Certificate number: 83805/A0 BV
File number: TCF12_351
Product code: 4600H

This certificate is not valid when presented without the full attached schedule composed of 7 sections. Full certificate is to be requested to the manufacturer

www.veristar.com

TYPE APPROVAL CERTIFICATE

This certificate is issued to

IXON B.V.

Beugen - NETHERLANDS

for the type of product

NETWORK CYBERSECURITY GATEWAY

SecureEdge (IX5000, IX5005, IX5010, IX5015) & SecureEdge Pro (IX6000, IX6005, IX6010, IX6015)

Requirements:
NR659 Bureau Veritas Rules on cyber security for the classification of marine units.
IACS UR E27 Rev.1 Sep 2023 Cyber resilience of on-board systems and Equipment.

This certificate is issued to attest that Bureau Veritas Marine & Offshore did undertake the relevant approval procedures for the product identified above which was found to comply with the relevant requirements mentioned above.

This certificate will expire on: 07 Sep 2031

For Bureau Veritas Marine & Offshore,
At BV ROTTERDAM, on 07 Sep 2026,
Jan LEIJTEN

This certificate was created electronically and is valid without signature

THE SCHEDULE OF APPROVAL

1. PRODUCT DESCRIPTION :

1.1 - SecureEdge (IX5000, IX5005, IX5010, IX5015) & SecureEdge Pro (IX6000, IX6005, IX6010, IX6015) are industrial edge gateway combining secure remote access (VPN), an integrated firewall and data logging in a single DIN-rail mounted device, connecting industrial machines and systems to the IXON Cloud platform. Built on a security-by-design hardware platform with a security-focused operating system, Secure Boot and a TPM for cryptographic key storage. The SecureEdge Pro additionally provides extended processing power, expandable storage, Docker-based edge computing and a dedicated OT port for network segregation.

2. DOCUMENTS AND DRAWINGS :

Filename	Reference
SecureEdge Pro Gateway Data Sheet Brochure EN	Dated 27/01/2026
Secure Baseline Guide	Version 1.0
Advanced Hardening Guide	Version 1.0
IXON IEC 62443-4-1 Certificate	Ref. Certif. No. FR_Cyber10211
IXON IEC 62443-4-2 Certificate	Ref. Certif. No. FR_Cyber10270
IXON IEC 62443-4-2 Certificate	Ref. Certif. No. FR_Cyber10287

No departure from the above documents shall be made without the prior consent of the Society. The manufacturer must inform the Society of any modification or changes to these documents and drawings.

3. TEST REPORTS :

3.1 - Test report '17930783/CN818640' dated 22/01/2026 was reviewed and approved for this attestation.

The following subjects were investigated:
1. Protect against casual or coincidental access by unauthenticated entities
   - IEC 62443-3-3/SR 1.1 : Human user identification and authentication
   - IEC 62443-3-3/SR 1.2 : Software process and device identification and authentication
   - IEC 62443-3-3/SR 1.3 : Account management
   - IEC 62443-3-3/SR 1.4 : Identifier management
   - IEC 62443-3-3/SR 1.5 : Authenticator management
   - IEC 62443-3-3/SR 1.7 : Strength of password-based authentication
   - IEC 62443-3-3/SR 1.10 : Authenticator feedback
   - IEC 62443-3-3/SR 1.11 : Unsuccessful login attempts
   - IEC 62443-3-3/SR 1.12 : System use notification
2. Protect against casual or coincidental misuse
   - IEC 62443-3-3/SR 2.1 : Authorization enforcement
   - IEC 62443-3-3/SR 2.5 : Session lock
   - IEC 62443-3-3/SR 2.6 : Remote session termination
   - IEC 62443-3-3/SR 2.8 : Auditable events
   - IEC 62443-3-3/SR 2.9 : Audit storage capacity
   - IEC 62443-3-3/SR 2.10 : Response to audit processing failures
   - IEC 62443-3-3/SR 2.11 : Timestamps
3. Protect the integrity of the CBS against casual or coincidental manipulation
   - IEC 62443-3-3/SR 3.1 : Communication integrity
   - IEC 62443-3-3/SR 3.3 : Security functionality verification
   - IEC 62443-3-3/SR 3.5 : Input validation
   - IEC 62443-3-3/SR 3.8 : Session integrity
4. Prevent the unauthorized disclosure of information via eavesdropping or casual exposure

IEC 62443-3-3/SR 4.1 : Information confidentiality
IEC 62443-3-3/SR 4.3 : Use of cryptography
5. Monitor the operation of the CBS and respond to incidents
IEC 62443-3-3/SR 6.1 : Audit log accessibility
6. Ensure that the control system operates reliably under normal production conditions
IEC 62443-3-3/SR 7.1 : Denial of service protection
IEC 62443-3-3/SR 7.2 : Resource management
IEC 62443-3-3/SR 7.3 : System backup
IEC 62443-3-3/SR 7.4 : System recovery and reconstitution
IEC 62443-3-3/SR 7.6 : Network and security configuration settings
IEC 62443-3-3/SR 7.7 : Least Functionality

3.2 - Test report '17930783/CN822168' dated 01/04/2026 was reviewed and approved for this attestation.

The following subjects were investigated:
1. Protect against casual or coincidental access by unauthenticated entities
IEC 62443-3-3/SR 1.1 : Human user identification and authentication
IEC 62443-3-3/SR 1.2 : Software process and device identification and authentication
IEC 62443-3-3/SR 1.3 : Account management
IEC 62443-3-3/SR 1.4 : Identifier management
IEC 62443-3-3/SR 1.5 : Authenticator management
IEC 62443-3-3/SR 1.7 : Strength of password-based authentication
IEC 62443-3-3/SR 1.10 : Authenticator feedback
IEC 62443-3-3/SR 1.11 : Unsuccessful login attempts
IEC 62443-3-3/SR 1.12 : System use notification
2. Protect against casual or coincidental misuse
IEC 62443-3-3/SR 2.1 : Authorization enforcement
IEC 62443-3-3/SR 2.5 : Session lock
IEC 62443-3-3/SR 2.6 : Remote session termination
IEC 62443-3-3/SR 2.8 : Auditable events
IEC 62443-3-3/SR 2.9 : Audit storage capacity
IEC 62443-3-3/SR 2.10 : Response to audit processing failures
IEC 62443-3-3/SR 2.11 : Timestamps
3. Protect the integrity of the CBS against casual or coincidental manipulation
IEC 62443-3-3/SR 3.1 : Communication integrity
IEC 62443-3-3/SR 3.3 : Security functionality verification
IEC 62443-3-3/SR 3.5 : Input validation
IEC 62443-3-3/SR 3.8 : Session integrity
4. Prevent the unauthorized disclosure of information via eavesdropping or casual exposure
IEC 62443-3-3/SR 4.1 : Information confidentiality
IEC 62443-3-3/SR 4.3 : Use of cryptography
5. Monitor the operation of the CBS and respond to incidents
IEC 62443-3-3/SR 6.1 : Audit log accessibility
6. Ensure that the control system operates reliably under normal production conditions
IEC 62443-3-3/SR 7.1 : Denial of service protection
IEC 62443-3-3/SR 7.2 : Resource management
IEC 62443-3-3/SR 7.3 : System backup
IEC 62443-3-3/SR 7.4 : System recovery and reconstitution
IEC 62443-3-3/SR 7.6 : Network and security configuration settings
IEC 62443-3-3/SR 7.7 : Least Functionality

All tests were successful and elements demonstrating compliance are provided in the appendix of each reports

4. APPLICATION / LIMITATION :

4.1 - IACS UR E27 Rev.1 Sep 2023 Cyber resilience of on-board systems and equipment.
NR659 Bureau Veritas Rules on cyber security for the classification of marine units.
4.2 - This certificate does not include the components. If required by Bureau Veritas Rules, the components are to be type approved or design appraised.
4.3 - Only Hardware and Firmware / Software successfully tested together in compliance with the rules as referred to in page one, according to the declaration of the manufacturer are covered by this certificate.
4.4 - The installation shall comply with the Manufacturer's recommendation described in the above-referenced documentation.
4.5 - It is manufacturer’s responsibility to inform the Society of any modification or changes which could impact the validity of

this attestation.

5. PRODUCTION SURVEY REQUIREMENTS :

5.1 - This product is to be supplied by **IXON B.V.** in compliance with the type described in this attestation.
5.2 - This product is within the category HBV of Bureau Veritas Rule Note NR320 and as such does not require a BV product certificate.
5.3 - **IXON B.V.** has to make the necessary arrangements to have its works recognised by Bureau Veritas in compliance with the requirements of NR320 for HBV products.
5.4 - For information **IXON B.V.** has declared to Bureau Veritas the following production site:

IXON B.V.
Zuster Bloemstraat 20
5835DW Beugen
NETHERLANDS

6. MARKING OF PRODUCT :

N/A.

7. OTHERS :

7.1 - It is **IXON B.V.** responsibility to inform shipbuilders or their sub-contractors of the proper methods of fitting, use and general maintenance of the approved equipment and the conditions of this approval.

***** END OF CERTIFICATE *****