Data-Centric Engineering (2025), 6: e14
doi:10.1017/dce.2024.59

CAMBRIDGE UNIVERSITY PRESS

TRANSLATIONAL ARTICLE

Development, verification, and certification of a digital twin for a voyage data recorder

Nikolaos Stavrou[1], Joseph Morelos[2], Domenic Di Francesco[3], Apostolos Meliones[4], Pavlos Progias[1] and Duffy Duncan[5]

[1]Research & Development Department, Furuno Hellas, Glyfada, Greece
[2]Lloyd's Register Marine and Offshore, Lloyd's Register Global Technology Centre, Southampton, UK
[3]Partner Institution University of Cambridge, The Alan Turing Institute, London, UK
[4]Department of Digital Systems, University of Piraeus, Piraeus, Greece
[5]Technology and Technical Governance, Lloyd's Register EMEA, London, UK
Corresponding author: Domenic Di Francesco; Email: ddifrancesco@turing.ac.uk

Received: 31 March 2023; **Revised:** 29 April 2024; **Accepted:** 1 July 2024

Keywords: digital twin; maritime safety; separated by semicolons; verification

Abstract

This paper documents the details of the design, verification, and certification of a novel technology: a remote monitoring system (digital twin) for a voyage data recorder, referred to as the HermAce Gateway. The electronic components, data transfer, and storage principle explain how the HermAce Gateway communicates and records safety-critical messages. Various prospective benefits to the industry are provided, primarily regarding the opportunities for remote support and testing that the digital twin facilitates. The HermAce Gateway was independently verified through a combination of semi-automated software in the loop and selected complimentary hardware in the loop tests. Different types of communication were simulated in multiple ways, including approximating real-world scenarios. Alarms contained in correctly formed messages were found to be detected and recorded by the HermAce Gateway, and a discussion of how this evidence can be quantified in the context of reducing uncertainty in the reliability of a digital twin. Certification of a digital system is a new concept in the maritime industry. The identification of functional requirements, which informed the verification testing, and the development of an AI register for what is expected to be an increasing number of such systems are also documented.

Impact Statement

Information collected by a voyage data recorder is important in understanding the features of marine incidents, leading to improvements in safety. Installation, calibration, and testing of these devices typically require personnel to be on board the ship. The development of a remote monitoring system (digital twin) allows for many of these tasks or be performed, or assisted remotely, as required. Such systems, following verification and certification, as have been completed for this technology (HermAce) have the potential to create safer and more economical risk management of ships.

1. Introduction

A key challenge in the era of data-centric engineering is the design and verification of digital twins. These systems are required to collect, communicate, and analyze data (often in real-time) to solve industrial

challenges. The technology is expected to have a transformative impact across various sections. This paper details a digital twin solution through an Edge Device installed on board the ship called HermAce Gateway of the voyage data recorders (VDRs), enabling various activities to be completed remotely more safely and efficiently. The HermAce Gateway employs real-time data streaming from the ship's bridge equipment. It is part of the HermAce Solution, which also consists of a Cloud Infrastructure that integrates different applications living in various cloud environments (i.e., Azure, AWS, On-premises) to gather data quickly and in real time, process, and visualize them in one platform called "HermAce Platform" centrally supported in a multi-platform environment utilizing the strength of each platform, see Stavrou (2020).

Data collected from VDRs describe the condition and behavior of multiple devices on ships. This data informs diagnostics, failure reports, and necessary checks. In the case of the HermAce Solution, when an abnormality occurs in the electronic equipment mounted on the ship, this information is available to shore engineers. In contrast, previously, the onboard crew would need to connect to the VDR. Installation, commissioning, maintenance work, and Annual Performance Tests (APTs) can all benefit from this solution.

The eruption of bandwidth allocation through satellite communication has facilitated such a service, and thus, increasing needs for remote access to the ships are anticipated. Various signals from electronic devices on board the vessel are collected in the cloud using satellite communication, and troubleshooting occurs in case of abnormality.

The marine industry is changing, and the development of new maritime software as a service application, including monitoring and AI solutions, is anticipated in the coming years. Digital twins in the shipping industry are comprised of the collection and processing of data, validation of outputs, and transmission to diagnostic centers, Glaessgen (2012) and Assani (2022). Information, such as alerts, equipment health status, power status indications, downloaded data for further equipment analysis, bridge security, and connectivity, is valuable for these applications. In the case of the HermAce Solution, remote access to the equipment onboard the ships will help customers and equipment integrators control the equipment status and perform pre-survey checks. It will also provide the foundation for successful remote APTs. The digital twin provides equipment information to the shore engineers and, along with remote repair services, provides an eye to integrators' digital transformation.

The globally ubiquitous trend towards digitalization has long reached the maritime industry. As detailed in Gausdal (2018), this transformation is driven to reduce costs, increase business effectiveness, and improve regulation. In the maritime industry, this can be achieved by utilizing a large quantity of already processed data Giering (2021). At the same time, it is essential to identify that large technology organizations in the shipping industry are investing enormous amounts of money providing high implementation costs, which is in contrast with low-quality offshore connections, aging decision-makers, an overly technology-oriented culture, and lack of investment initiatives operators, as well as a low level of modern diffusion of digital technology through the supply chain as primary barriers for implementation, Gausdal (2018), cause difficulty in the adoption of the specific technologies and initiatives.

Digital systems are systems installed on board the ship that would conventionally be controlled by the ship's crew but which, through recent advances in Information Technology (IT) and Operational Technology (OT), Lloyd's Register (2018) now include the capability to be monitored and controlled. This can be achieved remotely or autonomously with or without a crew on board. Remotely monitored and controlled means any changes to operating parameters, settings, or software that directly affect operation (e.g., changes to heading or speed) or an indirect effect on the ship's operation (e.g., changing navigation charts, equipment settings, or software versions). The functionality provided by digital systems can range from simple remote monitoring with a crew on board to fully autonomous ships without a crew on board.

Modern maritime ships include many electronic devices, which must all be monitored. One such device is the Voyage Data Recorder (VDR), Furuno (2020). A VDR records data from multiple devices on the ship, as required by the maritime industry's IMO and IEC standards. This data can be crucial to investigators in locating the cause of marine incidents. VDRs are currently required to undergo APTs conducted by qualified personnel trained by the manufacturer in accordance with SOLAS Convention,

https://doi.org/10.1017/dce.2024.59 Published online by Cambridge University Press

Annex Chapter V, Regulation 18.8, and IMO Guidelines MSC.1/Circ 1222/Rev.1. This requires an on-board engineer to connect a laptop computer to the VDR and verify the accuracy of the operational data.

Using a remote monitoring solution (the HermAce Solution) and the Remote VDR Annual Performance Test (APT) service, much of this same performance data for VDRs can be obtained remotely, as required. The opportunity to effectively perform these tests on an ad hoc basis offers potential improvements to safety and efficiency.

Like other electrical and mechanical equipment, the electronic bridge equipment is inspected, tested, and maintained periodically by the original equipment manufacturer and by international standards, classification societies, and statutory requirements. During testing and maintenance, the equipment is taken out of service to be evaluated by qualified crew, service engineers, and class surveyors. Since these inspections, tests, and servicing activities are completed periodically (i.e., quarterly or annually), there is a risk of operating with faults that may have developed since the previous inspection/servicing interval. Human errors may result in similar issues if the testing and servicing are done incorrectly. As detailed in this paper, in the case of VDRs, this challenge is directly addressed by the remote monitoring functionality of the HermAce system.

This paper details the design, principle of operation, verification testing, and certification of the HermAce digital twin and discusses its significance to the maritime industry. Section 2 introduces the digital twin, including a summary of the key design features and its principle of operation. Section 3 details the verification tests performed to demonstrate the reliability of the digital twin. A discussion of how the solution was added to an industrial AI register of a leading certification body is provided in Section 4. Finally, critical conclusions from the project are listed in Section 5.

2. Digital twin solution

In the Digital Twin Era, large organizations worldwide struggle to manage a large amount of data quickly and on time. Companies are investing enormous amounts to develop solutions that meet this goal. Many devices and subsystems will be incorporated and integrated in the future, significantly changing our daily lives.

Furuno has developed an innovative solution called the "HermAce Solution," which consists of a smart edge device (HermAce Gateway) positioned onboard the ship to fulfill the increasing need for real-time information by virtually connecting the ship's equipment (Navigation and Communication Equipment—NAV/COM) with the shore (referred to elsewhere as the HermAce Portal). The HermAce Solution seeks to fulfill the increasing need of shore staff for real-time information from ships currently considered "remote offices."

The HermAce Gateway provides a real-time virtual replica representation of a ship's equipment NAV/COM and can, therefore, be considered a "Digital Twin." More analytically, data streamed from the ship's equipment provides information such as alerts, health status, on/off status, and features such as data download for further equipment analysis by the remote Diagnostic Center (HermAce Portal), Bridge Security status, and Data Connectivity with other third party applications and services. It provides remote access, helps the shipping company monitor the equipment status, makes pre-survey checks to the VDR, and provides the mainframe for successful remote APTs throughout advanced remote repair services. The HermAce Gateway ensures the security of the overall monitoring system by utilizing network segregation between a Ship OT and IT networks, as well as data protection, integrity, and password policy when accessing information related to the ship's equipment. It further provides traffic segregation and bandwidth allocation between traffic data routes to the HermAce Platform on Shore using three different Satellite Communication Links. This utilizes the respective strengths of each platform. The HermAce Portal provides a user interface (remote diagnostic center), and the HermAce IoT portal manages the device and connectivity.

The Digital Twin solution consists of the Physical infrastructure, the Digital Infrastructure, and the Solution in Practice outlined below.

https://doi.org/10.1017/dce.2024.59 Published online by Cambridge University Press

2.1. Physical infrastructure

Figure 1 graphically shows the ship's physical infrastructure and the proposed digital twin solution using the HermAce Gateway. The NAV/COM equipment builds a network with sensors and nautical instruments. The HermAce gateway is a physical security edge device installed on the ship and placed on the boundary between the NAV/COM equipment and other networks (i.e., the Ship's IT network). As mentioned, it receives information from the ship's equipment (for instance, the RADAR and ECDIS). It sends it to the diagnostic centers on the cloud (HermAce Platform) for further diagnosis and actions.

Currently, the HermAce Solution complies with the requirements of the LR ShipRight Cyber Security Capability (Level:3 Accomplished) notation, which was awarded in August 2021. However, its scope extends to other cybersecurity regulations IACS addresses, such as UR E26 and E27, International Association of Classification Sociates (IACS).

The HermAce gateway also allows traffic from one network to another based on the applications and services it runs under security rules and legislation. These are based on primary, international marine security standards, policies, agreements, and contracts between all parties involved. It provides physical network segregation and controls data communicated between the ship's OT and IT Zones (Firewalls/routers, simplex serial link, TCP/IP diodes, etc.).

Apart from physical network segregation, the HermAce gateway also acts as a firewall between trusted (OT) and Untrusted (IT) networks, which shall be protected against excessive data flow rate and other events that could impair the quality of service of NAV/COM equipment. It further denies traffic from other networks and implements minor DoS functionalities, prohibiting port protocols and services not equivalent to the NAV/COM equipment functionalities.

Another critical role of the HermAce gateway is network operation monitoring. The HermAce gateway continuously monitors the OT private network. It generates alarms if a malfunction, reduced/degraded capacity, or high data traffic and latency occurs, and it also generates audit Logs of storage capacity and

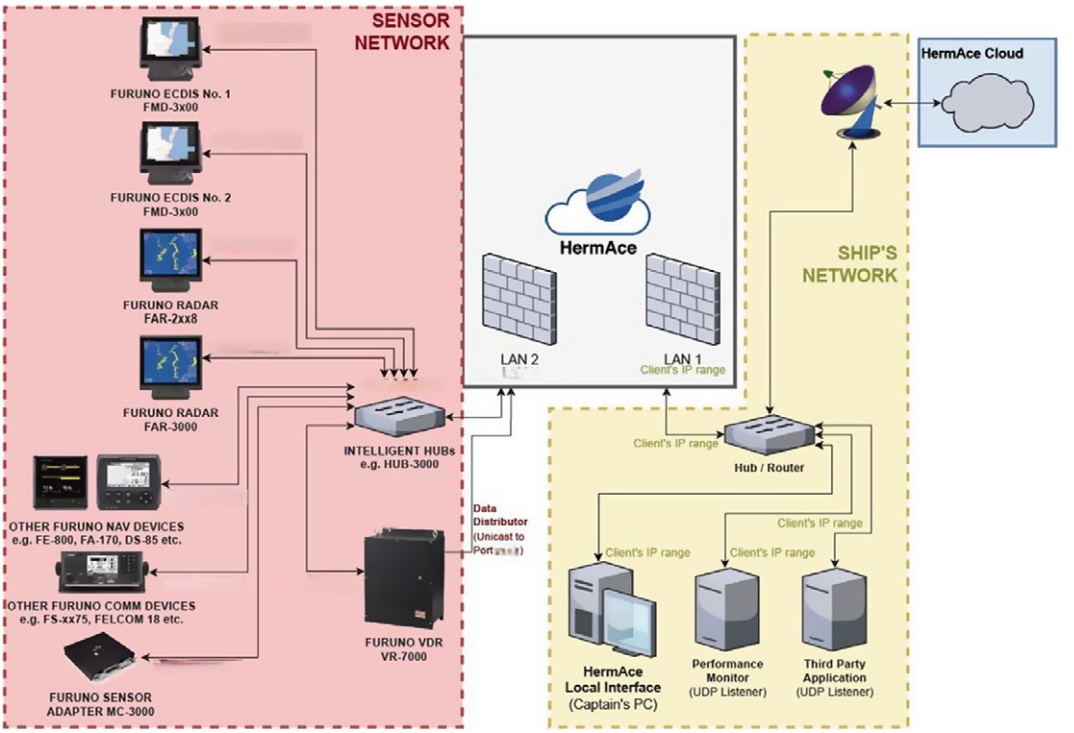

Figure 1. *Network diagram of HermAce gateway digital twin solution on the ship.*

https://doi.org/10.1017/dce.2024.59 Published online by Cambridge University Press

accessibility. Also, a backup and restore functionality applies to the HermAce gateway to ensure the operational continuation of the NAV/COM equipment.

This paper will detail the design, verification, and certification of the HermAce gateway as a digital twin for a voyage data recorder (VDR). Nevertheless, the HermAce gateway has many more functions, combining multiple technologies and protocols. For instance, it has a built-in HTTPS web server called "HermAce Local Interface," a local onboard user interface that provides a quick overview of monitoring the ship's NAV/COM equipment status, analysis, and resolution of eventual problems. The specific Web service is a virtual replica of the HermAce portal onshore. It can be accessed following a dedicated network configuration from a computer (i.e., Captain PC) sitting on the ship's network, issuing NAV/COM equipment troubleshooting instructions or remote access allowance from shore for remote maintenance. The HermAce Gateway is a role-based user identification and authentication system that does not apply to individual accounting management, where users can store and manage their usernames and passwords. The Login page of the HermAce local Interface has role access capabilities according to the specific set of policies/users. For example, suppose the captain wants to access the HermAce Gateway-built Local Interface through his PC. In that case, the shipping company's IT department should provide the configuration required to access the HermAce Local Interface physical LAN port (i.e., LAN 1). Then, a dedicated user with the proper permission will be authorized on the HermAce Gateway so that the captain can access the HTTPS built-in web application features related to NAV/COM equipment status, either in online or Off-Line mode, to gain first-level support and provide remote access to shore engineers.

Every year, Furuno conducts penetration tests at the HermAce Solution to keep up to date with malicious attackers' techniques and take appropriate protections. The HermAce Gateway is a consistent and key part of the HermAce solution. It could not be absent from the Solution penetration test activities. Physical hardware installed on the ship, communication with NAV/COM equipment, and the core of the "digital twin" solution transmitting secure information to Shore Diagnostic Center are key factors of the HermAce Gateway.

The HermAce Gateway built-in Web Application "HermAce Local Interface" takes all the measurements of protection against mobile code, removes the permissions for users to execute SQL queries from the web application API, or changes data causing fault positives/negatives to the application. It further has SSL communication using a new self-signed certificate, which is the norm, especially when the Gateway works in Offline Mode (not connected to the internet), and all general ports (i.e., port 80) are closed. The remote SSH server of the HermAce gateway is also shielded from allowing weak exchange algorithms. Furthermore, it is not vulnerable to ClickJacking attacks, preventing attackers from leading any application in an iframe. In addition, the HermAce Gateway built-in web application supports protection against Cross-Origin Resource Sharing (CORS) to avoid any two-way interaction from the web application domain name. It further follows the appropriate policy not to allow any third party to carry out privileged actions and retrieve sensitive information. The built-in Web application's CORS policy also prevents attackers from bypassing IP-based access control by proxying through "user" browsers. At last, the HermAce Gateway built-in web application HTTPheaders in all responses contain non-sniff options, as found at the PwC Penetration test (2023).

2.2. Digital infrastructure

Figure 2 illustrates the "Hybrid" methodology infrastructure of the HermAce gateway connecting to the Cloud infrastructure and the Ship's NAV/COM equipment. This hybrid architecture includes three satellite communication Links. The first satellite Link goes to the HermAce environment on Azure on the land, which is a secure, isolated Vnet, part of the HermAce remote diagnostic center (HermAce portal) providing Administration Accounts, User Access, Vessel Alerts, troubleshooting and Service Steps, ticketing functionality, and more. The second satellite Link goes to the HermAce environment on AWS, providing a deeper and in-depth analysis of the HermAce Remote Diagnostic Center (HermAce Portal) for the equipment condition and failure, such as health status and Syslog information, the

https://doi.org/10.1017/dce.2024.59 Published online by Cambridge University Press

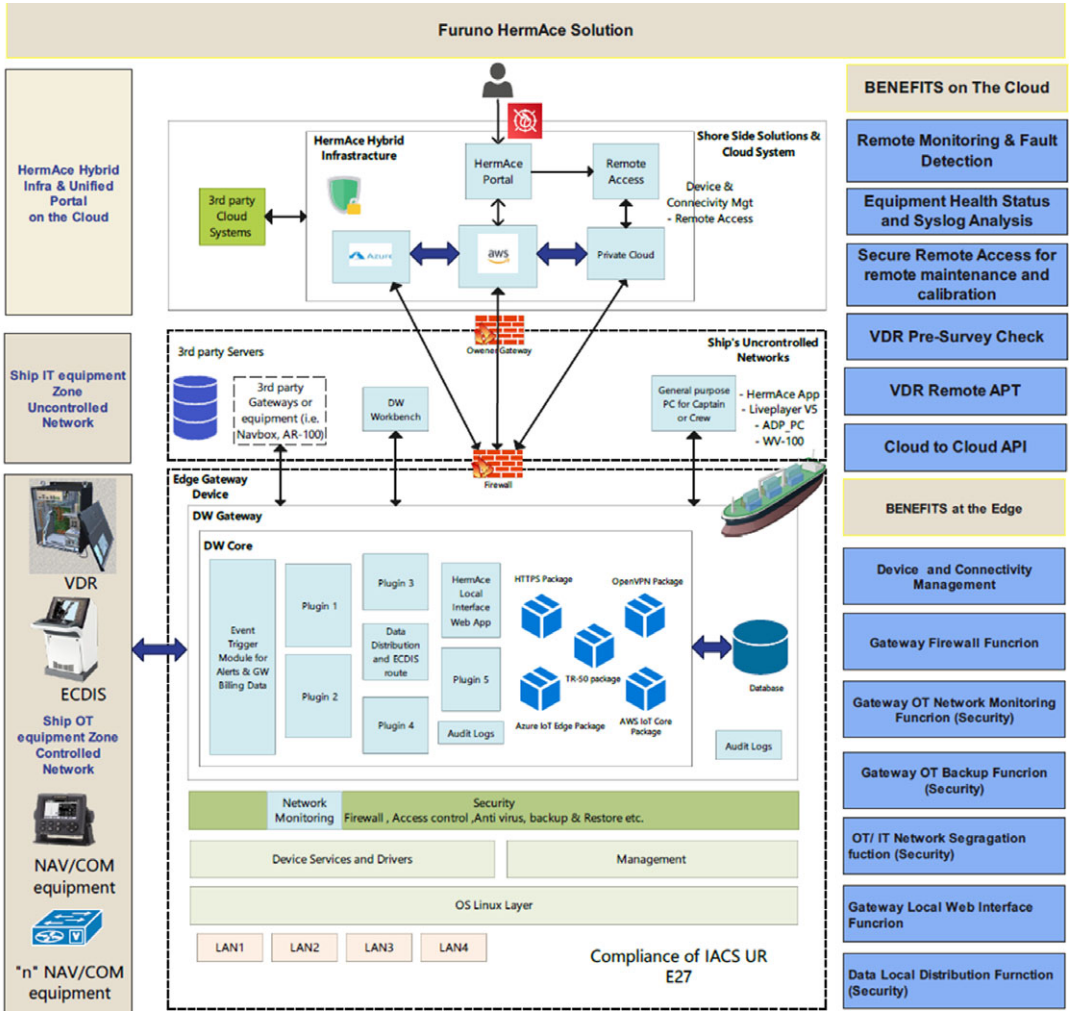

Figure 2. *HermAce hybrid infrastructure.*

ECDIS route coordinated to define the exact vessel's Estimation Time of Arrival (ETA optional functionality), providing a better quality of service experience to the engineers who will attend the ship along with the spare parts required and more. The third Satellite Communication Link goes to the HermAce IoT portal. This Portal is an integral part of the hybrid architecture of the HermAce solution where the Remote Diagnostic Center (HermAce Portal) uses it to support large-scale Device Management (DM) and connectivity Management (DM), provide command control to the HermAce Gateways, execute various actions such as APIs for the Data Consistency Analyzer (DCA) software process providing the VDR remote APT procedure, configures the ship's NAV/COM equipment that HermAce Gateway monitors, support for Software/Firmware Upgrades of the HermAce Gateways and other maintenance tools.

The primary goal is to monitor the Furuno devices on the ships 24/7 and, if not prevent, manage and troubleshoot all problematic or erroneous situations related to vessel equipment as soon as possible.

The HermAce Gateway is a Linux machine and is an Edge hardware (smart device) that is placed on the boundary between the NAV/COM equipment OT network (elsewhere considered a Trusted Network) and the Ship's IT network (elsewhere considered as Untrusted or Uncontrolled networks).

https://doi.org/10.1017/dce.2024.59 Published online by Cambridge University Press

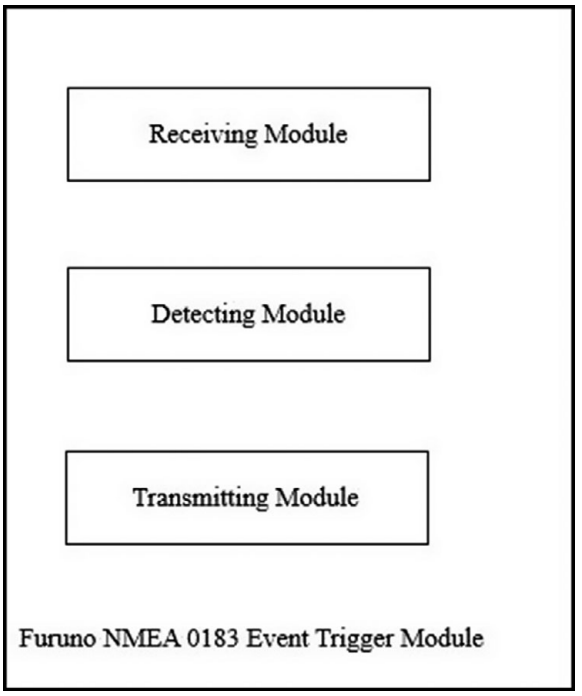

Figure 3. *Components of the event trigger module.*

The Edge Gateway device comprises a DW Gateway. This software application is a sub-module of the Edge Gateway and acts as an intermediate management gateway device among a user, the triggers, other services, and the Ship's NAV/COM equipment, where the user is notified about equipment condition. The DW Gateway uses DW Core, a sub-module that connects with the NAV/COM equipment and is an intermediate to any app, bringing data from the edge to a business application. The DW Gateway further includes a database that directly communicates with DW Core. DW Core consists of an Event Trigger Module and Plugins. The specific hybrid infrastructure allows the Event Trigger Module and plugins to transmit data to the remote diagnostic center, enhancing system portability and simplifying the troubleshooting methodology by eliminating the intermediate point of failures that may cause risk if providing troubleshooting instructions.

This paper explains how to monitor the ship's NAV/COM equipment by utilizing a large data volume via a cost-effective equipment diagnostic device associated with equipment failures, which provides troubleshooting instructions. The digital monitoring infrastructure comprises a Main Trigger Module (Figure 4 the Event Trigger Module) and three submodules (Figure 3 the Receiving, Detecting, and Transmitting Module).

2.2.1. Event trigger module

The Event Trigger Module is a server that constantly listens to the networks and waits for messages from the ship's equipment. Each message includes both identification and specification data, as shown in Figure 4. This combined data is based on the National Marine Electronics Association message standard, BSI (2016). The messages from each ship's NAV/COM equipment illustrate their operational and functional condition through the entire equipment private network (MULTICAST) or each equipment directly (UNICAST) within the private network of the OT devices.

https://doi.org/10.1017/dce.2024.59 Published online by Cambridge University Press

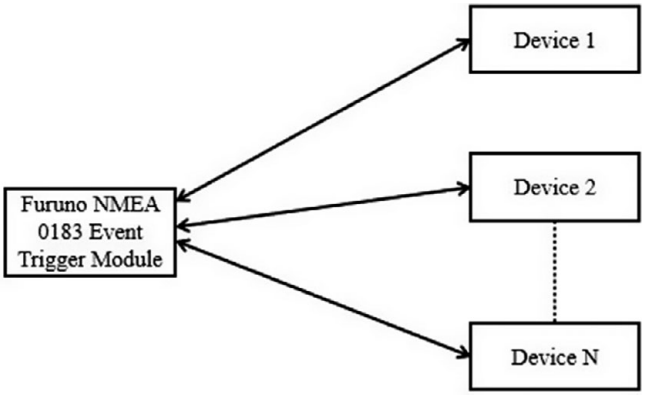

Figure 4. *Communication between nautical devices and event trigger module.*

2.2.2. Receiving module

The "Receiving Module" parses the messages from the ship's equipment and provides valuable information about the equipment itself, including the status, name, IP address, message type, timestamp, and the severity of the failure, if any.

The following is an actual ALR message the module receives from a device, as shown in Figure 5.

Specifically, each NAV/COM equipment may or may not send different data types from other devices. The HermAce gateway Event Trigger Module can parse and analyze each message data block from each device accordingly. So, the module can implement a separate algorithm (logic) based on the messages originating from the device. The Event Trigger module can parse the message blocks based on another type. For the module to be able to do this, the user (R&D) can set the type of the message to be parsed through the module UI at the workbench and can set the module's network interface, IP address, and port number to listen to the message from the devices.

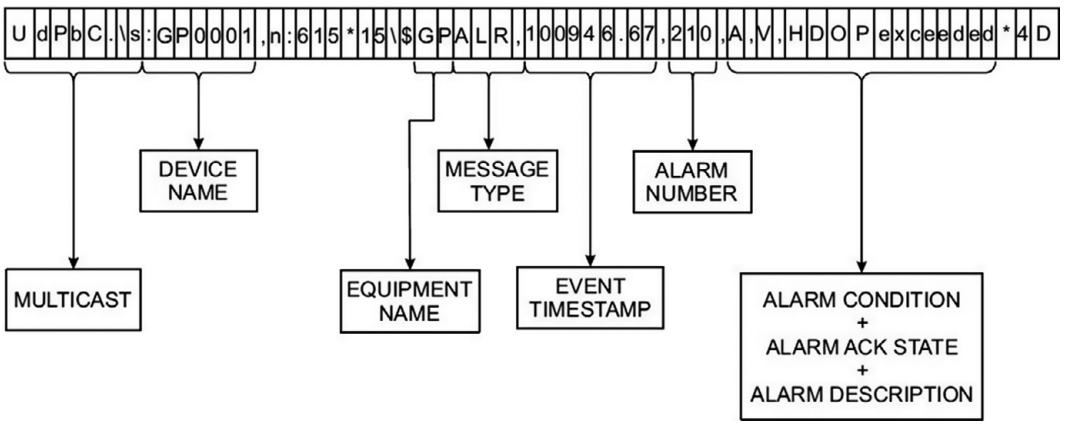

Figure 5. *Structure of an ALR alarm.*

https://doi.org/10.1017/dce.2024.59 Published online by Cambridge University Press

Table 1. *Properties of alarms*

Alarm types	Description	Destination (to)
ALR	Local alarm condition and status. This sentence reports an alarm condition on a device and its current state of acknowledgment.	Send telemetry to the cloud.
ALC	Cycle Alert List. This sentence is intended to satisfy the need for a safe and consistent data distribution with minimum data traffic. The ALC message is currently used only for the UNICAST transmission type.	Send telemetry to the cloud.
ALM	Proprietary protocol sentence of VR3000.	Send telemetry to the cloud.
ALF	This sentence reports an alert condition and a device's alert state. An ALF message shall be published for an alert each time the alert information in the sentence changes and on alert request.	Send telemetry to the cloud.

Table 2. *Processed information from an alarm*

ID	Component	Description
1	Thread of received message	The thread that handles the received message.
2	Listening interface	The network interface is used to listen to device messages.
3	IP address to listen to	The IP address is used to listen to device messages.
4	Port	The port is used to listen to device messages.
5	The IP address of the device	The IP address of the device that sent the message.
6	Socket	The socket is used to listen to device messages.
7	Unicast/multicast	The transmission type of the received message.
8	Stop flag	A flag that indicates the end of the received message.
9	Message type	The type of the received message.
10	Variables	The NMEA message.

2.2.3. Detecting module

The "Detecting Module" decides whether the received message needs additional processing and is, therefore, one of the most critical components of digital monitoring. It caches all the message information inside a database (DB) and formats outgoing messages before they are sent to the diagnostic centers on the cloud. It expects to receive messages from the ship's equipment over the network, with either MULTICAST or UNICAST types. It receives the information via the "Receiving Module." It parses the message by extracting specific information from each type of equipment, such as the name, IP address, type and timestamp of the message, and the severity of any failure(s). Some example message types are shown in Table 1.

Table 2 presents an example of a valid ALR message originating from a device. For every message received, the module needs to process and store the information in an array.

2.2.4. Local DB

The HermAce Gateway provides a Local SQL DB that connects to the "Detecting Module." Any status change may be considered an error or failure and needs to be addressed. Upon every new message received, the device's current state is compared to the previous state (stored in the DB), and according to

https://doi.org/10.1017/dce.2024.59 Published online by Cambridge University Press

the result of the comparison, the system decides whether an outgoing message needs to be transmitted to the diagnostics center on the cloud.

Additionally, because the "Detecting Module" receives a high volume of messages, it minimizes the satellite communication bandwidth and usage cost to the end customer. The user can also set the transmission interval (usually in minutes) between DB queries. Suppose the device status is transmitted to the diagnostic center. In that case, the module will create a record in a specific table of the system's DB with all the information the outgoing message must contain. That is because a corresponding outgoing message must be sent for every device and received message type.

The "Detecting Module" currently prepares an outgoing message if a device's status has changed even once in the last 5 minutes. In this case, the module will prepare an outgoing message communicating the previously recorded and current status to the diagnostic center. This message will also include detailed information about the duration of equipment failure.

Yet, if the submodule detects changes, the device may malfunction, and a more extensive log of the status changes must be sent to the diagnostic center to perform more advanced troubleshooting. In this case, the entire log of the device's status changes is sent to the diagnostic center on the cloud. The beginning of the log is the 1st record stored upon receiving the 1st message from this device over the ship's private network.

2.2.5. Transmitting module

The last submodule of the digital infrastructure is the "Transmitting Module." This module transmits information associated with the equipment failure and outgoing messages to the remote diagnostic center. All outgoing messages are stored in the system's DB for logging and statistical reasons. They are JSON-formatted.

Figures 6 and 7 show that the HermAce gateway minimizes the end customer's satellite communication bandwidth and usage cost. Figure 6 shows a capture time chart when NAV/COM equipment data is received and sent to the cloud. As can be observed from the time chart, an average of a high volume of bytes is transmitted.

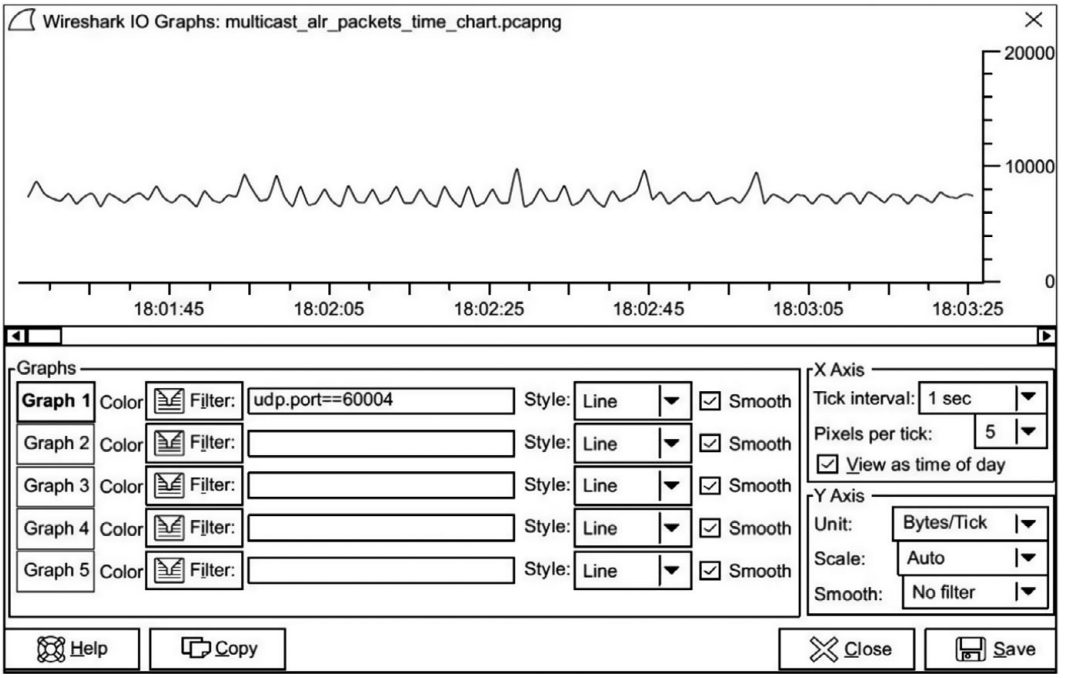

Figure 6. *Image of constant data flowing from NAV/COM equipment and sent to the cloud.*

https://doi.org/10.1017/dce.2024.59 Published online by Cambridge University Press

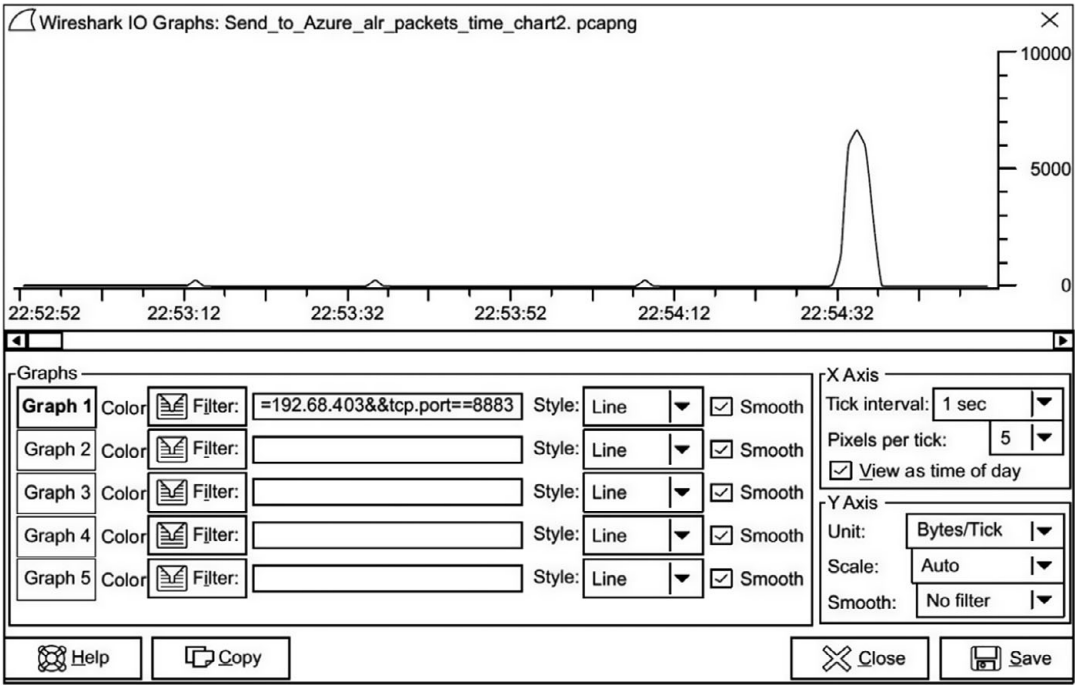

Figure 7. *Image of data flow after HermAce gateway processing and sending to the cloud.*

On the other hand, Figure 7 shows an example capture time chart stating that only the necessary information is finally published to the cloud following the HermAce Gateway processing function.

2.3. Solution in practice

The above descriptions summarize the processing of large data via one of the biggest NAV/COM manufacturers Furuno's authorized gateway. The HermAce Gateway uses identification and authentication methods to access the built-in applications it supports to control the product's hardware and software. This information can also be accessed using a built-in HTTPS web Interface, where the user (field engineer) can monitor the ship's equipment within the private network and the data received.

One of the built-in HTTPS web page functionalities is speeding up the configuration process. It features an option to fill in the table automatically from the data already received and stored in the HermAce Gateway's database, as shown in Figure 8.

Furuno aims to continuously improve its products and services and act as a leading worldwide technical company in the marine industry. Furuno Hellas has established procedures and rules to ensure that the Company follows the rules for the secure development lifecycle of software and the overall system, all matters related to the User Acceptance Test (2023) and identification, reporting, and fixing of bugs in the software products/applications, keeping records/documents of the process, until the commissioning and delivery to customer, providing Reports to the customer about the Gateway security measurements and Configuration, according to the Furuno Hellas ISMS for the and IACS regulations.

The below essential information explains without limitations how a company like Furuno Hellas ensures the continued security of the HermAce system, beneficial for the device (NAVCOM) higher quality of service, security of the OT network, and remote Annual Inspections (i.e. VDR Remote Annual Performance Test).

https://doi.org/10.1017/dce.2024.59 Published online by Cambridge University Press

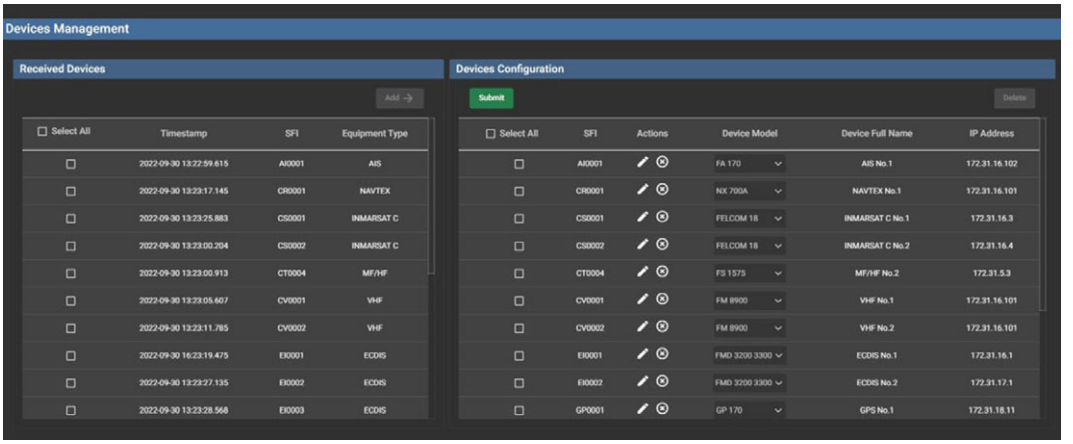

Figure 8. *The device management image is taken from the HermAce gateway.*

- HermAce gateway, like any other device on board the ship, is a Linux-based computer system that needs occasional updates and reconfiguration if required.
- Establish the routines in case any unexpected behavior is identified in the software during Acceptance Testing, either before or after an official version release from a User Acceptance Test perspective, according to the Furuno Hellas ISMS for the User Acceptance Test (2023).
- Ensures the requirements of the involved and influenced parties in the Design and Development process lifecycle, conforming to the requirements of the relevant International Standards, such as ISO 9001, ISO /IEC 27001:2013 (2023), and IEC 62443–3-3, which are among the most recognized standards.
- Organize a yearly class survey when an LR (Lloyds Register) auditor performs a Certificate renewal visit at the Furuno Hellas office and re-accesses the objectives previously noted for the established or new procedures and rules followed for the continual improvement of the HermAce Solution. For example, the Technical Audit Plan is one item that the auditor is looking for during the audit.
- Due to its importance in identifying and planning audits/test and review management, Furuno Hellas provides vulnerability tests at least every 2 years at the Edge devices (HermAce Gateway) and the Cloud (HermAce Portal and infrastructure). The tests are relevant to Internal and External processes where ethical Hackers used and ensure that HermAce Solution has taken all those security measures against the latest vulnerabilities, where access rights (physical and network access) are carefully managed, according to the PwC Penetration test (2023).
- Secure Account Management and Authentication and Identification measurements. It has a rigorous access policy based on users and roles. Some users have "Administration" rights over the device, and users like the technicians have minimal access rights just for the ship's nautical electronic devices monitoring and troubleshooting operations. Each user and role of the HermAce gateway is based on the Access Control policy framework decided and agreed upon by all interested parties and companies.

It is a global trend to use Off-The-Shelf systems rather than plan a solution from scratch using a Do-It-Your-Self (DIY) approach. The HermAce Gateway is following this method to improve HermAce Solution's stability and reliability in the long run. Using an SDK inside the DW Core component, we leveraged the DW Gateway Off-The-Shelf software to enhance the system's portability to its fullest functionality. We implemented the Event Trigger Module and plugins described above to get MULTI-CAST/UNICAST messages from NAV/COM equipment MULTICAST/UNICAST messages. This method eliminated DIY applications using native programming languages (for example, C#, SQL, etc.), which might be vulnerable or unmaintainable in the future.

https://doi.org/10.1017/dce.2024.59 Published online by Cambridge University Press

The physical and Digital Infrastructures of the HermAce Gateway and the security measurements are explained above. However, although one of the roles of the HermAce Gateway is the network segregation between the NAV/COM OT network (Trusted) and the Ship's IT network (Untrusted), it shall not isolate these networks entirely. For this reason, the HermAce Gateway acts as a Data Collector for other UDP and TCP/IP listeners outside of the Ship's OT network. The purpose of the Data distribution is to facilitate VDR data to 3rd party equipment while supporting the cyber security requirement not to allow connection of any unauthorized 3rd party device on the sensor network, which is often a vulnerable method, causing unexpected events to NAV/COM equipment. Only authorized staff has the right to Administer/Manage/Upgrade and Update the firewall rules through the identification and authentication method required to configure Zone Segregation data flow with uncontrolled networks. The HermAce Gateway also allows the Furuno Service Engineer to manage/access the data flow distribution functionality from the built-in HermAce HTTPS Web Local Interface to third-party equipment, as shown in Figure 9 below.

It is worth mentioning that the strategy and development of products, services, and new solutions in the software or hardware of the HermAce gateway are performed and tested under detailed software development plans, following all international and involved parties' standard procedures and policies. Furuno Hellas establishes and maintains all matters related to verifying the core functionality of newly developed software for the HermAce product, according to Furuno Hellas ISMS Verification Procedure (2023).

The Digital Infrastructure described in this paper explains that the HermAce Gateway transmits alerts, health status, and ship navigation properties to the shore diagnostic center (HermAce Portal) at planned intervals (real-time) over Message Queuing Telemetry Transport (MQTT) & Transport Layer Security (TLS). It is also shown that apart from the Event Trigger module and the Plugins, the DW Core also consists of built-in packages enclosed within the application, meaning that the HermAce is a centrally Administered/managed/Monitored and tested application with secure functions. The HermAce Gateway encloses three MQTT packages for connection to the cloud. The first connects to Azure IoT Hub through IoT Edge, which by default only accepts connections secured with Transport Layer Security (TLS). The second connects with AWS IoT Core, leveraged from AWS Cloud security over Transport Layer Security (TLS). The last connects TR50 with a private Cloud again over Transport Layer Security (TLS). The TR50 is a Telecommunications Industry Association (TIA) framework responsible for developing and maintaining access agnostic interface standards for monitoring and bi-directional communication of events and information between machine-to-machine (M2M) systems and smart devices, applications, or networks. TR50 works with international standards and encloses many other protocols, such as (Open

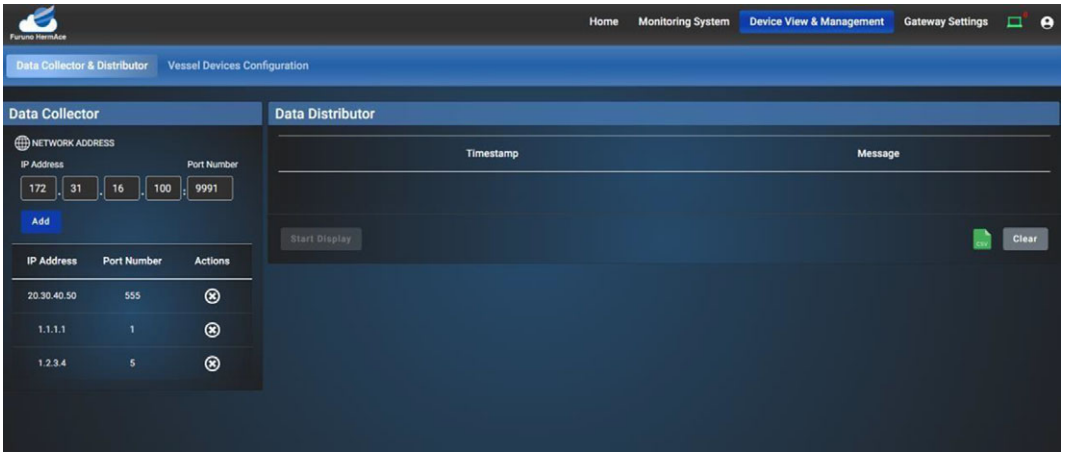

Figure 9. *The data collector and distributor image is taken from the HermAce gateway.*

https://doi.org/10.1017/dce.2024.59 Published online by Cambridge University Press

VPN, HTTP/S, SSH, etc.) to secure the communications and agnostic vertical application domain of the Industrial Internet of Things IIoT, such as HermAce provides to the shipping industry, Telecommunication Industry Association (TIA).

Using the TR50, the HermAce gateway also monitors the connectivity status of each connection to the cloud. It provides a notification message at the shore in case an event happens. It is also important to mention that during the vulnerability tests that Furuno Hellas very often provides, none of those ethical hackers hired for the work could manage to decrypt the communication and become a Man-in-the-middle (MITM) attacker.

One of the most important protocols that HermAce supports over the TR50 framework is the Virtual Private Network (VPN) connection with the appropriate latency and Heartbeat intervals; the HermAce gateway periodically sends information to the HermAce IoT portal, allowing a healthy and fast tunnel router communication for secured remote services. The Heartbeat decreases the chances of poor network quality. Furthermore, a display informs the SATCOM latency of the gateway and the onshore router for the connection bandwidth, allowing the user to start remote services. This bi-directional communication between the gateway and shore diagnostic center (HermAce Portal) provides real-time monitoring and actions with the capability to perform on-demand remote access referenced as the "Digital Twin" mechanism, where data is transferred via a secure tunnel and communicated through various protocols such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP), File Transfer Protocol Secure (FTPS) or HyperText Transfer Protocol (HTTPS). The remote connection from the Shore to the Ship starts with the MQTT over TLS connection from the Ship to Shore over a TR50 framework. Then, an authenticated user can establish a VPN connection that runs other protocols, such as HTTPS, ensuring that end-to-end communication is secured.

The Cloud part of the HermAce solution is not part of this paper. However, it is important to mention that, like the Gateway, the Cloud also meets Confidentiality, Integrity, and Availability (CIA). ISO /IEC 27001 is the most significant standard for this purpose, and every year, LR auditors must confirm that Furuno Hellas and the HermAce solution meet the standard Information Security Management System (ISMS) policies required, ISO /IEC 27001 (2022). Apart from the ISM code, another method to protect the HermAce solution against unethical attacker methodologies is the Penetration Test conducted every 2 years in the Cloud, PwC Penetration Test (2023). PricewaterhouseCoopers (PwC), in 2023, conducted an internal and external penetration test on the HermAce web applications and infrastructure both at the edge and on the cloud. To identify potential vulnerabilities, the test attempted to simulate the risk of an authorized/unauthorized malicious threat agent attacking the HermAce Solution remotely.

Satellite connectivity is also a significant factor in the HermAce Solution. The shipping Industry is a conservative market in which ship owners or managers want to adapt and follow fundamental trends. Although Starlink seems to be the leading connectivity technology provider, installing it on board is not mandatory, keeping lower technological and cheapest SATCOM solutions such as VSAT or Broadband standardized on Ships, whether retrofit or new buildings. The fact that satellite connectivity issues have not been overcome yet means that the HermAce solution still needs to perform well in case data volume is sent to the cloud or remote access under the current, often poor, satellite communication conditions.

Regarding the high volume of data, a percentage compression minimizes the amount of data consumed between the HermAce Gateway and the Cloud infrastructure, avoiding any customer doubts that HermAce may increase the cost of the Satellite Provider or consume high bandwidth. Remote Access is also a significant challenge that needs extended and continuous development on latency and heartbeat interval to make it robust with the current SATCOM solutions.

Finally, the requirements of cloud computing and Machine Learning are worth mentioning. The Edge devices cannot process the high volume of data on Ship. Although the HermAce Gateway is a smart device that provides algorithms and troubleshooting actions, it can process only its own Ship's data, and cloud computing becomes vital for extensive data analysis. Especially when required to provide statistics and failure symptoms relevant to the substantiation of many failures, more advanced processing, monitoring, reporting, and troubleshooting of data from the ships' NAV/COM equipment are required. The cloud infrastructure provides compelling processing and storage capabilities and the necessary level of remote administration and security enhancement.

https://doi.org/10.1017/dce.2024.59 Published online by Cambridge University Press

2.4. Benefits and potential significance to the maritime industry

The International Association of Classification Societies (IACS) published the Unified Requirements (UR) for the cyber security of ships in April 2022. The NAV/COM equipment of a ship is also included in this requirement. The URs adopted for the cyber security resilience of ships are the E26 and E27. The E26 primarily addresses ship-wide cybersecurity requirements concerning the detection, response, and recovery of traditional cyber-attack prevention. E27, on the other hand, focuses on the cybersecurity of onboard systems and equipment. A ship's NAV/COM equipment should first comply with E27 but also cover E26 requirements. The IACS will apply these uniform requirements in association with ships contracted for construction after July 2024, International Association of Classification Sociates (IACS). The scope of applicability is for passenger Ships engaged in international voyages, Cargo Ships of 500 GT and upwards engaged in international voyages, High-Speed craft of 500 GT and upwards engaged in international voyages, Mobile shore drilling Units of 500 GT and Upwards, and Self-propelled mobile offshore units involved in construction.

As with every Furuno device, the HermAce gateway is an essential device that needs to comply with IACS UR E27 but as mentioned above, should also cover the E26 requirements. For this reason, the gateway's role is essential to this applicability application. To meet the IACS requirements, the functional overview of the gateway is to be placed as a boundary of the NAV/COM system (segment). It has the following roles as a cyber-security measure.

The first role is to meet the E26 4.2.1 Security Zone requirements. All ships constructed after July 2024 should have the OT and IT zones physically separated. Firewalls/routers, unidirectional links, TCP/IP, and UDP diodes should be controlled in place. As described in IACS documents, the HermAce Gateway should meet the international Standards IEC 62443-3-3, including but not limited to the paragraphs: SR 5.1 Network segmentation and SR 5.1 RE1 Physical network segmentation. Separate Zones have been implemented on the gateway for physical or logical segmentation.

The second role of the HermAce gateway is to meet E26 4.2.2 Safeguards to protect the network. A firewall must protect network boundaries and the OT network against excessive data flow and other events that could degrade the quality of service of network resources. Also, unnecessary features, ports, and services should be disabled or prohibited, providing the necessary principles to restrict connections from other networks using the firewall functionality as well as it will access and monitor the OT network, providing alerts-notifications in case of events according to the IEC 62443-3-3 paragraphs: SR 5.2 Zone boundary protection, SR 5.2 RE1 Deny by default. For this purpose, dedicated firewall rules with separated zone boundaries have been configured.

SR 5.3 General Purpose P2P, according to the gateway firewall rules and endpoints of communication with untrusted zones, SR 5.4 Application partitioning, by separating the applications, data, and services for different reasons, SR 7.1 Denial of service protection when in case DOS attack the gateway automatically attempts to disable the network traffic, re-installs the application and restore its basic functionality.

The third role of the HermAce gateway is to meet E26 4.3.1 Monitoring network activity. The OT network should be continuously monitored to generate an alert for a failure or functional decline. It should also meet the E27 4.1 Required security functions/IEC 62443–3-3 paragraphs: SR 2.9 Audit storage capacity, where the gateway saves audit logs, SR 6.1 Audit log accessibility, where the gateway syslog can be accessible as well as reporting on the cloud all the auditable events.

The fourth role of the HermAce gateway is to meet E26 4.5.2 Backup and restore functions. The gateway must support backup and restore functions entirely and securely. The backups must be maintained and tested regularly, equivalent to the User Settings backup and audit log. It should also meet E27 4.1 Required security functions/IEC 62443-3-3 paragraph: SR 7.3 Backup, where the gateway backs up all its functionalities to be re-stored at any time from the cloud.

The fifth and last role of the HermAce gateway is to meet E26 4.2.6 Control of remote access and communication with untrusted networks. The OT network must be protected against unauthorized access from untrusted networks and other cyber threats. It should also meet the E27 4.2 Additional security features/IEC 62443-3-3 paragraph: SR 1.1 RE 2 Multifactor authentication, where the gateway takes all

https://doi.org/10.1017/dce.2024.59 Published online by Cambridge University Press

measures, accessing through MFA on the portal and One-Time Password at the gateway, SR 1.2 Endpoint authentication, with specific software processes, SR 1.11 Unsuccessful login attempts, where the maximum logging attempts are limited to three, SR 1.12 System use notification, using an email notification when someone accesses the gateway from an untrusted network, SR 1.13 Access via untrusted networks monitored and controlled either from the HermAce gateway or the portal, SR 1.13 RE 1 Explicit access approval is given by authorized personnel on board, utilizing an ON/OFF digital switch, SR 2.6 Remote session termination, either from the authorized personnel on board or from the portal, SR 3.1 RE 1 Cryptographic integrity protection using the latest version of Cyphers, SR 3.2 RE 1 Malicious code protection, through antivirus and antimalware protection patched regularly, SR 3.8 Session integrity, SR 3.8 RE 1 Invalidation of session ID, SR 3.8 RE 2 Session integrity, using at least 128-bit encryption and the best of the most efficient algorithms controlling the communication IDs avoiding session mismatch or attempt of hijack.

In recent years, large organizations in the shipping industry have engaged in a digital transformation with an eye to Industry 4.0. Though there are common challenges (e.g., expandability, interoperability, and security), each manufacturer or service provider's solutions to the end customer (shipping company) are still independent and have many cross-compatibility limitations. Multiple Hardware Edge devices continuously installed on board the ship may introduce cyber security vulnerabilities to the NAV/COM equipment and add complexity to their support and asset management.

The interoperability between manufacturers or service providers fails due to each OEM's proprietary protocols. At this moment, there is a huge competition between manufacturers and service providers to expand their solutions to the market and gain a higher market share, which does not open the road to interoperability between them. Nevertheless, as long as autonomous technology comes across the near future, the expandability of each OEM seems inevitable.

In the feature, the HermAce gateway will support expandability, interoperability, centralized management, and security by integrating many solutions based on processing power, features, and cost. Each solution will be independent; only its service provider will be able to access it. There will not be interoperability issues, as each of these independent solutions can communicate through an internal communication channel, with only a certified gateway working as a service platform at the edge.

However, even now, the HermAce Gateway is trying to solve this issue by providing functionality to bridge the sensor data and external devices outside the OT network. In the framework of the HermAce Gateway, data collection and distribution from VDR to third-party devices, the Gateway's latest version of firewall rules provides bidirectional transfer for the necessary data, connecting the supported external devices to operate without being physically connected to the Furuno proprietary network. This feature is designed according to the supported external devices, including the port numbers and data types that will be transmitted to meet this requirement. For this reason, the HermAce Gateway includes a configuration page that creates the firewall rules feature of the local web interface, offering the ability to change the features' settings. Figure 10 shows the user's ability to configure the target IP addresses for each external device and individually turn data forwarding to each supported external device on or off.

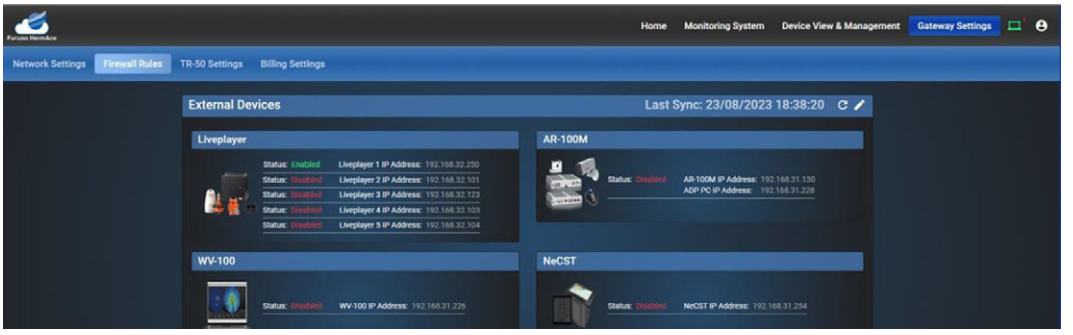

Figure 10. *Image taken from HermAce gateway.*

https://doi.org/10.1017/dce.2024.59 Published online by Cambridge University Press

The Digital Twin of a VDR provided by the HermAce gateway provides safe and reliable real-time monitoring of ship equipment. This data, including detection and isolation of faults and failure modes, facilitates remote APTs of the VDR, improves its reliability and availability, and includes access to a Furuno authorized personnel for remote maintenance and troubleshooting. This minimizes operational disruption, multiple hardware on the ship, and the cost to the end customer.

The HermAce system monitors all the NAV/COM equipment on a ship. Although this paper focuses on the digital twin of a VDR, one of the most significant advantages is the opportunity to integrate the digital twin technology with all NAV/COM equipment on a ship. The capability of this Virtual twin of the NAV/COM equipment on shore will soon change the ship's operation. Furuno endeavors to introduce Digital Transformation into the marine industry. The HermAce solution expands the digital transformation business in this direction by providing intelligent solutions to customers' shipping companies and operators based on "Digital Twins." However, as with every new disruptive product built within a big organization, creating a new market and transforming the organization's staff to use this new innovative technology is essential. On the one hand, it will minimize operational costs and expand the quality of service regardless of the individual skills of service personnel using remote services (e.g., remote APT).

Furuno is not the only company that has tried to embrace digital transformation in the marine industry. JRC, Kongsberg, Danelec, and Sperry Marine are also moving in a similar direction to provide Remote Services to their customers' users. More specifically, the JRC Remote Maintenance System (RMS) utilizes its VDR to accurately diagnose the malfunction of all the NAV/COM equipment of Japan Radio Co. Ltd (JRC). Like JRC, Danelec also accesses and manages the ship's VDR for adequate service preparation, alarm analysis, and Pre-APT Danelec 2024 (Access Your VDR Data Anytime, anywhere). Furthermore, Sperry Marine and Danelec have partnered to create remote VDR management through Marine VoyageMaster Connect, Danelec 2024 (Sperry Marine & Danelec). Sperry has also created SperrySphere, evolving additional services, including smart support enabling remote monitoring, diagnostics, and service navigation equipment by connecting onshore and offshore, Sperry Marine (Smart Support). Kongsberg 2025 has launched an Insight Marketplace called Cognifai, where integrated third-party applications can provide insights to the end users through the data coming from the vessel. Kongsberg provides a smart Edge device on board the ship that collects data from the NAV/COM equipment or the engine and sends it to the cloud. It combines many services through one platform to accurately diagnose malfunctions through Cloud processing, Konsberg (Kognifai).

In conclusion, the "HermAce Solution" consists of a smart edge device (HermAce Gateway) positioned onboard the ship that acts as a barrier between the NAV/COM equipment and other networks and the HermAce Remote Diagnostic Center (HermAce Portal) that provides better insights and holistic approach analysis respective to the equipment failure, the spare parts required, but also offer remote services, such remote VRD APT and maintenance services. The HermAce gateway is a critical factor of the Digital Twin of the VDR, as it determines in real time that both the hardware and software of the equipment are working normally and verifies that a Remote APT can be followed without any unexpected situation, which is very common during the current physical on ship attendances. The Gateway also transmits the VDR status information to the cloud, where authorized personnel verifies HermAce Digital Twin technology and performs remote APT and other remote actions. The combination of functions both at the edge and on the cloud associates with a Center of Excellence that provides many solutions under one Platform that is interoperable with other OEMs or customer shipping companies/operators that want to utilize these data and gain from exposing insights of better solutions along with cost-effective operational and maintenance tools.

3. Verification testing

3.1. Introduction

Assurance is critical to realizing a digital twin's operational, commercial, and safety benefits. Lloyd's Register has developed an assurance framework for evaluating digital twins in the maritime and offshore

https://doi.org/10.1017/dce.2024.59 Published online by Cambridge University Press

industries. Lloyd's Register's assurance framework comprises four phases, "Digital Twin Ready, Approved, Commissioned, and Live," involving audits, systems engineering review, software conformity assessment, design review, risk assessment, verification, and validation activities. These different activities help improve the effectiveness, dependability, and safety of the digital twin by identifying and isolating poor engineering and software engineering practices, errors of commission and omission during development, and cyber security vulnerabilities to minimize the potential for faults, failures, cyber-attacks, and accidents during digital twin deployment.

Independent verification (digital twin approved) involves different evaluation and testing techniques to confirm that the digital twin can satisfy different technical requirements relevant to operational benefits. Verification begins with identifying digital twin target credits, that is, operational benefits generated by the digital twin. The target credits are derived by identifying different inspection, survey, maintenance, servicing, and testing tasks relevant to the voyage data recorder and describing how the digital twin can complement, improve, or automate the crew and service engineer's task burden during operations and annual functional testing. The target credits are further refined by analyzing the functions and failure modes of the sub-assemblies and replaceable parts of the VDR by carrying out a VDR Failure Modes and Effects Analysis (FMEA). The different inspection, survey, and functional testing credits are consequently mapped against the failure modes to understand the digital twin's minimum fault detection, diagnostics coverage, and sophistication. This is followed by requirements derivation, which defines and explains the functional, performance, and safety requirements relevant to achieving the target credits and digital twin capabilities.

Verification testing provides information on the reliability of the outputs from a digital twin. Each message from the HermAce System indicating a fault with another component can be categorized as a true-positive (should the indication be genuine) or a false-positive (if the fault is not present). Conversely, the absence of a message from the HermAce System can be categorized as a true-negative (in the event where no fault is present) or a false-negative (where a real error has not been recorded). Understanding the probabilities of these false-positive and false-negative errors is important in the ship's risk management.

Section 3.2 outlines the testing procedure, Section 3.3 presents the results, and Section 3.4 outlines how the results can be used to model the reliability of HermAce outputs.

3.2. Test protocols

A software-in-the-loop (SiL) testing strategy was used to simulate error messages from the network. A Python script was used to automate the BSI (2016) compliant generation of messages containing error alarms. These were sent to the digital twin via a secure shell protocol (SSH) connection to the operator's network. The response was then stored in a SQLite database, which was queried to ensure the alarms were recorded as expected. A screenshot of this database is shown in Figure 11.

Alarms from all network components were repeatedly and in various ways simulated. First, each alarm was simulated sequentially, as illustrated in Figure 12. Testing using simulated malformed messages (mimicking erroneously encoded bytes) was also completed to check that the system did not erroneously record alarms when supplied with incorrect syntax or non-existing alarms.

The digital twin's response was tested against large numbers of simultaneous inputs. This testing was linked to a credible scenario of mechanical (vibration) and/or electrochemical (corrosion) induced degradation of connections. The test scenario shown in Figure 12 illustrates how many alarms were simulated simultaneously.

Note that each type of test was repeated, as indicated by the Test ID labels in Figure 12 and Figure 13. Repeated testing was used to check whether results could be reliably produced. Section 3.4 discusses how evidence from multiple tests can be quantified.

In the event of false-positive (failing to detect an error that was communicated as part of a valid message sent to the VDR) and false-negative (detecting an error that was not sent to the VDR) events arising, the associated test conditions can be characterized so that more tests of this type can be completed.

https://doi.org/10.1017/dce.2024.59 Published online by Cambridge University Press

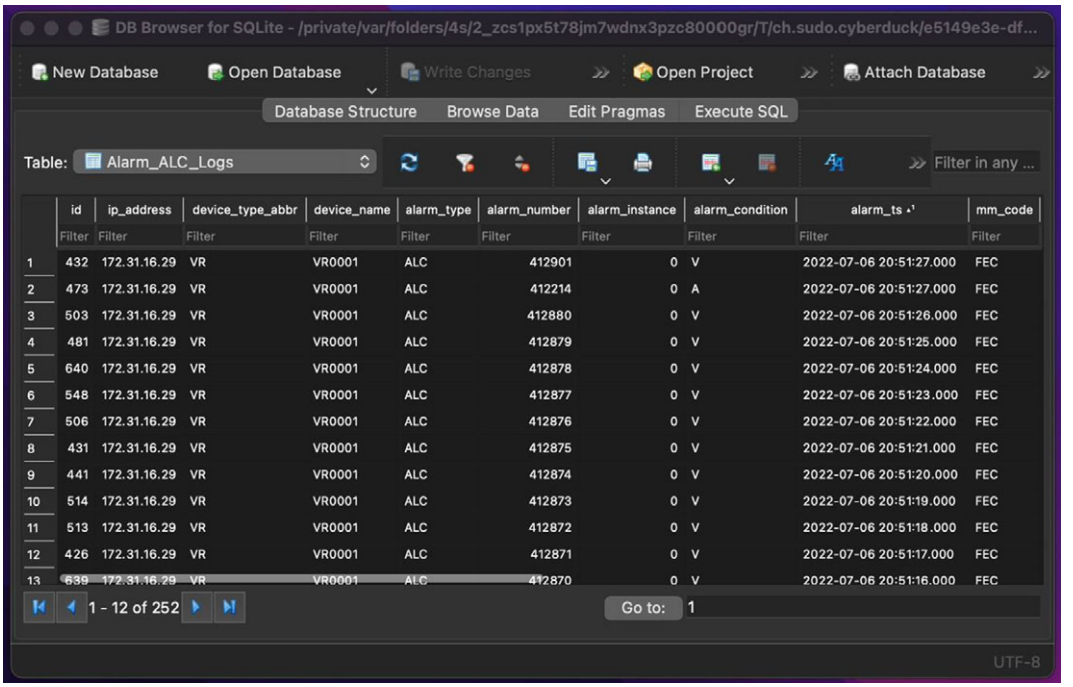

Figure 11. *SQLite alarm database for the HermAce system.*

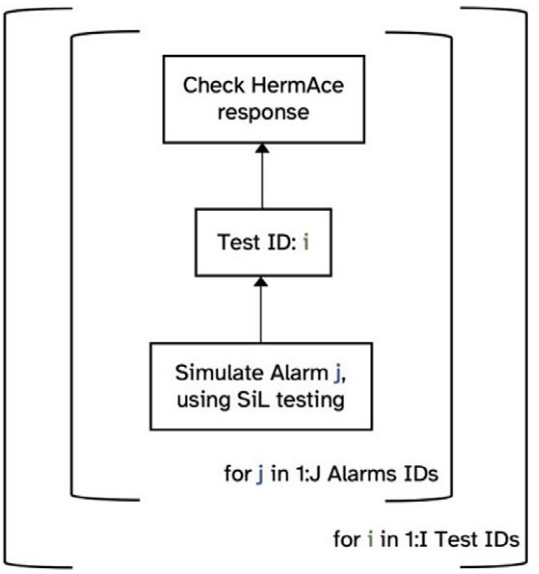

Figure 12. *SiL testing of sequential alarm cases.*

Adaptive synthetic data generation can help testing target more informative scenarios. Since errors are expected to be rare, these methods can assist in understanding and quantifying their rate.

In addition to the above-mentioned semi-automated SiL, complimentary hardware-in-the-loop (HiL) testing was also completed for a selection of functional requirements. Independently produced procedures were provided to one test engineer, and a separate test engineer monitored the database

https://doi.org/10.1017/dce.2024.59 Published online by Cambridge University Press

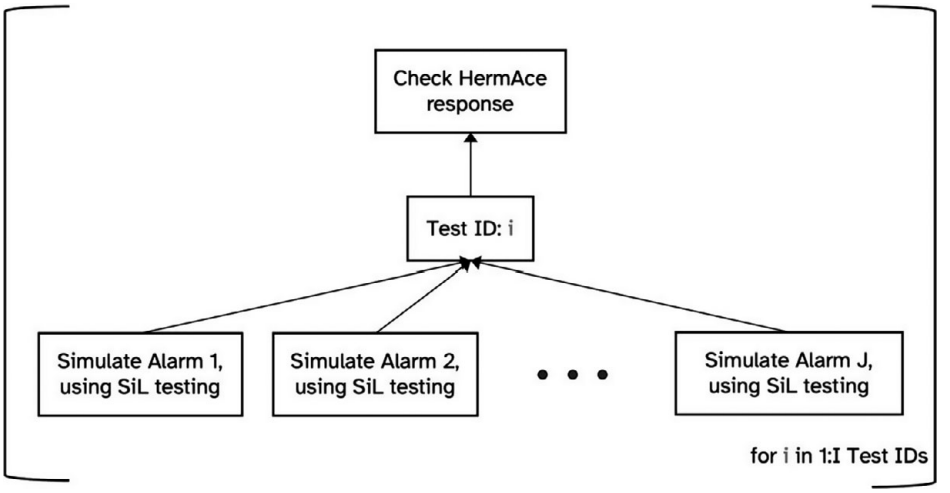

Figure 13. *SiL testing of simultaneous alarm cases.*

response. Sequences of disconnections, re-connections, and sometimes repeated or simultaneous disconnections of physical devices to a VDR were specified and carried out. This also included testing and monitoring the VDR battery following power disconnection. The battery test during the APT procedure is vital and part of the process where the engineer must clarify with evidence that VDR works normally even in battery mode for 2 hours. When the VDR returns to battery mode, the equipment transmits an alarm to the HermAce gateway, which then monitors that the alarm is coming for 1 hour and 55 minutes. With this function, the onshore engineer who performs the remote VDR APT has evidence of the battery running period but is also aware that VDR has been shut down after 2 hours and 5 minutes.

3.3. Test results

The results of SiL testing are presented in Table 3. Testing various types of malformed messages also did not produce unexpected behavior in the database. In addition to identifying the proportion of successful (true positive) outcomes, SiL testing also helped identify required wait times before querying the database before alarms were parsed, processed, and saved.

An independent review of the data collected following HiL testing identified that each test event occurred in the correct sequence and was successfully recorded. The collective information obtained from the digital twin and associated software recorded all loss of data events with sufficient detail to identify the timestamp and affected sensors in each case.

Furthermore, it is important to highlight that before SIL/HIL testing for the VDR Digital Twin technology Digital Twin Approved (September 2022), LR (Lloyds Register) had verified that Furuno HermAce can implement Digital Twins, digital Twin Ready (September 2020) providing independent verification of digital twin technology in the maritime industry. In more detail, LR reviewed the correct, complete translation of Annual performance testing tasks into functional requirements. Reviewing the

Table 3. *Results of SiL testing*

Test category	Number of tests	Number of successful tests
A: Sequential alarms	1,245	1,245
B: Simultaneous alarms	535	535

https://doi.org/10.1017/dce.2024.59 Published online by Cambridge University Press

fault detection and isolation method, i.e., the logic behind acquiring network messages, parsing each message, locating the presence of alarms, and then comparing the alarm to a defined fault class. Specificity of each alarm code to a granular fault type. Type testing records using different physical/electronic stimuli to trigger the alarm codes. Also, it is important to clarify that Python Simulator's Data, used to execute the SIL/HIL test, was extracted from a real ship sensor network with format IEC:61162–450 and was not beta data driven from the market Simulator.

3.4. Quantification of evidence

The verification testing aimed to better understand the reliability of the digital twin's output. By definition, the probability of correct functionality (true positive and true negative results) will be between 0 and 1. A common probabilistic model for such a quantity is the Beta distribution, Gelman et al. (2014), which has 2 parameters, as shown in Equation (1).

$$\Pr(correct) = Beta(\alpha, \beta) \tag{1}$$

This (prior) probabilistic model can be updated following verification tests with a Binomial (pass or fail) outcome based on the number of tests, cap N sub cap T, and the number of correct results, cap N sub cap T (see Equation (2)), Gelman et al., 2014).

$$\Pr(correct) = Beta\left(\alpha + N_P, \beta + N_T - N_{passes}\right) \tag{2}$$

An example is presented in Figure 14, showing how even when there is significant uncertainty in the performance of such a model pre-verification after 100 successful verification tests.

Repeated testing further reduces uncertainty in this estimate. In Table 4, the proportion of the posterior model that exceeds 0.99 increases as more verification tests are completed (when tests are assumed to demonstrate correct functionality, that is, no false-positive or false-negative errors are observed). This results from the prediction becoming increasingly precise (narrower) when more tests are completed. Methods in experimental design, Chaloner (1995) and, similarly, the value of information, Di Francesco (2021), can identify how many verification tests are expected to be required for a defined use case. Still,

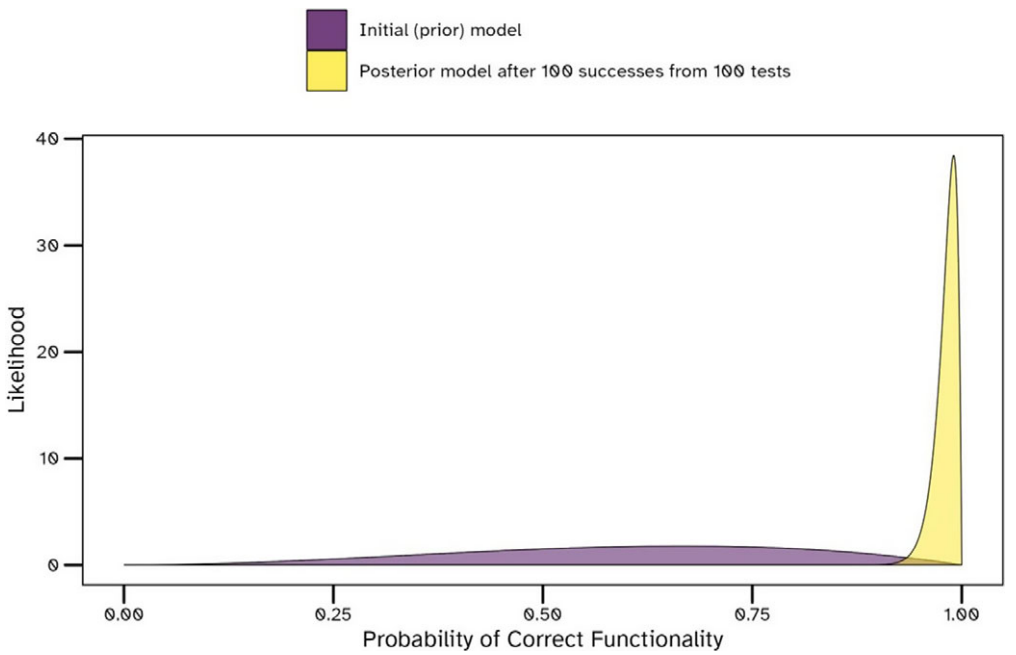

Figure 14. *Effect of 100 successful verification tests on probabilistic estimate of digital twin reliability.*

https://doi.org/10.1017/dce.2024.59 Published online by Cambridge University Press

Table 4. *Results of SiL testing*

Number of tests	Number of successful tests	The probability that the probability of correct functionality exceeds 99%
0	NA	0.0005920300
1	1	0.0009801496
10	10	0.0084012440
100	100	0.2790235461
535	535	0.9713875286
1,245	1,245	0.9999518703
1,780	1,780	0.9999996893

such calculations are not detailed in this paper. For the prior model in Figure 8 and Table 4, Equation (1) was used, with $\alpha = 3$ and $\beta = 2$.

4. Certification and development of industrial AI register

Lloyd's Register is a global professional services company founded in 1760 to improve the performance and safety of maritime assets. In 1764, Lloyd's Register printed its first "Register of Ships" to give underwriters and merchants an idea of the condition of the ships they insured and chartered.

LR's artificial intelligence (AI) register is a standardized directory of certified developers and AI applications for the maritime industry. The AI Register was established to promote the safe and effective commercialization of AI systems, including digital twins, in the maritime sector. This is achieved by improving the trust and confidence of asset owners, operators, charterers, regulators, and other stakeholders in maritime AI systems. The data and insights presented in the AI register are derived from the test and evaluation activities required by LR's assurance framework.

Developers in the AI register have been assessed against LR's "Digital Twin Ready," proving their capability to deliver and sustain AI-enabled systems, including digital twins, with appropriate engineering and software engineering processes, development tools, and subject matter experts. LR evaluates each developer's systems engineering approach, including machine learning development and operations ML DevOps, followed by a software conformity assessment and audit of subject matter experts involved in the system's engineering, integration, testing, and through-life support.

Applications listed in the AI register are evaluated against LR's "Digital Twin Approved" independent verification activities that prove the system's capability to deliver operational and safety benefits. Furuno's HermAce System, independent verification begins with defining target operational benefits (credits). One of the benefits of the HermAce System is that it can facilitate improved APTs of VDRs. All maritime VDRs are subjected to a statutory APT, which includes functional tests, evaluation of the VDR interface with other bridge and engine room equipment, the integrity of recording devices, and visual inspection. Working together with Furuno, the different APT tasks were explicated and detailed to define their test coverage of the replaceable parts and unit functions of the VDR. This was followed by a VDR Failure Modes and Effects Analysis (FMEA) defining all hardware, interface, and software failures relevant to the VDR, including their symptoms and consequences. Lloyd's Register reviewed the VDR APT document and the VDR FMEA report for correctness, completeness, and consistency to derive the minimum functionality and capability of the VDR digital twin.

The minimum detection coverage and sophistication of the VDR digital twin were derived from the different tasks executed by the test engineer during the APT, including the identification of typical VDR fault and failure conditions. The digital twin functional requirements describe the identification and isolation of fault symptoms and their failure manifestation affecting VDR replaceable parts, for example, failure of recording hardware, loss of junction box interfaces, network failures, others, and functionality,

https://doi.org/10.1017/dce.2024.59 Published online by Cambridge University Press

such as buffer overflow, loss of synchronization, and incorrect configurations. Detailed performance requirements, for example, time to incipient fault detection, fault to failure progression, and remaining useful life accuracy, were not defined given the implementation of the target credit, the APT being carried out once a year. Reliability requirements describe the proficiency expected of the digital twin using empirical metrics such as false and false negative rates, as defined in Section 3.

Following the definition of digital twin functional and reliability requirements, Lloyd's Register evaluated the anomaly detection and fault detection algorithm (i.e., event handler algorithm) of the HermAce VDR digital twin. The independent review confirmed the ability of the VDR digital twin to acquire network data when interfaced with IEC 61162, BSI (2016), compliant devices and equipment. In addition, the review established that the minimum network data sampling rate is sufficient to identify and isolate fault and failure conditions in the VDR and connected network equipment. Furthermore, the digital twin's ability to recognize valid network messages, parse the message to locate the segment indicative of a fault condition, and identify unique descriptors specific to the faults and failure types were evaluated. During the review, the effectiveness of the fault detection algorithm was found to be heavily dependent on receiving BSI (2016) compliant network messages, having the correct sentence types (see Table 1), and correct sentence syntax to initiate message parsing and identification of the fault and failure descriptors. This means the fault detection algorithm will not analyze dropped network messages (those not logged by the network), sentences with the wrong identifiers, and non-compliant syntax, even if such sentences contain descriptors indicative of failure modes.

Software in the loop SIL testing of the VDR Digital Twin was organized into three categories of test cases. Test Category A simulated all observable faults, including VDR functional faults, component faults, interface faults, etc., sequentially, with varying appearance times, for example, 15, 10, and 5-second intervals. The fault detection algorithm of the digital twin demonstrated a 100% true positive rate against all test cases in test category A. This was followed by Test Category B with scenarios of fault/failure concurrency (i.e., faults appearing at milliseconds of one another ending up in a single data packet) replicating adverse operating conditions such as corrosive environments, electromagnetic interference, and extreme vibrations. The fault detection algorithm of HermAce digital twin demonstrated a 100% true positive rate against all test cases in test category B. Finally, test category C emulated different uncertainties that can occur in the network environment in addition to fault/failure concurrency. The categories of uncertainties simulated in the test environment include intermittent data loss (drop-out of data packets), invalid message heading, incorrect message syntax, insertion of random alpha-numeric codes, and substitution of incorrect six-digit codes. While the HermAce VDR digital twin cannot monitor and address these data and network uncertainties, the faults were detected upon the reinstatement of valid network messages.

Hardware-in-the-loop HIL testing and remote engineer demonstration were carried out over 3 days using physical fault seeding, failure simulation, and process errors relevant to the VDR annual performance testing. Some physically induced failure conditions include power loss and VDR interface connection loss complemented by real-time simulations of network equipment failures (i.e., for unavailable equipment or when the failure results in costly repairs/replacement). The HermAce System achieved a 100% true positive rate against the test cases, and the remote HermAce engineer effectively demonstrated the use of supporting software applications for carrying out a remote VDR annual performance test.

5. Conclusions

Furuno developed a digital twin of a voyage data recorder (HermAce System) that allows remote monitoring and assistance in installation, commissioning, and maintenance work. APTs can benefit from the HermAce System, as they no longer require personnel on the ship to complete the task.

Following the development of the HermAce System, it was independently verified through (predominantly) a large number of semi-automated software tests, with complementary hardware testing, designed and implemented by AQ Live and the Alan Turing Institute. The requirements for these tests were identified in accordance with Lloyd's Register's assurance framework.

https://doi.org/10.1017/dce.2024.59 Published online by Cambridge University Press

It is noted that APTs using the HermAce System should demonstrate equivalence to (or exceedance of) the benefits of existing approaches using visits by a service engineer so that both safety and economy can. This was considered during the certification of the digital twin solution.

The real-time information and remote support opportunities facilitated by the HermAce System could improve ship operation efficiency and safety.

The scope of applicability of cyber security—IACS E26 and E27—is for vessels signed in contract after July 2024. These vessels should be over 500GT engaged in international voyages, and NAVCOM systems should be resilient in case of cyber-attacks for safety operations on crew and the environment. The AICS E27 requires manufacturers to prove that their products are addressing cyber security risks so that the entire ship meets the requirement of E26.

It is essential to consider cyber security measurements before any remote service. Proving the requirements against the regulations assures that the HermAce gateway can securely conduct a remote Annual Performance test on the VDR.

Data availability statement. The system code and data used to implement the presented work cannot be disclosed because it is not in line with Furuno's intellectual property protection policy.

Acknowledgments. I want to express my sincere gratitude to Furuno Hellas Managing Director Mr. Katemidis for his significant support and insights that helped us complete this project. My heartfelt gratitude also goes to the five other Authors of this work for their hard work and professionalism. Also, I am grateful for my family's patience and understanding over the last 4 years it took to complete this work.

Author contribution. Conceptualization: N.S, D.D, J.M. Methodology: N.S, D.D, J.M, D.D. Data curation: N.S, P.P, D.D. Data visualisation: N.S, P.P, D.D, J.M. Writing original draft: N.S, D.D, J.M. Paper structuring, Review and Corrections: A.M. All authors approved the final submitted draft.

Competing interest. A statement about any financial, professional, contractual, or personal relationships or situations that could be perceived to impact the presentation of the work --- or "None" if none exists.

Ethical standard. The research meets all ethical guidelines, including adherence to the legal requirements of the study country.

References

Assani N, **Matic P**, **Katalinic M** (2022) Ship's Digital Twin—A Review of Modelling Challenges and Applications. Available at: https://www.mdpi.com/2076-3417/12/12/6039.

BSI (2016) BS EN 61162–1:2016: Maritime navigation and radiocommunication equipment and systems – Digital interfaces. Available at: https://www.en-standard.eu/bs-en-61162-1-2016-maritime-navigation-and-radiocommunication-equipment-and-systems-digital-interfaces-single-talker-and-multiple-listeners/.

Chaloner K. Verdinelli I (1995) "Bayesian Experimental Design: A Review." Statist. Sci. *10* (3) 273 – 304, https://doi.org/10.1214/ss/1177009939

Danelec (2024) Access Your VDR Data Anytime, Anywhere. With VDR Remote Services, You Can Boost Safety, Efficiency and Decrease Downtime. Available at: https://www.danelec.com/campaigns/VDR-remote-services.

Danelec (2024) Sperry Marine & Danelec partner to unlock savings creating remote VDR management through Sperry Marine VoyageMaster Connect. Available at: https://www.danelec.com/insights/news/sperry-marine-danelec-partner-to-unlock-savings-creating-remote-vdr-management-through-sperry-marine-voyagemaster-connect/.

Di Francesco D *et al.* (2021) Decision-theoretic inspection planning using imperfect and incomplete data, *Data-Centric Engineering*, *2*, e18. https://doi.org/10.1017/dce.2021.18.

Gausdal A, **Czachorowski K and Solesvik M** (2018) Applying blockchain technology: Evidence from Norwegian companies. *Sustainability*, *10*(6), 1985. https://doi.org/10.3390/su10061985.

Gelman A, **Carlin JBB**, **Stern HSS and Rubin DBB** (2014) *Bayesian Data Analysis* (F. Dominici, J. J. Faraway, M. Tanner, & J. Zidek (eds.); 3rd ed.). Chapman & Hall / CRC. https://doi.org/10.1007/s13398-014-0173-7.2.

Giering J-E and Dyck A (2021) Maritime Digital Twin architecture. Available at: https://www.degruyter.com/document/doi/10.1515/auto-2021-0082/html?lang=en.

Glaessgen E and Stargel D (2012) The Digital Twin Paradigm for Future NASA and U.S. Air Force Vehicles. *In Proceedings of the 53rd AIAA/ASME/ASCE/AHS/ASC Structures*, Structural Dynamics and Materials Conference, Honolulu, HI, USA, 23–26.

International Association of Classification Sociates (IACS) (n.d.) IACS UR E26 and E27 Press Release. Available at: https://iacs.org.uk/news/iacs-ur-e26-and-e27-press-release.

ISO /IEC 27001 (2022) Information Security, Cybersecurity and Privacy Protection. Available at: https://www.iso.org/standard/27001.

ISO /IEC 27001:2013 (2023) Furuno Hellas S.A. Development, operation, and support of the HermAce Remote Monitoring and Support System. Available at: https://furunoeur.sharepoint.com/:b:/r/sites/FHLIntranet/ISO%20Documents/ISO%2027001_2013%20CERTIFICATE_2021.PDF?csf=1&web=1&e=WkWc2a.

Japan Radio Co. Ltd (JRC) (n.d.) Remote Maintenance System (RMS). Available at: https://www.jrc.co.jp/en/product/rms.

Kongsberg (2025) Vessel Insight Marketplace. Available at: https://kognifai.com/.

Lloyds Register (September 2018) Ship Right Design and Construction Procedure for assignment of digital descriptive notes for autonomous and remote access ships. Available at: https://www.lr.org/en/shipright-procedures/.

Marine S. SMART SUPPORT. Available at: https://www.sperrymarine.com/smart-support.

Microsoft Azure (July 2023) Security Standards for Azure IoT Edge. Available at: https://learn.microsoft.com/en-us/azure/iot-edge/security?view=iotedge-1.4.

PwC Penetration Test (2023) Furuno Greece SA engaged PricewaterhouseCoopers ("PwC") to conduct a Penetration Test performed during March & April 2023.

Stavrou N (2020) Apparatus and method for remote monitoring. European Patent Application RP 3 993 345 A1. Available at: https://patents.google.com/patent/EP3993345A1/.

Telecommunication Industry Association (TIA) (2010) TR-50 | M2M – Smart Device Communications. Available at: https://standards.tiaonline.org/all-standards/committees/tr-50.

User Acceptance Test (2023) Furuno Hellas S.A. User Acceptance Test and identification, reporting, and fixing of bugs in the software/applications, keeping records/documents and process.

Verification Procedure (2023) Furuno Hellas S.A. verification of the core functionality of any newly developed software for the HermAce products/applications.

Cite this article: Stavrou N, Morelos J, Di Francesco D, Meliones A, Progias P and Duncan D (2025). Development, verification, and certification of a digital twin for a voyage data recorder. *Data-Centric Engineering*, 6, e14. doi:10.1017/dce.2024.59