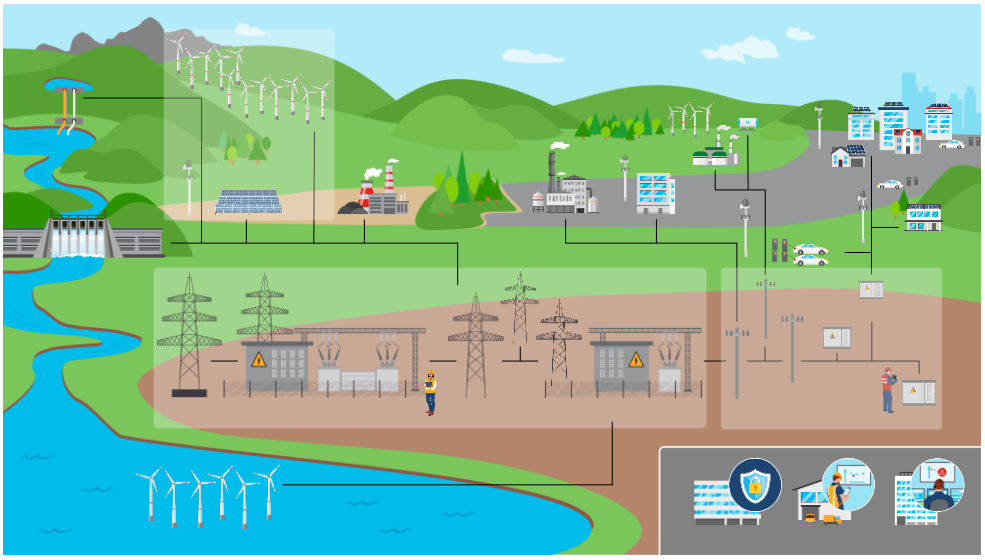
Cisco Digital Utilities: Sichere Integration erneuerbarer Energien & Digitaler Ortsnetzstationen

Sichere Integration erneuerbarer Energien und Digitaler Ortsnetzstationen



Energiewende und Telekommunikation

Der Klimawandel rückt die Energiebranche ins Zentrum der Dekarbonisierung. Denn ohne sie gibt es zukünftig weder flächendeckende Elektromobilität noch grünen Wasserstoff für die Industrie. Das Energienetz ändert sich aufgrund der erneuerbaren Energien aktuell fundamental: Wind- und Photovoltaikanlagen, mehr Offshore und Dezentralität – all das erfordert neue Steuerungs- und Speichertechnologien, um die hohe Stabilität im Netz zu erhalten. Dabei müssen Erzeuger und VerbraucherInnen gleichermaßen eingebunden werden. Denn können wir die Versorgungssicherheit nicht gewährleisten, bricht die Akzeptanz der Gesellschaft und der Wirtschaft für Klimaneutralität weg und die Energiewende scheitert.

VerbraucherInnen versorgen sich zukünftig teilweise selbst mit Energie oder speisen diese in das Stromnetz ein, beispielsweise durch Solaranlagen auf dem Dach. Diese Veränderung hin zum „Prosumer“, die zunehmende Einspeisung aus erneuerbaren Energien und die steigende Nachfrage nach Ladestrom für Elektromobilität gefährden durch ihre starken Schwankungen die Versorgungssicherheit. Eine weitere Einflussgröße sind immer häufigere Extremwetterlagen, die die Verfügbarkeit von Solar- und Windenergie beeinflussen.

In der Vergangenheit erfolgte die Versorgung mit Energie durch ca. 150 konventionelle Kraftwerke, die auf der Hoch- oder Höchstspannungsebene angebunden sind. Ein Netzbereich, der kommunikationstechnisch gut angebunden und damit auch gut kontrollierbar ist. Betrachtet man die gesamte installierte Leistung in Deutschland für das Jahr 2020, zeigt sich, dass ca. 56 Prozent der installierten Leistung von insgesamt 225 GW auf erneuerbare Energien entfallen. In der Energieerzeugung werden ca. 42 Prozent der verbrauchten 540 TWh durch erneuerbare Energien gestellt (Quelle: BDEW 2021, Kapazität und Erzeugung 2020). 2019 sind insgesamt 1,9 Millionen erneuerbare Energieanlagen gelistet, von denen ca. 450T Anlagen nach §9 (1,2) regelbar sind und eine Gesamtleistung von 104 GW erbringen. Differenziert man diese Anlagen nach den Spannungsebene, so sind ca. 60 GW auf der Mittel- und Niederspannung angebunden (Quelle: BNetzA, EEG in Zahlen 2019). Dieser Wert stellt rund ein Viertel der gesamten installierten Leistung dar.

Daraus ergibt sich ein Bedarf für mehr digitale Messung (Visibilität, Strom und Spannung, Power Quality, Kurzschluss- und Erdschlussüberwachung), Steuerung (Eingriff aus dem Leitsystem, Schalten) und Regelung (dezentrale Automatiken, regelbare Transformatoren) der Stromnetze im Bereich der Mittel- und Niederspannung (MS/NS). Ortsnetzstationen und auch Standorte der erneuerbaren Energieerzeugung müssen kommunikationstechnisch angebunden werden.

Die Versorgung, insbesondere der Mittelspannungsebene, mit schwarzfallfesten Kommunikationsdiensten ist eine Aufgabe mit höchster Priorität. Denn während in der Höchst- und Hochspannungsebene Energieversorger eigene Glasfasernetze und Kupferinfrastruktur betreiben, kommen in der Mittel- und Niederspannungsebene überwiegend Telekommunikationsdienste externer Anbieter zum Einsatz. Insbesondere im Schwarzfall (Brownout, Blackout) stehen diese Dienste für die systemkritische Steuerung der erneuerbaren Energiequellen bei Netzwiederanlauf nicht zur Verfügung. Darüber hinaus benötigen im Schwarzfall alle Netzbetreiber zur Koordination von NetztechnikerInnen und NetzführerInnen die Möglichkeit zur Sprachkommunikation. Hier besteht Nachholbedarf.

Um erneuerbare Energien sicher in unser Energienetz zu integrieren, werden Kommunikationslösungen benötigt, die digitale Ortsnetzstationen und die verteilten Erzeugungspunkte anbinden. Sie sorgen für eine bessere Steuerbarkeit und Transparenz von Mittel- und Niederspannungsnetzen. Der Einsatz der Kommunikationstechnologie trägt entscheidend dazu bei, die Versorgungssicherheit im Zuge der Energiewende zu gewährleisten.

Im Folgenden wird beschrieben, wie eine generelle Anbindung von Standorten in Form von Kommunikationsstrukturen aussehen kann. Dabei geht es zunächst um den klassischen Aufbau einer solchen Anbindung, danach um die Möglichkeiten eines moderneren Aufbaus am Beispiel von SD-WAN. Auch potenzielle erweiterte Funktionen werden in einem eigenen Kapitel behandelt. Ein wichtiger, nicht zu vernachlässigender Faktor bei kritischen Infrastrukturen ist selbstverständlich die Sicherheit von Kommunikationsstrukturen, die ebenfalls in diesem Papier besprochen wird. Das abschließende Kapitel zum Management stellt dar, welche Lösungen zur Steuerung und Verwaltung existieren und welche Anforderungen auf Kundenseite bestehen.

Generelle Anbindung der Standorte

In Deutschland sind die meisten Anlagen im Mittel- und Niederspannungsbereich kommunikationstechnisch noch nicht angebunden. Diese müssen jetzt durch IP-basierte Systeme erschlossen werden. In der Umsetzung werden dabei Komponenten zur Kommunikation (Router) und zur Prozessanbindungen eingesetzt. Router sind Systeme, die eine ganze Reihe an Funktionen mitbringen. Neben Hardware-Flexibilität (modularer Aufbau der Geräte) zur Anbindung unterschiedlicher Schlüsseltechnologien wie LTE, DSL, Private LTE oder LTE 450 MHz werden auch Software-Features immer relevanter. Dazu zählen z.B. die Optionen, eigene Software zu hosten oder umfangreichere Sicherheitsfunktionen zu realisieren.

Um eine sichere Anbindung der digitalen Ortsnetzstationen und anderer Standorte zu gewährleisten, muss die Kommunikationsinfrastruktur bestimmte Funktionen aufweisen. Dazu gehören Schnittstellen, die eine Standardisierung der Anbindung ermöglichen. Folgende Verbindungskategorien werden heute in der Regel genutzt:

- DSL

  Als digitale Breitband-Verbindung über das Telefonnetz via Kupferleitungen bietet DSL eine hohe Datenübertragungsrate. Als Gegenstelle kommen hier öffentliche Carrier zum Einsatz.

- Fiber (Glasfaser)

  Als Alternative zu DSL können auch Fiber-Anbindungen zum Einsatz kommen. Oftmals werden auch die Glasfaserleitungen von öffentlichen Carriern zur Verfügung gestellt.

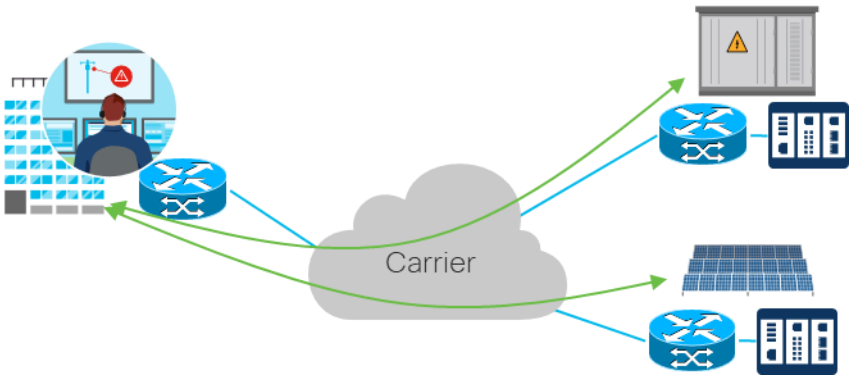
- Public LTE

  Neben den kabelgebundenen Lösungen wie DSL und Glasfaser, werden auch öffentliche Mobilfunknetze zur Anbindung genutzt. Sie stellen oftmals die einzige Lösungsoption zur Erschließung von Anlagen dar. DSL-Verbindungen oder sogar Glasfaseranschlüsse sind meistens nur mit Kostenbeteiligungen durch die Energieversorger realisierbar.

- LTE450

  Eine Alternative zum öffentlichen Mobilfunknetz wird das schwarzfallfeste Netz der 450Connect bieten. Es werden ähnliche Technologien wie im öffentlichen LTE-Bereich eingesetzt. Zu beachten ist hierbei die reduzierte Bandbreite in der Übertragung im Vergleich zu einem öffentlichen Mobilfunknetz. Die Sprachkommunikation zur Koordination von NetztechnikerInnen und NetzführerInnen im Schwarzfall ist ebenfalls mit LTE450 möglich.

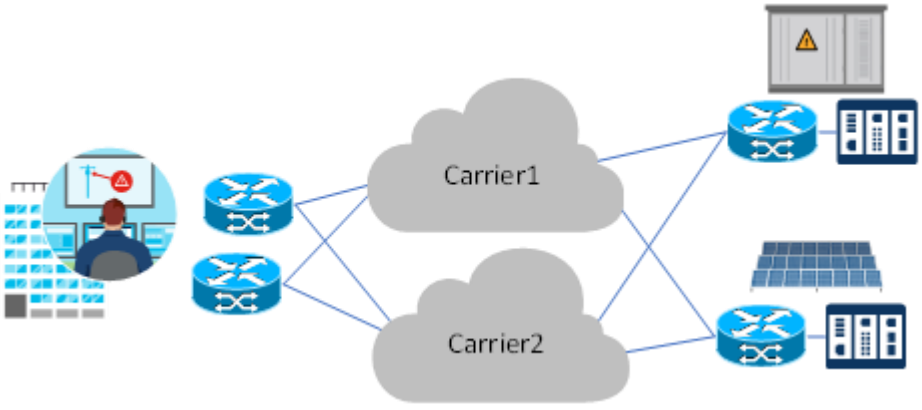
Der generische Aufbau einer Topologie besteht immer aus einer zentralen Komponente, dem Headend-Router und den verteilten Außenstellen (Edge) in der Fläche. Zusätzlich sind Systeme zum Betrieb erforderlich, die z.B. die Identität der Edge-Systeme überprüfen können, Zertifikate verteilen und prüfen oder den gesamten Lebenszyklus von der Inbetriebnahme bis zur Deaktivierung eines Routers in der Fläche managen. Die Kommunikation hat grundsätzlich verschlüsselt zu erfolgen. Hierbei müssen vom BSI freigegebene Verschlüsselungsverfahren und -tiefen eingesetzt werden.



Das Kommunikationssystem muss derart gestaltet sein, dass die geplante Anzahl von Außenstellen (Edge) mit den gewünschten Funktionen gleichzeitig bedient werden kann. Als Grundlage stehen hier Architekturen auf Basis von Generic Routing Encapsulation (GRE) Tunneln, FlexVPN oder DMVPN Konzepten zur Verfügung. Routingprotokolle aus den Familien BGP, EIGRP, OSPF oder ISIS unterstützen beim Aufbau der Topologien. Sind Abgrenzungen zwischen Anwendungen erforderlich, können virtuelle Routing Forwarding Instanzen (vrf) genutzt werden.

Die geplanten Kommunikationsbeziehungen sind eine wichtige Grundlage für das Design eines Netzwerkes. Werden nur Verbindungen von den Außenstellen zur Zentrale gewünscht (Headend to Edge), so kann die Konfiguration recht einfach gehalten werden. Sind Kommunikationen zwischen den Außenstellen (Edge to Edge) notwendig oder kommen weitere zu separierende Anwendungen hinzu, so werden die Konfigurationen komplexer und der Verwaltungsaufwand steigt.

Einen weiteren Einfluss auf die Planung haben die notwendigen Redundanzen in der Anbindung. Werden alternative Anbindungen zur Verfügung gestellt, z.B. eine primäre Anbindung über DSL und eine Backup Strecke über öffentlichen Mobilfunk, müssen die dabei zu verwendenden Verschlüsselungstechnologien und Protokolle für die Nutzung der Redundanzen ausgelegt werden.



Viele Lösungen für die Anforderungen sind verfügbar und müssen aufeinander abgestimmt werden. Erst eine ganzheitliche Planung ermöglicht ein zielgerichtetes Design. Neben den mehr technischen Parametern aus Sicht

des Kommunikationssystems sind auch Rahmenparameter aus Sicht der Führung des Energienetzes zu berücksichtigen. Als Beispiel ist die Frage zu klären, wie viele Außenstellen aus Gründen der Ausfallsicherheit auf einer einzelnen Plattform betrieben werden dürfen.

Einsatz von SD-Wan

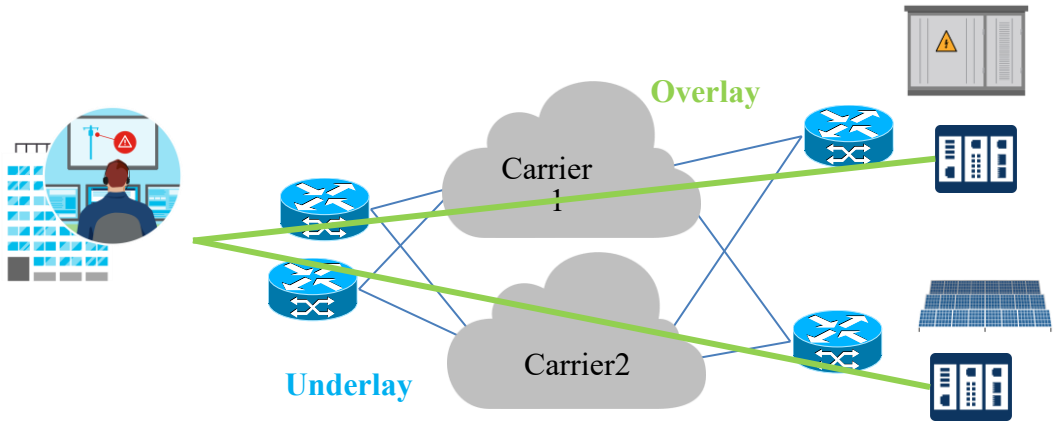
Für viele Anwendungsfälle lohnt sich der Blick auf einen moderneren Aufbau der Kommunikationsstruktur von Standorten. Ein Beispiel hierfür ist das Software Defined WAN.

Eine Software Defined WAN Lösung (SD-WAN) ist eine Overlay Architektur aus dem Enterprise Bereich, die Unternehmen eine hochflexible Plattform für die Digitalisierung zur Verfügung stellt. Eine SD-WAN Lösung integriert Routing, Sicherheit, Flexibilität und zentrale Orchestrierung. Anwendungsorientierung und Mandantenfähigkeit sind Grundelemente einer SD-WAN Lösung.

Zu den Vorteilen zählen:

- Zentralisiertes Netzwerk- und Richtlinienmanagement zur Realisierung einfacher Betriebsabläufe und zur Einhaltung von Compliance Regeln
- Transportnetz unabhängige Overlay-Struktur, die im Edge, in der Zentrale und auch in der Cloud eingesetzt werden kann
- Beliebige Kombination von Anbindungsoptionen im Transportnetz mit der Möglichkeit, eine einfache Redundanz zur Verfügung zu stellen oder alternativ eine anwendungsabhänge Lastverteilung auf Schnittstellen im Transportnetz zu realisieren
- Flexible Gestaltung von Overlay-Topologien mit Sterninfrastrukturen, Mesh Umgebungen, partiellem Mesh oder weiteren Kombinationen
- Mandantenfähigkeit der Overlay-Infrastruktur mit dedizierten Overlay-Topologien je Mandant
- Strikte Trennung von Kontroll- und Datenebene zur Erhöhung der Sicherheit und Stabilität
- Robuste und umfassende Sicherheit, einschließlich starker Verschlüsselung von Daten, End-to-End-Netzwerksegmentierung, Router- und Controller-Zertifikatsidentität mit Zero-Trust-Sicherheitsmodell, Schutz auf Kontrollebene und Anwendungs-Firewall
- Einfache Integration des Cloud-Anbieters sowohl im Umfeld der Private als auch Public Cloud
- Anwendungstransparenz und -erkennung sowie anwendungsorientierte Richtlinien, dynamische Optimierung von Anwendung zur Einhaltung von SLA

SD-WAN ist eine Technologie, die im Enterprise-Umfeld seit etlichen Jahren standardmäßig eingesetzt wird und sich erfolgreich etabliert hat. Im Wesentlichen besteht sie aus Routern für die Weiterleitung der Nutz-Daten und aus zentralen Komponenten (Controller) für die Steuerung und Administration. Eine SD-WAN-Lösung stellt eine Plattform dar, in der die Weiterleitung von Daten zwischen Endpunkten durch zentrale Controller gesteuert und vorgegeben wird. Die Controller sind bei dieser Lösung nie aktiv an der Weiterleitung oder der Entscheidungsfindung beteiligt. Controller können in der Cloud aber auch vollständig ohne Cloud bereitgestellt werden. Ihre Funktionen sind in einer verteilten Architektur vollkommen redundant zu realisieren.



Die in der Skizze beispielhaft gezeigten Carrier 1 und 2 können unterschiedliche Anbieter und Technologien sein. Carrier 1 könnte z.B. das öffentliche LTE-Netz und Carrier 2 das 450MHz LTE sein. Im Overlay-Netzwerk werden die eigentlichen Anwendungsdaten, z.B. IEC 60870-5-104, transportiert.

Wie lassen sich die Vorteile der Technologie im Umfeld der Anbindung erneuerbarer Energien und Ortsnetzstationen einsetzen? Geht man von einem Szenario mit einer (redundanten) Zentrale und vielen Außenstellen aus, die im Schwerpunkt die Anbindung mit dem Protokoll IEC60870-5-104 zwischen Außenstellen und Leitsystem zur Verfügung stellt, so ergeben sich folgende Vorteile:

- Im alltäglichen Betrieb gibt es unterschiedliche Tätigkeiten, die durch die Controller vollumfänglich unterstützt werden (move, add, change, delete). Es finden hier keine geräteorientierten Konfigurationen statt, sondern zentrale Richtlinien werden auf einem zugelassenen neuen Gerät ausgerollt. Bestandteile der Richtlinien sind Betriebs- und Sicherheitsanforderungen. Modifikationen der Richtlinien sind einfach auch für bereits ausgerollte Geräte möglich. Hierdurch ergibt sich eine sehr einfache und effiziente Betriebsumsetzung.
- Eine klare Trennung von Overlay- und Underlay-Netzwerken, sodass die unternehmensspezifischen Richtlinien vom Underlay-Netzwerk des Carriers getrennt sind. Carrier können einfach ausgetauscht oder gemischt werden.
- Mandanten können einfach mit sicherheitsspezifischen und topologischen Anforderungen definiert und in der Fläche ausgerollt werden. Aktuell ist es im Schwerpunkt ein Mandant, der die verschlüsselte Kommunikation zwischen den Außenstellen und der Zentrale in einem Stern für das Protokoll IEC60870-5-104 realisiert. Ein weiterer Mandant könnte zum Beispiel für die Fernwartung ergänzt werden.
- Die Qualität der Anbindungen kann leicht überwacht und gemessen werden. Überwachungen finden hier nicht nur auf Ebene der Schnittstellen statt, sondern die bereitgestellte Übertragungsqualität für eine Anwendung kann gemessen werden.

Anforderungen im Bereich der Ortsnetzstationen und erneuerbaren Energien werden über die Zeit steigen. Aus diesem Grund müssen die Infrastruktur und die Architektur der Underlay- und Overlay-Netzwerke enorme Flexibilität aufweisen. Jede Interaktion, die einen Vor-Ort-Einsatz oder den Austausch von Komponenten bzw. zusätzliche Komponenten erfordert, ist möglichst zu vermeiden. Die einfache Anpassung von zentralen Richtlinien ermöglicht einen flexiblen und effizienten Betrieb der Infrastruktur.

Erweiterte Vorteile und Umsetzungen:

- Integration weiterer Mandanten

  Ein Mandant ist eine technische Abbildung einer isolierten Anwendergruppe. Beispiele sind Administratoren, Fernservicetechniker etc. Die Ergänzung von Services auf der gleichen Infrastruktur, wie z.B. der Fernservice von Komponenten der Station, die zusätzliche Aufnahme von Sensordaten, die Integration von Outtasking für betriebliche Funktionen und die Übertragung von Smartmeter-Daten sind Anforderungen, die sich einfach über Mandanten lösen lassen. Neben der sicherheitstechnischen Trennung der Mandanten in einem dedizierten Overlay, können sie auch in der Übertragung auf dem Underlay entsprechend priorisiert und überwacht werden.

- Anbindung Cloud-Dienste

  Ein Cloud-Dienst ist aus Sicht einer SD-WAN-Infrastruktur nur ein weiterer möglicher Endpunkt in der Topologie eines Mandanten. Er kann daher einfach in Underlay- und Overlay-Definitionen eingebunden werden. Die Konnektivität zu einem Cloud-Dienst erfolgt auf Basis der gleichen Sicherheitsrichtlinien, wie auch die Anbindung einer anderen Außenstelle. Die sicherheitstechnischen Aspekte sind also nicht von den Möglichkeiten eines eingesetzten Protokolls abhängig und müssen auch nicht pro Protokoll definiert, konfiguriert und gemonitort werden, sondern sind auf der Kommunikationsstrecke implementiert. Protokolle wie z.B. OPC-UA, MQTT oder COAP nutzen einfach die Sicherheitsfunktionen des Overlays.

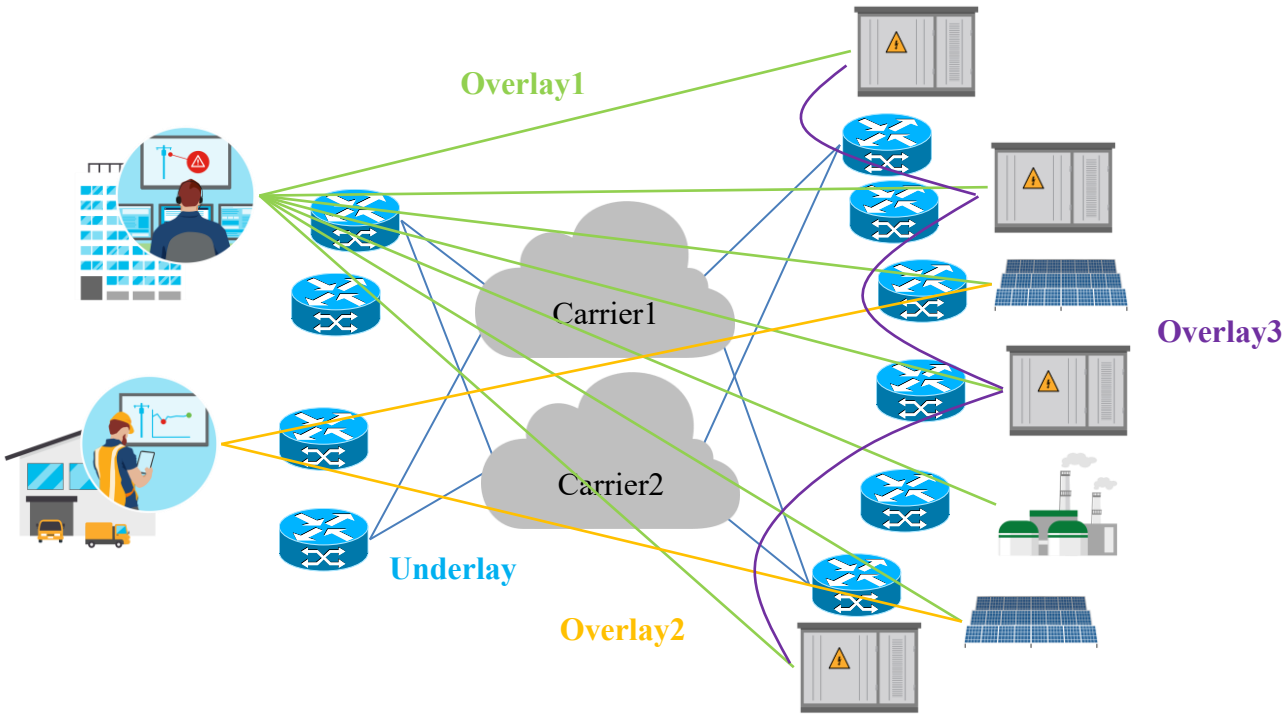
- Flexible Gestaltung von Topologien

  Heutige Implementierungen im Bereich IEC 60870-5-104 erfordern eine Kommunikation in einer Sterntopologie: Die Außenstellen kommunizieren ausschließlich sternförmig mit einer Zentrale. Die zukünftige Einführung von z.B. regelbaren Ortsnetztransformatoren unter dem Gesichtspunkt Microgrid erfordert auch eine Kommunikation zwischen den Ortsnetzstationen, die auf dem gleichen Mittelspannungsabgang der Umspannanlage in Reihe geschaltet sind. In einer sternförmigen Kommunikation muss ein solcher Verkehr immer über die zentrale Stelle laufen, ein Ansatz, der schnell an Skalierungsgrenzen kommen wird. Das Ausbilden von partiellen Mesh-Elementen im Overlay eines SD-WAN kann hier einfach eine sichere Lösung bereitstellen. Eine Anzahl der Ortsnetzstationen kann mit der zugehörigen Umspannanlage zur Steuerung kommunizieren, ohne andere Teilnehmer zu involvieren oder Sicherheitsanforderungen zu verletzen.

- Redundanzen in der Anbindung

  Die Konnektivität zu Außenstellen kann über eine dedizierte Leitung bereitgestellt werden. Ergänzt man Redundanzen, so gibt es unterschiedliche Konzepte der Integration. Eine Anbindung, die vollständig im „cold Standby“ ist, wird nicht aktiv auf Funktionsfähigkeit geprüft und stellt eine kritische Implementierung dar. Eine Leitung im „hot Standby“ wird aktiv einbezogen und z.B. über ein Routingprotokoll kontinuierlich überwacht. Im Fehlerfall kann damit auf die zweite Leitung verlässlich geschwenkt werden. Eine SD-WAN-Lösung geht technologisch noch deutlich weiter und macht die Umschaltung auf andere Verbindungen von der Qualität der Kommunikation abhängig. So können

partielle Ausfälle, die von Routingprotokollen nicht einfach erkannt werden, direkt die Nutzung von Leitungen steuern. Eine weitere interessante Option ist ein Routing auf Basis der verwendeten Applikationen. In diesem Fall kann eine Verbindung mit IEC 60870-5-104 über das LTE450 Netzwerk geleitet werden, während der Fernservice das öffentliche Mobilfunk-Netz oder einen DSL-Anbieter nutzt. Über Richtlinien innerhalb von SD-WAN können einzelne Applikation in unterschiedlichen Betriebszuständen gemäß ihrer Kritikalität weitergeleitet werden.

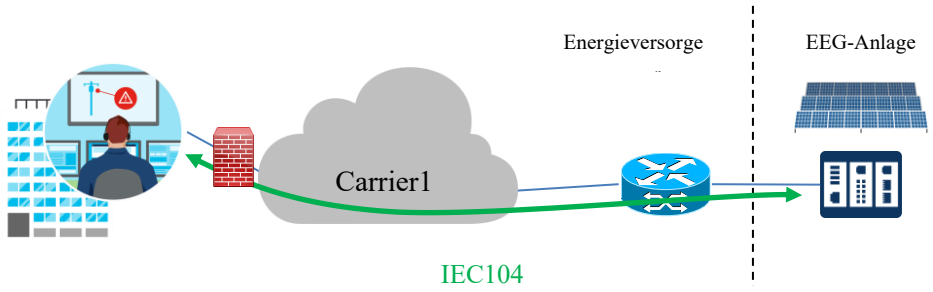


Erweiterte Funktionen

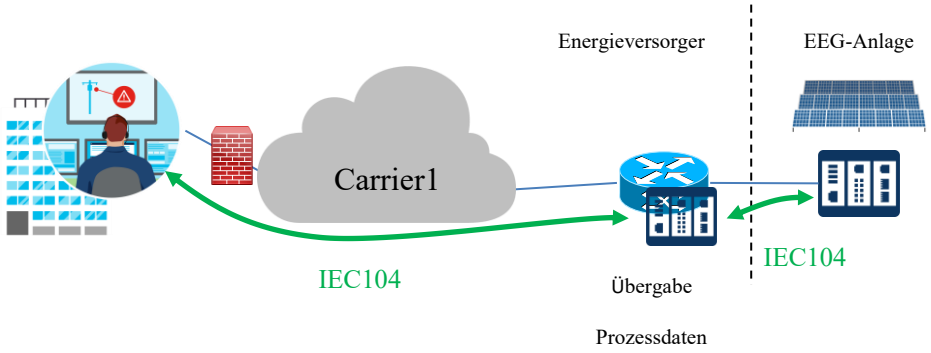
Manche Kommunikationsstrukturen erfordern bereits erweiterte Funktionen, die über den einfachen Aufbau eines Kommunikationsnetzes hinausgehen. Dieses Kapitel stellt Funktionen vor, wie Netzbetreiber den Funktionsumfang ihrer Standorte einfach erweitern können.

- Fernwirk-Gateway (RTU)

  Durch das Fernwirk-Gateway (Remote Terminal Unit = RTU) entsteht eine kontrollierte Übertragungsebene zwischen den Teilnehmern im Feld und der Leitebene. Die Anbindung von Marktteilnehmern im Bereich der EEG-Anlagen erfordert oftmals die Übertragung mit IP-Protokollen wie IEC 60870-5-104, IEC 61850 MMS, Modbus TCP oder OPC-UA. Die analoge Prozessanschaltung findet meistens nicht statt. Die inhaltliche Bewertung der Prozessdaten in den verwendeten Protokollen erfolgt an einem Terminierungspunkt, der sich zentral beim Energieversorger befindet.



Alternativ terminiert das Fernwirk-Gateway auf dem Router bereits in der Außenstelle die IP-Verbindung zur EEG-Anlage und überträgt nur die abgestimmten Daten bidirektional als Prozessgrößen. Das Fernwirk-Gateway wird vom Netzbetreiber kontrolliert und baut eine neue IP-Verbindung zu dem Leitsystem auf. Auf diese Weise können die erforderlichen Daten sicher und störungsfrei übertragen werden. Eine inhaltliche Prüfung der Daten oder auch die flexible Anpassung an unterschiedliche Protokolle ist einfach möglich. Aus Sicherheitsgründen gibt es keine durchgehende IP-Anbindung zwischen der EEG-Anlage und den Netzbetreibern.



Gateways können heutzutage andere Hardware durch Virtualisierung einsparen. Verschiedene Lösungen können nicht nur Protokolle umwandeln, Netzinfrastruktur zur verbesserten Visibilität überwachen und OT-Daten auswerten, sondern auch über die Datenhoheit entscheiden und Kommunikationsflüsse regeln.

- Cloud Connect (Edge Intelligence)

  Auch Netzbetreiber verlagern ihre nicht echtzeitkritischen Daten zunehmend in die Cloud, um die Datenflut zu bewältigen und flexibler zu sein oder zusätzliche Funktionalitäten zu nutzen. Dabei verlassen sie sich wie viele andere Unternehmen auch auf die Funktionalität großer Hyperscaler. Routing-Entscheidungen erfolgen hierbei auf Basis der Daten und nicht der IP-Netze. Ein Router in einer Ortsnetzstation oder einer EEG-Anlage muss in der Lage sein, Daten zu erfassen, auf Basis von

Datensätzen eine Vorverarbeitung zu machen und dann die Daten gezielt an die Cloud-Dienste weiterzugeben. Das betrifft auch die Anonymisierung von Daten. Wichtige Prozesse und sensible Daten sollten daher immer vom Netzbetreiber gesteuert werden.

- Edge Computing

  Ein Router in einer Außenstelle, z.B. einer EEG-Anlage, einer e-Mobility Ladestation oder einer Ortsnetzstation, muss neben der reinen Konnektivität weitere universelle Funktionen für den Netzbetreiber zur Verfügung stellen können. Um diese Funktionen zu nutzen, werden in den Edge-Komponenten Containersysteme zur Verfügung gestellt. Ein Containersystem ist ein abgeschlossener Bereich des Routers, in dem kundenspezifische Anwendungen installiert und ausgeführt werden. Anwendungen in den Containern können unterschiedliche Zwecke verfolgen und werden vom Kunden oder Partnern beigestellt. Einsatzgebiete sind z.B. die Ausführung von Datenreduktionen, die lokale Entscheidungsfindung, um Latenzen in der Übertragung zu vermeiden, Offline-Funktionalitäten oder auch zusätzliche Sicherheitsfähigkeiten. Das Fernwirk-Gateway setzt als praktisches Beispiel auf diese Technologie auf.

Die Skalierbarkeit und Management-Fähigkeit der zusätzlichen Funktionen sind wichtige Aspekte in der Nutzung und Realisierung. Die zentrale Verwaltung ist elementar für einen effizienten Betrieb.

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. IP-basierte Kommunikationssysteme dürfen im Bereich Energienetze, beispielsweise kritische Infrastruktur, nur zusammen mit wirksamen Maßnahmen für Cybersicherheit eingesetzt werden. Eine Selbstverständlichkeit sollten hierbei verschlüsselte Protokolle in der Kommunikation oder zur Administration sein. Sicherheit in Kommunikationsnetzen baut nicht nur auf eine einzelne Funktion einer Komponente auf, sondern ist ein Zusammenspiel vieler einzelner Sicherheitselemente, Designs und Prozesse.

Cybersicherheit gemäß eines Zero-Trust-Ansatzes zu gestalten, ist daher unerlässlich: Dieses Konzept basiert darauf, grundsätzlich keinem Gerät, Nutzer oder Dienst innerhalb oder außerhalb des eigenen Netzwerks zu vertrauen. Entsprechend umfangreich muss daher auch die Authentifizierung und Rechtevergabe erfolgen. Neue Sicherheitsstandards werden zudem vom neuen IT-Sicherheitsgesetz 2.0 gefordert und etabliert.

Bestandteile eines Sicherheitskonzeptes sind IDS- und IPS-Bausteine. Cisco Cyber Vision wurde speziell für die Prozessnetze und die Zusammenarbeit von OT- und IT-Teams entwickelt, um Produktionskontinuität, Widerstandsfähigkeit und Sicherheit zu gewährleisten. Netzbetreiber können damit Technologien des Industrial Internet of Things (IIoT) einsetzen und die Vorteile ihrer industriellen Digitalisierungsprojekte nutzen. Dazu gehören umfassende Einblicke in die spezifischen Protokolle des Leitsystems, einschließlich des dynamischen Ressourcenbestands und der Echtzeitüberwachung von Prozessdaten. Sensorik kann auf den Routern in den Außenstellen, aber auch an zentralen Übergabepunkten aufgebaut und eingerichtet werden.

Eine vertrauenswürdige IT-Infrastruktur basiert auf strikten Richtlinien, Prozessen, Technologien und Produkten, die sichtbar und kontrollierbar sind. Das erfordert sogenannte **Trustworthy Systems** – vertrauenswürdige Systeme oder Lösungen. „Vertrauenswürdig“ ist eine Lösung, die das, was von ihr erwartet wird, auf nachprüfbare Weise erledigt. Zum Aufbau vertrauenswürdiger Lösungen muss Sicherheit eine der wichtigsten Überlegungen schon beim Entwurf von Systemen sein und ganzheitlich über den gesamten Produktlebenszyklus vom Design, über die Produktion, Lieferung, dem Einsatz beim Kunden, bis hin zur Verwertung nach Lebensende umgesetzt werden. Auf diese Weise lassen sich Schwachstellen und Risiken reduzieren, Einblicke in die Plattformintegrität ermöglichen und Bedrohungen schneller beheben.

Um das interne Netzwerk nach außen hin zu schützen, müssen zudem Trennungspunkte vorgegeben werden, welche die kritischen Kommunikationsinfrastrukturen für den Notfall definiert von der Außenwelt trennen und dadurch sicher abschirmen. Darüber hinaus sind anwendungsspezifische Filterfunktionen am Perimeter einzurichten. NextGeneration Firewalls mit Regelwerken für prozessnahe Kommunikationen sind eine Möglichkeit einen Schutzperimeter aufzubauen. Das vorgestellte dezentrale Fernwirk-Gateway (Application Layer Gateway) ist eine weitere Sicherheitskomponente, die die Kommunikation zwischen Clients und Applikationsservern trennt, auf Applikationsschicht kontrolliert und als Proxy eingesetzt werden kann.

Management

Für Netzbetreiber ist es wichtig, ihre Kommunikationsinfrastruktur vollständig im Griff zu haben. Besonders wichtig ist an dieser Stelle die bereichsübergreifende Zusammenarbeit: Die verantwortlichen Abteilungen sollten Anwendungsfälle gemeinsam planen und erstellen – dies ist ein zentraler Arbeitsschritt. Neben den Fachbereichen der Kommunikationstechnik, müssen auch die Bereiche der zentralen Leittechnik und der Sekundärtechnik einbezogen werden. Die zentrale Administration oder Parametrierung von Feldleit- und Schutzkomponenten werden möglich, sofern die Sicherheitsrichtlinien berücksichtigt sind.

Monitoringsysteme überwachen dann den Datenverkehr im Prozessnetz 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.

Da das System jederzeit in der Lage sein muss, digitale Ortsnetzstationen und dazugehörige Komponenten hinzuzufügen, sind entsprechende Optionen zur Skalierung erforderlich. Hierbei geht es nicht nur um das Management der Hardwarekomponenten, sondern auch um Container Management. Dafür bieten sich Software-as-a-Service-Lösungen oder Lösungen beim Kunden mit großem Funktionsumfang an, beispielsweise Cisco DNA Center, SD-WAN oder ein modernes IoT-Dashboard. Das Cisco DNA Center ist ein umfassendes Kontrollzentrum für das Netzwerk, das auf einer physischen Appliance implementiert wird. Es unterstützt durch geführte Workflows sämtliche IT-Bereiche, von NetOps und AIOps bis hin zu SecOps und DevOps. Die SD-WAN-Controller sind die zentralen Bausteine für den Aufbau und Betrieb einer Software Defined Network-Umgebung. Das IoT-Dashboard stellt alle Funktionen und Lösungen als Software-as-a-Service zur Verfügung. Wichtig ist hierbei, dass Netzbetreiber zunächst genau ihre Anforderungen analysieren und sich dann anhand von Experten-Beratung für die individuell optimalen Lösungen entscheiden.

Eine große Herausforderung für die Betreiber stellt die Sichtbarkeit im Stromnetz dar. Die Verfügbarkeit im Kommunikationsnetz ist hierfür essenziell. Vor allem die zentralen Komponenten und die kontinuierliche Überwachung der Services, auch in den zubringenden Netzen der öffentlichen Anbieter, ist eine wesentliche Anforderung aus Sicht der Verfügbarkeit des Kommunikationsnetzes. Der Lösungsansatz ThousandEyes stellt hier eine Basis zur Transparenz für alle Marktteilnehmer dar. Die Überwachung der Verfügbarkeit von Kommunikationswegen ermöglicht dem Energienetzbetreiber, proaktiv auf Störungen zu reagieren und so den Betrieb zu optimieren.

Zusammenfassung

Zur erfolgreichen Umsetzung der Energiewende ist eine moderne Kommunikationstechnik für Energienetze unerlässlich. Dabei spielt die ständige Verfügbarkeit und Echtzeitfähigkeit der Kommunikationsdienste, mit denen Energienetze überwacht und gesteuert werden, eine entscheidende Rolle für die Versorgungssicherheit moderner Energiesysteme. Darüber hinaus sind robuste und mehrstufige Lösungen für Cybersicherheit sowie ein ganzheitliches Management für die Prozessnetze essenzielle Voraussetzungen, um einen sicheren Stromnetzbetrieb zu gewährleisten. Neben dem klassischen Aufbau stehen viele Optionen aus den Bereichen Software Defined Networks und Edge Funktionalitäten zur Verfügung, um aktuelle und zukünftige Anforderungen realisieren zu können.