Certificate number: 82485/A0 BV
File number: TCF09_249
Product code: 4603H

This certificate is not valid when presented without the full attached schedule composed of 7 sections

www.veristar.com

TYPE APPROVAL CERTIFICATE

This certificate is issued to
Danelec
Farum - DENMARK

for the type of product
CYBER MONITORING SYSTEM
Danelec Onboard Insights

Requirements:
NR659 Bureau Veritas Rules on Cyber Security or 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: 25 Feb 2031

For Bureau Veritas Marine & Offshore,
At BV FREDERICIA, on 25 Feb 2026,
Jesper JENSEN

This certificate was created electronically and is valid without signature

THE SCHEDULE OF APPROVAL

1. PRODUCT DESCRIPTION :

Danelec Onboard Insights is a ship performance monitoring system allowing to collect, process and visualize data from engine, hull and propeller sensors.

2. DOCUMENTS AND DRAWINGS :

Name	Revision Number / Date
F030 - System topology	V 1.3
F141 - Guidelines for hardening and configuration of security capabilities	V 1.1
F021 - Description of security capabilities	V 1.1
Secure development lifecycle, modification strategy and change management	V 1.2
F071 - Asset Inventory	V 1.1
F252 - Procedure for test of security capabilities	V 1.4

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 :

Test reports "Test report for Danelec Onboard Insights as IACS UR E27 equipment_signed" dated 16/10/2025 were reviewed and approved for this certificate.

The following items 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 1.3 : 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 1.6 : Wireless access management
      IEC 62443-3-3/SR 1.7 : Strength of password-based authentication
2. Protect against casual or coincidental misuse
      IEC 62443-3-3/SR 2.1 : Authorization enforcement
      IEC 62443-3-3/SR 2.2 : Wireless use control
      IEC 62443-3-3/SR 2.3 : Use control for portable and mobile devices
      IEC 62443-3-3/SR 2.4 : Mobile code
      IEC 62443-3-3/SR 2.5 : Session lock
      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 3.2 : Malicious code protection
      IEC 62443-3-3/SR 3.3 : Security functionality verification
      IEC 62443-3-3/SR 3.5 : Input validation
      IEC 62443-3-3/SR 3.6 : Deterministic output
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 7.5 : Alternative power source
>   IEC 62443-3-3/SR 7.6 : Network and security configuration settings
>   IEC 62443-3-3/SR 7.7 : Least Functionality

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. (e.g switches)
4.3 - Only Hardware and Firmware / Software version 2.XX since 2.25 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 certificate.

5. PRODUCTION SURVEY REQUIREMENTS :

5.1 - This system is to be supplied by **DANELEC** in compliance with the type described in this certificate.
5.2 - This system product is within the category HBV of Bureau Veritas Rule Note NR320 and as such does not require a BV product certificate.
5.3 - **DANELEC** 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 **DANELEC** has declared to Bureau Veritas the following production site(s):

GPV ASIA (THAILAND) Co. LTD.
834 MOON 4, BANGPOO INDUSTRIAL ESTATE SOI 11-12
SUKHIMVIT ROAD, PRAKSA
MUANG DISTRICT
10280 SAMUTPRAKARN
THAILAND

6. MARKING OF PRODUCT :

N/A

7. OTHERS :

7.1 - It is **DANELEC** 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 ***