Attestation number: 82350/A0 BV
File number: TCE09_166
Product code: RA-CYBER-MED

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

REVIEW ATTESTATION

This attestation is issued to

Danelec
Farum - DENMARK

for

CYBERSECURITY REVIEW (MED EQUIPMENT)

Voyage Data Recorder, Simplified Voyage Data Recorder

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 document is issued to attest that BUREAU VERITAS Marine & Offshore reviewed the technical documentation submitted for the equipment identified above. Details of this review are to be found in the "Schedule of Review" in the subsequent pages of this attestation.

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

This attestation was created electronically and is valid without signature

SCHEDULE OF REVIEW

1. PRODUCT DESCRIPTION :

1.1 - Voyage Data Recorde is described in the EC-Type-Examination Certificate MEDB00005J4, Simplifled Voyage Data Recorder is described in the EC-Type-Examination Certificate MEDB00009DU.

2. DOCUMENTS AND DRAWINGS :

Name	Revision Number / Date
RD15008-12 - Secure development lifecycle, modification strategy and change management	V 1.2
DBS14746-11- Type approval specification (IACS UR E27 / IEC 61162-460 ed. 3) for DM100	V 1.1
MAN14904 - Cybersecurity guidelines for DM100 installations	V 1.0
DBS14890-11 - Test Specification for DM100 VDR as IEC 61162-460 ed. 3 node / IACS UR E27 equipment	V 1.1

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 DM100 VDR / VRS as IACS UR E27 equipment " 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 - This attestation does not constitute by a BV Type Approval Certificate. This attestation is limited to cyber resilience of products described in 1. as per UR E27 Rev. 1 dated Sept.2023.

4.2 - This attestation has been issued solely based on the review of cyber documentation provided in §2 and §3 for the product covered by EC-Type-Examination Certificate MEDB00005J4 & MEDB00009DU for VDR and SVDR respectively. This attestation does not include the review of the product covered by the EC-Type-Examination Certificate MEDB00005J4 & MEDB00009DU for VDR and SVDR respectively, neither the integration of cyber modules to the equipment.

4.3 - This attestation is only valid when provided with MED (or UK) Modules B MEDB00005J4, revision X from revision 14, for Voyage Data Recorder (VDR) and MEDB00009DU, revision X from revision 1, for Simplified Voyage Data Recorder (SVDR).

4.4 - Only Hardware and Firmware / Software version 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.

4.5 - The installation shall comply with the Manufacturer's recommendation described in the above-referenced documentation.

4.6 - 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 :

N/A

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 ATTESTATION ***