TYPE APPROVAL CERTIFICATE

This is to certify:

that the Voyage Data Recorder (VDR)

with type designation(s)
DM100 VDR (trade name Sperry Marine Voyage Master IV VDR),
DM100 VDR G2 (trade name Sperry Marine Voyage Master IV VDR G2, Wärtsilä VDR 4380),
DM100 S-VDR G2 (trade name Sperry Marine Voyage Master IV S-VDR G2, Wärtsilä S-VDR 4380),
DM100 L-VDR G2 (trade name Sperry Marine Voyage Master IV L-VDR G2)

issued to
Danelec Marine A/S
Farum, Hovedstaden, Denmark

is found to comply with
  DNV rules for classification – Ships Pt.6 Ch.5 Sec.21 Cyber security
  IEC 61162-460 Ed. 3.0 (2024-04) Maritime Navigation and radiocommunication equipment and systems –
  Digital interfaces – Part 460: Multiple talkers and multiple listeners – Ethernet interconnection – Safety and
  security

Application:
This type approval covers security capabilities for DNV security profiles SP0 and SP1 (edition July 2023), including IACS UR E27.
Product(s) approved by this certificate is/are accepted for installation on all vessels classed by DNV.

Issued at **Høvik** on **2024-05-29**

This Certificate is valid until **2026-05-28**.
DNV local unit: **Denmark CMC**

Approval Engineer: **Knut Omberg**

for **DNV**

Digitally signed by: Jarle Coll Blomhoff
Location: DNV Høvik, Norway

Product description

The Voyage Data Recorders serve as data collection devices and record data received from a number of interfaces (audio, serial, network), stores the data on various storage media which are part of the VDR system, and provides access to data as well as device configuration via a network interface.

This type approval covers cyber security capabilities in accordance with requirements of DNV class notation Cyber secure(Essential) of VDR/S-VDR/L-VDR firmware version 2.30, including peripherals connected to the VDR Device network (zone 0) as per Danelec installation manual MAN14904.

All product models listed on the front page of this certificate have the same firmware version and are covered by this type approval.

Application/Limitation

The VDR/S-VDR/L-VDR and its peripherals connected to the VDR Device network are considered a separate security zone and may interface other security zones as specified in Danelec installation manual MAN14904.

The IP video interface (IPVI) used with the VDR must be version 1.10 or higher.

Communication between the VDR/S-VDR/L-VDR and untrusted networks shall be implemented via a Gateway compliant with IEC 61162-460.

Approval conditions

For each delivery to DNV class notation Cyber secure or Cyber secure(Essential), the integrated bridge system to which the VDR/S-VDR/L-VDR is connected shall be certified in accordance with DNV rules Pt.6 Ch.5 Sec.21. The product certificate (PC) shall be issued based on approval of the following documentation submitted by the system integrator:

- System topology: Project-specific architecture diagram of the integrated bridge system demonstrating that the VDR/S-VDR/L-VDR is arranged in accordance with this type approval (Danelec installation manual MAN14904). Communication interfaces shall be illustrated in the topology (i.e., with other systems/devices in the same security zone, other security zones or in untrusted networks).

- Asset inventory: Project-specific asset inventory of the integrated bridge system, demonstrating that the VDR/S-VDR/L-VDR is covered by this type approval.

- Test report: Demonstrating that the VDR/S-VDR/L-VDR has been configured in accordance with DANELEC installation manual MAN14904.

After installed on board, all changes to the VDR/S-VDR/L-VDR are to be recorded. Documentation of major changes is to be forwarded to DNV for evaluation and approval before implemented on board.

Major design changes of the VDR/S-VDR/L-VDR shall be informed to DNV by updated product documentation, including records of the change management process in Danelec document RD15008. If the changes are judged to affect functionality for which rule requirements apply, a new functional type test may be required, and the certificate may have to be renewed to identify the new software version.

Type Approval documentation

DBS14746 Ver.1.1 (2024-05-21) Type approval specification (IACS UR E27 / IEC 61162-460 ed.3) for DM100
- F071 Asset inventory, chapter 2.3
- I030 System topology, chapter 2.2
- F021 Description of security capabilities, chapter 5

DBS14890 Ver.1.1 (2024-05-23) Test Specification for DM100 VDR as IEC 61162-460 ed. 3 node/ IACS UR E27 equipment
- Z252 Procedure for type testing

MAN14904 Ver.1.0 (2024-04-30) Installation Manual for DM100 VDR G2 and DM100 S-VDR G2
- F141 Guidelines for security configuration, chapter 6
- Z251 Procedure for security functionality verification, chapter 6

RD15008 Ver.1.0 (2024-05-24) Secure Development Lifecycle for embedded products

- Z250 Description of SDL processes
- Z100 Modification strategy
- I320 Change management procedure

Initial TA assessment report dated 2024-02-29

Tests carried out

Tested DM100 VDR with firmware version 2.26.33 on November 27th – 28th 2023 in accordance with:
- cyber security requirements for DNV class notation Cyber secure(Essential), security profile 1, and
- requirements for 460-node in IEC 61162-460 (Ed.3, 2024)

Marking of product

The products to be marked with:
- manufacturer name
- model name
- serial number
- power supply ratings

Software version is displayed on the Bridge control panel HMI.

Periodical assessment

The scope of the periodical assessment is to verify that the conditions stipulated for the type are complied with, and that no alterations are made to the product design or choice of systems, software versions, components and/or materials. The main elements of the assessment are:
- Ensure that type approved documentation is available
- Inspection of factory samples, selected at random from the production line (where practicable)
- Review of production and inspection routines, including test records from product sample tests and control routines
- Ensuring that systems, software versions, components and/or materials used comply with type approved documents and/or referenced system, software, component and material specifications
- Review of possible changes in design of systems, software versions, components, materials and/or performance, and make sure that such changes do not affect the type approval given
- Ensuring traceability between manufacturer's product type marking and the type approval certificate

A renewal assessment will be performed at renewal of the certificate.

END OF CERTIFICATE