IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE)

Certificate of Conformity – Industrial Cyber Security Capability

Type	**Product Capability Assessment**
Name and address of the applicant	**Westermo Network Technologies** Metallverksqatan 6, 721 30 Västerås - SWEDEN
Certificate Coverage (including Version)	Product: Viper 3500 Series Version: WeOS 5.25 x
Standard	IEC 62443-4-2:2019

Requirements Assessed
The 3-tuple represents (Passed requirements, requirements assessed as Not Applicable, Total number of requirements)

Identification and authentication control (13,9,22)
Use control (11,10,21)
System integrity (9,10,19)
Data confidentiality (3,2,5)
Restricted data flow (1,3,4)
Timely response to events (2,1,3)
Resource availability (9,2,11)
Device specific
Network device requirements (14,3,22)
Software application requirements (0,3,3)
Embedded device requirements (0,13,13)
Host device requirements (0,14,14)

Security Level 2

Additional information (if necessary may also be reported on page 2)	The product has been developed following Process Application of Capabilities Assessment (IEC 62443-4-1) as certified in Cert.No FR_Cyber10228 ☒ Additional Information on page 2
As shown in the Test Report Ref. No. which forms part of this Certificate	26929581-812805-A

This Certificate of Conformity, issued by the National Certification Body, certifies that the above have been found to be in conformity with the requirements of the Industrial Cyber Security Capability Scheme (IECEE OD-2061) as it relates to the claims declared by the Applicant.

LABORATOIRE CENTRAL DES INDUSTRIES ELECTRIQUES - LCIE
33 avenue du Général Leclerc
92260 Fontenay-aux-Roses, FRANCE
www.lcie.fr

Date: 22/12/2025

Signature: Julien GAUTHIER
Certification Officer

IEC 62443-4-2 ID	Requirement Name	Results-Remarks	Verdict
CCSC 1	Support of essential functions	Not in scope	N/A
CCSC 2	Compensating countermeasures	Not in scope	N/A
CCSC 3	Least privilege	Not in scope	N/A
CCSC 4	Software development process	Not in scope	N/A
CR 1.01	Human user identification and authentication		Pass
CR 1.01 RE(1)	Unique identification and authentication		Pass
CR 1.01 RE(2)	Multifactor authentication for all interfaces	Not in scope	N/A
CR 1.02	Software process and device identification and authentication		Pass
CR 1.02 RE(1)	Unique identification and authentication	Not in scope	N/A
CR 1.03	Account management		Pass
CR 1.04	Identifier management		Pass
CR 1.05	Authenticator management		Pass
CR 1.05 RE(1)	Hardware security for authenticators	Not in scope	N/A
CR 1.06	Wireless access management	Not in scope	N/A
NDR 1.06	Wireless access management	Not in scope	N/A
NDR 1.06 RE(1)	Unique identification and authentication	Not in scope	N/A
CR 1.07	Strength of password-based authentication		Pass
CR 1.07 RE(1)	Password generation and lifetime restrictions for human users	Not in scope	N/A
CR 1.07 RE(2)	Password lifetime restrictions for all users (human, software process, or device)	Not in scope	N/A
CR 1.08	Public key infrastructure certificates		Pass
CR 1.09	Strength of public key-based authentication		Pass
CR 1.09 RE(1)	Hardware security for public key-based authentication	Not in scope	N/A
CR 1.10	Authenticator feedback		Pass
CR 1.11	Unsuccessful login attempts		Pass
CR 1.12	System use notification		Pass
CR 1.13	Access via untrusted networks	Not in scope	N/A
NDR 1.13	Access via untrusted networks		Pass
NDR 1.13 RE(1)	Explicit access request approval		0
CR 1.14	Strength of symmetric key-based authentication		Pass
CR 1.14 RE(1)	Hardware security for symmetric key-based authentication	Not in scope	N/A
CR 2.01	Authorization enforcement		Pass
CR 2.01 RE(1)	Authorization enforcement for all users (humans, software processes and devices)		Pass
CR 2.01 RE(2)	Permission mapping to roles		Pass
CR 2.01 RE(3)	Supervisor override	Not in scope	N/A
CR 2.01 RE(4)	Dual approval	Not in scope	N/A

LABORATOIRE CENTRAL DES INDUSTRIES ELECTRIQUES - LCIE
33 avenue du Général Leclerc
92260 Fontenay-aux-Roses, FRANCE
www.lcie.fr

Date: 22/12/2025

Signature: Julien GAUTHIER
Certification Officer

CR 2.02	Wireless use control	Not in scope	N/A
CR 2.03	Use control for portable and mobile devices	Not in scope	N/A
CR 2.04	Mobile code	Not in scope	N/A
EDR 2.04	Mobile code	Not in scope	N/A
HDR 2.04	Mobile code	Not in scope	N/A
NDR 2.04	Mobile code		Pass
SAR 2.04	Mobile code	Not in scope	N/A
EDR 2.04 RE(1)	Mobile code authenticity check	Not in scope	N/A
HDR 2.04 RE(1)	Mobile code authenticity check	Not in scope	N/A
NDR 2.04 RE(1)	Mobile code authenticity check		Pass
SAR 2.04 RE(1)	Mobile code authenticity check	Not in scope	N/A
CR 2.05	Session lock		Pass
CR 2.06	Remote session termination		Pass
CR 2.07	Concurrent session control	Not in scope	N/A
CR 2.08	Auditable events		Pass
CR 2.09	Audit storage capacity		Pass
CR 2.09 RE(1)	Warn when audit record storage capacity threshold reached	Not in scope	N/A
CR 2.10	Response to audit processing failures		Pass
CR 2.11	Timestamps		Pass
CR 2.11 RE(1)	Time synchronization		Pass
CR 2.11 RE(2)	Protection of time source integrity	Not in scope	N/A
CR 2.12	Non-repudiation		Pass
CR 2.12 RE(1)	Non-repudiation for all users	Not in scope	N/A
CR 2.13	Use of physical diagnostic and test interfaces	Not in scope	N/A
EDR 2.13	Use of physical diagnostic and test interfaces	Not in scope	N/A
HDR 2.13	Use of physical diagnostic and test interfaces	Not in scope	N/A
NDR 2.13	Use of physical diagnostic and test interfaces		Pass
EDR 2.13 RE(1)	Active monitoring	Not in scope	N/A
HDR 2.13 RE(1)	Active monitoring	Not in scope	N/A
NDR 2.13 RE(1)	Active monitoring		0
CR 3.01	Communication integrity		Pass
CR 3.01 RE(1)	Communication authentication		Pass
CR 3.02	Protection from malicious code	Not in scope	N/A
EDR 3.02	Protection from malicious code	Not in scope	N/A
HDR 3.02	Protection from malicious code	Not in scope	N/A
NDR 3.02	Protection from malicious code		Pass
SAR 3.02	Protection from malicious code	Not in scope	N/A
HDR 3.02 RE(1)	Report version of code protection	Not in scope	N/A

LABORATOIRE CENTRAL DES INDUSTRIES ELECTRIQUES - LCIE
33 avenue du Général Leclerc
92260 Fontenay-aux-Roses, FRANCE
www.lcie.fr

Date: 22/12/2025   Signature: Julien GAUTHIER
Certification Officer

CR 3.03	Security functionality verification		Pass
CR 3.03 RE(1)	Security functionality verification during normal operation	Not in scope	N/A
CR 3.04	Software and information integrity		Pass
CR 3.04 RE(1)	Authenticity of software and information		Pass
CR 3.04 RE(2)	Automated notification of integrity violations	Not in scope	N/A
CR 3.05	Input validation		Pass
CR 3.06	Deterministic output	Not in scope	N/A
CR 3.07	Error handling		Pass
CR 3.08	Session integrity		Pass
CR 3.09	Protection of audit information		Pass
CR 3.09 RE(1)	Audit records on write-once media	Not in scope	N/A
CR 3.10	Support for updates	Not in scope	N/A
EDR 3.10	Support for updates	Not in scope	N/A
HDR 3.10	Support for updates	Not in scope	N/A
NDR 3.10	Support for updates		Pass
EDR 3.10 RE(1)	Update authenticity and integrity	Not in scope	N/A
HDR 3.10 RE(1)	Update authenticity and integrity	Not in scope	N/A
NDR 3.10 RE(1)	Update authenticity and integrity	Ensure that Application Form is for Viper-3500 series only	Pass
CR 3.11	Physical tamper resistance and detection	Not in scope	N/A
EDR 3.11	Physical tamper resistance and detection	Not in scope	N/A
HDR 3.11	Physical tamper resistance and detection	Not in scope	N/A
NDR 3.11	Physical tamper resistance and detection		Pass
EDR 3.11 RE(1)	Notification of a tampering attempt	Not in scope	N/A
HDR 3.11 RE(1)	Notification of a tampering attempt	Not in scope	N/A
NDR 3.11 RE(1)	Notification of a tampering attempt		0
CR 3.12	Provisioning product supplier roots of trust	Not in scope	N/A
EDR 3.12	Provisioning product supplier roots of trust	Not in scope	N/A
HDR 3.12	Provisioning product supplier roots of trust	Not in scope	N/A
NDR 3.12	Provisioning product supplier roots of trust		Pass
CR 3.13	Provisioning asset owner roots of trust	Not in scope	N/A
EDR 3.13	Provisioning asset owner roots of trust	Not in scope	N/A
HDR 3.13	Provisioning asset owner roots of trust	Not in scope	N/A
NDR 3.13	Provisioning asset owner roots of trust	Not in scope	N/A
CR 3.14	Integrity of the boot process	Not in scope	N/A
EDR 3.14	Integrity of the boot process	Not in scope	N/A
HDR 3.14	Integrity of the boot process	Not in scope	N/A
NDR 3.14	Integrity of the boot process		Pass
EDR 3.14 RE(1)	Authenticity of the boot process	Not in scope	N/A

LABORATOIRE CENTRAL DES INDUSTRIES ELECTRIQUES - LCIE
33 avenue du Général Leclerc
92260 Fontenay-aux-Roses, FRANCE
www.lcie.fr

Date: 22/12/2025   Signature: Julien GAUTHIER
Certification Officer

HDR 3.14 RE(1)	Authenticity of the boot process	Not in scope	N/A
NDR 3.14 RE(1)	Authenticity of the boot process		Pass
CR 4.01	Information confidentiality		Pass
CR 4.02	Information persistence		Pass
CR 4.02 RE(1)	Erase of shared memory resources	Not in scope	N/A
CR 4.02 RE(2)	Erase verification	Not in scope	N/A
CR 4.03	Use of cryptography		Pass
CR 5.01	Network segmentation		Pass
CR 5.02	Zone boundary protection	Not in scope	N/A
NDR 5.02	Zone boundary protection		Pass
NDR 5.02 RE(1)	Deny all, permit by exception		Pass
NDR 5.02 RE(2)	Island mode		0
NDR 5.02 RE(3)	Fail close		0
CR 5.03	General-purpose person-to-person communication restrictions	Not in scope	N/A
NDR 5.03	General purpose, person-to-person communication restrictions		Pass
CR 5.04	Application partitioning	Not in scope	N/A
CR 6.01	Audit log accessibility		Pass
CR 6.01 RE(1)	Programmatic access to audit logs	Not in scope	N/A
CR 6.02	Continuous monitoring		Pass
CR 7.01	Denial of service protection		Pass
CR 7.01 RE(1)	Manage communication load from component		Pass
CR 7.02	Resource Management		Pass
CR 7.03	Control System backup		Pass
CR 7.03 RE(1)	Backup integrity verification		Pass
CR 7.04	Control system recovery and reconstitution		Pass
CR 7.05	Emergency Power	Not in scope	N/A
CR 7.06	Network and security configuration settings		Pass
CR 7.06 RE(1)	Machine-readable reporting of current security settings	Not in scope	N/A
CR 7.07	Least functionality		Pass
CR 7.08	Control system component inventory		Pass