User Datagram Protocol) in der Transportebene. Die sogenannte Anwendungsschicht (Schicht 7) basiert in den Energiesystemen in Deutschland auf den von der International Electrotechnical Commission (IEC) entwickelten Protokollen. Ein weit verbreitetes Protokoll ist das IEC 60870-5-104. Dieses Protokoll wird zur Steuerung von Umspannwerken verwendet, aber auch zur Anbindung von Windkraftanlagen. Diese Anlagen sind oft physikalisch nicht besonders geschützt, deshalb können Unbefugte unter bestimmten Umständen auf die Kommunikationsverbindungen zugreifen. Kommt an der zentralen Übergabestelle zum Prozessnetz eine Schicht-7-Firewall zum Einsatz, so lässt sich etwa die Kommunikation zwischen Windrad und Netzleitstelle exakt auf die vorgesehene Kommunikation eingrenzen. Auch der Missbrauch durch Nutzung weiterer Befehle im Funktionsumfang des IEC-104-Protokolls lässt sich damit unterbinden.

Diese Eingrenzung wird durch entsprechende Firewall-Regeln erzielt. Sie müssen allerdings über das gesamte Prozess-Kommunikationsnetz konsistent eingehalten werden, um den gewünschten Schutz zu bieten. Hierfür sind wiederum Firewall-Management-Systeme erforderlich, die sämtliche Regeln auf Konsistenz prüfen und die Regelverwaltung automatisieren. So lassen sich nicht nur Fehler in manuellen Prozessen vermeiden, sondern auch noch die Betriebskosten senken.

Zudem muss das Prozess-Kommunikationsnetz unbedingt in mehrere Zonen eingeteilt werden. So ist bei einem Angriff nicht das gesamte Netz betroffen, sondern lediglich ein kleiner funktionaler Teil. Aus dieser Segmentierung folgt allerdings, dass es eine große Zahl an Firewall-Regeln zu verwalten gilt. Das spricht zusätzlich dafür, ein entsprechendes Firewall-Regel-Managementsystem einzusetzen.

Monitoringsysteme und Sicherheitsplatformen

Nach diesen Basisschutzmaßnahmen folgt der Einsatz von Monitoringsystemen für die Prozessnetze. Sie überwachen den Datenverkehr im Prozess-Kommunikationsnetz und untersuchen ihn auf Abweichungen von konfigurierten und zu erwartenden Kommunikationsmustern. Diese Systeme müssen nicht nur das IP-Protokoll beherrschen, sondern auch die in der Energieinfrastruktur eingesetzten IEC-Anwendungsprotokolle analysieren können. Hierfür kommen beispielsweise die Protokolle IEC 60870-5-104, IEC 61850 oder auch TASE.2/ICCP zur Anwendung. Letztgenanntes wird verwendet, um Netzleitsysteme zu koppeln. Diese Monitorsysteme überwachen nicht nur die Datenströme und schauen nach unbekannten Netzwerkadressen. Sie erkennen so mögliche Angriffsmuster im Kontext des jeweiligen Anwendungsprotokolls. In diesem Fall spricht man von Intrusion-Detection.

Im Falle eines erkannten Problems werden – ähnlich wie bei Firewall-Systemen – vom Monitorsystem Alarmmeldungen generiert. Dies kann jedoch dazu führen, dass im Problemfall sehr viele Alarme ausgelöst werden. Dadurch kann es für den Operator unmöglich werden, einen Überblick über die Lage zu erhalten. Deshalb setzt man im IT-Umfeld schon seit geraumer Zeit sogenannte Security Information and Event Management (SIEM)-Systeme ein. Auch im OT-Umfeld komprimieren die SIEM-Systeme den Informationsgehalt der vielen Alarm- und Statusmeldungen durch Korrelation und Bündelung. So erhält der Operator nur eine Essenz der Informationen und somit schnell einen Überblick über die Lage im Prozess-Kommunikationsnetz. Auf diese Weise kann er entsprechend schnell Entscheidungen treffen und effektive Maßnahmen zum Schutz der Infrastruktur einleiten.

Arbeitswelt

Wie kann die Digitalisierung der Arbeitswelt gestaltet werden?

Arbeitswelten unterliegen einem konstanten Wandel. In den letzten Jahren haben sich viele neue Dienste und Technologien im Konsumentenbereich etabliert, die ihren direkten Weg in das Arbeitsleben suchen – und das gilt auch für den Bereich der Energieversorgung. Viele dieser Technologien lassen sich im professionellen Umfeld problemlos integrieren, hierzu zählen zum Beispiel Lösungen aus dem Bereich der Sprach- und Videokommunikation, dem Chat oder dem Sharing von Anwendungen oder Dateien. Gerade angesichts des Fachkräftemangels und immer komplexeren Anforderungen, die einen verstärkten Austausch erfordern, bieten sie eine Möglichkeit, das Arbeitsleben effizienter zu gestalten.

Zudem entstehen auch Veränderungen in der Anwendung von Daten und Applikationen, viele bisher auf Papier realisierte Lösungen werden digitalisiert und den Mitarbeitenden online zur Verfügung gestellt. Neue Technologien erlauben Veränderungen in der täglichen Arbeitsplanung und Umsetzung, Augmented Reality etwa unterstützt Mitarbeitende beim Zugriff auf online verfügbare Dokumentationen. Räumlich getrennte KollegInnen können per Videokonferenz live unterstützen und mit Rat und Tat zur Seite stehen. Bei allen Vorteilen muss die Maßgabe hier allerdings stets lauten, nur Geräte und Dienste zu verwenden, die höchsten Sicherheitsstandards genügen.

Neben Technologien aus dem Bereich Kollaboration kommen beim Thema Arbeitswelt auch weitere Aspekte, wie Sicherheit im Zugriff, Erreichbarkeit sowie der Übergang zwischen unterschiedlichen Medien, hinzu. Sie müssen ganzheitlich betrachtet werden. Das Weitverkehrs-MPLS/IP-Netzwerk kann eine gute Grundlage für eine skalierbare und sichere Erreichbarkeit darstellen. Aber es sollte nicht nur in den Blick genommen werden, wie sich Technologie nutzen lässt und welche Vorteile sie mit sich bringt. Ebenso wichtig sind die Funktionsfähigkeit und Robustheit der Lösungen im Krisenfall. Die Abhängigkeit, aber auch die Nutzungsgewohnheit, muss von Fall zu Fall bewertet und entschieden werden.

Zusammenfassung

Zusammenfassend lässt sich festhalten, dass die Kommunikationstechnik unabdingbare Voraussetzung für eine erfolgreiche Umsetzung der Energiewende ist. Gleichzeitig hängt die Versorgungssicherheit moderner Energiesysteme unmittelbar von der Verfügbarkeit der zur Steuerung und Überwachung der Energienetze eingesetzten Kommunikationsdienste ab. Ein höchsteffektiver Schutz in Form von Cyber-Security für die Prozess-Kommunikationsnetze ist deshalb essentielle Voraussetzung für einen sicheren Stromnetzbetrieb.

Sie wollen mehr erfahren? Nähere Infos finden Sie auf unsere Website für den Energiesektor: www.cisco.de/Energiesektor