Restricted
Dokumentennr.: 0081-2724 V00
2018-10-17

VestasOnline® Mk5-Netzwerk

Allgemeine Beschreibung

Vestas Wind Systems A/S · Hedeager 42 · 8200 Aarhus N · Dänemark · www.vestas.com

Version Nr.	Datum	Änderungsbeschreibung
0	2018-10-17	Erste Ausgabe

Inhaltsverzeichnis

1 Einleitung

Das VestasOnline® Mk5-Network stellt eine Überarbeitung der Architektur der gesamten Anlagenkommunikationsinfrastruktur dar. Es verwendet weiterhin gängige Industriestandards, damit sich die Einrichtung und Integration mit externen Systemen einfach gestaltet. Die Netzwerk-Hardware und die zugehörige Software wurden jedoch aktualisiert. Sie unterstützen jetzt eine Architektur, die eine verbesserte Sicherheitskonfiguration ermöglicht. Die neue Hardware ersetzt alle Switches im Windpark, einschließlich der Switches in der Windenergieanlage (WEA).

Das VestasOnline®-Network ist so konzipiert, dass es eine granulare Sicherheitsebene schafft. Dazu werden unter Einsatz von Layer-2-VLAN-Technologie innerhalb des Windparks diskrete Sicherheitszonen geschaffen. Die Schaffung dieser Sicherheitszonen ermöglicht die Trennung von Geräten mit unterschiedlichen Vertrauensstufen. Die Interaktion dieser Geräte, sofern vorhanden, kann mittels Access Control-Listen (ACL, Zugangskontrolllisten), Network Address Translation (NAT, Umsetzung von Netzwerkadressen) und Port Address Translation (PAT, Umsetzung von Port-Adressen) im VOC/VOB-Layer-3-Netzwerkgerät verwaltet werden.

Die neue Hardware für das VestasOnline® Network ist in Industriequalität ausgeführt. Sie kann unterschiedliche Transceiver-Typen verwenden und erfüllt folgende Bedingungen:

- Kompakter Industrieformfaktor
- Betriebsfähig in einem großen Temperatur- und Feuchtigkeitsbereich
- Korrosionsbeständig
- Elektromagnetische Störfestigkeit, einschließlich Spannungsstößen und Spannungsspitzen
- Stöße und Vibrationen
- Einfache Aufstellung und Service
- Hohe mittlere Betriebsdauer zwischen Ausfällen (MTBF)
- Hohe Ausfallsicherheit
- Gigabit-Windpark-Backbone

1.1 Kompatible Systeme

Das VestasOnline® Mk5-Network ist für den Einsatz mit folgenden Systemen und ihren zukünftigen Versionen gedacht:

- VestasOnline® Business (VOB) Mk5
- VestasOnline®-Windenergieanlagensteuerung (PPC) Mk5
- VestasOnline® Compact (VOC) Mk4 (Baumuster 2)
- Windenergieanlage (WEA) Vestas 2MW Mk11D
- Windenergieanlage (WEA) Vestas 4MW Mk3E

1.2 Sicherheitszonen

Das VestasOnline® Mk5-Network ist in diskrete Sicherheitszonen unterteilt. Diese Sicherheitszonen ermöglichen die Kontrolle darüber, wie Geräte im Netzwerk mit anderen Geräten kommunizieren können. Sicherheitszonen sind in funktionale und logische Gruppen unterteilt, beispielsweise Park, WEA, DMZ/Fremdanbieter und Vestas Backend-Services. Innerhalb jeder dieser Gruppen existieren Sicherheitszonen. Dies schafft eine granulare Segmentierung des Netzwerks:

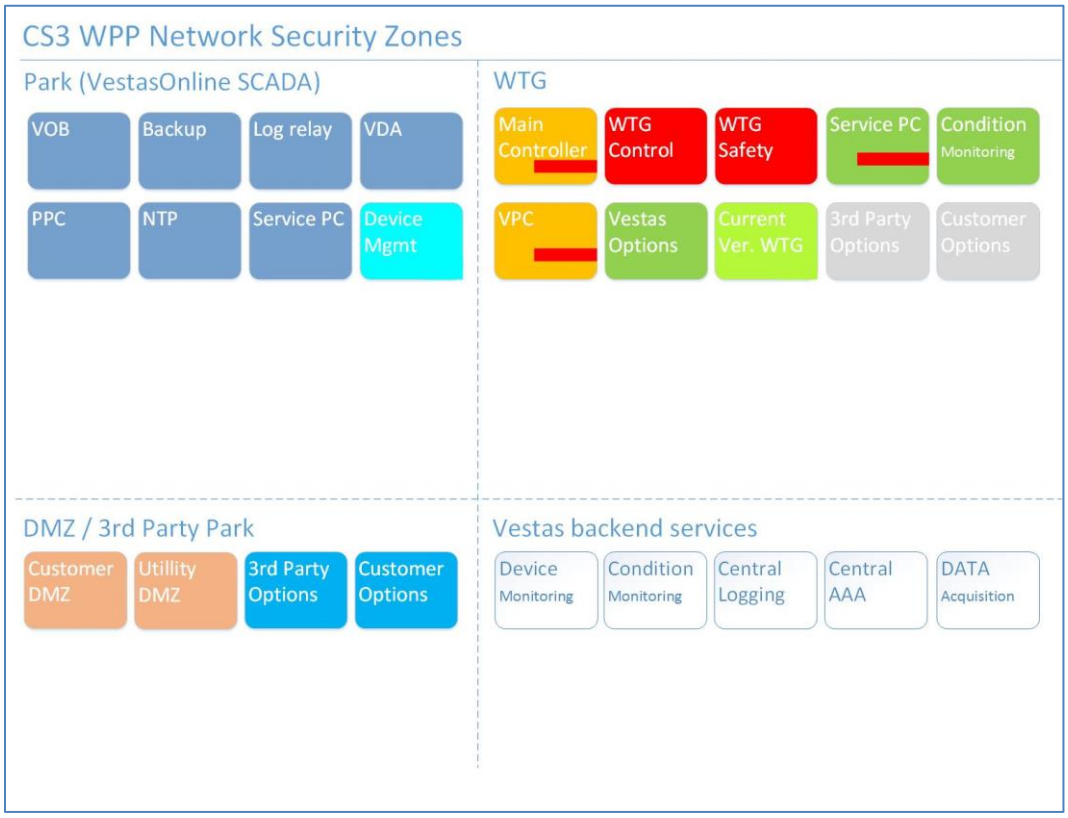

Abbildung 1-1:Konzept der Netzwerksicherheitszonen

Sicherheitszonen werden im VestasOnline® Mk5-Network durch die Implementierung folgender Technologien geschaffen:

- **VLANs** dienen zur Aufteilung des physischen Netzwerks in kleinere, logisch getrennte Netzwerke. Geräte in einem VLAN können in der Voreinstellung nicht mit Geräten in einem anderen VLAN kommunizieren. VLAN-übergreifender Verkehr ist nur in VOC/VOB-Layer-3-Netzwerkgeräten möglich. Innerhalb der meisten VLANs können alle Geräte ungehindert kommunizieren.

  Die spezifischen VLANs sind physischen Ports an den Switches zugeordnet. Im Normalfall gehören Endgeräte zu einem spezifischen VLAN. Der Netzwerk-Port ist im „Zugangsmodus“ und dem entsprechenden VLAN zugewiesen. Bestimmte Komponenten benötigen Zugriff auf mehrere VLANs. In einem solchen Fall werden die Netzwerk-Ports in den „Trunk-Modus“ (Hauptleitungsmodus oder Leitungsbündelmodus) versetzt. Dem Trunk werden dann spezifische VLANs zugewiesen.

VOC/VOB-Layer-3-Geräte routen sämtlichen VLAN-übergreifenden Netzwerkverkehr, und ACLs regeln, welcher Verkehr VLAN-übergreifend abgewickelt werden kann.

- **Private VLAN (PVLAN)** wird dazu eingesetzt, Kommunikation innerhalb desselben VLAN zu unterbinden. Dadurch werden Geräte wie die Laptops der Monteure weitgehend isoliert, während der Konfigurationsaufwand beschränkt bleibt.

- **ACLs** sind eine Filterliste, in der zulässige Netzwerk-Verkehrsströme eines konfigurierten Geräts verzeichnet sind. Diese Filterlisten enthalten folgende Einstellungen für die Verwaltung des Verkehrs:
    - Quell- und Ziel-IP-Adresse
    - Quell- und Ziel-Port-Nummern
    - UDP- oder TCP-Protokoll.

  Geroutete ACLs (RACL), die einer Layer-3-Schnittstelle zugewiesen werden, dienen der Einschränkung des Verkehrs zwischen VLANs (Sicherheitszonen).

  Port ACLs (PACL) kommen an einer physischen Schnittstelle zum Einsatz. Sie ermöglichen höhere Granularität innerhalb eines VLAN oder einer Sicherheitszone.

  Alle ACLs werden über „Whitelisting“ realisiert: Verkehr ist in der Grundeinstellung nicht zugelassen. Nur ausdrücklich zugelassene Verkehrsströme können fließen.

1.3 Skalierbarkeit

Das VestasOnline® Mk5-Network ist eine skalierbare Lösung mit einem IP-Adressierungsschema, das hinsichtlich der Anzahl der Sicherheitszonen und der Geräte im Netzwerk erweiterbar ist.

- Unterstützung von Lösungen von Fremdanbietern
- Flexibilität hinsichtlich der zukünftigen Aufnahme von IP-Bereichen für derzeit nicht bekannte Funktionen/Lösungen von Fremdanbietern
- Skalierbare Struktur für mehr Geräte in der WEA und anderen Plattformen
- Skalierbare Struktur für mehr WEAs pro Windpark
- Uniforme Struktur in allen Windparks

Alle Windparks, in denen diese Lösung zum Einsatz kommt, haben dasselbe interne IP-Schema. Dieses IP-Adressschema ermöglicht die Skalierbarkeit auf mehr WEAs innerhalb der Einschränkungen der VOB- und PPC-Plattformen.

Port Address Translation (PAT) wird dazu verwendet, multiple IP-Adressen im VestasOnline® Network in eine einzige externe IP-Adresse umzusetzen. Dazu wird jeder Verbindung ein eindeutiger Port zugewiesen. Diese Technologie kommt zum Einsatz, weil alle Windpark-LANs in Zukunft denselben IP-Bereich verwenden werden.

Network Address Translation (NAT) ordnet eine IP-Adresse oder einen IP-Adressbereich einer anderen IP-Adresse oder einem anderen Adressbereich zu. Durch den Einsatz von NAT kann ein Kunde sein eigenes IP-Adressschema zur Kommunikation mit internen Komponenten des VestasOnline® Mk5-Network verwenden.

1.4 Netzwerktopologie

Die Netzwerkstruktur kann der tatsächlichen Mittelspannungskabelverlegung des Windparks entsprechen, da die Datenaustauschkabel normalerweise auf dieselbe Weise verlegt werden. Jedoch können selbst bei einer gegebenen Topologie mit Mittelspannungskabeln die Glasfaserkabel je nach Anforderungen an Redundanz, Sicherheit, Stabilität, Umschaltzeit und andere Faktoren auf unterschiedliche Weise verlegt werden.

Ring-Topologie ist die einzig mögliche Netzwerktopologie, da sie einen guten Kompromiss zwischen Zuverlässigkeit und Sicherheit im Vergleich zu den Kosten und der Komplexität des Aufbaus darstellt. Bei der Ringtopologie werden die Windenergieanlagen-Switches und die Hauptserver-Switches in einer ringförmigen Struktur mit einer redundanten Datenaustausch-Rückleitung verbunden.

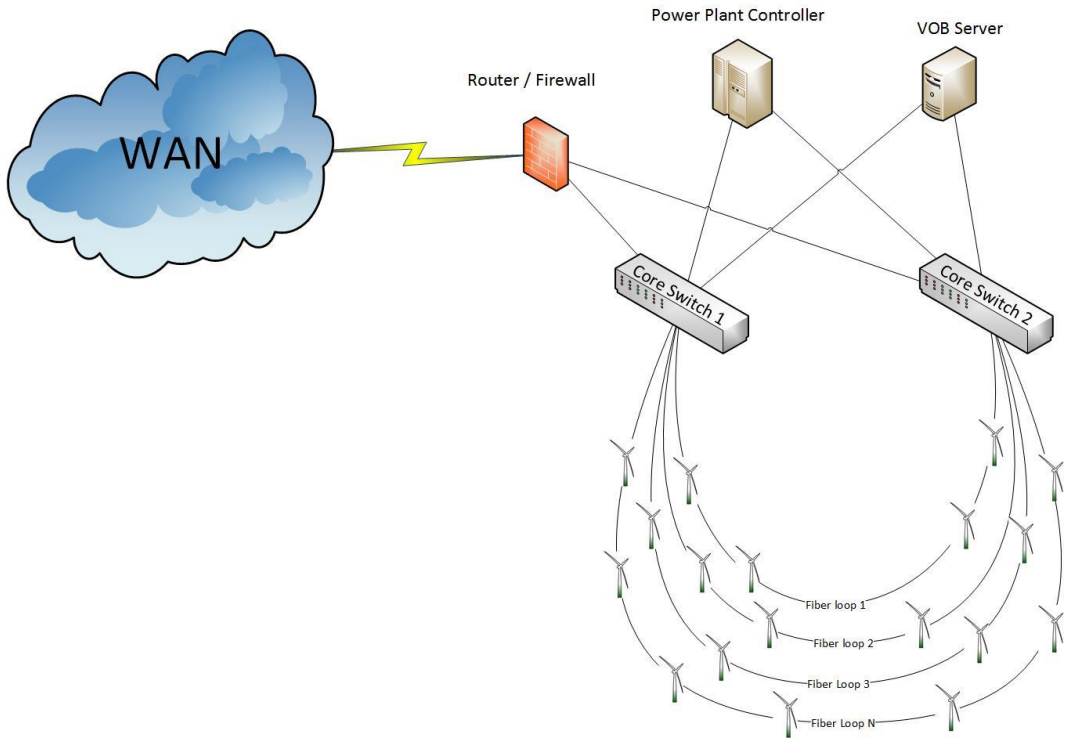

Abbildung 1-2: Konzept Windparknetzwerk und Ringleitungen zu WEAs

1.5 Sicherheitsfähigkeiten

Das VestasOnline® Mk5-Network verfügt außerdem über verschiedene zusätzliche Sicherheitsfähigkeiten.

Quality of Service (QoS): eine Technologie, die sicherstellen soll, dass bei hoher Netzwerkauslastung wichtiger Verkehr gegenüber weniger wichtigem Verkehr Vorrang hat. Ist das Netzwerk aus irgendeinem Grund überlastet, bewerten die Switches die Verkehrsströme und priorisieren Verkehr in Warteschlangen mit höherer Priorität gegenüber Verkehr in Warteschlangen mit geringerer Priorität. Dies stellt sicher, dass im Bedarfsfall Pakete aus Verkehrsströmen mit geringerer Priorität verworfen werden.

Mögliche Beispiele:

- Die Windparksteuerung hat höhere Priorität als die Erfassung von Protokolldaten für VOB/VOC.
- Die Erfassung von Protokolldaten hat höhere Priorität als eine Überwachungskameralösung
- VoIP hat höhere Priorität als eine Überwachungskameralösung
- Das Zustandsüberwachungssystem hat höhere Priorität als eine Überwachungskameralösung, aber geringere Priorität als VoIP

Die Aktivierung von QoS in der Infrastruktur und die Zuordnung aller Verkehrsströme zu Prioritätsklassen können sicherstellen, dass zunächst für den Windpark wichtiger Verkehr und dann der weniger wichtige Verkehr zugestellt wird. Hierzu gehört auch Unterstützung für Lösungen von Fremdanbietern, welche die verfügbare Netzwerkkapazität nutzen können sollen, ohne den normalen Betrieb des Windparks zu stören.

Authentifizierung, Autorisierung und Kontenverwaltung (engl. Authentication, Authorization, and Accounting, AAA): Sämtliche Benutzerzugriffe auf die Komponenten werden mittels einer AAA-Lösung überprüft.

Für AAA wird das Protokoll RADIUS mit den zentralen Vestas RADIUS-Servern verwendet. Die zentralen RADIUS-Server sind in dreifach redundanter Konfiguration ausgeführt. Richtlinienknoten stehen geografisch verteilt in den drei globalen Vestas-Datenzentren. Eine Anmeldeanfrage für ein System wird zunächst mit den durch den Benutzer angegebenen Anmeldedaten authentifiziert. Ist der Benutzer anmeldeberechtigt für die spezifische Komponente, wird ihm die Genehmigung für die Ausführung der spezifischen Aufgabe(n) erteilt. Dann werden Audit-Angaben zu der Benutzeranmeldung und die durch den Benutzer vorgenommenen Änderungen protokolliert und aufgezeichnet.

Allen Benutzern werden eine Rolle und eine Ressource zugewiesen, die ihren Zugriff speziell auf jene Geräte beschränkt, für die sie zugriffsberechtigt sind. Hat beispielsweise ein Vestas-Benutzer in einer Zone die Rolle „Network Operator“, kann er sich nur an Geräten in dieser spezifischen Zone anmelden und Aufgaben ausführen, zu denen ein „Network Operator“ berechtigt ist. Gemeinsam genutzte Benutzerkonten sind nicht zulässig.

Die gesamte Benutzerverwaltung wird zentral in der RADIUS-Lösung durchgeführt. Dies soll sicherstellen, dass Änderungen hinsichtlich des Personals bei Vestas effizient verwaltet werden können und dass das Prinzip der geringsten erforderlichen Rechte (Least Privilege) eingehalten wird.

Anmeldung: Sämtliche Netzwerkkomponenten werden so konfiguriert, dass sie das zentralisierte Protokollierungssystem von Vestas nutzen.

Sichtbarkeit der Verkehrsströme: Alle Netzwerkgeräte unterstützen sitzungsbasierte Protokollierung mittels NetFlow. Zentrale Komponenten senden Flussinformationen an das Vestas 24/7 Surveillance Center.

Systemhärtung: Gerätehärtung stellt sicher, dass nur erforderliche Dienste auf den Geräten ausgeführt werden und dass die erforderlichen Dienste so weit wie möglich abgesichert sind. Hinsichtlich der empfohlenen Systemhärtungseinstellungen werden externe Quellen herangezogen. Dies können entweder der Hersteller der Komponente sein oder Fremdanbieter, die Anleitungen zur Härtung zur Verfügung stellen.

Beispiel: Remote-Verwaltung des interaktiven Zugriffs auf eine Komponente.
Nur ein sicheres Protokoll ist zulässig. Telnet ist deaktiviert und SSH ist aktiviert. Darüber hinaus existiert eine ACL, die einschränkt, von welchen Orten aus der Fernzugriff zulässig ist. Die Prüfung wird zentral mittels der AAA-Lösung verwaltet.

Nur validierte Endpunktgeräte erhalten Zugriff auf das Netzwerk. Nicht autorisierten Geräten wird in der Voreinstellung der Zugriff verweigert.

Sicherheitsfunktionen der Layer 2
Auf Layer 2 existieren verschiedene Sicherungsmechanismen, welche zusätzliche Sicherheit bieten können. Dazu zählen unter anderem:

- Sturm-/Flutkontrolle
- Dynamische ARP-Inspektion
- DHCP-Snooping
- IP-Quellensicherung
- Port-Sicherheit (Begrenzung der Anzahl von MAC-Adressen pro Port)

Gemeinsam bieten diese Ansätze Schutz gegen verschiedene Sicherheits- und Betriebsprobleme, indem sie das Netzwerk sowohl vor problematischen Anwendungen als auch vor böswilligen Angriffen schützen.

Konfigurationsverwaltung und Überwachung: Alle Netzwerkgeräte im Windpark werden zentral verwaltet. Dadurch lassen sich die Software von Netzwerkgeräten und Konfigurationsparameter effizient aktualisieren.

Netzwerkgeräte senden planmäßig (alle 24 Stunden) eine Sicherungskopie an eine zentrale Sicherungslösung. Nach einer Änderung in einem Flash-Speicher findet ebenfalls ein Sicherungslauf statt. Die Übertragung wird mittels SCP v2 verschlüsselt. Die Sicherungskopie enthält eine vollständige Kopie der Konfiguration, inklusive Angaben dazu, wer die letzte Änderung vorgenommen hat.

Alle Konfigurationsänderungen werden auditiert und ein Alarm wird an das Vestas 24/7 Surveillance Center gesendet.

Zeitsynchronisierung: Alle betriebskritischen Geräte im Windpark verwenden vertrauenswürdige und redundante Network Time Protocol (NTP)-Quellen, damit konsistente Zeitangaben in den Ereignisprotokollen gewährleistet sind. Dies ist zur Überwachung der Sicherheit und für die Protokollierung im Allgemeinen von kritischer Bedeutung.

Kunden steht die Option zur Verfügung, pro Windpark eine dedizierte NTP-Quelle anzufordern (mit Genauigkeitsniveau Stratum 1). Dies kann bei der Bestellung ausgewählt werden.

1.6 Vestas WAN-Verbindungen

Damit die Verwaltung und der Betrieb des Windparks möglich sind und die Datenerfassung sichergestellt ist, kommt eine sichere IPSec-VPN-Lösung zum Einsatz.

Die Standardlösung von Vestas beruht auf der Authentifizierung von Zertifikaten des Perimetergeräts und verwendet branchenerprobte Verfahren zur Verschlüsselung des Verkehrs und Gewährleistung der Unversehrtheit der Daten.

Andere Standardimplementierungen stehen je nach den Erfordernissen hinsichtlich des Anschlusses an das Datenzentrum des Kunden zur Verfügung. Mehr Informationen sind bei Contact Vestas Customer Care erhältlich.

1.6.1 Sicherer Fernzugriff für Kunden/Fremdanbieter/Versorgungsunternehmen

Sämtliche Verbindungen zu dem Vestas Windpark enden in individuellen DMZ-Sicherheitszonen und passieren eine Stateful Firewall, welche die Pakete auf bestimmten Geräten eingehend untersucht (Deep Packet Inspection).

Für den sicheren Fernzugang zu relevanten Diensten im Windpark stehen verschiedene Verfahren zur Verfügung. Sie orientieren sich hinsichtlich ihrer sicheren Implementierung an branchenerprobten, bewährten Verfahren.

- Client VPN – eine durch den Benutzer initiierte VPN-Sitzung, bei der VPN-Client-Software auf dem Computer des Benutzers zum Einsatz kommt (zentralisierte Benutzerkontenverwaltung)
- Site-to-Site – ein IPSec VPN-Tunnel wird durch zwei Endpunkt-Sicherheitsgeräte initiiert
- Direkte Ethernet-Verbindung von innerhalb des Windparks
- IPSec VPN-Tunnel zur Vestas Backend-Lösung, dann geroutet in den Windpark

2 Abkürzungen und Definitionen

Kurzbezeichnung	Langbezeichnung	Beschreibung
WPP	Windpark (Wind Power Plant)	Besteht aus vielen einzelnen *Windenergieanlagen,* die an das elektrische Leistungsübertragungsnetz angeschlossen sind.
WEA	Windenergieanlage	
HW	Hardware	
LAN	Local Area Network	Internes Netzwerk im Windpark
VLAN	Virtual Local Area Network	Virtuelle Netzwerke in einem gemeinsam genutzten physischen Netzwerk-LAN
PVLAN	Private Virtual Local Area Network	Peer-2-Peer-Verkehr in demselben VLAN unzulässig
WAN	Wide Area Network (Fernnetz)	Verbindungen außerhalb des Windparks, z. B. über das Internet
RADIUS	Remote Authentication Dial-In User Service	Dient zum Validieren von Benutzern in einer zentralen Verwaltungslösung
AAA	Authentifizierung, Autorisierung und Kontenverwaltung (engl. Authentication, Authorization, and Accounting)	Wird auch als „Triple-A“ bezeichnet. Dient der Validierung von Benutzerzugriffen auf sichere und eingeschränkte Weise, mit Protokollierung

Kurzbezeichnung	Langbezeichnung	Beschreibung
IP	Internet Protocol	Eindeutige Kennung auf OSI-Layer 3. Alle Geräte in einem gerouteten Netzwerk benötigen eine eindeutige IP, damit sie kommunizieren können
MAC	Media Access Control-Adresse	Eindeutige Kennung auf OSI-Layer 2. Alle Geräte in einem VLAN benötigen eine eindeutige MAC, damit sie kommunizieren können
ACL	Access Control Liste	Filterliste mit IP-Adressen und Portnummern zur Einschränkung/Gewährung segmentübergreifender Zugriffe
PACL	Port ACL	ACLs an einem physischen Schnittstellenanschluss werden als Port ACL (PACL) bezeichnet
RACL	Routed ACL	ACLs an einer virtuellen Layer-3-Schnittstelle
PAT	Port Address Translation	Netzwerkadressen zwischen Segmenten durch Einsatz von Multiplexing mit Port-Nummern umsetzen
NAT	Netzwerkadressübersetzung	Netzwerkadressen zwischen Segmenten durch Einsatz einer dedizierten IP-Adresse pro Gerät umsetzen
QoS	Quality of Service	Priorisierung des Netzwerkverkehrs
Access Port	Physische Ethernet-Schnittstelle in Netzwerkkomponenten, die im Zugriffsmodus konfiguriert sind	Ein VLAN pro physischem Port. Wird normalerweise für Endgeräte verwendet
Trunk Port	Physische Ethernet-Schnittstelle in Netzwerkkomponenten, die im Trunk-Modus (Hauptleitungs-, Leitungsbündelmodus) konfiguriert sind	VLAN-Tagging pro physischem Anschluss (Port). Wird normalerweise für Verbindungen zwischen Switches, Routern oder Servern verwendet, auf denen Virtualisierung läuft
OSI	Open System Interconnection Reference Model	Besteht aus sieben Layern. Physisch Data-Link Netzwerk Transport Sitzung Präsentation Anwendung

Kurzbezeichnung	Langbezeichnung	Beschreibung
Layer-3-Netzwerkkomponenten	Netzwerk-Switches oder Router, die auf Layer 3 arbeiten können – Routing zwischen Segmenten	Layer 3 ist Netzwerk – IP-Adresse – im OSI-Modell
Sicherheitsgehärtet		Begrenzung der Angriffsfläche eines Geräts ausschließlich auf die erforderlichen Funktionen und Implementierung der erforderlichen Funktion auf sichere Weise
Netflow	Sitzungsbasierte Protokollierung	Erfasste Netzwerk-Metadaten. Liefert +90 % des Wertes eines echten IDS-Systems
RBAC	Role Based Access Control	Die Fähigkeit, Benutzern Zugriffsrechte auf der Grundlage von Rollen zu gewähren
Principle of least privilege (Prinzip der geringsten erforderlichen Rechte)		Die Fähigkeit, Benutzern Zugriffsrechte nach dem „Prinzip der geringsten erforderlichen Rechte“ zu gewähren
Whitelisting	Positiv-Liste	Alles wird geblockt, mit Ausnahme zugelassener Protokolle/Anwendungen
CCTV	Closed-Circuit Television	Verwendet für Überwachungssysteme mit Kameras
VoIP	Voice over IP	Telefonsysteme, die das Netzwerk als Basis nutzen
CMS	Conditional Monitoring Systems/Zustandsüberwachungssystem	Spezielles System zur Überwachung verschiedener Umgebungsbedingungen mit Meldung der bzw. Reaktion auf die Bedingungen.
NTP	Network Time Protocol	Netzwerkprotokoll zur Synchronisierung der Uhrzeit zwischen Endgeräten und einer Referenzuhr (Stratum-Zeitquellen)
Stratum	Hierarchisches Zeitquellensystem	Stratum 0 ist das Zeitnormal. Der Wert 1 bis x gibt den Abstand in Ebenen zum Zeitnormal an
DMZ	Demilitarized Zone (Entmilitarisierte Zone)	Eine Zone zur Terminierung von Funktionen, deren Kommunikation in den/aus dem Windpark verläuft
ARP	Address Resolution Protocols (Adressauflösungsprotokolle)	Protokoll zur Zuordnung einer IP-Adresse zu einer MAC-Adresse
DHCP	Dynamic Host Configuration Protocol	Dient der automatischen Zuweisung einer IP-Adresse

Kurzbezeichnung	Langbezeichnung	Beschreibung
SCP v2	Secure Copy Protocol Version 2	Verschlüsselte Dateiübertragung
IPSec	Internet Protocol Security	Verschlüsselte Tunnel zur sicheren Verbindung

Tabelle 2-1: Abkürzungen und Definitionen