



Marine & Offshore



Attestation number: 80121/A1 BV

File number: TCF02_67

Product code: RA-CYBER

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

REVIEW ATTESTATION

This attestation is issued to

DEIF A/S

Skive - DENMARK

for

CYBERSECURITY REVIEW

iE 250, iE 350 and iE 650

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 08 Jul 2025,

Jesper JENSEN

This attestation was created electronically and is valid without signature



This attestation will not be valid if the applicant makes any changes or modifications to the product which have not been notified to, and agreed in writing with Bureau Veritas Marine & Offshore. This attestation is issued within the scope of the General Conditions of BUREAU VERITAS Marine & Offshore Division available on the internet site www.veristar.com. Any Person not a party to the contract pursuant to which this document is delivered may not assert a claim against BUREAU VERITAS for any liability arising out of errors or omissions which may be contained in said document, or for errors of judgment, fault or negligence committed by personnel of the Society or of its Agents in establishment or issuance of this document, and in connection with any activities for which it may provide.

SCHEDULE OF REVIEW

1. PRODUCT DESCRIPTION :

iE 250, iE 350 and iE 650 are described in the certificate 80626/XX BV

2. DOCUMENTS AND DRAWINGS :

Filename	Reference
iE 350 E27 test specification	v. 1.0.0
iE 650 E27 test specification	v. 1.0.0
iE 250 E27 test specification	v. 1.1.0
CODESYS E27 test specification	v. 1.1.0
Handbook for Software development	v. 41.0.0
CODESYS Security Whitepaper	v. 9.0.0
Software life-cycle overview	v. 1.0.0
iEx50 Cyber Security E27 Recovery Plan	rev. A
iEx50 Cyber Security E27 Security Requirements	rev. B
iEx50 Security Capabilities	v. 1.0.0
iE x50 Asset Inventory	v. 1.2.0
PICUS PC Utility Software User's manual	v. 1.0.0
HW – Guide to construction changes	v. 1.0.0
Secure Development Lifecycle	v. 1.0.1
DEP SW Test Strategy	v. 1.0.0

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 “CODESYS E27 testplan signed”, “iE 350 E27 testplan signed”, “iE 250 E27 testplan signed”, and “iE 650 E27 testplan signed” dated 06/04/2024 were reviewed and approved for this attestation.

The following subjects were investigated:

- Identification & Authentication Control (FR 1):
 - 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 1.7: Strength of password-based authentication
 - IEC 62443-3-3/SR 1.10: Authenticator feedback
- Use Control (FR 2):
 - IEC 62443-3-3/SR 2.1: Authorization enforcement
 - 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

-System Integrity (FR 3):

- 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 3.6: Deterministic output

- Data Confidentiality (FR 4):

- IEC 62443-3-3/SR 4.1: Information confidentiality
- IEC 62443-3-3/SR 4.3: Use of cryptography

- Timely Response to Events (FR 6):

- IEC 62443-3-3/SR 6.1: Audit log accessibility

- Resource Availability (FR 7):

- 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 back-up
- IEC 62443-3-3/SR 7.4: System recovery and reconstitution
- IEC 62443-3-3/SR 7.6: Network and security configuration
- IEC 62443-3-3/SR 7.7: Least functionality

4. APPLICATION / LIMITATION :

4.1 - This attestation is an intermediate document and does not constitute by itself a BV Type Approval Certificate. This attestation is limited to cyber resilience of product described in 1. as per UR E27 Rev. 1 dated Sept.2023.

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

4.3 - This attestation is only valid when attached to the valid Type Approval Certificate 80626/XX BV.

4.4 - This attestation has been issued based on the review of documentation provided for the Type Approval Certificate 80626/A0 BV.

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 system product is to be supplied by **DEIF A/S** in compliance with the type described in this attestation.

5.2 - For information **DEIF A/S** has declared to Bureau Veritas the following production site:

**Frisenborgvej 33
DK-7800 Skive
DENMARK**

6. MARKING OF PRODUCT :

N/A

7. OTHERS :

7.1 - It is **DEIF A/S** 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 ***