CERTIFICADO ◆ 인증서 ◆ CERTIFICATO ◆ 認証 ◆ CERTIFICATE ◆ 认证证书 ◆ ZERTIFIKAT

CERTIFICATE

CERTIFICATO

Number:
Numero:
TUV IT 26 CYB A 031 rev. 00

Holder of the certificate:
Titolare del certificato:
Danfoss Drives A/S
Ulsnæs 1, DG 1206, 6300 Gråsten
Denmark

Site(s):
Sede/i:
Danfoss Drives Oy
Runsorintie 7, 65380 Vaasa
Finland

Scope of certificate:
Oggetto della certificazione:
iC7-Marine and iC7-Hybrid products
iC7-60SLxxyy-zzzzE00Fw+ccccc

Applied standards:
Norme applicate:
IEC 62443-4-1:2018
IEC 62443-4-2:2019

Parameters:
Parametri:
Product type: ED, (see Annex for details)

Certification Mark:
Marchio di certificazione:



Technical Report:
Assessment report:
DH107114T

We herewith certify that the scope of certificate meets the requirements of the applied standards

Si certifica che l'oggetto della certificazione soddisfa i requisiti delle norme applicate.

Date of 1st issue: **2026-07-23**
Data 1ª emissione:
Issue date: **2026-07-23**
Data emissione:
Expiry date: **2029-07-22**
Data scadenza:

00077 PRD
Membro degli Accordi di Mutuo Riconoscimento
EA, IAF e ILAC
Signatory of EA, IAF and ILAC Mutual
Recognition Agreements

TÜV Italia S.r.l.

Alberto Carelli
I&I Division Manager

CERTIFICADO ◆ 인증서 ◆ CERTIFICATO ◆ 認証 ◆ CERTIFICATE ◆ 认证证书 ◆ ZERTIFIKAT

Annex to the Certificate

Allegato al Certificato

n° TUV IT 26 CYB A 031 rev. 00

Additional parameters:

SL-C (F): (2, 0, 2, 4, 4, 4, 4)
SL-C (F+S): (2, 3, 2, 4, 4, 4, 4)
SL-C (F+S+P): (2, 3, 2, 4, 4, 4, 4)

Security Guidelines: Cybersecurity for Danfoss Drives, “Danfoss cyber security user guide to iC7”

List of relevant component requirements (CR+EDR):

ID	Requirement	Result	Notes
CR 1.1	Human user identification and authentication	F	
CR 1.1 (1)	Unique identification and authentication	F	
CR 1.1 (2)	Multifactor authentication for all interfaces	N	
CR 1.2	Software process and device identification and authentication	F	
CR 1.2 (1)	Unique identification and authentication	F	
CR 1.3	Account management	F	
CR 1.4	Identifier management	F	
CR 1.5	Authenticator management	F	
CR 1.5 (1)	Hardware security for authenticators	N	
CR 1.7	Strength of password-based authentication	F	
CR 1.7 (1)	Password generation and lifetime restrictions for human users	N/A	
CR 1.7 (2)	Password lifetime restrictions for all users (human, software process, or device)	N/A	
CR 1.8	Public key infrastructure (PKI) certificates	F	
CR 1.9	Strength of public key-based authentication	F	
CR 1.9 (1)	Hardware security for public key-based authentication	F	
CR 1.10	Authenticator feedback	F	
CR 1.11	Unsuccessful login attempts	F	
CR 1.12	System use notification	F	
CR 1.14	Strength of symmetric key-based authentication	N/A	
CR 1.14 (1)	Hardware security for symmetric key-based authentication	N/A	
CR 2.1	Authorization enforcement	F	
CR 2.1 (1)	Authorization enforcement for all users	F	
CR 2.1 (2)	Permission mapping to roles	F	
CR 2.1 (3)	Supervisor override	F	
CR 2.1 (4)	Dual approval	N	
CR 2.2	Wireless use control	N/A	
EDR 2.4	Mobile code	N/A	
EDR 2.4 (1)	Mobile code authenticity check	N/A	
CR 2.5	Session lock	N/A	
CR 2.6	Remote session termination	F	
CR 2.7	Concurrent session control	F	

CERTIFICADO ◆ 인증서 ◆ CERTIFICATO ◆ 認証 ◆ CERTIFICATE ◆ 认证证书 ◆ ZERTIFIKAT

ID	Requirement	Result	Notes
CR 2.8	Auditable events	F	
CR 2.9	Audit storage capacity	S	(1)
CR 2.9 (1)	Warn when audit record storage capacity threshold reached	S	(1)
CR 2.10	Response to audit processing failures	F	
CR 2.11	Timestamps	F	
CR 2.11 (1)	Time synchronization	F	
CR 2.11 (2)	Protection of time source integrity	N	
CR 2.12	Non-repudiation	F	
CR 2.12 (1)	Non-repudiation for all users	F	
EDR 2.13	Use of physical diagnostic and test interfaces	F	
EDR 2.13 (1)	Active monitoring	F	
CR 3.1	Communication integrity	F	
CR 3.1 (1)	Communication authentication	F	
EDR 3.2	Protection from malicious code	F	
CR 3.3	Security functionality verification	F	
CR 3.3 (1)	Security functionality verification during normal operation	F	
CR 3.4	Software and information integrity	F	
CR 3.4 (1)	Authenticity of software and information	F	
CR 3.4 (2)	Automated notification of integrity violations	N	
(CR 3.5	Input validation	F	
CR 3.6	Deterministic output	F	
CR 3.7	Error handling	F	
CR 3.8	Session integrity	F	
CR 3.9	Protection of audit information	F	
CR 3.9 (1)	Audit records on write-once media	N	
EDR 3.10	Support for updates	F	
EDR 3.10 (1)	Update authenticity and integrity	F	
EDR 3.11	Physical tamper resistance and detection	F	
EDR 3.11 (1)	Notification of a tampering attempt	N	
EDR 3.12	Provisioning product supplier roots of trust	F	
EDR 3.13	Provisioning asset owner roots of trust	F	
EDR 3.14	Integrity of the boot process	F	
EDR 3.14 (1)	Authenticity of the boot process	F	
CR 4.1	Information confidentiality	F	
CR 4.2	Information persistence	F	
CR 4.2 (1)	Erase of shared memory resources	F	
CR 4.2 (2)	Erase verification	F	
CR 4.3	Use of cryptography	F	
CR 5.1	Network segmentation	F	
CR 6.1	Audit log accessibility	F	
CR 6.1 (1)	Programmatic access to audit logs	F	
CR 6.2	Continuous monitoring	F	
CR 7.1	Denial of service protection	F	

CERTIFICADO ◆ 인증서 ◆ CERTIFICATO ◆ 認証 ◆ CERTIFICATE ◆ 认证证书 ◆ ZERTIFIKAT

ID	Requirement	Result	Notes
CR 7.1 (1)	Manage communication load from component	F	
CR 7.2	Resource management	F	
CR 7.3	Control system backup	F	
CR 7.3 (1)	Backup integrity verification	F	
CR 7.4	Control system recovery and reconstitution	F	
CR 7.6	Network and security configuration settings	F	
CR 7.6 (1)	Machine-readable reporting of current security settings	F	
CR 7.7	Least functionality	F	
CR 7.8	Control system component inventory	F	

Notes:

(1) See report DH107114T for details

Aggregated summary (CR+EDR):

Security Level	F	N	N/A	S	P	Grand Total
1	32	0	3	1	0	*36*
2	23	0	2	0	0	*25*
3	9	4	2	1	0	*16*
4	2	3	1	0	0	*6*
Grand Total	*66*	*7*	*8*	*2*	*0*	*83*

Key (fulfilment relies on the listed security guidelines and application conditions):

F	Fulfilled
S	Fulfilled by integration at system level
P	Partly fulfilled
N	Not fulfilled
N/A	Not Applicable

Related certificate:

TUV IT 25 CYB A 018 rev. 00 (Security Development Lifecycle)