Technische Spezifikation

Anforderungen an Systemhersteller

Bedarfsgerechte Nachtkennzeichnung (BNK)

ENERCON
ENERGIE FÜR DIE WELT

Freigabe: 2024-01-30 15:18

Herausgeber

ENERCON 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: Dr. Jürgen Zeschky, Dr. Martin Prillmann, Dr. Michael Jaxy
Zuständiges Amtsgericht: Aurich ▪ Handelsregisternummer: HRB 411
Ust.Id.-Nr.: DE 181 977 360

Dokumentinformation

Dokument-ID	D0611773/4.0-de
Vermerk	Originaldokument

Datum	**Sprache**	**DCC**	**Werk / Abteilung**
2024-01-09	de	EC	WRD Wobben Research and Development GmbH / Documentation Department

Inhaltsverzeichnis

Abkürzungsverzeichnis

ASCII	American Standard Code for Information Interchange (amerikanischer Standard-Code für Informationsaustausch)
AVV	Allgemeine Verwaltungsvorschrift
BCMT	Begin of civil morning twilight (Beginn der bürgerlichen Morgendämmerung)
BNK	Bedarfsgerechte Nachtkennzeichnung
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certificate authority (Zertifizierungsstelle)
CN	Common name (gemeinsamer Name)
CRC	Cyclic redundancy check (zyklische Redundanzprüfung)
CRL	Certificate revocation list (Zertifikatsperrliste)
ECET	End of civil evening twilight (Ende der bürgerlichen Abenddämmerung)
EPK	ENERCON PartnerKonzept
HMAC	Keyed-hash message authentication code (hashbasierte, schlüsselabhängige kryptographische Prüfsumme)
PKI	Public key infrastructure (Sicherheitsinfrastruktur mit öffentlich hinterlegtem Schlüssel)
SSL	Secure Sockets Layer (Netzwerkprotokoll zur sicheren Datenübertragung)
TLS	Transport Layer Security (Netzwerkprotokoll zur sicheren Datenübertragung)
URL	Uniform Resource Locator (eindeutige Adresse innerhalb eines Computernetzwerks)

1 Anforderungen

Zur bedarfsgerechten Steuerung der Nachtkennzeichnung von ENERCON Windenergieanlagen über die ENERCON BNK-Schnittstelle muss das steuernde System die in diesem Dokument aufgeführten Anforderungen erfüllen.

Umsetzung

Grundlage für die Umsetzung der bedarfsgerechten Nachtkennzeichnung ist die zum jeweiligen Zeitpunkt gültige Allgemeine Verwaltungsvorschrift (AVV) zur Kennzeichnung von Luftfahrthindernissen. Insbesondere in Anhang 6 wird auf die Funktion der bedarfsgerechten Nachtkennzeichnung von Windenergieanlagen eingegangen. Des Weiteren sind folgende Anforderungen zu erfüllen:

Tab. 1: Funktionale Anforderungen

ID	Anforderung	Kriterium	Verantwortlichkeit	
			ENERCON	Systemhersteller
BNK01	Ein Betrieb der Befeuerung außerhalb der Zeit von ECET und BCMT ist durch einen Dämmerungsschalter zu gewährleisten. BNK inaktiv → autonomer Betrieb der Befeuerung Dies ist durch das verteilte BNK-Signal sicherzustellen. BNK → ENERCON SCADA Server/ENERCON SCADA Edge Server→ Windenergieanlage → Befeuerung	muss	X	
BNK02	Die Nachtkennzeichnung darf unterdrückt werden, wenn sich kein relevantes Luftfahrzeug im Wirkungsraum befindet. (gewünschte Funktion von BNK)	muss		X
BNK03	Die Nachtkennzeichnung darf unterdrückt werden, wenn die Systemintegrität sowie eine ausreichende Detektionsleistung durch die Selbstdiagnose signalisiert werden (ordnungsgemäßer Betrieb, kein Fehler). Ein Fehler einer Komponente → alle Befeuerungsleuchten an Signal: Fehler/kein Fehler an ENERCON SCADA Server/ ENERCON SCADA Edge Server	muss		X

ID	Anforderung	Kriterium	Verantwortlichkeit	
			ENERCON	Systemhersteller
BNK04	Wenn die Bedingungen für ein Unterdrücken der Befeuerung nicht erfüllt sind, ist die gesamte Befeuerung sofort in Betrieb zu versetzen (100 % Nennlichtstärke).	muss		X
BNK05	Das Gesamtsystem BNK muss durch eine durch das Bundesministerium für Verkehr und digitale Infrastruktur benannte Stelle anerkannt sein.	muss	X	X
BNK06	Die Paketlaufzeit bei der Kommunikation muss anhand der Antwort des ENERCON SCADA Servers/ENERCON SCADA Edge Servers überwacht werden.	muss		X
BNK07	Eine RJ45-Schnittstelle zur Anbindung des BNK-Systems an den ENERCON SCADA Server/ ENERCON SCADA Edge Server muss vorhanden sein.	muss	X	X

Tab. 2: Allgemeine Anforderungen

ID	Anforderung	Kriterium	Verantwortlichkeit	
			ENERCON	Systemhersteller
A01	Das BNK-System (System und Kommunikation zum Windpark) muss eine Jahresverfügbarkeit von mindestens 90 % aufweisen. Die Betreuung muss den Bedingungen eines EPK-Vertrags unterliegen.	muss	X	X
A02	Das IT-Sicherheitsgesetz muss unter dem Gesichtspunkt der kritischen Infrastruktur eingehalten werden.	muss	X	X
A03	Die Software der Befeuerungssteuerung der Windenergieanlagen muss geprüft und ggf. durch ein Update aktualisiert werden.	muss	X	

2 Schnittstellendefinition

Die Schnittstelle zwischen dem BNK-System und dem ENERCON SCADA Server/ ENERCON SCADA Edge Server wird bidirektional ausgeführt. Basis hierbei ist eine TCP-Socket-Verbindung, die mit TLS ausgeführt wird. Die Authentifizierung und Autorisierung erfolgt zertifikatbasiert. Um die Latenz in der Kommunikation so klein wie möglich zu halten, muss hier mit einer etablierten Socket-Verbindung (d. h. ohne ständigen Verbindungsaufbau und Verbindungsabbau) gearbeitet werden.

Daten vom BNK-System

Zur Steuerung der Befeuerung müssen Informationen vom BNK-System an den ENERCON SCADA Server/ENERCON SCADA Edge Server übertragen werden. Dabei müssen die folgenden Eigenschaften beachtet werden:

- Byte-Reihenfolge: **Big-Endian**
- Datensätze werden zyklisch von der BNK-Schnittstelle des ENERCON SCADA Servers/ENERCON SCADA Edge Servers erwartet.
  - Zeit zwischen einem erneuten Empfang: 1,5 Sekunden (±0,05 Sekunden)
- Timeout: 4,5 Sekunden

Der durch das BNK-System überwachte Luftraum muss um die Strecke erweitert werden, die ein Luftfahrzeug innerhalb des Timeouts zurücklegt.

Tab. 3: Steuerdatensatz

Byte-Nr.	Bit-Nr.	Information	Gültige Werte	Ungültige Werte
0	0-7	Versionsnummer (SCADA-Schnittstelle)	1	Sonstige
1	8-15	eindeutiger Paket-Identifier	0x42 (ASCII-Code für "B")	Sonstige
2	16-23	lfd. Paketnummer	0-255	-
3	24	Befeuerung unterdrücken	0: Befeuerung nicht unterdrücken 1: Befeuerung unterdrücken	-
3	25	aktiver BNK-Betrieb	0: passiver BNK-Betrieb; Befeuerung soll nicht bedarfsgerecht gesteuert werden (z. B. außerhalb des zulässigen Zeitfensters) 1: aktiver BNK-Betrieb; Befeuerung soll bedarfsgerecht gesteuert werden (z. B. innerhalb des zulässigen Zeitfensters)	-
3	26	Fehler des BNK-Systems (z. B. keine verlässliche Detektion möglich)	0: kein Fehler 1: Fehler	-

Byte-Nr.	Bit-Nr.	Information	Gültige Werte			Ungültige Werte
3	27-28	Startsequenz der Befeuerung	Bit 28	Bit 27	Variante	11
			0	0	A	
			0	1	B	
			1	0	C	
3	29-31	nicht verwendet	000			Sonstige
4-6	32-55	CRC-Prüfsumme (über die Bytes 1-3; ohne Versionsnummer in Byte 0)	-			-

Beispiel für Bit-Muster von Byte 3

Das Beispiel soll die Verwendung des Steuerdatensatzes verdeutlichen. Bei dem Beispiel werden folgende Signale gesendet:

- Befeuerung unterdrücken (Bit 24 = 1)
- aktiver BNK-Betrieb (Bit 25 = 1)
- kein Fehler des BNK-Systems (Bit 26 = 0)
- Startsequenz der Befeuerung: C (Bit 27 = 0, Bit 28 = 1)

Tab. 4: Beispiel für Bit-Muster von Byte 3

Bit-Nr.	31	30	29	28	27	26	25	24
Signal	0	0	0	1	0	0	1	1

Dieses entspricht dem hexadezimalen Wert 0x13.

Spezifikation der CRC-Berechnungsmethode

- Polynom: 0xCBA785
- Grad des Polynoms: 24
- Initialwert: 0xFFFFFF
- Wert für finales XOR: 0xFFFFFF
- non-direct

Beispiele 1 für CRC-Prüfsumme

Für das Beispiel werden folgende Daten angenommen:

- Byte 1: Identifier =0x42
- Byte 2: laufende Paketnummer = 0x1
- Byte 3: Steuerdaten 0x13 (siehe Beispiel für Bit-Muster von Byte 3))

Die Daten ergeben einen Byte-Stream von 0x420113.

Daraus ergibt sich eine CRC-Prüfsumme des Byte-Streams von 0x994054.

Beispiel 2 für CRC-Prüfsumme

Für das zweite Beispiel werden folgende Daten angenommen:

- Byte 1: Identifier = 0x42

- Byte 2: laufende Paketnummer = 0x2
- Byte 3: Steuerdaten 0x13 (siehe Beispiel für Bit-Muster von Byte 3)

Die Daten ergeben einen Byte-Stream von 0x420213.

Daraus ergibt sich eine CRC-Prüfsumme des Byte-Streams von 0xEC6994.

Daten an das BNK-System

Der ENERCON SCADA Server/ENERCON SCADA Edge Server antwortet umgehend auf eingehende BNK-Informationen. Dabei muss die folgende Eigenschaft beachtet werden:

- Byte-Reihenfolge: **Big-Endian**

Tab. 5: Antwortdatensatz

Byte-Nr.	Information	Gültige Werte	Ungültige Werte
0	Versionsnummer	1	Sonstige
1-6	gespiegelte Daten vom BNK-System	siehe Steuerdatensatz des BNK-Systems (Byte 1-6)	
7-8	aktuelles Jahr vom ENERCON SCADA Server/ENERCON SCADA Edge Server	0-65535	-
9	aktueller Monat vom ENERCON SCADA Server/ENERCON SCADA Edge Server	1-12	Sonstige
10	aktueller Tag vom ENERCON SCADA Server/ENERCON SCADA Edge Server	1-31	Sonstige
11	aktuelle Stunde vom ENERCON SCADA Server/ENERCON SCADA Edge Server	0-23	Sonstige
12	aktuelle Minute vom ENERCON SCADA Server/ENERCON SCADA Edge Server	0-59	Sonstige
13	aktuelle Sekunde vom ENERCON SCADA Server/ ENERCON SCADA Edge Server	0-59	Sonstige
14	Anzahl vorhandener Windenergieanlagen im Windpark	0-255	-
15	Anzahl der Windenergieanlagen mit Kommunikationsstörungen	0-255	-
16	Anzahl der Windenergieanlagen mit gestörter Befeuerung	0-255	-

3 TLS-Kommunikation

3.1 Funktion

Zwischen dem ENERCON SCADA Server/ENERCON SCADA Edge Server und einem BNK-System in der Rolle als Client wird eine TLS-gesicherte Kommunikation etabliert. Zur gegenseitigen Authentifizierung werden X509-Zertifikate eingesetzt, welche aus der ENERCON SCADA-PKI abgeleitet sind.

Die ENERCON SCADA-PKI besteht aus der Root-CA mit dem CommonName (CN) „EC2-SCADACA-1“ sowie der Intermediate-CA für Kommunikationsstrukturen mit dem CN „EC2-CommCA-1“. Aussteller der Server- bzw. Client-Zertifikate ist die Intermediate-CA.

Jedes X509-Zertifikat dient als eindeutiges Identifizierungsmerkmal und Authentifizierungsmerkmal und darf nur in einem System verwendet werden. Der im Zertifikat hinterlegte CN muss eindeutig sein und einen exakten Rückschluss auf das verwendete System ermöglichen (Beispiel ENERCON SCADA: Der CN „SCADA_1234“ beschreibt das ENERCON SCADA Server/ENERCON SCADA Edge Server-Zertifikat eines Windparks mit der Windpark-ID 1234).

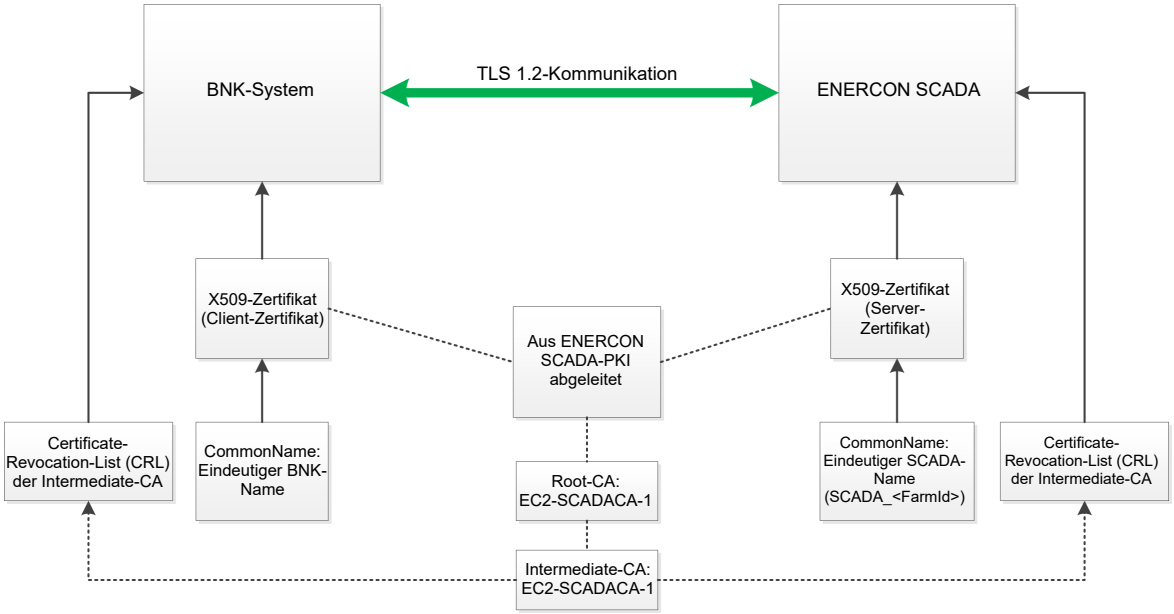

Abb. 1: Übersicht TLS

Bei einem Austausch oder einer Kompromittierung des Systems wird das verknüpfte X509-Zertifikat durch die Intermediate-CA zurückgerufen. Hierzu wird in regelmäßigen Abständen eine Certificate-Revocation-List (CRL) erstellt und veröffentlicht.

Alle an einer TLS-Kommunikation teilnehmenden Systeme müssen diese CRL regelmäßig aktualisieren und validieren.

3.2 Konfiguration

Die Konfiguration der TLS-Kommunikation basiert auf der technischen Richtlinie TR-02102-2 (Version 2017-01) vom Bundesamt für Sicherheit in der Informationstechnik (BSI) über die Verwendung von Transport Layer Security (TLS).

Der ENERCON SCADA Server/ENERCON SCADA Edge Server unterstützt folgende Konfigurationen:

- SSL/TLS-Version: TLS 1.2 (nicht abwärtskompatibel zu älteren Versionen)
- elliptische Kurven: secp256r1, secp384r1
- Cipher Suites:

TLS_	ECDHE_RSA_	WITH_	AES_128_	CBC_	SHA256
				GCM_	
			AES_256_	CBC_	SHA384
				GCM_	
	ECDH_RSA_		AES_128_	CBC_	SHA256
				GCM_	
			AES_256_	CBC_	SHA384
				GCM_	

Cipher Suites mit Pre-Shared Key werden grundsätzlich nicht unterstützt.

- Session Renegotiation darf nicht unterstützt/verwendet werden.
- Kompression muss deaktiviert sein.
- Verkürzung der HMAC-Ausgabe (truncated_hmac) darf nicht unterstützt/verwendet werden.
- Heartbeat-Erweiterung darf nicht unterstützt/verwendet werden.

3.3 Zertifikatsvalidierung

Abb. 2: Zertifikatsvalidierung

Die Validierung des Zertifikats des Kommunikationspartners wird wie folgt umgesetzt:

Tab. 6: Schritte der Zertifikatsvalidierung

Schritt	Beschreibung
1	(Optional) Das Root-CA-Zertifikat sollte grundsätzlich bereits auf dem System vorhanden sein. Wird das Root-CA-Zertifikat nicht in einem vertrauenswürdigen Zertifikatsspeicher vorgehalten, kann eine zusätzliche Überprüfung des Fingerprints durchgeführt werden, um einen potenziellen Austausch bzw. eine Kompromittierung auszuschließen. Bei Erfolg wird die Root-CA als Vertrauensanker der gesamten Kommunikation angesehen. Der Fingerprint sollte zwecks Root-CA-Wechsel konfigurierbar sein.

Schritt	Beschreibung
2	Die Überprüfung der Zertifikatskette (certificate chain) ist in 2 Teilbereiche aufgeteilt.
2a	Im ersten Schritt wird die gesamte Kette bis zum Vertrauensanker (Root-CA) verifiziert.
2b	Zusätzlich wird überprüft, ob das Zertifikat von der erwarteten Intermediate-CA (für TLS-Verbindungen die „EC2-CommCA-1“) ausgestellt wurde. Der hierfür erforderliche CN der Intermediate-CA sollte als konfigurierbarer Parameter vorgehalten werden.
3	(Optional) Im nächsten Schritt kann zusätzlich die im Zertifikat hinterlegte Schlüsselverwendung „Key usage“ anhand eines Erwartungswerts überprüft werden.
4	In jedem Zertifikat ist eine Gültigkeitsdauer durch ein Start- und ein End-Datum angegeben, wobei die aktuelle Zeit (Systemzeit) innerhalb dieses Fensters liegen muss.
5	Um den Widerrufstatus eines Zertifikats überprüfen zu können, wird durch die ENERCON SCADA-PKI eine CRL bereitgestellt. In jedem Zertifikat ist hinterlegt, unter welchen Adressen (URL) die aktuelle CRL bezogen werden kann.
5a	Wird eine neue CRL initialisiert, müssen die Signatur sowie die Gültigkeitsdaten überprüft werden.
5b	Auf Basis dieser CRL wird für jedes Zertifikat während des Kommunikationsaufbaus überprüft, ob ein Zertifikat zurückgezogen wurde. Sollte keine aktuelle CRL vorliegen, wird der Widerrufstatus (RevocationStatus) zur Aufrechterhaltung einer funktionierenden Kommunikation ignoriert. In diesem Fall muss eine entsprechende Alarm-Meldung generiert werden.
6	Abschließend wird der im Zertifikat hinterlegte CN mit dem erwarteten Wert verglichen. Der erwartete CN sollte als konfigurierbarer Parameter hinterlegt werden.

3.4 Zertifikatsinfrastruktur

Für eine funktionierende Zertifikatsinfrastruktur müssen durch alle Systeme 2 wesentliche Prozesse unterstützt werden:

Zertifikatswechsel

Üblicherweise haben Zertifikate aus der ENERCON SCADA-PKI eine Gültigkeitsdauer von 5 Jahren. Aus diesem Grund muss es einen Prozess bzw. ein Verfahren geben, um ein Zertifikat auszutauschen, wobei das auszutauschende Zertifikat aus derselben Zertifikatskette abgeleitet wird.

Root-CA-Wechsel

Die Gültigkeitsdauer des Root-CA-Zertifikats ist wesentlich länger, jedoch nicht unbegrenzt. Aus diesem Grund muss es einen Prozess bzw. ein Verfahren geben, um das Stammzertifikat auszutauschen. Üblicherweise wird das Vertrauen zu einer neuen Root-CA über eine Kreuzsignierung zwischen alter und neuer Root-CA hergestellt, weshalb für einen begrenzten Zeitraum mindestens 2 Stammzertifikate gültig sein können.

4 Aufzeichnung und Auswertung des Betriebs

Der Status der bedarfsgerechten Nachtkennzeichnung wird vom ENERCON SCADA Server/ENERCON SCADA Edge Server aufgezeichnet. Es gibt folgende Möglichkeiten zur Aufzeichnung der Daten:

- Standard-Aufzeichnung (Lediglich die TLS-Verbindung wird aufgezeichnet.)
- erweiterte Aufzeichnung (mehr Information)

Die erweiterte Aufzeichnung muss durch den ENERCON Service aktiviert werden. Die Auswertung der Daten ist nur durch den ENERCON Service möglich. Der ENERCON Service kann bei Bedarf kontaktiert werden.