TÜVNORD

C E R T I F I C A T E

TÜVNORD
TÜV NORD CERT GmbH
IEC 62443
tuev-nord.de

Cybersecurity-related processes as per
IEC 62443-4-1 : 2018
IEC 62443-4-2 : 2019

In accordance with TÜV NORD CERT procedures, it is hereby certified that

congatec GmbH
Auwiesenstraße 5
94469 Deggendorf
Germany

meets the requirements of the standards listed above with the following development:

conga-zones bootloader

Certificate Registration No. 44 331 25116502
Audit Report No. 3542 8102

Valid from 2026-07-07
Valid until 2029-07-06
Initial certification 2026

Certification Body
at TÜV NORD CERT GmbH

Essen, 2026-07-07

This certification was conducted in accordance with the TÜV NORD CERT auditing and certification procedures and is subject to regular surveillance audits.

TÜV NORD CERT GmbH Am TÜV 1 45307 Essen www.tuev-nord-cert.com

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-12007-01-00

ANNEX

to Certificate Registration No. 44 331 25116502

Remarks:

To perform an assessment of a complete cybersecurity-related system, all relevant requirements of the IEC 62443 series of standards must be applied to the overall system in which the assessed conga-zones bootloader is to be integrated for the required security levels.

The assessed conga-zones bootloader is designed as a “generic component” that requires application configuration to operate in the final application that needs to be developed by congatec´s clients. For an IEC 62443 conformity statement of the final system, it is required to assess the conga-zones bootloader including the application configuration in its final application.

The Security Levels as documented in this Annex are only confirmed if the conga-zones bootloader version R2.1.01 or a later version is used.

*) The specified achievable Security Levels marked with *) require compensating countermeasures to be implemented in or provided by the security context of the conga-zones bootloader in the final application.

**) The component requirements marked with **) are requirements that do not apply to a software application component.

For further information related to the fulfilment of the Security-Levels listed in this Annex, please also refer to the “conga-zones bootloader User’s Guide”, the “conga-zones bootloader Cyber Security Guidelines” and referenced documentation that is provided in its latest available version.

Certification Body
at TÜV NORD CERT GmbH

Essen, 2026-07-07

DAkkS Deutsche Akkreditierungsstelle D-ZE-12007-01-00

ANNEX

to Certificate Registration No. 44 331 25116502

The assessed component including its user documentation is compliant with the following Security-Levels:

FR 1: Identification and authentication control:

CR 1.1:	Human user identification and authentication	**n/a**
CR 1.2:	Software process and device identification	**SL 2**
CR 1.3:	Account management	**n/a**
CR 1.4:	Identifier management	**n/a**
CR 1.5:	Authenticator management	**n/a**
CR 1.6:	Wireless access management	**n/a **)**
CR 1.7:	Strength of password-based authentication	**n/a**
CR 1.8:	Public key infrastructure certificates	**SL 0**
CR 1.9:	Strength of public key authentication	**n/a**
CR 1.10:	Authenticator feedback	**n/a**
CR 1.11:	Unsuccessful login attempts	**n/a**
CR 1.12:	System use notification	**n/a**
CR 1.13:	Access via untrusted networks	**n/a **)**
CR 1.14:	Strength of symmetric key-based authentication	**n/a**

FR 2: Use control:

CR 2.1:	Authorization enforcement	**n/a**
CR 2.2:	Wireless use control	**n/a**
CR 2.3:	Use control for portable and mobile devices	**n/a **)**
SAR 2.4:	Mobile code	**n/a**
CR 2.5:	Session lock	**n/a**
CR 2.6:	Remote session termination	**n/a**
CR 2.7:	Concurrent session control	**n/a**
CR 2.8:	Auditable events	**SL 2**
CR 2.9:	Audit storage capacity	**SL 0**
CR 2.10:	Response to audit processing failures	**n/a**
CR 2.11:	Timestamps	**SL 2** *)
CR 2.12:	Non-repudiation	**n/a**
CR 2.13:	Use of physical diagnostic and test interfaces	**n/a **)**

Certification Body
at TÜV NORD CERT GmbH

Essen, 2026-07-07

DAkkS Deutsche Akkreditierungsstelle D-ZE-12007-01-00

ANNEX

to Certificate Registration No. 44 331 25116502

FR 3: System integrity:		
CR 3.1:	Communication integrity	**n/a**
SAR 3.2:	Malicious code protection	**SL 2**
CR 3.3:	Security functionality verification	**SL 2**
CR 3.4:	Software and information integrity	**SL 2**
CR 3.5:	Input validation	**SL 2**
CR 3.6:	Deterministic output	**n/a**
CR 3.7:	Error handling	**SL 2**
CR 3.8:	Session integrity	**n/a**
CR 3.9:	Protection of audit information	**SL 0**
CR 3.10:	Support for updates	**n/a **)**
CR 3.11:	Physical tamper resistance and detection	**n/a **)**
CR 3.12:	Provisioning product supplier roots of trust	**n/a **)**
CR 3.13:	Provisioning asset owner roots of trust	**n/a **)**
CR 3.14:	Integrity of the boot process	**n/a **)**

FR 4: Data confidentiality:		
CR 4.1:	Information confidentiality	**SL 0**
CR 4.2:	Information persistence	**n/a**
CR 4.3:	Use of cryptography	**SL 2**

FR 5: Restricted data flow:		
CR 5.1:	Network segmentation	**n/a**
CR 5.2:	Zone boundary protection	**n/a **)**
CR 5.3:	General purpose person-to-person communication restrictions	**n/a **)**
CR 5.4:	Application partitioning	**n/a **)**

FR 6: Timely response to events:		
CR 6.1:	Audit log accessibility	**SL 2** *)
CR 6.2:	Continuous monitoring	**n/a**

FR 7: Resource availability:		
CR 7.1:	Denial of service protection	**n/a**
CR 7.2:	Resource management	**n/a**
CR 7.3:	Control system backup	**SL 0**
CR 7.4:	Control system recovery and reconstitution	**SL 0**
CR 7.5:	Emergency power	**n/a **)**
CR 7.6:	Network and security configuration settings	**n/a**
CR 7.7:	Least functionality	**n/a**
CR 7.8:	Control system component inventory	**SL 2**

Certification Body
at TÜV NORD CERT GmbH

Essen, 2026-07-07

DAkkS Deutsche Akkreditierungsstelle D-ZE-12007-01-00