Certificate no.:
TAA00003ZK

TYPE APPROVAL CERTIFICATE

This is to certify:

that the Data Collection Infrastructure

with type designation(s)
Vessel Insight

issued to
Kongsberg Maritime AS
Kongsberg, Norway

is found to comply with
DNV rules for classification – Ships and offshore units
DNV rules for classification – Ships Pt.6 Ch.5 Sec.21 Cyber security
DNV rules for classification – Ships Pt.6 Ch.11 Sec.1 Data collection infrastructure (D-INF)

Application:

Product(s) approved by this certificate is/are accepted for installation on all main class and D-INF(G) vessels classed by DNV.

This type approval covers security capabilities for DNV Cyber security profile level 1 (SP1) and IACS UR E27, subject to conditions stated in this certificate.

Scope	**D-INF(G) End-to-end solution, Cyber Security (SP1) see Product description**
Temperature	**D**
Humidity	**B 2)**
Vibration	**A**
EMC	**B 1)**
Enclosure	**Required protection according to the Rules to be provided upon installation onboard**

Issued at **Høvik** on **2026-11-03**

This Certificate is valid until **2028-03-20**.
DNV local unit: **East & South Norway CMC**

Approval Engineer: **Mai H. Tran**

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

This Certificate is subject to terms and conditions overleaf. Any significant change in design or construction may render this Certificate invalid.
The validity date relates to the Type Approval Certificate and not to the approval of equipment/systems installed.

LEGAL DISCLAIMER: Unless otherwise stated in the applicable contract with the holder of this document, or following from mandatory law, the liability of DNV AS, its parent companies and their subsidiaries as well as their officers, directors and employees ("DNV") arising from or in connection with the services rendered for the purpose of the issuance of this document or reliance thereon, whether in contract or in tort (including negligence), shall be limited to direct losses and under any circumstance be limited to USD 300 000.

Product description

The main purpose of KONGSBERG Vessel Insight (VI) is to capture data onboard a vessel, transfer this data securely to the cloud, and provide operational insights to the onshore fleet operations crew based on this data.

Changes to the type approved system shall be managed in accordance with document KM-PROC-0080. Major changes shall be documented and submitted to DNV for verification of compliance with applicable requirements, witness new type test and revise this TA certificate. Minor changes are covered by this type approval.
A log of all change reports shall be submitted upon renewal of this TA certificate.

The following components of the Vessel Insight are covered:

Onboard components:

Component description	Type designation	OS SW version	Application SW version
Router/Switch/Firewall (SP1)	Cisco 892FSP-8 Cisco C891-24 Cisco C1121x-8P Cisco C1000-24P FortiGate HN FS-124F	IOS 15.y.z (15.7.3.M9 or newer) IOS XE 17.x.y (17.03.05.spa or newer) IOS 15.y.z (15.2.7.E6 or newer)	GSN 2.2.z.p revisions (2.2.1.0 or newer)
Edge device (SP1)	Lenovo P330 (MC330) Lenovo P340 (MC340) Lenovo P360 (MC360) Lenovo P380 (MC380)	Ubuntu LTS (18.04, 20.04, 22.04 or newer with SP y.z)	Edge base 2.y.z revisions (2.3.0 or newer)
Serial to ethernet device *	Moxa Nport 5232(I-T) Moxa Nport 5230I Moxa Nport 5240I	Firmware v2.12 or newer	GSN 2.2.z.p revision (2.2.1.0 or newer)
Serial splitter *	Øverland UPC-3002 1) 2) Øverland UPC-3005 1) 2)	N/A	GSN 2.2.z.p revision (2.2.1.0 or newer)
Application firewall *	Moxa EDR-810 Moxa EDR-G-902 Moxa EDR-8010 series	Firmware v5.10.2 or newer Firmware v5.6 or newer Firmware v3.1 or newer	Moxa cfg v1.y.z (v1.y.z or newer)
VI Edge Workload application	IOT application	Ubuntu LTS (18.04, 20.04, 22.04 or newer with SP y.z)	VI Edge 3.y.z revisions

Optional components are denoted with an asterisk (*).

Onshore components:

Component description	Type designation	OS SW version	Application SW version
Border gateway - GSN Backend HUB (SP1) 3)	Cisco ISR4331/K9 Cisco ISR4451/K9 Cisco Catalyst C8300/K9/HSEC C8500/K9/HSEC	16.y.z (16.12.1a or newer) 17.y.x (17.06.3a or newer)	GSN 2.2.z.p revision (2.2.1.0 or newer) (SP1)
Border gateway – virtual servers	GSN backend services: - PKI - GeoDNS - NTP Sync	Azure VM over Windows Server 2019 (SP y.z)	GSN 2.2.z.p revision (2.2.1.0 or newer) (SP1)
Border gateway – virtual servers	GSN monitoring and M-Sport tools (admin, jump host & repository serve)	Azure VM over Ubuntu LTS	GSN 2.2.z.p revisions (2.2.1.0 or newer) (SP1)

		(18.04, 20.04, 22.04 or newer with SP y.z)	

See the approved document 110-0015201, Vessel Insight Approved components, Rev. C for the full details of onboard and onshore inventory, including hardware, software and virtual components.

See document 110-0000733, Vessel Insight Approved Interfaces, Rev. F for full details of approved interfaces to Vessel Insight.

See Application/Limitation for notes related to superscripts used in the tables above.

Approval conditions

- If the type approved product is used in applications subject to D-INF or Cyber Secure notations by DNV rules for classification, correct configuration shall be verified by DNV.

Cyber Secure(Essential, +):
If the type approved system is part of scope (SuC) for class notation Cyber Secure(Essential, +) it shall be delivered with a vessel-specific Product Certificate (PC). The product certificate shall be issued based on the following verification as per DNV-RU-SHIP Part 6 Chapter 5 Section 21:

1) It shall be demonstrated the architecture of each delivery is documented in a project-specific system topology (F030) and consistent with the type approved document.
2) It shall be demonstrated each delivery is correctly represented by a vessel-specific system topology (F030) and this inventory is consistent with type approved document.
3) It shall be demonstrated by a test report (Z262) that each delivery has been configured and hardened.

- Changes to onboard components listed in product description that affect their capabilities, shall be informed to DNV. Such modifications may require additional type test witnessing and revision of this type approved certificate.
- Changes to onboard components listed in product description that affect their cyber security capabilities or functional requirements related to D-INF notation shall be informed to DNV. Such modifications may require additional type test witnessing and revision of this type approved certificate.
- Version and revision of application software is reflected on format x.y.z.(p) which denotes changes in category “major.minor.update.(patch)”. Any relevant changes in operating system or application software resulting in modification in the fixed digit of version shall be informed to DNV by forwarding a description of the modification(s) including the corresponding new version/revision identifier.

D-INF(G):
If the type approved system is part of scope for class notation D-INF(G) it shall be delivered with a vessel-specific Product Certificate (PC). The product certificate shall be issued based on the following verification as per DNV-RU-SHIP Part 6 Chapter 11 Section 1:

1) It shall be demonstrate the architecture of each delivery is documented in a project-specific system topology (F030) and consistent with the type approved document.
2) It shall be demonstrated each delivery is correctly represented by a vessel-specific system topology (F030) and this inventory is consistent with type approved document.
3) It shall be demonstrate by a test report (Z262) that each delivery has been configured and hardened.

Application/Limitation

Thys type approval covers an end-to-end data collection infrastructure according to D-INF(G) with following applications and limitations:

Installation:

- The onboard type approved product shall be installed according to manufacturer’s approved installation manual.
- For components marked with [1)] in product description, EMC in the range 2 GHz to 6 GHz according to DNV-CG-0339 August 2021, has not been documented. EMC up to 6 GHz must additionally be documented for installation on ships contracted for construction on or after 2022-01-01.
- Components marked with [2)] in product description must be placed in a location where special precautions are taken to avoid condensation.
- For approved source system connections see Design Verification Report 262.1-036801-J-3 (110-0001254A).
- For other source system connections through router/firewall to Vessel Insight see document 110-0000733, Vessel Insight Approved Interfaces, Rev. F.

Cyber security:

- Components and applications marked with (SP1) in the product description have been assessed towards DNV-RU-SHIP Pt.6 Ch.5 Sec.21, security profile 1 (SP1). Interface between onboard and onshore components (GSN) have been assessed in accordance with SP1. Source systems shall be interfaced via secure communication or located in trusted network zones.
- Kongsberg components shall share common firewall, and all Kongsberg components shall be installed in trusted network. See document 110-0001414, Router configuration Connection Drawing, Rev. E.

- The design of GSN (Global Secure Network) backbone network solution (ref. above Table for Onshore components in product description) has been assessed towards DNV-RU-SHIP Pt.6 Ch.5 Sec.21 with security profile 1 (SP1) and partially security profile (SP3) indicated with (3).
- The international ISO 23807 for ship-to-shore data transmission include the cyber security requirements for integrity, authenticity, confidentiality and non-repudiation. Some ships may require Cyber Secure(Advanced) notation, i.e. SP3, and therefore the ship-to-shore communication or component may require a type approval certificate for SP3. For those use cases, selected SP3 requirements are covered in this design assessment of GSN, including the following 3):
    - SR 1.1, 1.2, 1.5: Multi-factor authentication (MFA), Device and software process authentication, Authenticator management.
    - SR 2.8, 2.11: Auditor log, Time Synchronisation
    - SR 2.12: Non-repudiation
    - SR 3.3, 3.4: Security function verification, Software and information integrity check
    - SR 4.3: Use of cryptography
    - SR 5.1, 5.2: Network segmentation, Zone boundary protection
    - SR 6.2, 7.4: Continuous monitoring, Auto recovery
    - SR 7.1, 7.3, 7.6, 7.8: DoS protection, Automatic backup, Auto configuration & reporting

Type Approval documentation

Doc. Ref.	Description	Rev.
110-0015201	Vessel Insight Approved components (including hardware, software and virtual for both onboard and onshore)	C
110-0000733	Vessel Insight Approved Interfaces	F
404330	Certificate: DNV, TAA0000019 Rev 1, UPC-series Serial Line Splitters UPC-3002 UPC-3005 UPC-5000P UPC-6000 Miscellaneous	A
355997	Certificate: DNV, TAA000006K Rev 4, EtherDevice Switches Network and Communication Components	G
415730	Certificate: DNV, TAA000006T Rev 4 Serial to Ethernet Device Server Series NPort IA NPort 5200 NPort 5400 and MGate MB Peripheral Equipment	D
389139	Certificate: DNV, TAA00001H4 Rev 1, K-Malware Panel Computer Maritime Computer	D
110_0016787	Certificate: DNV, TAA00002CU Rev 1, Phoenix Contact Firewall FL MGUARD Series	A
463149	Certificate: DNV, TAA00002MD Rev 2, P330_Tiny_DNV_20200506~20250203 Personal Computer	A
463340	Certificate: DNV, TAA00002ME, C891-24x Network and Communication Components	A
405223	Certificate: DNV, TAA00002R1, C892FSP Network and Communication Component	B
483082	Certificate: DNV, TAA00002ZN, P340 Tiny DNV 20210517 20260516	A
489199	Certificate: DNV, TAA000035N, Cisco SwitchRouter C1000 and C1121X and Fiberworks SFP Modules	B
110-0041399	Certificate: DNV, TAA000038U, P360 Tiny Marine Computer	
110-0137372	Certificate: DNV, TAA00003SE, ThinkStation P3 Tiny Gen 2 (30K4) and ThinkStation P3 Ultra SFF G2 (30J4) – “MC380”	
459139	Certificate: DNV, TAA00003VA, Fortigate Fortinet switch HN FS-124F	
442484	Doc: Router configuration Connection Drawing	H
487318	Doc: Vessel Insight Edge System Design Description	B
487319	Doc: Vessel Insight Functional Design Document-KFDD Kognifai Vessel Insight	G
490264	Doc: Vessel Insight Modbus Internal Connector Design Description	C
490430	Doc: Vessel Insight NEA Internal Connector Design Description	C
435723	Manual: Application Framework Portal OPM_rev.P-1	Y

458029	Manual: Global Secure Network (Release 2.5.0.3) Self Service Portal User Manual	E
460818	Manual: Kognifai Edge - Device Provisioning Manual	B
460821	Manual: Kognifai Edge - Sensor Replication Configuration Manual	C
460816	Manual: Kognifai Edge Assembly and Installation Manual	C
460823	Manual: Kognifai Linux Edge Onboard Installation Manual	D
403847	Manual: Kongsberg Remote Services OPM	A
487315	Manual: Vessel Insight Connector Security Configuration Manual	B
490192	Manual: Vessel Insight Edge Health Instruction Manual	A
487313	Manual: Vessel Insight Interface Manual-Vessel Insight User Guide	D
488192	Manual: Vessel Insight IoT Management portal Instruction manual	A
110-0001254A	Report: DVR-262.1-036801-J-3, Vessel Insight external connectors design verification report (a.k.a. “Approved connectors”)	
416665	Report: KM, Moxa NPort 5232-T IEC61162-1 Test report	A
TL21143	Report: MS Testing, Type Approval Testing Cisco 890 Series Network Switch	
487317	Report: Vessel Insight Certification Test program	C
489224	Report: Vessel Insight Edge Test Report	A
489222	Report: Vessel Insight End-to-end Test Report for Class Approval checklist	B

Tests carried out

Tested in accordance with requirements for

- DNV rules for ships Pt.6 Ch.11 Sec.1 for D-INF(G)
- Pt.6 Ch. 5 Sec 21 for Cyber Secure (Essential), i.e. DNV Cyber security profile level 1 (SP1)
- IACS UR E27, Sec.5 on Secure Development Lifecycle (SDLC) Requirements

Marking of product

The type designation and name and contact address of the manufacturer shall be affixed visibly, legibly and indelibly to the onboard product. In addition, the onboard product shall be marked with serial number, safe distance to magnetic compass, power consumption and/or supply voltage.

Place of manufacture

- Kongsberg Maritime AS, Kongsberg Norway.
- Kongsberg Maritime AS, Horten, Norway

Renewal assessment

A renewal assessment will be performed at renewal of the certificate. The scope of the renewal 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 version, components and/or materials. The main elements of the assessment are:

- Ensuring that type approved documentation is available
- Inspecting factory samples, selected at random from the production line (where practicable)
- Reviewing 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.
- Reviewing of possible changes in design of systems, software version, 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 type approval certificate
- Reviewing documented evidence of adherence to secure development lifecycle processes

END OF CERTIFICATE