Attestation number: 83676/A0 BV

File number: TCF11_304

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

Autronica Fire and Security AS

TRONDHEIM - NORWAY

for

CYBERSECURITY REVIEW

Fire Detection System

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 OSLO, on 30 Mar 2026,
Jonny Pettersson

This attestation was created electronically and is valid without signature

SCHEDULE OF REVIEW

1. PRODUCT DESCRIPTION :

AUTRONICA Fire Detection System is described in the certicate 23170/XX BV and 09859/XX BV.

2. DOCUMENTS AND DRAWINGS :

Filename	Reference
Product Cybersecurity Change Management Standard	Version 2.0
Product Cybersecurity Operational Incident Response, Backup & Recovery Guide	Version 1.0
Autronica Secure Development Lifecycle (SDL) Process	Version 2.0
Plans for Maintenance and Verification of the Computer Based Systems (CBS)	Dated 29/01/2026
System topology - BV E27 FIRE DETECTION SRtP SYSTEMS 4 - 6 MVZ, XX AUTROMASTER	Dated 08/12/2025
F071 - Inventory list	Dated 08/12/2025
Description of Security Capabilities	Version 2.2.0
Test Procedure for Security Capabilities	Version 2.1.0
Certificate of Conformity - Industrial Cyber Security Capability	Dated 10/11/2025
IEC 62443-4-2-compliant configuration of the FL SWITCH (TSN) 2000 product families User manual	Revision 01
IEC 62443-4-2-compliant configueation of the FL MGUARD product family User Manual	Revision 04

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 report 'TEST REPORT - E27 Type Approval' dated 19/03/2026 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 1.1 RE2 : Multifactor authentication for human users
   - 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
   - IEC 62443-3-3/SR 1.13 : Access via Untrusted Networks
   - IEC 62443-3-3/SR 1.13 RE1 : Explicit access request approval
2. Protect against casual or coincidental misuse
   - IEC 62443-3-3/SR 2.1 : Authorization enforcement
   - 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 2.6 : 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 2.11 : 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 3.1 RE1 : Cryptographic integrity protection
   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
   IEC 62443-3-3/SR 3.8 : Session integrity
   IEC 62443-3-3/SR 3.8 RE1 : Invalidation of session IDs after session termination
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 4.1 RE1 : Protection of confidentiality at rest or in transit via untrusted networks
   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 5.1 : Network segmentation
   IEC 62443-3-3/SR 5.1 RE1 : Physical network segmentation
   IEC 62443-3-3/SR 5.2 : Zone boundary protection
   IEC 62443-3-3/SR 5.2 RE1 : Deny by default, allow by exception
   IEC 62443-3-3/SR 5.2 RE2 : Island mode
   IEC 62443-3-3/SR 5.3 : General purpose person-to-person communication restrictions
   IEC 62443-3-3/SR 5.4 : Application partiioning
   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 : Emergency power
   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 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 - 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 attestation.
4.3 - The installation shall comply with the Manufacturer's recommendation described in the above-referenced documentation.
4.4 - It is manufacturer’s responsibility to inform the Society of any modification or changes which could impact the validity of this attestation.
4.5 - This attestation is only valid when attached to the valid Type Approval Certificate 23170/XX BV or 09859/XX BV.
4.6 - This attestation has been issued based on the review of documentation provided for the Type Approval Certificate 23170/D0 BV and 09859/F0 BV.

5. PRODUCTION SURVEY REQUIREMENTS :

5.1 - This product is to be supplied by **Autronica Fire and Security AS** in compliance with the type described in this attestation.
5.2 - For information, **Autronica Fire and Security AS** has declared to Bureau Veritas the following production site(s):

Autronica Fire and Security AS
Bromstadvegen 59
7047 TRONDHEIM
NORWAY

6. MARKING OF PRODUCT :

N/A

7. OTHERS :

7.1 - It is **Autronica Fire and Security AS** 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 *****