

Technische Beschreibung

ENERCON Shield & FortiGate Rugged 70F

SAP 1085637

Herausgeber

ENERCON Global GmbH ▪ Dreekamp 5 ▪ 26605 Aurich ▪ Deutschland
Telefon: +49 4941 927-0 ▪ Telefax: +49 4941 927-109
E-Mail: info@enercon.de ▪ Internet: <http://www.enercon.de>
Geschäftsführer: Uwe Eberhardt, Ulrich Schulze Südhoff
Zuständiges Amtsgericht: Aurich ▪ Handelsregisternummer: HRB 202549
Ust.Id.-Nr.: DE285537483

Urheberrechtshinweis

Die Inhalte dieses Dokuments sind urheberrechtlich sowie hinsichtlich der sonstigen geistigen Eigentumsrechte durch nationale und internationale Gesetze und Verträge geschützt. Die Rechte an den Inhalten dieses Dokuments liegen bei der ENERCON Global GmbH, sofern und soweit nicht ausdrücklich ein anderer Inhaber angegeben oder offensichtlich erkennbar ist.

Die ENERCON Global GmbH räumt dem Verwender das Recht ein, zu Informationszwecken für den eigenen, rein unternehmensinternen Gebrauch Kopien und Abschriften dieses Dokuments zu erstellen; weitergehende Nutzungsrechte werden dem Verwender durch die Bereitstellung dieses Dokuments nicht eingeräumt. Jegliche sonstige Vervielfältigung, Veränderung, Verbreitung, Veröffentlichung, Weitergabe, Überlassung an Dritte und/oder Verwertung der Inhalte dieses Dokuments ist – auch auszugsweise – ohne vorherige, ausdrückliche und schriftliche Zustimmung der ENERCON Global GmbH untersagt, sofern und soweit nicht zwingende gesetzliche Vorschriften ein Solches gestatten.

Dem Verwender ist es untersagt, für das in diesem Dokument wiedergegebene Know-how oder Teile davon gewerbliche Schutzrechte gleich welcher Art anzumelden.

Sofern und soweit die Rechte an den Inhalten dieses Dokuments nicht bei der ENERCON Global GmbH liegen, hat der Verwender die Nutzungsbestimmungen des jeweiligen Rechteinhabers zu beachten.

Geschützte Marken

Alle in diesem Dokument ggf. genannten Marken- und Warenzeichen sind geistiges Eigentum der jeweiligen eingetragenen Inhaber; die Bestimmungen des anwendbaren Kennzeichen- und Markenrechts gelten uneingeschränkt.

Änderungsvorbehalt

Die ENERCON Global GmbH behält sich vor, dieses Dokument und den darin beschriebenen Gegenstand jederzeit ohne Vorankündigung zu ändern, insbesondere zu verbessern und zu erweitern, sofern und soweit vertragliche Vereinbarungen oder gesetzliche Vorgaben dem nicht entgegenstehen.

Dokumentinformation

Dokument-ID	D03118089/0.2-de		
Vermerk	Originaldokument		
Datum	Sprache	DCC	Werk / Abteilung
2025-04-09	de	DB	ENERCON Global GmbH

Mitgeltende Dokumente

Der aufgeführte Dokumenttitel ist der Titel des Sprachoriginals, ggf. ergänzt um eine Übersetzung dieses Titels in Klammern. Die Titel von übergeordneten Normen und Richtlinien werden im Sprachoriginal oder in der englischen Übersetzung angegeben. Die Dokument-ID bezeichnet stets das Sprachoriginal. Enthält die Dokument-ID keinen Revisionsstand, gilt der jeweils neueste Revisionsstand des Dokuments. Diese Liste enthält ggf. Dokumente zu optionalen Komponenten.

Dokument-ID	Dokument
D0140738	Spezifikation ENERCON SCADA Datenanbindung des ENERCON SCADA Servers und ENERCON SCADA Edge Servers
D02957398	FortiGate Rugged 70F (Datasheet)
D03120568	FortiGate Rugged 70F Series (QuickStart Guide)
D03120569	FortiGate Subscriptions and FortiGuard Bundles (Ordering Guide)

Inhaltsverzeichnis

	Mitgeltende Dokumente	3
1	Allgemeines	6
2	ENERCON Shield Produktübersicht	7
2.1	Übersicht Netzwerksegmentierung	7
2.2	Übersicht SD-WAN	7
2.3	Übersicht Intrusion Detection & Prevention (IDS/IPS)	8
2.4	Hardware von Fortinet	8
3	Verfügbare Abo-Modelle/Ausbaustufen	10
3.1	Voraussetzung an die Windpark Kommunikationsinfrastruktur	10
3.2	Basic Security	10
3.3	Active Security	13
3.4	OT Pro Security	14
3.5	Optionale Erweiterungen	15
3.5.1	ENERCON Shield Cluster	15
3.5.2	Site-to-Site (S2S) VPN Interface	15
3.6	Vergleich der verschiedenen Abo-Modelle/Ausbaustufen	15
4	Datenverarbeitung und Datenspeicherung	17

Abkürzungsverzeichnis

CIS	Center for Internet Security
DSGVO	Datenschutz-Grundverordnung
IDS	Intrusion Detection System (Angriffserkennungssystem)
IoT	Internet of Things (Internet der Dinge)
IPS	Intrusion Prevention System (Angriffsverhinderungssystem)
IPsec	Internet Protocol Security (gesichertes Internetprotokoll)
LTE	Long Term Evolution (Mobilfunkstandard)
NIS	Netzwerk- und Informationssicherheit
NOC	Network Operations Center (Netzwerkbetriebszentrum)
OPC	Open Platform Communications (plattformunabhängige Kommunikation)
OT	Operational technology (Betriebstechnologien)
SCADA	Supervisory Control and Data Acquisition (überwachende Steuerung und Datenerfassung)
SD	Software-Defined
SIEM	Security Information and Event Management
SOC	Security Operations Center (Sicherheitsbetriebszentrum)
TCP	Transmission Control Protocol (Übertragungsprotokoll)
UA	Unified Architecture
VLAN	Virtual Local Area Network (virtuelles Netzwerk)
VPN	Virtual private network (virtuelles privates Netzwerk)
WAN	Wide Area Network (Weitverkehrsnetz)

1 Allgemeines

In den letzten Jahren sind die Anforderungen an die Cybersecurity sowohl auf technologischer als auch auf gesetzlicher Seite stetig gestiegen. Unternehmen und Organisationen sehen sich mit immer raffinierteren Bedrohungen konfrontiert, die eine kontinuierliche Anpassung und Weiterentwicklung der Sicherheitsmaßnahmen erfordern. Gleichzeitig werden die gesetzlichen Vorgaben durch internationale und nationale Regulierungen verschärft, um den Schutz kritischer Infrastruktur zu gewährleisten und der zunehmenden Cyberkriminalität entgegenzuwirken.

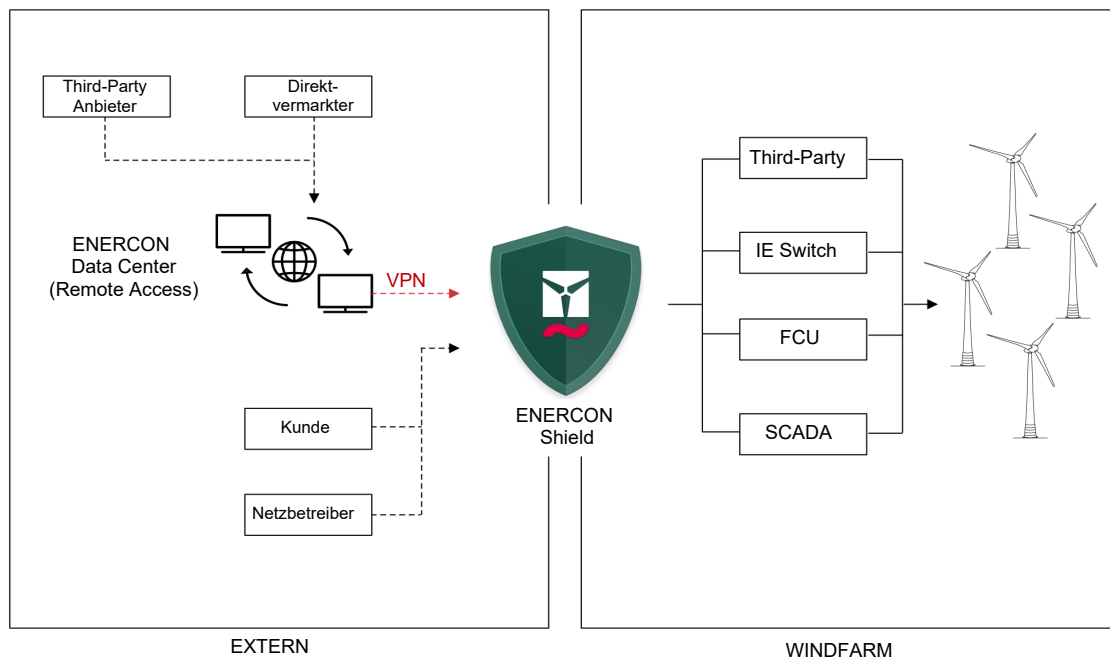


Abb. 1: ENERCON Shield Netzwerkarchitektur

Im Zuge dieser nötigen technologischen Neubewertung hat sich ENERCON entschieden, die bisherige Windparkanbindung (meistens über Router der Firma „Cisco“) auf eine umfassendere OT-Security Struktur umzustellen. Technologisches Kernstück hierbei ist eine sogenannte „Next Generation Firewall“, eine Hardware-Komponente, die Routing- und Sicherheitsfeatures für die gesamte innere und äußere Windpark-Kommunikation bereitstellt. Zusammen mit dem KI-basierten Monitoring des gesamten Netzwerk-Traffics und einer besonders angriffssicheren Netzwerktopologie stellt dies das Digitalprodukt „ENERCON Shield“ dar.

Das Dokument wird eine detaillierte Technik- und Produktübersicht, die Funktionsweise sowie die verschiedenen erhältlichen Funktionen und Ausbaustufen von ENERCON Shield erläutern, um ein umfassendes Bild der technologischen Innovation und der Sicherheitsmaßnahmen zu vermitteln, die ENERCON Shield bietet.

2 ENERCON Shield Produktübersicht

Mit der Einführung von ENERCON Shield hat sich ENERCON für eine zukunftssichere Cybersecurity-Lösung entschieden, die speziell für die OT-Umgebungen und kritische Infrastruktur in den Windparks entwickelt wurde.

Die Fortinet Fortigate Rugged 70F bildet dabei die technische Basis und bietet eine Kombination aus:

- Netzwerksegmentierung: Sicherstellung einer strikten Trennung und Absicherung von Steuerungsnetzen
- SD-WAN: Optimierung und Ausfallsicherheit von Netzwerkanbindung für dezentralisierte Windparks
- IDS/IPS: Erkennung und Abwehr moderner Bedrohungen in Echtzeit, speziell für industrielle Netzwerke

Die Implementierung dieser Technologien gewährleistet einen maximalen Schutz vor Cyberangriffen und erfüllt gleichzeitig die gesetzlichen Anforderungen zur Absicherung kritischer Infrastrukturen.

Durch ENERCON Shield wird eine moderne, hochsichere Netzwerktopologie geschaffen, die sowohl innovativ als auch zukunftssicher ist.

2.1 Übersicht Netzwerksegmentierung

ENERCON Shield bietet fortschrittliche Netzwerksegmentierung, um das Kommunikationsnetzwerk eines Windparks sicher und effizient zu strukturieren.

Funktionen Netzwerksegmentierung:

- virtuelle LANs (VLANs)
 - strikte Trennung zwischen Management-Netzwerken, SCADA Systemen, IoT-Geräten und externen Diensten
 - unterstützt 802.1Q VLAN -Tagging, um Netzwerke in logische Segmente zu unterteilen
- Security Zones & Mikrosegmentierung:
 - Einführung von dedizierten Sicherheitszonen für Windparks, um Bedrohungen gezielt abzuwehren
 - wurde in Anlehnung an das Purdue Reference Model / IEC-62443 entwickelt
 - regelbasierte Kommunikation zwischen verschiedenen OT-Geräten nur über definierte Schnittstellen
- Minimierung von Sicherheitsrisiken durch Isolation potenziell unsicherer Geräte
- Erschwerung von lateralen Angriffen, selbst wenn ein Endpunkt kompromittiert wird

2.2 Übersicht SD-WAN

ENERCON Shield nutzt die integrierte SD-WAN-Funktionalität der Fortigate Rugged 70F, um Windparks sicher und effizient an zentrale Kontrollsysteme anzubinden.

✓ Voraussetzung für SD-WAN ist die Bereitstellung eines Multi-WAN.

Funktionen SD-WAN:

- optimiertes Routing durch SD-WAN
 - dynamische Auswahl der besten WAN-Verbindung basierend auf Latenz, Jitter und Paketverlust
 - Priorisierung von zeitkritischen Datenströmen wie z. B. SCADA-Kommunikation
- Application-Aware Routing
 - Identifikation von OT-spezifischen Protokollen (z. B. Modbus TCP, IEC-104) und priorisierte Übertragung über die sicherste Verbindung
- stabile und zuverlässige Netzwerkverbindung unabhängig von Standort und Infrastruktur
- automatische Ausfallsicherheit durch SD-WAN, falls eine Verbindung ausfällt

2.3 Übersicht Intrusion Detection & Prevention (IDS/IPS)

Mit der steigenden Bedrohung durch Cyberangriffe auf industrielle Steuerungssysteme und damit einhergehender steigender regulatorischen Anforderungen (z.B: NIS-2), sind automatisierte Angriffserkennungs- und Präventionsmechanismen unerlässlich. Die FortiGate Rugged 70F bietet ein integriertes IDS/IPS, das für OT-Netzwerke/Windparks optimiert ist. Es dient dem Schutz der Windpark-Infrastruktur vor Cyberangriffen und der Erkennung und Blockierung von Zero-Day-Exploits in Echtzeit.

Funktionen Intrusion Detection & Prevention (IDS/IPS)

- signaturbasierte Bedrohungserkennung:
 - Überwachung des Netzwerkverkehrs in Echtzeit auf bereits bekannte Angriffsmuster
 - regelmäßige Updates der IPS-Signaturen (meist mehrfach täglich)
 - spezielle angepasste IDS/IPS Profile für SCADA, Windparkregler (z. B. FCU E2), HMI, Switch-Infrastruktur
- verhaltensbasierte Anomalie-Erkennung:
 - Erkennung von ungewöhnlichem Traffic, der auf Ransomware oder Zero-Day-Angriffe hindeuten könnte.
 - Nutzung von Machine Learning, um sich an neue Bedrohungen anzupassen.
- Deep Packet Inspection (DPI) für OT-Protokolle:
 - Modbus TCP, IEC-104 und OPC UA werden bis auf die Protokollebene untersucht, um unerlaubte Befehle zu blockieren.
 - Schutz vor Man-in-the-Middle-Angriffen, Command Injection und Spoofing.

2.4 Hardware von Fortinet

ENERCON verwendet Hardware von Fortinet. Die FortiGate Rugged 70F bietet robuste und zuverlässige Sicherheitslösungen, die speziell für industrielle Anwendungen konzipiert sind. Diese Hardware ist besonders darauf ausgelegt, die Einhaltung der NIS-2-Richtlinien zu gewährleisten. Mit erweiterten Funktionalitäten und technischen Spezifikationen, die für den Einsatz in rauen Umgebungen optimiert sind, stellt die FortiGate Rugged 70F eine ideale Lösung für den Schutz kritischer Infrastrukturen dar. Sie bietet umfassenden Schutz gegen eine Vielzahl von Cyberbedrohungen und sorgt so für die Sicherheit und Integrität der betrieblichen Abläufe.

Nähere Informationen zur FortiGate Rugged 70F sind in der Herstellerdokumentation verfügbar. Diese ist kann entweder direkt vom Hersteller oder von ENERCON (siehe Mitgelte Dokumente) bezogen werden.

3 Verfügbare Abo-Modelle/Ausbaustufen

Folgende Abo-Modelle/Ausbaustufen stehen zur Verfügung:

- Basic Security – Basis-Firewall-Schutz für industrielle Netzwerke
- Active Security – Erweiterte Sicherheitsfunktionen für proaktive Bedrohungsabwehr
- OT Pro Security – Maximaler Schutz für kritische Infrastrukturen und industrielle Steuerungssysteme

3.1 Voraussetzung an die Windpark Kommunikationsinfrastruktur

Tab. 1: Infrastrukturvoraussetzung für ENERCON Shield Ausbaustufen

	Basic Security	Active Security	OT Pro Security
WAN-Datenverbindung	X	X	X
SCADA Legacy oder neuere Version	X	X	X
Fernüberwachungsschrank V5 oder höher	X	X	X
zentraler Komponentenstandort		X	X
digitale Netzbetreiberkommunikation		X	X
Switch vorhanden			X

3.2 Basic Security

Das Basic-Security-Modell bietet grundlegende Sicherheitsfunktionen für industrielle Netzwerke. Es eignet sich für kleinere Netzwerke, die eine einfache, aber stabile Absicherung benötigen.

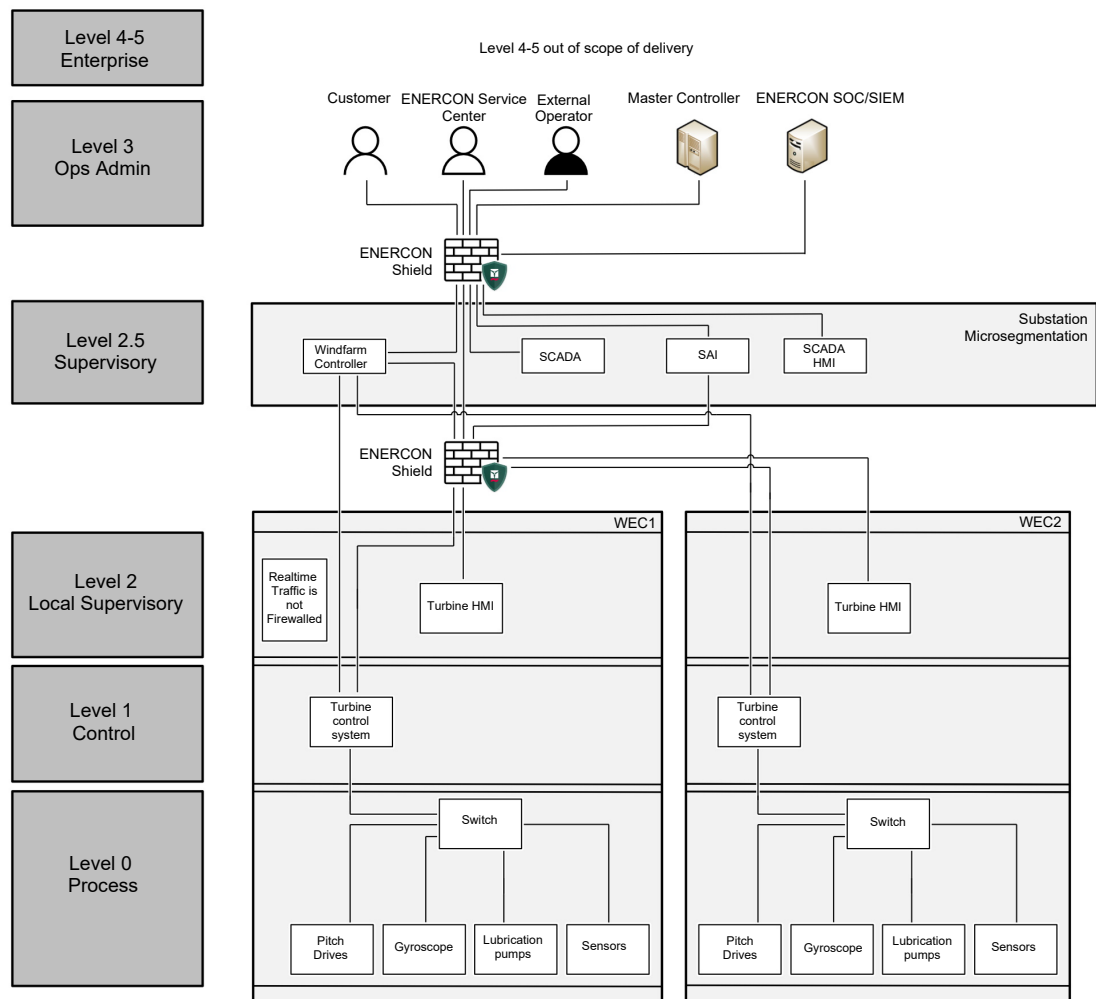


Abb. 2: Netzwerkarchitektur Basic Security

Hauptfunktionen

- Next-Generation Firewall, jedoch ohne aktivierte Features wie z. B. Intrusion-Detection, Intrusion-Prevention und OT-Applikationserkennung
- VPN IPsec Unterstützung
- 1 Kunden Ethernet Port, über den sämtliche Dienste, die vom SCADA Edge Server bereitgestellt werden, erreicht werden:
 - SCADA OPC UA
 - SCADA OPC XML DA
 - SCADA REST API
 - SCADA Remote
 - SCADA IEC-104
- 1 Energieversorger Ethernet Port, über den sämtliche geforderte Ethernet basierte Regelungsprotokolle am Windparkregler erreicht werden:
 - IEC-104
 - Modbus TCP

- Redundante WAN-Ports für hohe Ausfallsicherheit (müssen vom Kunden mit einem 100 Mbit/1 Gigabit Ethernet Port bereitgestellt werden – vgl. D0140738 „Spezifikation ENERCON SCADA Datenanbindung des ENERCON SCADA Servers und ENERCON SCADA Edge Servers“)
- Redundante Netzteile: Die Firewall ist redundant an die Spannungsversorgung im Schaltschrank angeschlossen.
- Netzwerksegmentierung und Mikrosegmentierung: Ermöglicht eine feingranulare Trennung von Netzwerkinfrastrukturen, wodurch sensible Systeme isoliert, laterale Bewegungen von Bedrohungen erschwert und Sicherheitsrichtlinien durchgesetzt werden können.
- Read-Only Zugriff auf die Firewall: Ermöglicht sichere und unveränderbare Einsicht in die Konfigurations- und Protokolldaten, wodurch eine transparente und revisionssichere Auditierung gemäß regulatorischen Anforderungen gewährleistet wird.
- Managed by ENERCON: Die Firewall wird vollständig von ENERCON verwaltet, wodurch eine kontinuierliche Überwachung und regelmäßige Firmware- und Sicherheitsupdates gewährleistet sind - für eine höchst zuverlässige und abgesicherte Netzwerkinfrastruktur.

3.3 Active Security

Das Active Security-Modell erweitert den Funktionsumfang zur aktiven Bedrohungsabwehr (IPS/IDS) und zur Netzwerkoptimierung. Es eignet sich für Unternehmen mit höheren Anforderungen an die Cybersecurity.

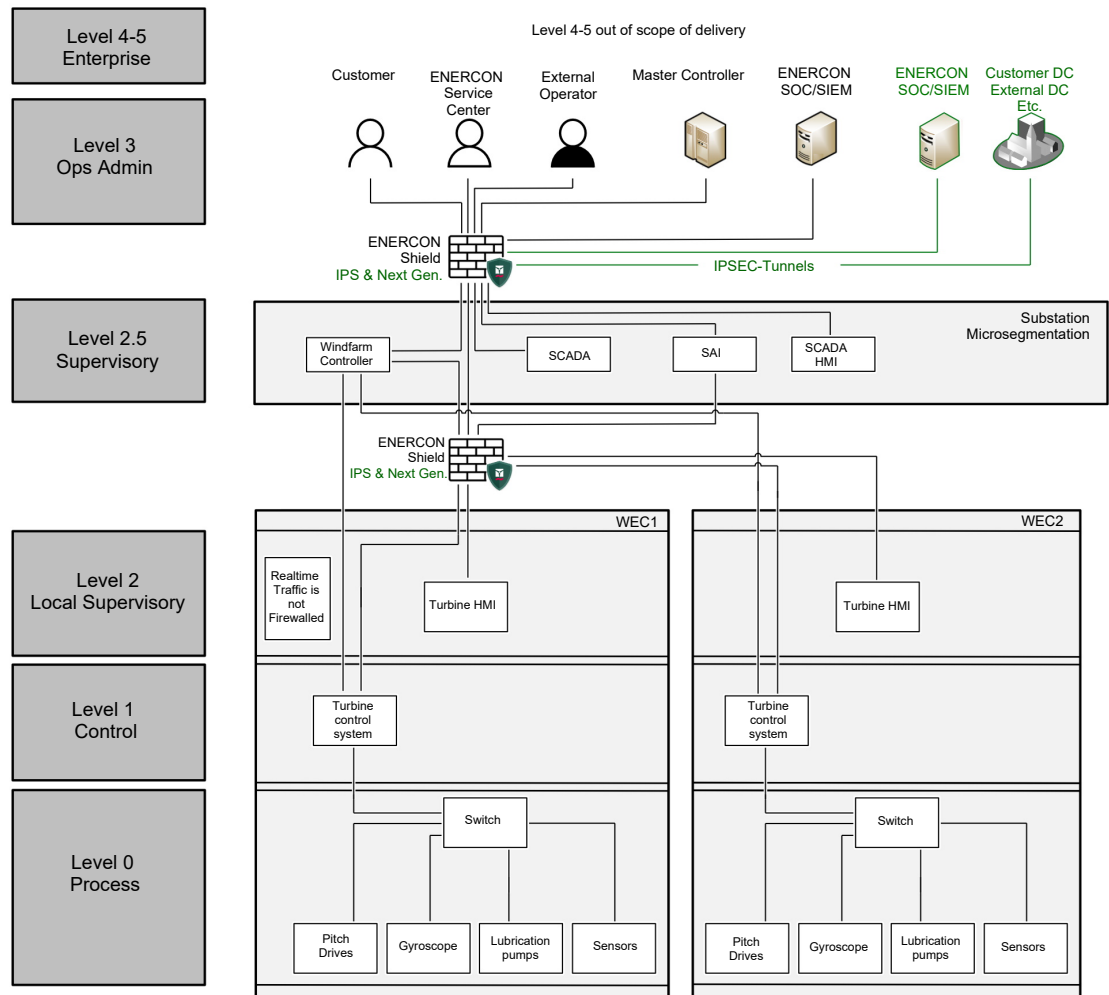


Abb. 3: Netzwerkarchitektur Active Security

Hauptfunktionen (zusätzlich zu Basic Security)

- VPN mit Remote Access ermöglicht einen sicheren Fernzugriff
- Intrusion Detection und Intrusion Prevention System (IDS/IPS) zur Erkennung und Blockierung von böartigem Datenverkehr in Echtzeit, Schutz vor Zero-Day-Angriffen und Schutz vor bekannten Schwachstellen.
- Deep Packet Inspection (DPI) für eine detailliertere Bedrohungserkennung auch bei verschlüsselten Protokollen.
- Echtzeit-Logdaten (Event- und Trafficlogs) können per Log-Forwarding einem Kunden-NOC/SOC zur Verfügung gestellt werden.

3.4 OT Pro Security

Das OT Pro Security-Modell ist die höchste Sicherheitsstufe und richtet sich speziell an kritische Infrastrukturen für das Höchstmaß an OT-Sicherheit im Windpark.

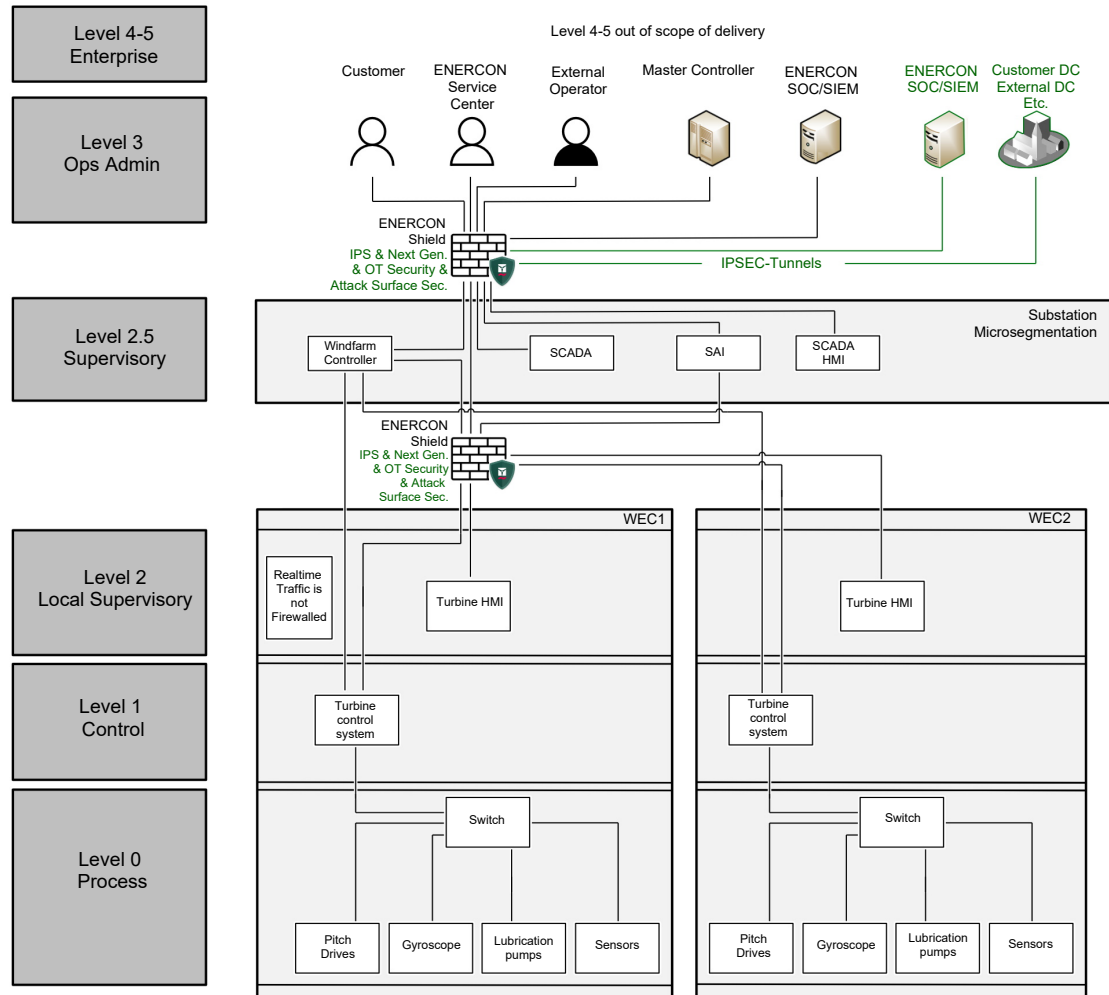


Abb. 4: Netzwerkarchitektur OT Pro Security

Hauptfunktionen (zusätzlich zu Active Security)

- **OT Application Control:** Kontrolle und Überwachung von industriellen Protokollen wie Modbus TCP, IEC-104, OPC UA, OPC XML DA)
- **OT Security Services:** Spezialisierte OT IPS Signaturen, die darauf abzielen, böswärtigen Datenverkehr in OT-Umgebungen zu erkennen und zu blockieren.
- **Attack Surface Security:** Kontinuierliche Überwachung und Bewertung der Firewall. Analysiert die vorhandenen Sicherheitsmaßnahmen und liefert eine Gesamtbewertung der Sicherheitslage. Dabei werden ungeschlossene Schwachstellen, Fehlkonfiguration und suboptimale Einstellungen identifiziert, die sich auf die Sicherheitsbewertung auswirken.
- **Anzeige von CIS-Compliance-Informationen:** Unterstützt bei der Einhaltung von Sicherheitsstandards und -richtlinien.

3.5 Optionale Erweiterungen

3.5.1 ENERCON Shield Cluster

ENERCON Shield Cluster bietet als Option für Kunden mit hohen Verfügbarkeitsanforderungen eine Redundanzlösung mit automatischem Failover, um eine unterbrechungsfreie Konnektivität und Sicherheit im Windpark zu gewährleisten. Durch den Einsatz eines Clusters lassen sich Ausfallrisiken minimieren und der sichere Betrieb auch bei einem Hardwarefehler aufrechterhalten. Die Firewall-Konfigurationen und -Regeln bleiben dabei synchronisiert, sodass ein nahtloser Wechsel zwischen den Systemen möglich ist. Zur Verfügbarkeit für ENERCON Shield Ausbaustufen siehe Tab. 2, S. 15.

3.5.2 Site-to-Site (S2S) VPN Interface

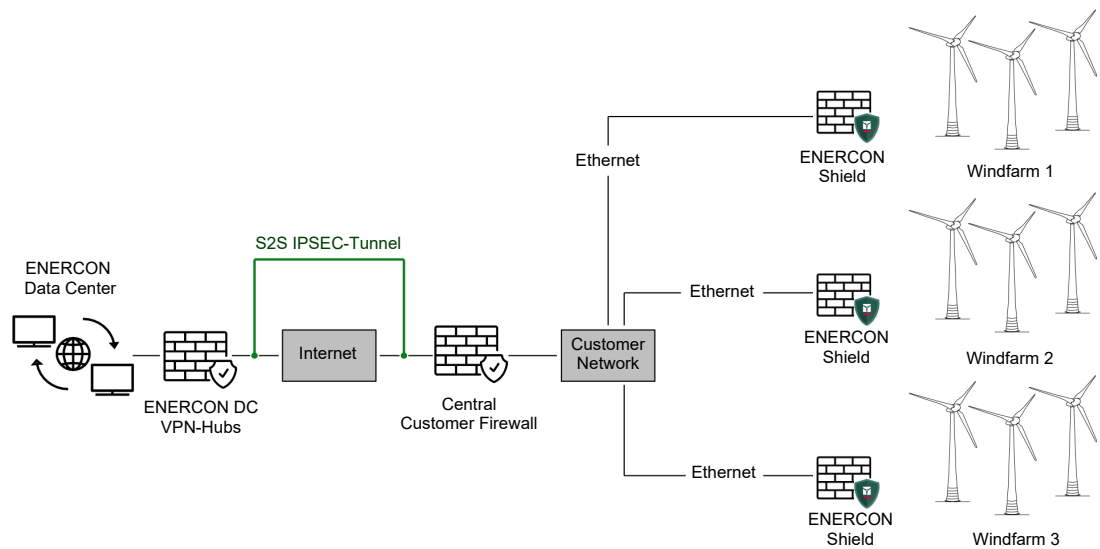


Abb. 5: Beispielhafte Konfiguration einer Site-to-Site-Verbindung (S2S)

Eine Site-to-Site-Verbindung vom ENERCON Rechenzentrum zum Rechenzentrum des Kunden bietet eine optionale Alternative zur Standard VPN-Anbindung zum Windpark. Sie ermöglicht eine indirekte, sichere Kommunikation zu den Zielsystemen und ist besonders relevant für Kunden mit erhöhten Sicherheits- und Compliance-Anforderungen, da sie die Datenverarbeitung innerhalb der kundeneigenen IT-Infrastruktur gewährleistet und externe VPN-Verbindungen minimiert. ENERCON bietet hierzu mehrere Konfigurationen, die je nach spezifischem Kundenbedarf implementiert werden können. Zur Verfügbarkeit für ENERCON Shield Ausbaustufen siehe Tab. 2, S. 15.

3.6 Vergleich der verschiedenen Abo-Modelle/Ausbaustufen

Tab. 2: ENERCON Shield Funktionen pro Ausbaustufe

Funktionen	Router ¹	Basic Security	Active Security	OT Pro Security
Hardware	Router	Firewall incl. Router	Firewall incl. Router	Firewall incl. Router

Funktionen	Router ¹	Basic Security	Active Security	OT Pro Security
Network ports	DSL, LTE, Ethernet	Ethernet	Ethernet	Ethernet
Internet Protocol Security	VPN	VPN	VPN, Direct Remote Access ²	VPN, Direct Remote Access ²
Redundant WAN-Ports		X	X	X
Redundant Power Supply		X	X	X
Autom. Software-Updates		X	X	X
SD-WAN		X	X	X
Network Segmentation		X	X	X
Read-Only Access for Audit		X	X	X
Intrusion Prevention System (IPS)			X	X
Next-Generation-Firewall			X	X
Realtime Provision of Data to customer's NOC & SOC			X	X
OT Application Control				X
OT Security Service				X
Attack Surface Security				X
Managed by ENERCON	X	X	X	X
ENERCON Shield Cluster			(X) ³	(X) ³
Site-to-Site (S2S) VPN Interface			(X) ³	(X) ³

¹ aktuelle Technik ohne ENERCON Shield

² ausgehendes IPSEC-S2S-VPN von Windpark zu Partner/Kunde/Direktvermarkter

³ optional

4 Datenverarbeitung und Datenspeicherung

Die untenstehenden Anwendungen gehören nicht zum Lieferumfang von ENERCON Shield, sondern werden von ENERCON gehostet und betrieben und ermöglichen die verschiedenen Serviceleistung im ENERCON Shield Produkt. Eine entsprechende Datenverarbeitung und -speicherung in ENERCONs Datencentern ist integriert.

FortiManager

Der FortiManager ist eine zentralisierte Plattform für das Firewall Management. Er ermöglicht die Verwaltung, Überwachung und Analyse der FortiGate Firewall. Der FortiManager vereinfacht die Sicherheitsadministration, automatisiert den Roll-Out des Regelwerkes und Updates, und unterstützt die Erkennung von Cyberbedrohungen.

Der FortiManager wird in Microsoft Azure gehostet und nutzt dadurch die cloudnative Funktionen für Skalierbarkeit, Hochverfügbarkeit und Sicherheit. Er entspricht den Anforderungen der ISO 27001 und gewährleistet die Einhaltung der DSGVO-Vorgaben durch folgende Merkmale und Funktionen:

- Die zentralisierte Richtlinienverwaltung stellt sicher, dass das Sicherheitsregelwerk über alle FortiGate Firewalls hinweg konsistent ausgerollt ist.
- Umfassende Protokollierung und Überwachung zur Unterstützung der Compliance Anforderungen
- Verschlüsselte Speicherung und Verarbeitung der Daten der Firewall zur Einhaltung des Datenschutzes
- Definierte rollenbasierte Zugriffskontrollen (RBAC), um Änderungen und Zugriffe Unbefugter zu verhindern
- Datenresidenz in Azure-Regionen: Für Deutschland gelten die Regionen Westeuropa und Deutschland Zentral West, die DSGVO-konforme Speicherung innerhalb der EU ermöglichen.
- Der FortiManager wird vom ENERCON SOC überwacht. Dadurch wird die Sicherheit der Verwaltung der Firewall zusätzlich sichergestellt.

FortiAnalyzer

Der FortiAnalyzer ist eine Plattform für Log-Management, Analyse und Reporting. Er bietet eine umfassende Einsicht in die Ereignisse der Firewall. Der FortiAnalyzer ermöglicht die Erfassung, Aggregation und Analyse von Logs, um die Überwachung zu optimieren und Compliance-Anforderungen gerecht zu werden. Warnungen und andere Ereignisse werden im FortiAnalyzer zentral aggregiert, was eine vereinfachte und konsolidierte Sicht auf die Sicherheitslage aller angeschlossenen FortiGate Geräte bietet. Zudem unterstützt FortiAnalyzer detaillierte Datenerfassung für forensische Zwecke und unterstützt dabei beispielsweise die Konformität mit den Anforderungen der NIS2 Direktive im Hinblick auf Untersuchung von Informationssicherheitsvorfällen und der einhergehenden Anforderungen zur Berichterstattung an Behörden.

Der FortiAnalyzer wird ebenfalls in Azure gehostet und unterstützt bei der Einhaltung des ISO 27001 und erfüllt die Anforderungen der DSGVO durch folgende Merkmale und Funktionen:

- Zentrale Erfassung und Speicherung von Logs ist für hohe Datenmengen optimiert und ermöglicht eine umfassende Netzwerküberwachung
- Sicherheitsrelevante Ereignisse können rechtzeitig identifiziert werden mit Hilfe von erweiterten Analysen und Korrelationen der Ereignisse.
- Dynamische Berichterstattung zur Unterstützung von Compliance und Audits
- Vereinfachte Integration mit SOC/SIEM Systemen der Kunden