Scuola Politecnica & Facoltà di Ingegneria

Laurea Magistrale in Ingegneria Strategica
International MSc in Engineering Technology for Strategy and Security
of Genoa University

SUPPORT FOR SHIPS ON NAVIGATION SOFTWARE AND IT NETWORKS

Advisor: Professor Marco Gotelli

Author
Adison Gomes

In partial fulfillment of the requirements for the degree of
Master of Science in Engineering Technology
for Strategy and Security

July 2026

Acknowledgements

Six months ago I walked into CAIM Sea in Genova knowing the theory of maritime navigation systems and very little about what actually keeps them running on a real ship. This thesis is the result of everyone who patiently helped close that gap, and I want to take a moment to thank them properly.

My first thanks go to my advisor, Professor Marco Gotelli, for his guidance throughout this internship and for helping me turn six months of scattered daily cases into a thesis that actually holds together.

I am just as grateful to my colleagues and supervisors at CAIM Sea, who welcomed me from day one, answered my endless questions without ever making me feel like I was asking too many, and trusted me with real vessels and real problems far sooner than I expected. What I learned working alongside you is not something any textbook could have taught me.

I would also like to thank the STRATEGOS programme and the Università degli Studi di Genova for building a Master's degree that prepared me to think seriously about maritime strategy and security, and that made a placement like this one possible in the first place.

Finally, thank you to my family and friends, for putting up with the weeks when this thesis was the only thing I could talk about, and for supporting me long before this internship ever began.

This thesis would not exist without all of you.

Abstract

This thesis examines the operational realities of maritime navigation software support and IT network management through a six-month professional placement at CAIM Sea, Genova, Italy. Drawing on daily support casework, system logs, internal documentation and direct coordination with the United Kingdom Hydrographic Office (UKHO), it analyses the NaviGate platform ecosystem, the Admiralty Vector Chart Service (AVCS) data supply chain and the troubleshooting methodologies required to maintain vessel compliance and operational readiness.

The principal findings are that platform reliability depends less on the application software itself than on the surrounding infrastructure: nGateway service configuration, Windows TLS settings, firewall rules and NaviServer account setup, which together account for the majority of support cases encountered. The diagnostic methodology required for effective resolution follows a structured evidence-based approach, reading the communications log to distinguish timeout errors from TLS handshake failures from authentication rejections, then testing hypotheses systematically rather than applying fixes at random. The AVCS chart management chain, from the UKHO server through NaviServer to the vessel, is vulnerable to synchronisation failures at each tier and maintaining consistency requires disciplined workflow practices that are not always followed under operational pressure.

These findings indicate that maritime IT support at this level requires not only technical knowledge of specific systems but a diagnostic reasoning discipline and communication calibration skill that can only develop through sustained operational engagement. The thesis offers recommendations for integrating industry-standard navigation tools into the STRATEGOS curriculum and for improving the preparedness of future interns entering maritime software support roles.

Keywords: maritime navigation software, ECDIS, AVCS, UKHO, TLS 1.2, nGateway, NaviServer, IT support, voyage planning, ISO 9001

Table of Contents

List of Figures

List of Tables

Chapter 1: Introduction

1.1 Background and Context

The United Kingdom Hydrographic Office stands at the centre of the global maritime navigation data infrastructure. Its products, including Electronic Navigational Charts distributed through the Admiralty Vector Chart Service, Admiralty Digital Publications and electronic Nautical Publications, are required for compliance with the International Convention for the Safety of Life at Sea [10] and are used on tens of thousands of commercial vessels worldwide. The UKHO provides the authoritative, legally recognised navigational record on which the safety of navigation depends [17].

Security is integral to the UKHO data architecture. Encrypted communication protocols including TLS 1.2 [12], digital signatures and licence control systems ensure that every chart cell displayed on an ECDIS can be verified as genuine and unaltered [14]. In an era of expanding maritime cyber threats, addressed directly by the IMO Guidelines on Maritime Cyber Risk Management [11], this security infrastructure is central to operations. A misconfigured TLS setting on a vessel PC, as the internship repeatedly demonstrated, can halt the entire chart update chain.

The Master's programme in Engineering Technology for Strategy and Security at the Università degli Studi di Genova requires a six-month professional internship as a mandatory component of the degree. The internship described in this thesis was undertaken at CAIM Sea, the maritime software and chart services division of the CAIM Group, located in Genova. The placement provided direct involvement in the support of vessels using the NaviGate navigation software platform and the full suite of Admiralty publication and chart services.

1.2 Objectives of the Internship

The primary objective of this internship was to bridge the gap between theoretical maritime engineering education and the operational realities of professional maritime IT support. This required engagement with the technical systems themselves, including their architecture, configuration requirements, failure modes, and diagnostic procedures, alongside the professional disciplines of clear communication, systematic problem-solving under pressure, and accurate operational record-keeping in a live support environment.

The specific learning objectives covered five areas. Safety in maritime navigation software support is an operational constant rather than a procedural abstraction. Every chart update applied, every permit renewed, and every communication failure resolved ultimately serves to keep vessels navigating on accurate, current, verified data. Environmental compliance was encountered as a functional feature embedded in the NaviGate voyage planning workflow, with MARPOL requirements, emission control zone monitoring, and EU MRV reporting integrated as designed system components rather than separate administrative obligations. Technical support skills such as reading communications logs, diagnosing TLS handshake failures, and troubleshooting S63 decryption errors could only be developed through real cases and the discipline of working methodically to resolution regardless of how unfamiliar the problem appeared. Regulatory awareness developed through direct operational engagement, as the IMO conventions, SOLAS carriage requirements, and EU MRV regulation became the context within which every support decision was made rather than background knowledge held separately from the work.

Cybersecurity principles from the BIMCO guidelines and NIST TLS standards were applied in practice through network configuration, registry-level diagnostics, and the daily operational rationale for the server enforcing TLS 1.2 as a minimum protocol standard..

1.3 Achievements

The work covered the following operational domains: NaviGate installation, activation and configuration support including nGateway communication management and TLS configuration; AVCS chart permit management through NaviServer including Holdings management, Active Folio maintenance and permit synchronisation with the UKHO server [17]; Admiralty Digital Publications lifecycle support [15]; electronic Nautical Publication reader management [16]; GPS and AIS integration via the ; NaviServer and NaviFleet account administration [2]; voyage plan support including UKC calculation review; and daily incident response through the Zoho Desk ticket management platform [18].

Each of these domains was encountered as part of a connected operational environment. A firewall configuration problem is simultaneously a chart update problem and a compliance problem. A machine identifier mismatch in the AENP viewer is simultaneously a publication access problem and potentially a vessel departure delay. Understanding those connections, tracing a symptom to its cause across system boundaries, was the core diagnostic skill the placement developed.

1.4 Internship Placement Details

Company: CAIM Sea, Genova, Italy

Role: Support for Ships on Navigation Software and IT Networks

Mode: On-site and Remote

Duration: May 2025 to November 2025

Key Focus: Navigation software support, NaviServer administration, AVCS and publication management, GPS and AIS configuration, system analysis and order approval

The placement operated in a combined on-site and remote format. On-site work permitted direct collaboration with experienced colleagues and immediate access to institutional knowledge. Remote work required clear, written communication as the sole medium for technical guidance, developing the discipline of writing support responses that were unambiguous and actionable for vessel officers reading them under time pressure on a working bridge.

1.5 Methodology for Report Compilation

The content of this thesis is grounded in practical tasks completed during the six-month internship and the documentation maintained throughout the placement. Monthly log submissions to the university portal provided a structured record of activities and reflections. Internal technical documentation authored for CAIM Sea, including support guides, troubleshooting procedures and case summaries, provided a detailed operational record.

Three sources informed the thesis. First, systematic technical analysis of the NaviGate ecosystem through repeated direct engagement under operational conditions [3]. Second, operational application of the platform and associated Admiralty publication services in a live support environment. Third, direct professional communication with the UKHO through the support workflow, anchoring the technical work to the hydrographic data standards and licensing frameworks that govern chart distribution [17].

1.6 Structure of the Report

Chapter 2 describes the company context and operational setting. Chapter 3 covers the tools and platforms encountered during the placement, drawing on the official NaviGate User Manual [3] and the IT/ICT Department Reference Guide [5]. Chapter 4 documents the technical issues and troubleshooting approaches developed. Chapter 5 addresses operations and incident monitoring. Chapter 6 covers documentation and professional communication. Chapter 7 presents the skills gained during the placement. Chapter 8 provides reflections grounded in specific cases. Chapter 9 offers conclusions and recommendations.

1.7 Internship Learning Goals and Activities

The following table, presented as submitted to the University of Genova as part of the internship documentation, summarises the key learning objectives of the placement, the tools applied and the practical activities undertaken across the six-month period. Each objective maps directly to a competency area of the Master's programme in Engineering Technology for Strategy and Security.

Table 1: Internship Learning Goals, Tools and Activities

Learning Goal	Tools Used	Tasks and Activities
Communication skills	Zoho Desk, Email	Managing daily ticket conversations with vessel officers and shore offices, coordinating with UKHO, escalating issues across departments
Software management	NaviGate, System Manager, NaviServer	Installing and configuring maritime platforms, managing vessel accounts, monitoring system status, applying software updates
Vessel collaboration	System Manager, NaviServer	Remote support for onboard crew, identifying vessel-side issues, checking connectivity and system health remotely
GPS and navigation	NaviGate, AVCS, ECDIS,	GPS and AIS integration using NMEA 0183 protocol [8], verifying chart permits and holdings, supporting ECDIS configuration
IT and system support	Zoho Desk, NaviServer, nGateway	First-line user support for vessels and shore offices, hardware and software troubleshooting, network connectivity diagnosis
Troubleshooting	nGateway logs, Firewall, Registry, TLS	Resolving firewall blocks, fixing stuck chart updates, repairing communication failures, reading system logs, diagnosing TLS and certificate errors [14]
Route and chart analysis	NaviGate, UKHO, AVCS, NaviServer	Analysing voyage routes, verifying ECA and SECA compliance, checking chart validity and permit status, supporting voyage plan generation
Documentation	Zoho Desk, Internal reports	Writing clear and actionable ticket summaries, maintaining complete case records, producing technical reference documents

Overview of the six-month internship phases at CAIM Sea, (Source: CAIM Sea)

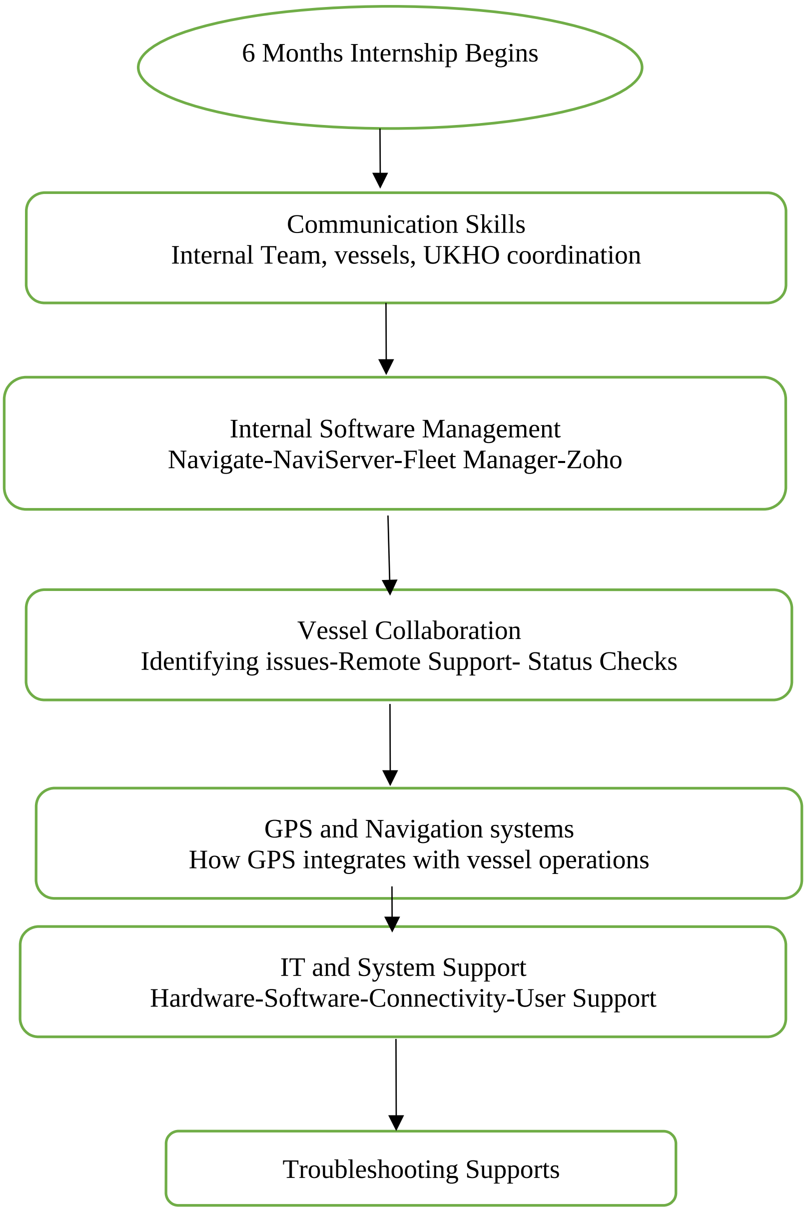

Figure 1: Overview of the six-month internship phases at CAIM Sea, from initial onboarding in May through to independent case handling by November 2025 (Source: CAIM Sea)

Chapter 2: Company Overview

CAIM was established in Genova on 14 August 1945, founded by Maestro Giuseppe Messina to create employment for veterans returning from the Second World War [4]. Eighty years later, the company remains headquartered in Genova with international offices in Miami and Singapore. It holds ISO 9001 quality management certification and RINA accreditation.

The company's core product is NaviGate, a voyage planning and vessel management platform used on commercial vessels worldwide [3]. NaviFleet and NaviDock extend the platform to shore-based fleet management. CAIM also operates as an authorised distributor of official nautical charts and publications from the UKHO [17].

The cybersecurity division develops NGBox and NGLink, hardware products that create encrypted communication channels between the ECDIS and shore-based servers, responding to the IMO maritime cyber risk management guidelines [11] and BIMCO cybersecurity standards [1]. The broader CAIM Group covers nautical signage, safety equipment and navigation aid manufacturing.

2.1 Why CAIM Selected This Candidate

CAIM Sea selected me for this placement based on a combination of academic preparation and professional background that matched the technical requirements of their support operations. My enrolment in the STRATEGOS Master's programme provided a strong foundation in maritime strategy and security maritime cybersecurity frameworks [11] and management systems. Beyond the academic programme, I brought practical IT experience from my previous role as a network engineer, where I worked with TCP/IP networking, firewall ,Windows server administration and troubleshooting methodologies that transferred directly to the maritime software support environment. My Bachelor's degree in Computer Engineering provided the underlying technical knowledge in operating systems, network protocols and system architecture that proved essential when diagnosing TLS handshake failures [12], configuring nGateway communication parameters [5] and resolving Windows registry issues [13] during the placement.

Chapter 3: Tools and Platforms

This chapter provides a systematic account of every software platform, technical system and operational tool encountered during the internship. The objective is not merely to describe these tools but to explain how they function in relation to each other, what their operational significance is and what working with them in a live support environment reveals that product documentation alone cannot convey.

3.1 NaviGate Navigation Software

NaviGate is an advanced software tool for the bridge, serving as a professional platform for voyage planning and monitoring [3]. The suite consists of three applications: NaviGate.exe (the main program with graphical interface), nGateway.exe (the communication gateway running as a Windows service), and nGatewayManager.exe (the administration tool for gateway settings). The platform is a Software-as-a-Service (SaaS) application deployed for voyage planning, ECDIS integration, chart management, environmental compliance monitoring and fleet oversight through its shore-based counterparts NaviServer and NaviFleet.

the platform offers a broad set of capabilities: it reduces voyage planning time, enables sharing of voyage plans via a web-based application, updates nautical charts and publications for the operational area, offers auto-routing, provides weather, NAVAREA, T and P and piracy data, contains a database of international environmental and flag state regulations covering ECA, SECA, PSSA and MARPOL areas, includes risk assessment and route optimisation tools, operates either in standalone mode or integrated with ECDIS, is compatible with Admiralty PAYS (Pay As You Sail), and is available as a SaaS subscription.

The platform consists of three applications: NaviGate.exe, the main program with a graphical user interface; nGateway.exe, the communication gateway running continuously as a Windows service; and nGatewayManager.exe, the administration tool for configuring gateway settings [5]. This three-component architecture has direct implications for support work. The nGateway service operates independently of the main application, meaning the platform can appear fully functional while the communication service has stopped. This architectural separation is the single most important diagnostic insight for communication support.

Working with the platform in a live support context established a foundational understanding that documentation does not prepare one for: the platform's reliability depends on the infrastructure that surrounds it. A correctly installed instance can be rendered non-functional by a stopped nGateway service, a misconfigured TLS setting [12], a firewall rule blocking port 443, or an Active Folio in NaviServer that does not reflect the vessel's actual trading area.

3.2 IT and ICT Infrastructure Requirements

The navigation applications, including the platform, Admiralty Digital Publications [15], and electronic Nautical Publications [16], are developed exclusively for Microsoft Windows [5]. They are not natively developed for Apple macOS or iOS devices and installation and operation on Apple devices is not supported. This is not a commercial preference but an engineering constraint: these systems rely on Windows-specific components including the .NET Framework 4.8 or higher for application runtime, the Windows Schannel security provider for TLS implementation [13], and the Windows registry for configuration storage.

3.2.1 Dedicated Hardware Requirements

According to the IT/ICT Reference Guide [5], PCs hosting these applications must be dedicated exclusively to navigation functions. These machines must not be used for general office tasks, email, web browsing, or any other purposes. The technical rationale for this requirement reflects accumulated operational experience: shared workstations introduce resource contention that degrades performance at critical moments; cloud synchronisation agents interfere with the file system locations where navigation data is stored; multi-purpose machines carry security exposure that systems handling encrypted hydrographic data should not be subjected to. These are not theoretical risks. They generate actual support calls and the resolution invariably involves returning the machine to the single-purpose configuration for which the software was designed.

Table 3: Not Supported Hardware Configurations (Source: [5])

Configuration	Reason
Thin Clients	Insufficient local processing power and storage; network dependency issues
Virtual Machines (VMs)	Performance unpredictability; resource contention; licensing concerns
Servers	Not designed for server environments; requires dedicated workstation
Shared/Multi-purpose PCs	Resource conflicts; potential data corruption; security risks

Network connectivity must be provided through a dedicated or segmented LAN Ethernet connection [5]. WiFi is technically functional but carries an unacceptable risk of connectivity interruption during chart update downloads, permit installations, or activation sequences. Any of these, if interrupted mid-process, can produce a corrupted installation state that requires manual recovery.

Cloud synchronisation services must be fully excluded from all directories associated with the navigation software. This includes software installation folders, data archive folders, the Desktop folder (full desktop synchronisation must be disabled), and the Documents folder if any navigation software stores data there [5]. Affected services include Microsoft OneDrive, DropBox, Google Drive, iCloud Drive, Box, Nextcloud, Syncthing and any other file synchronisation software. The safest configuration, consistently recommended and consistently effective, is to install no cloud synchronisation agent on a dedicated navigation PC at all.

3.2.2 nGateway Architecture Overview

The NaviGate suite operates as a client-service ecosystem deployed locally on the vessel's bridge PCs [3]. The architecture consists of three components working together:

NaviGate.exe is a 32-bit Windows Forms desktop application providing the graphical interface for bridge officers. It handles route planning, chart display, weather overlay and compliance logging.

nGateway.exe is a background Windows Service running continuously on the workstation. It serves as a communications bridge between the NaviGate client and the shore-based servers at maritimegate.net. When a user initiates an update request within NaviGate, the client establishes a local Windows Communication Foundation (WCF) connection to send the request to the nGateway service. The service then packages the request and communicates with the shore servers over HTTPS port 443 [5]. It handles the network handshakes, downloads the response and forwards it back into the NaviGate application. If the vessel lacks internet, the system falls back to Offline Mode where nGateway compiles encrypted .ngte zip files for satellite email exchange.

nGatewayManager.exe is the administrative utility used by shipboard IT or navigators to adjust communication protocols, connection settings and network parameters.

For vessel tracking, nGateway connects directly to the ship's NMEA instruments via serial COM ports or LAN connections [8]. It parses incoming NMEA strings to capture real-time GPS coordinates and uploads them to the shore server at approximately 30-second intervals for fleet tracking through NaviServer [2].

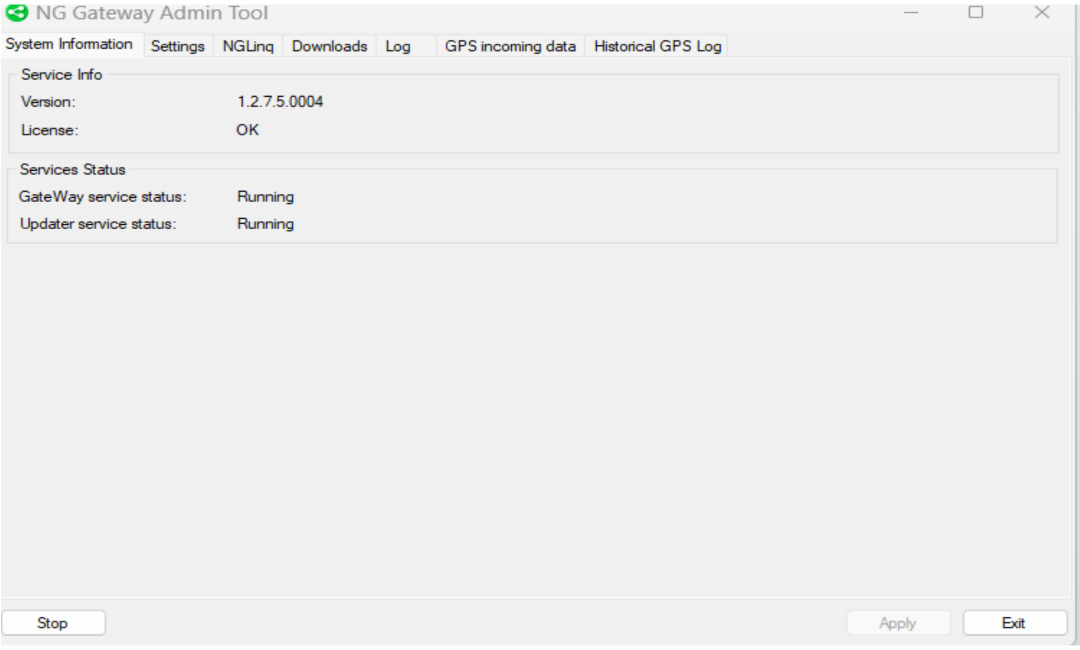

Figure 2: NaviGate network and system configuration showing the nGateway communication flow between vessel and shore (Source: CAIM Sea)

3.2.3 NaviGate Network and Firewall Configuration

All server communication is handled exclusively by the nGateway.exe Windows service [3]. This service must be running at all times for the platform to exchange any data with the server. The primary communication channel uses HTTPS on port 443 to maritimegate.net at the fixed IP address 52.30.174.254 [5]. An HTTP fallback on port 80 is available and configurable through the nGateway Admin Tool, but HTTP transmits data in plain text without encryption and should never be used as the primary communication method.

TLS 1.2 must be enabled and correctly configured at the Windows operating system level before the nGateway service will complete a connection to the server [14]. The server enforces this requirement at the protocol negotiation level. It will not accept connections over TLS 1.0, TLS 1.1, SSL 3.0, or SSL 2.0 [12]. On Windows 10 and 11 this requirement is met by default. On Windows 7 it requires deliberate configuration: Service Pack 1 must be installed, the KB3140245 cumulative update must be applied and TLS 1.2 must be explicitly enabled through the Advanced settings in Internet Options (Microsoft, 2023; [5]).

Table 4: Windows System Requirements for NaviGate Installation (Source: [5])

Component	Requirement
Operating System	Windows 7 SP1 (minimum), Windows 10/11 recommended
Processor	Intel quad-core i5 or higher
RAM	8 GB minimum
Display Resolution	1360 x 768 pixels or higher
Disk Space	250 MB (applications) + 5 GB minimum (data archive)
.NET Framework	4.8 or higher (mandatory)
TLS Protocol	TLS 1.2 (must be enabled)
User Privileges	Full Administrator rights (mandatory)

3.2.4 Admiralty Digital Publications Network Configuration

ADP requires internet access for both initial product activation and ongoing weekly updates [15]. The firewall whitelisting requirements are: IP address 137.135.243.254 on ports 80 and 443 for the update download server; domain www.admiralty.co.uk; the activation endpoint adpactivation.ukho.gov.uk at IP address 62.172.108.45 on ports 20 and 21; and sectigo.com for SSL certificate chain validation [5]. All of these addresses must be accessible. A common misconfiguration that permits update downloads but blocks the activation endpoint will prevent fresh installations from becoming operational.

3.2.5 e-Navigator and eNP Network Configuration

The e-Navigator application, which manages UKHO digital product licences on the vessel PC, requires access to IP address 62.172.108.10 on ports 80 and 443 via the domain enavigator.ukho.gov.uk [16]. Electronic Nautical Publications use the same domain and IP address but additionally require FTP access on port 21 in passive mode to ftp://ukho.gov.uk and access to a second IP address, 137.135.243.254, for file download operations [5]. Both IP addresses must be whitelisted. The failure to whitelist both is one of the most consistently encountered network configuration errors in eNP support.

3.2.6 Quick Reference: Firewall Whitelisting

Table 2: Firewall Whitelisting Requirements (Source: [5])

System	IP Address	Ports	Domain
NaviGate	52.30.174.254	443 (primary), 80	maritimegate.net
ADP Updates	137.135.243.254	80, 443	www.admiralty.co.uk
ADP Activation	62.172.108.45	20, 21	adpactivation.ukho.gov.uk
e-Navigator	62.172.108.10	80, 443	enavigator.ukho.gov.uk
eNP	62.172.108.10 + 137.135.243.254	80, 443, 21 (FTP)	enavigator.ukho.gov.uk + ftp://ukho.gov.uk

3.3 NaviGate User Interface: Top Menu Bar

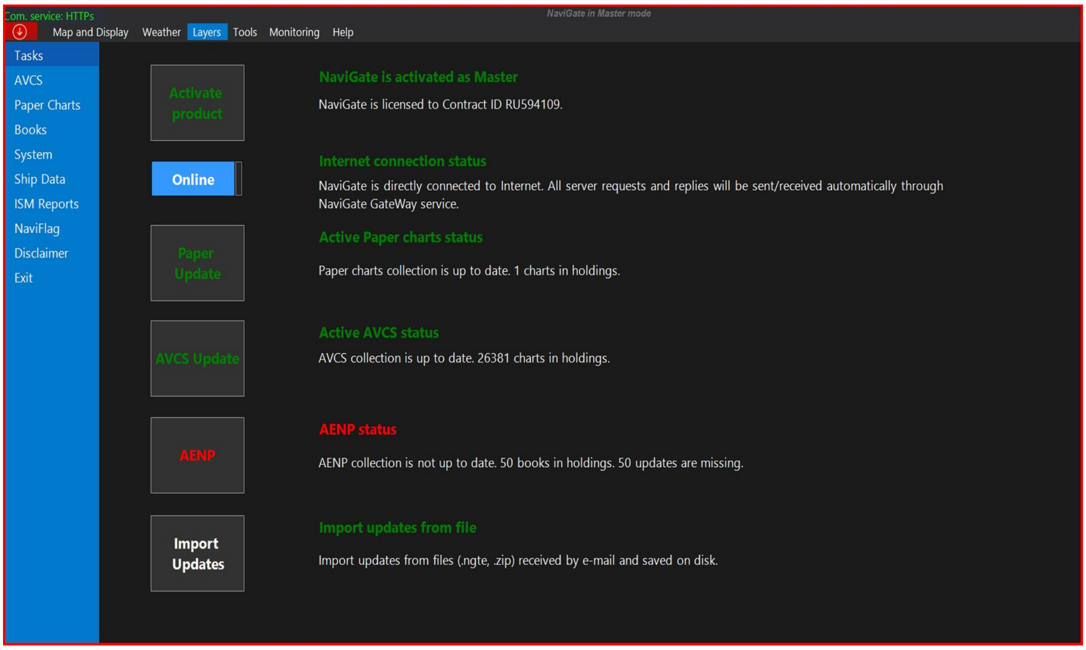

Figure 3: NaviGate top menu bar showing the Main Status button and primary function sections (Source: CAIM Sea)

The Main Status button at the far left of the toolbar is the system's primary health indicator [3]. It displays green when all publication types covered by the vessel's subscription are current and turns red when one or more require attention. Pressing the button opens the Tasks menu, which identifies specifically which publication type is outstanding and provides access to activation, communication mode switching and manual update import functions. The colour state of this button is typically the first thing asked about when a vessel contacts support, as it immediately indicates whether the system believes it is current, which is the starting point for any diagnostic conversation.

The remaining sections of the top menu bar each serve a specific operational domain. The AVCS section manages permit exports for the ECDIS, weekly update mode settings (for all holdings or active folio only), full AIO layer exchange set export and optional NGStick USB detection. Paper Charts covers NTM corrections, chart downloads and publication compliance reports. Books manages the paper publications catalogue and weekly update cycle. System handles software version control, full catalogue recovery, configuration backup and restore and licence settings. Ship Data stores vessel dimensions, draft, block coefficient and default route parameters that underpin UKC calculations and performance modelling throughout the platform. ISM Reports generates compliance reports for AVCS holdings, paper chart currency and publication status. Flag States and the NaviFlag module provide access to the international regulatory document database. Map and Display controls chart installation and display settings including safety depth and safety contour thresholds. Weather manages forecast file downloads and display. Layers enables the full suite of information overlays including T and P notices, NAVAREA warnings, TotalTide integration, piracy data, environmental zones and custom boundary files. Tools consolidates the route checking, risk assessment, voyage planning, ERBL navigation aid, time zone display, position finder and port search functions. Monitoring provides access to MRV emission reporting [7], parametric roll risk evaluation, vessel position centring from GPS and live sensor data from connected instruments.

3.4 Communication Modes: Online and Offline

One of the more practically important design choices in the architecture is the explicit support for two distinct communication modes, reflecting an honest acknowledgment that not all vessels have reliable, affordable internet access at all times [3].

In Online mode, the nGateway service communicates directly with the server over the vessel's internet connection. This is the standard mode for vessels with consistent satellite connectivity and represents the simplest workflow. Data requests are generated by the platform, transmitted by nGateway and responses are received and processed automatically without manual intervention.

Offline mode is designed for vessels where direct internet access to the server is unavailable, restricted by satellite plan limitations, or unreliable in the operating region. In Offline mode, all data exchange takes place through email [3]. When the platform needs to request an update, transmit holdings data, or send an Active Folio, nGateway packages the request into an encrypted zip file and prompts the vessel officer to send it manually from an email-capable device to updates@maritimegate.net with "Naviserver" as the subject. The server processes the request and replies with one or more encrypted .ngte format response files that are then imported back through the Import Updates function in the Tasks menu.

The sequential numbering system used in Offline mode assigns a unique sequential number to each request. The server mirrors this number in its reply, allowing the operator to match each response file to the request that generated it, a critical feature when multiple requests are in transit simultaneously [3]. If the volume of response data exceeds the email attachment size limit configured on the server, the reply is automatically split across multiple messages, each labelled with its sequential position and the total number of parts expected. All parts must be received, saved to a local folder and imported as a batch before the update is considered complete.

Supporting vessels through the Offline mode workflow became one of the more regularly recurring tasks of the internship, particularly for vessels operating in high-latitude regions, remote ocean areas, or on routes where satellite bandwidth allocation is managed conservatively. Understanding the distinction between Online and Offline mode and recognising the symptoms that indicate a mode mismatch between the vessel's actual connectivity and the mode configured in nGateway, was one of the first practical diagnostic skills developed during the placement.

3.5 Software Activation and Backup

Activating the platform establishes a verified link between the specific software installation on the vessel PC and the vessel's account in NaviServer, using a Contract ID and Activation Code provided by the distributor [3]. Once activated, the installation is registered on the server against that vessel and the server can track its software version, communication status and holdings update history. The activation process runs through the Tasks menu and is compatible with both Online and Offline communication modes.

Each activation code is machine-specific. It is tied to the hardware identity of the PC on which it is activated. A hardware replacement, a significant component change, or even certain Windows updates can alter the machine identity sufficiently to invalidate the existing activation, requiring reactivation through the distributor after the old machine registration is cleared on the server. This is one of the most common support escalations encountered during the internship. For example, in late August 2025, three vessels reported activation failures within the same week following unplanned hardware replacements at different ports.

Where two installations exist on the same vessel, one primary and one backup as is standard practice on many commercial vessels, one operates as Master and one as Slave [3]. Only the Master station reports AVCS holdings data, Active Folio status and position updates to the server. The Slave station uses the same chart data and is kept synchronised but does not transmit to the server. If the Master station fails, the Slave must be manually promoted to Master through the System settings before it begins fulfilling the server reporting function. This transition is not automatic and must be performed explicitly to maintain the vessel's official holdings record.

The backup and restore function in the System menu provides the mechanism for protecting the vessel's configuration and enabling rapid recovery [3]. The backup covers settings, subscriptions, catalogue data and the ship model. It runs in the background without interrupting normal navigation operations and saves to a NaviGate_Backup folder that can be copied to a USB drive and transferred to the secondary machine. Restoring from backup on the secondary machine is accomplished by pressing "Activate as Backup Station," which loads the configuration and sets the machine to Slave mode. After any fresh installation or recovery, the Recovery function in the System menu must be used to download the current full catalogues, followed by Check for Updates to confirm the system is fully current.

3.6 Route Management

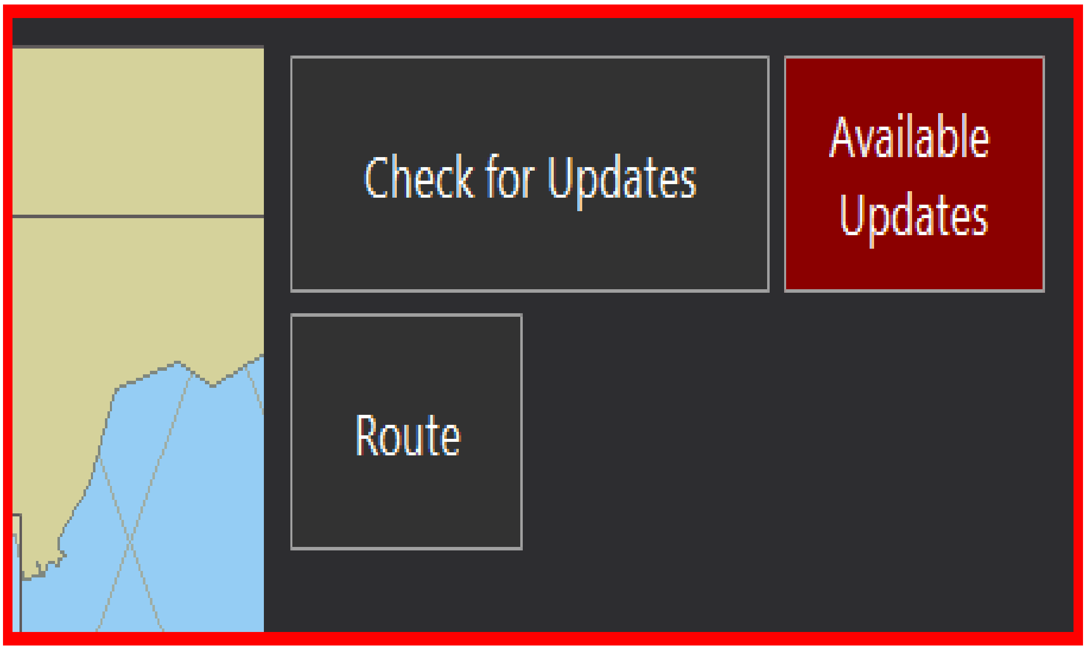

Figure 4: Route Management panel showing route archive list and controls (Source: CAIM Sea)

The Route Management panel is the operational centre for all passage planning activity in the platform [3]. It is accessed through the Route button at the top right of the chart display and presents the complete route archive with search functionality, creation and editing tools and all import, export and transmission functions in a unified interface.

Existing routes in the archive can be loaded onto the chart display by double clicking the route name. The search function allows specific routes to be located efficiently within a large archive, which is practically important on vessels that have accumulated extensive route libraries across multiple voyage seasons. New routes are created using the built-in editor, which allows waypoints to be plotted directly on the chart at geographic positions.

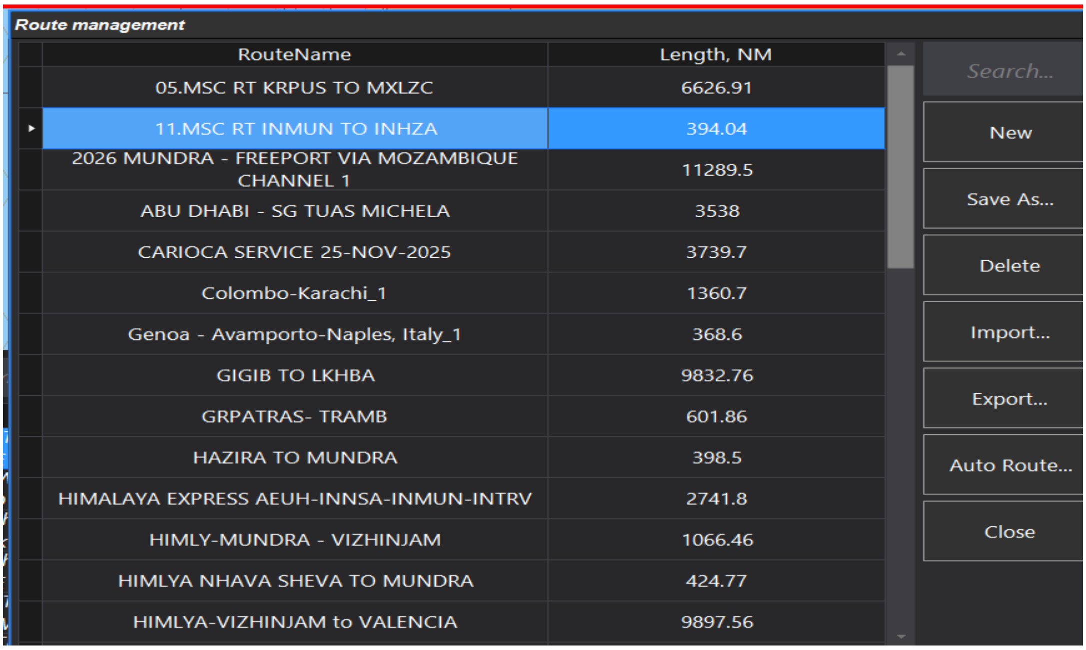

Figure 5: Route Management panel showing complete route list (Source: CAIM Sea)

Import and Export functions provide compatibility with the ECDIS route file formats used across the range of navigation systems found on different vessel types. The batch import function, which allows multiple route files to be selected simultaneously using the Shift key, provides a practical efficiency when transferring large route libraries from an ECDIS or external source, a task that arises regularly during vessel onboarding or system migration.

The Send function is the connection between route management and the NaviServer shore platform [2]. Routes can be transmitted in two modes: as an Active Route, which flags the route as the current live passage, displays it in real time on the NaviServer online map and allows shore-based management to track the vessel's planned track continuously; or as a non-active route, which stores the route securely on the server for review and approval without displaying it on the live map. This distinction has operational and compliance significance, as it enables pre-departure route approval by the shore office without prematurely committing the active route to the server, supporting the voyage oversight requirements of modern ISM management frameworks.

3.6.1 Auto Route and Route Editing

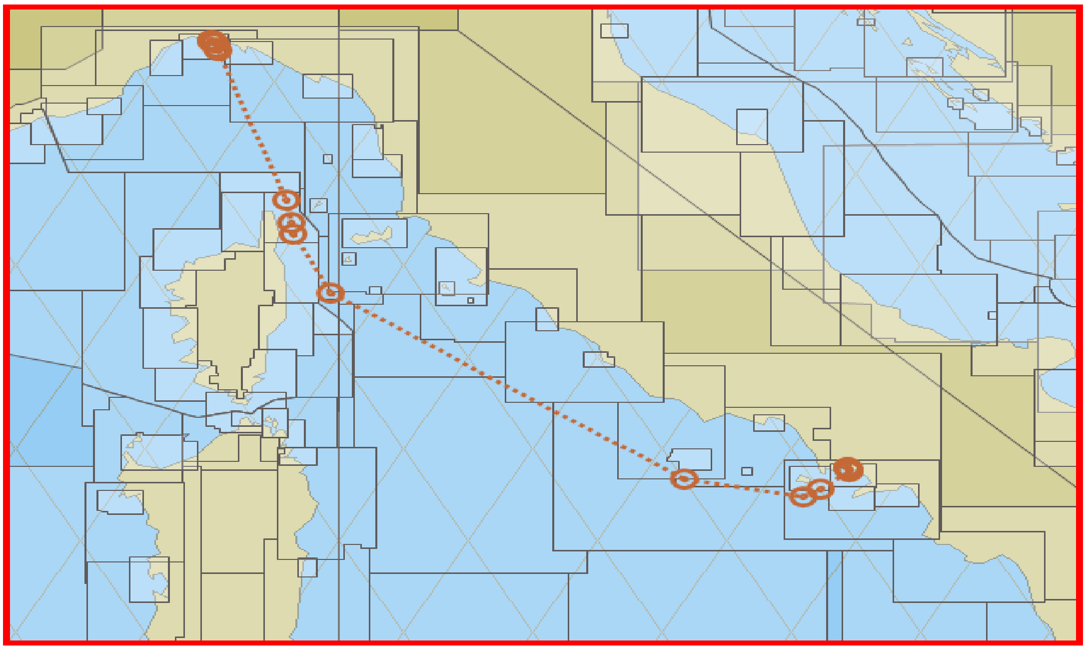

Figure 6: Auto Route function generating a route between two ports (Source: CAIM Sea)

The Auto Route function generates a complete route automatically between a specified departure and arrival port, with configurable constraints that allow or restrict passage through defined channels and straits [3]. The waypoints generated by this function are calculated by an external server on a subscription basis. Auto Route should be used judiciously and only when genuinely needed, as each calculation incurs a charge.

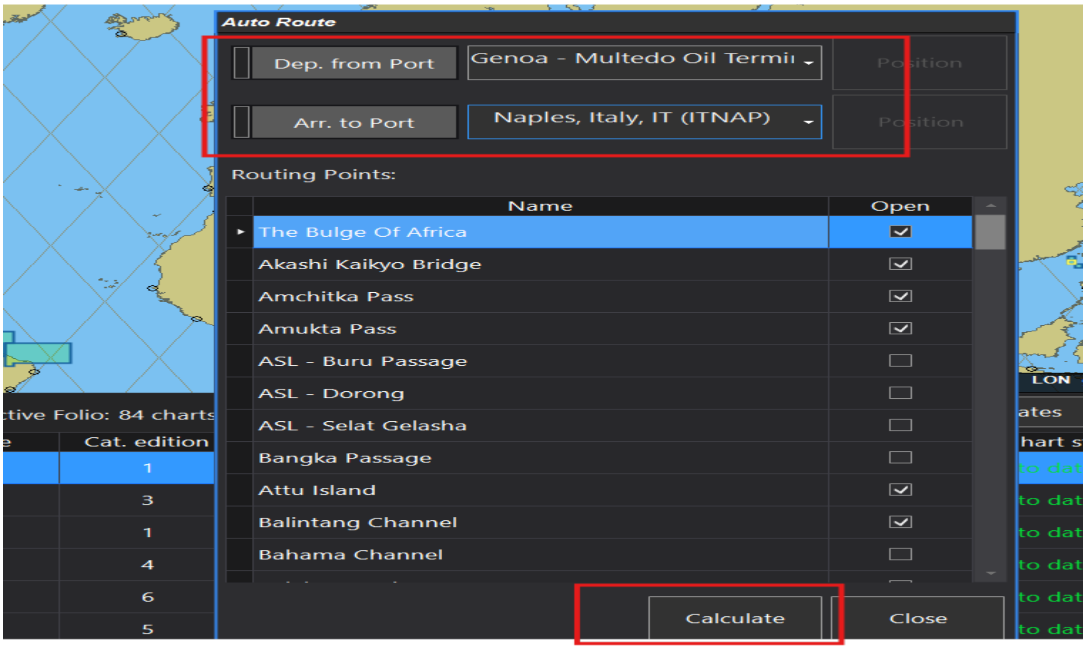

Figure 7: Graphical route editing with waypoint drag adjustment (Source: CAIM Sea)

Once a route is loaded it can be edited through two complementary methods. The graphical editor allows waypoints to be dragged to new positions directly on the chart, with individual waypoints deletable, insertable, or appendable through the dedicated toolbar buttons. The Route Plan table at the bottom of the screen provides numerical precision, allowing direct editing of waypoint names, types, speeds, Stbd and Port cross-track widths and pilot designations for legs that will be navigated under pilotage [3].

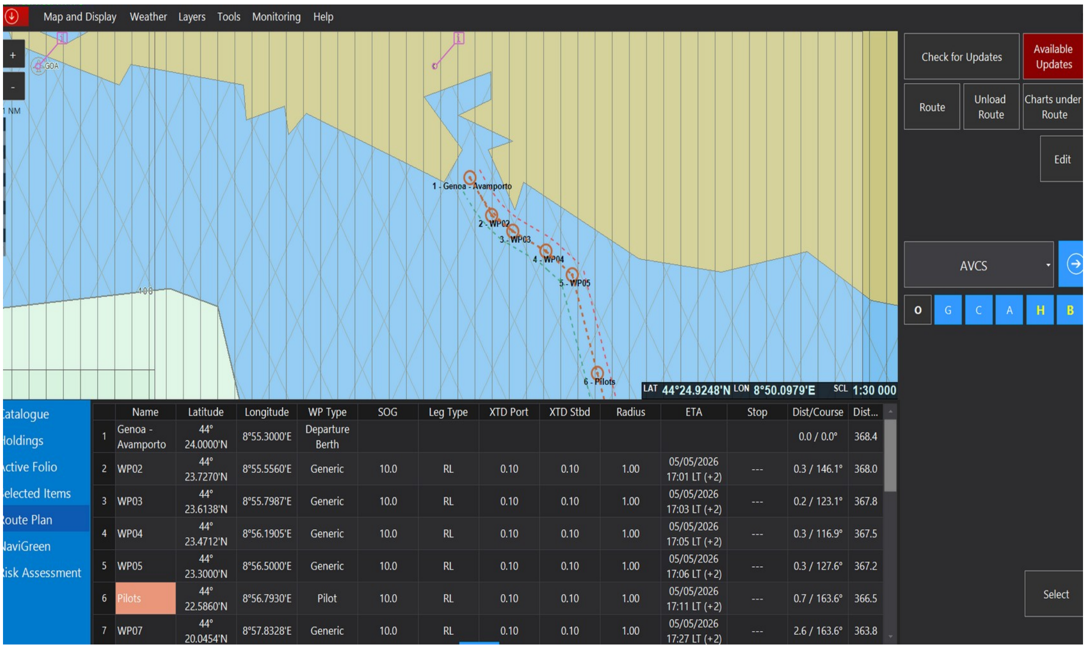

Figure 8: Route Plan table with editable waypoint parameters (Source: CAIM Sea)

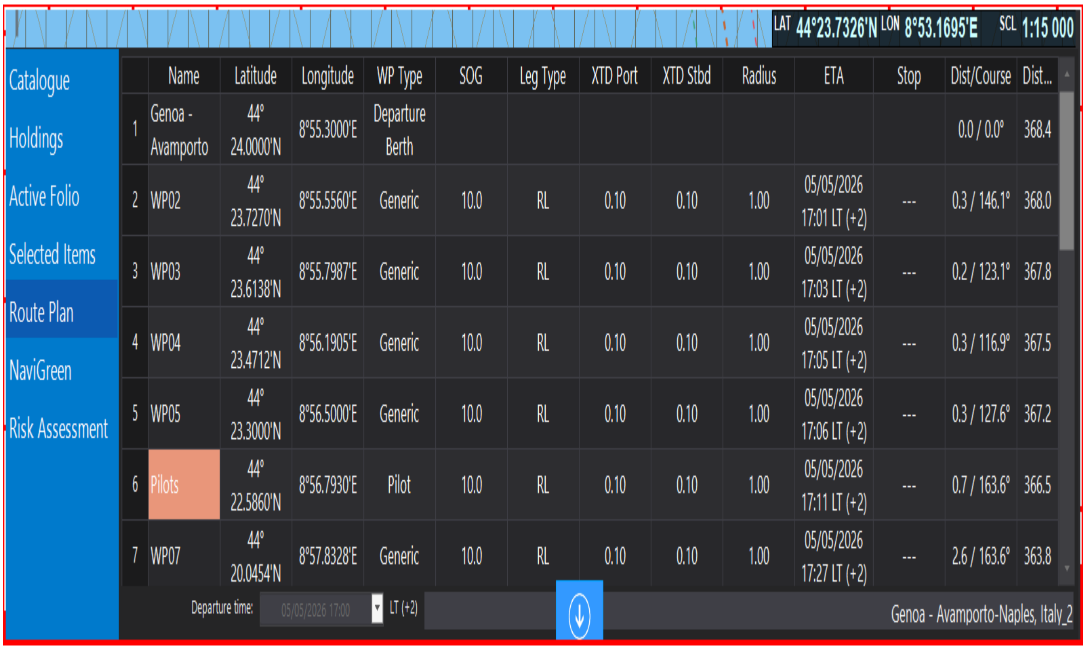

Figure 9: Multi-selection in the Route Plan table for simultaneous parameter adjustment across multiple waypoints (Source: CAIM Sea)

The multi-selection capability in the Route Plan table is a practical efficiency for routes with many waypoints. Clicking the first row, holding Shift and clicking the last row of the desired selection, then modifying a parameter such as speed over ground while holding Shift, applies the change uniformly across all selected waypoints when the Shift key is released. This eliminates the repetitive work of adjusting parameters leg by leg on long ocean passages.

3.7 AVCS Notifications: System Status Communication

3.7.1 Communication Status Notifications

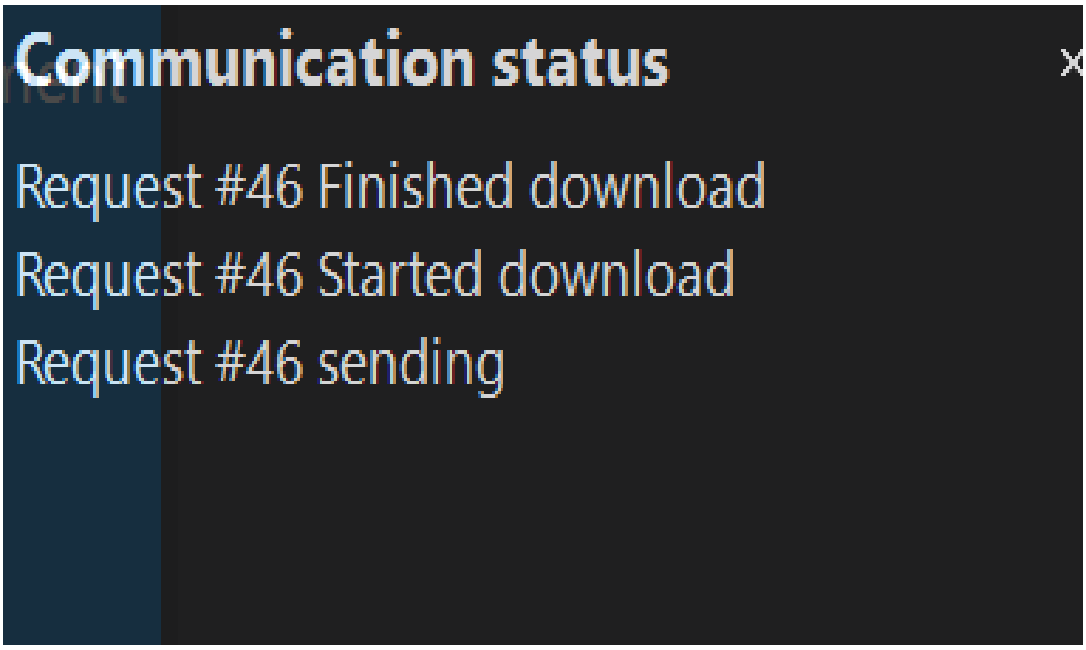

Figure 10: Communication Status Notifications showing a sequential server request in progress (Source: CAIM Sea)

The platform uses four categories of notification to keep operators informed of system activity: communication status notifications, data received notifications, available updates notifications and updating status notifications [3]. Together they provide a real-time picture of what the system is doing at any moment and whether any operator action is required.

Communication status notifications appear at the lower left corner of the screen on a dark notification panel. Each notification is labelled with the sequential request number and reports the current request state from initial sending through to download completion. A typical successful sequence progresses through Sending, Download Started and Download Complete. If the status shows Sending Failed, this is almost invariably a network connectivity or firewall issue rather than a software fault. The correct first diagnostic step is to verify the vessel's internet connection and check that port 443 to maritimegate.net is accessible [5] before investigating further.

3.7.2 Data Received Notifications

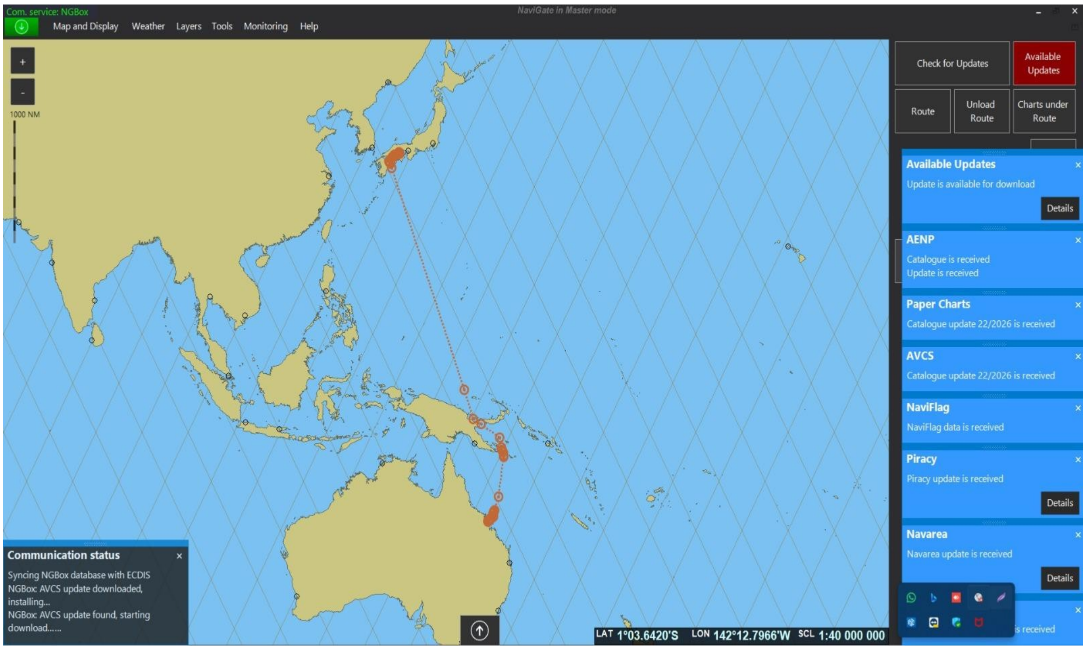

Figure 11: Data Received Notifications with NAVAREA warning, AVCS catalogue update and communications log access (Source: CAIM Sea)

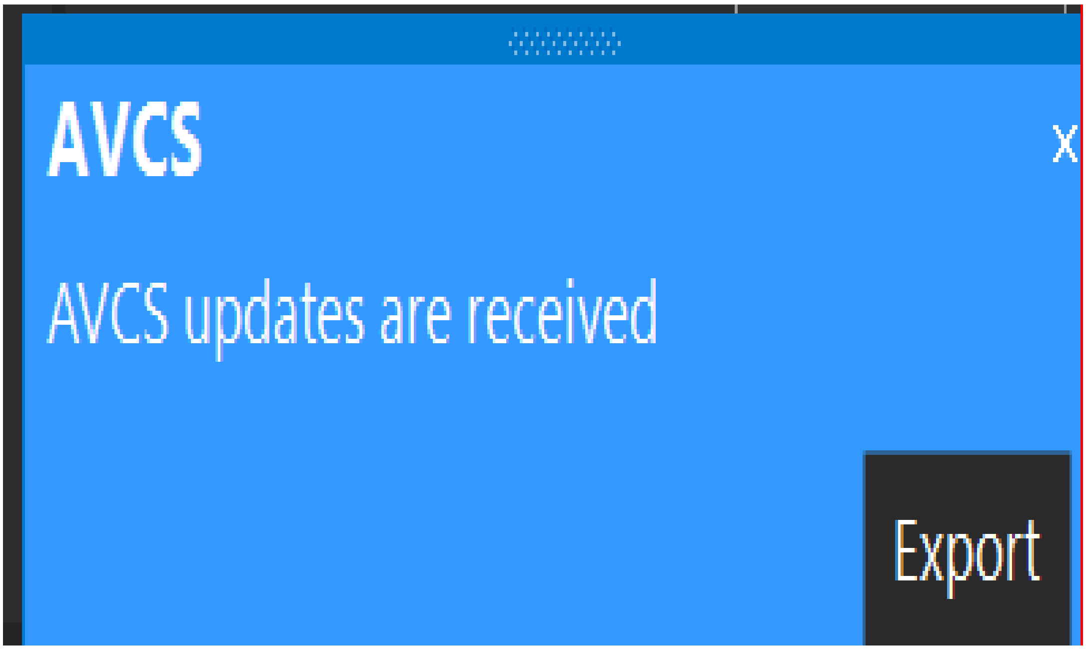

Figure 12: Available Updates notification and additional status notification (Source: CAIM Sea)

When the platform receives new data from the server, blue notification messages appear on the right side of the screen [3]. Each notification is specific to the data type received: NAVAREA warnings prompt the operator to press Details to review the message list; AVCS catalogue updates offer an Export option for USB transfer to the ECDIS; new software version notifications provide a Download button for immediate retrieval. All on-screen notifications can be dismissed simultaneously by right-clicking the notification area.

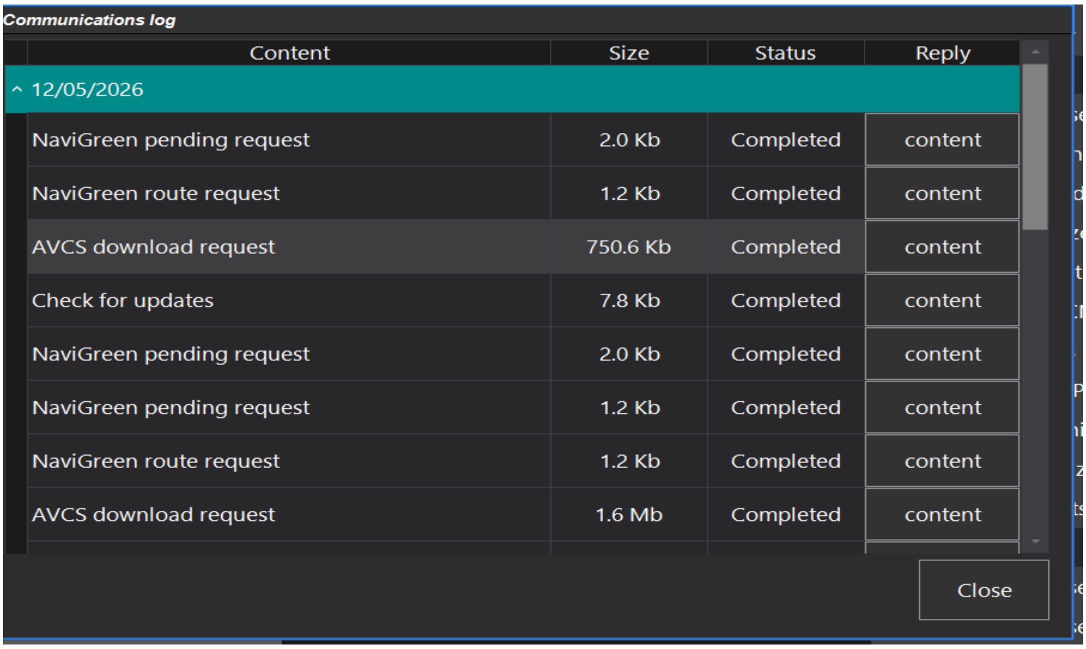

Figure 13: Communications Log showing server exchange history and error records (Source: CAIM Sea)

The Communications Log, accessible through the communication service button, records every server exchange with timestamps and error detail [3]. It is the primary evidence source for all communication diagnostics. Learning to read this log accurately was one of the foundational skills the internship developed.

3.8 AVCS Chart Management

The AVCS workflow is the daily operational framework for managing electronic nautical charts on board [17]. the platform manages the status of two AVCS charts databases: the ECDIS Database (the charts installed in ECDIS) and the internal database (the charts installed and displayed inside the platform) [3]. When all charts and updates are managed and downloaded only through the platform, the two databases are always synchronised. However, when chart installations occur from physical media, such as during drydock, these databases can diverge, causing confusion.

3.8.1 AVCS Catalogue

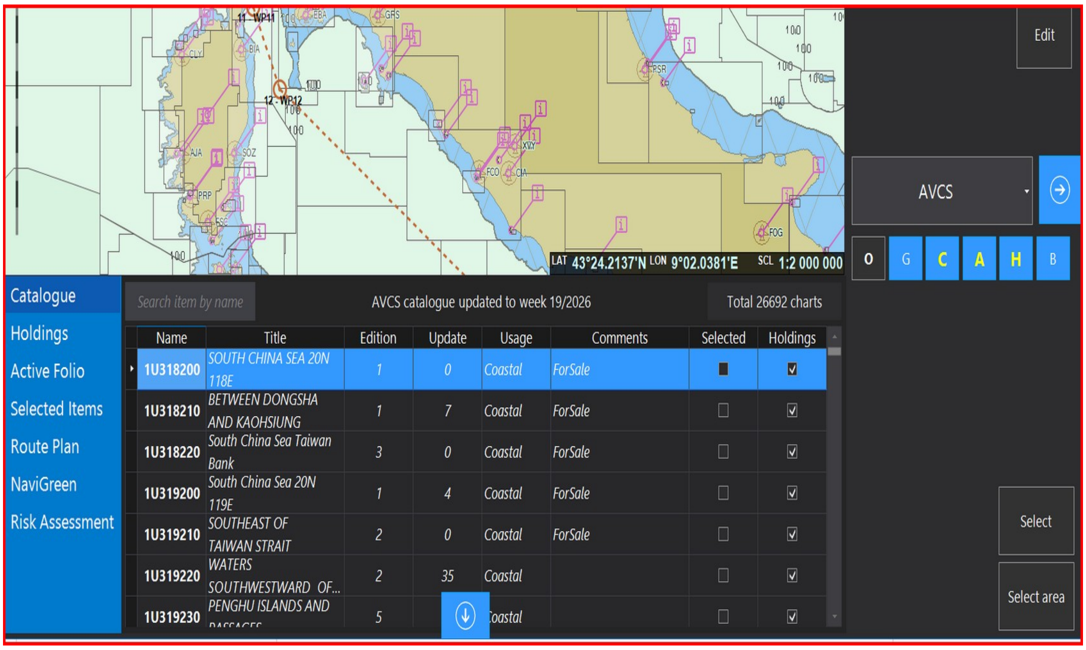

Figure 14: AVCS Catalogue interface with chart cell search and selection (Source: CAIM Sea)

The Catalogue is a searchable listing of all available AVCS chart cells worldwide [17]. Charts are selected from the Catalogue, added to Selected Items and submitted as orders through NaviServer for approval and permit generation.

3.8.2 AVCS Holdings and Active Folio

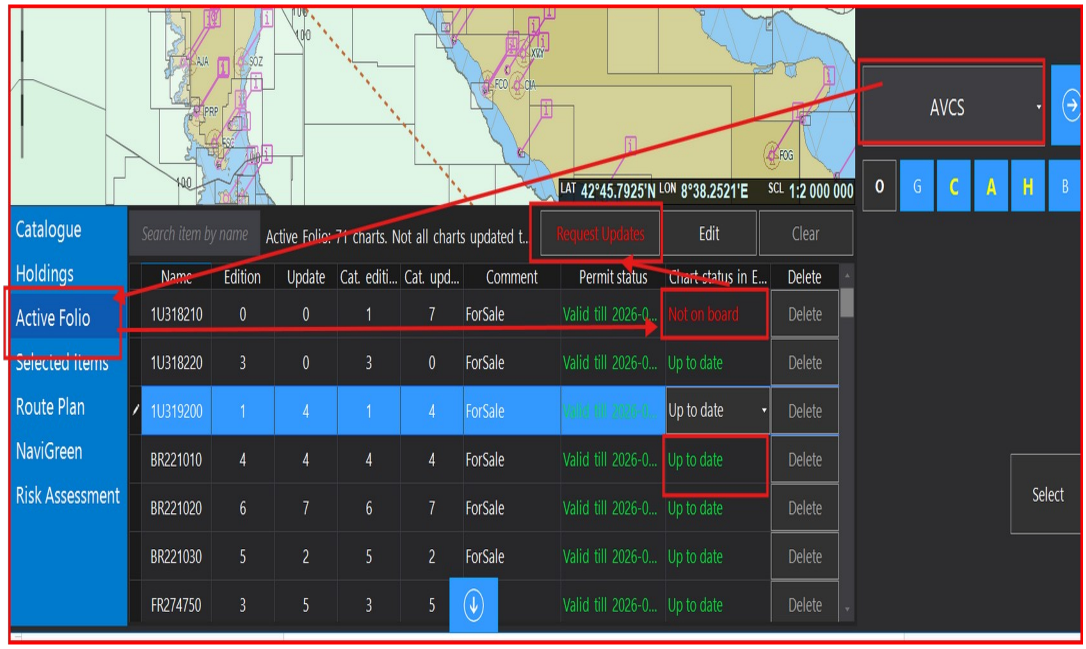

Figure 15: AVCS Holdings section showing current chart inventory (Source: CAIM Sea)

Holdings reflects the vessel's current chart inventory [3]. The Active Folio defines which chart cells are included in the vessel's weekly update package. Any chart cell not in the Active Folio will not receive updates through the regular download cycle, even if the vessel holds a valid permit. This distinction is operationally critical and is one of the most common sources of confusion in support interactions. During the internship, approximately one in five AVCS-related support tickets involved an Active Folio that did not match the vessel's actual trading area.

3.8.3 AVCS Selected Items and Ordering

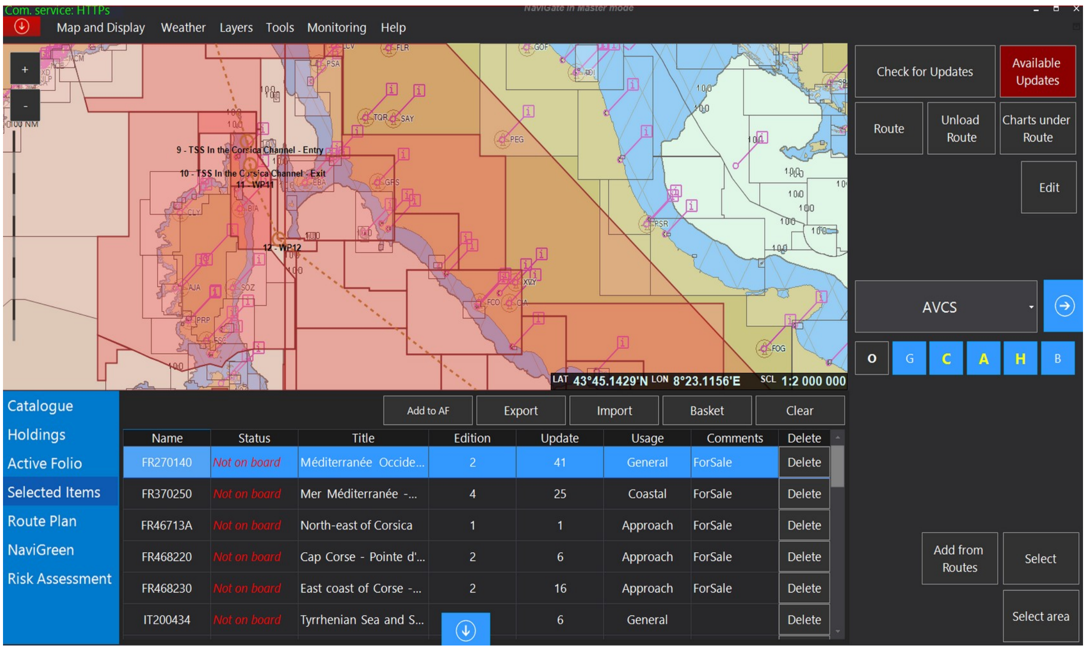

Figure 16: AVCS Selected Items and Ordering interface (Source: CAIM Sea)

Figure 17: AVCS chart ordering workflow from catalogue selection through to ECDIS installation (Source: Author)

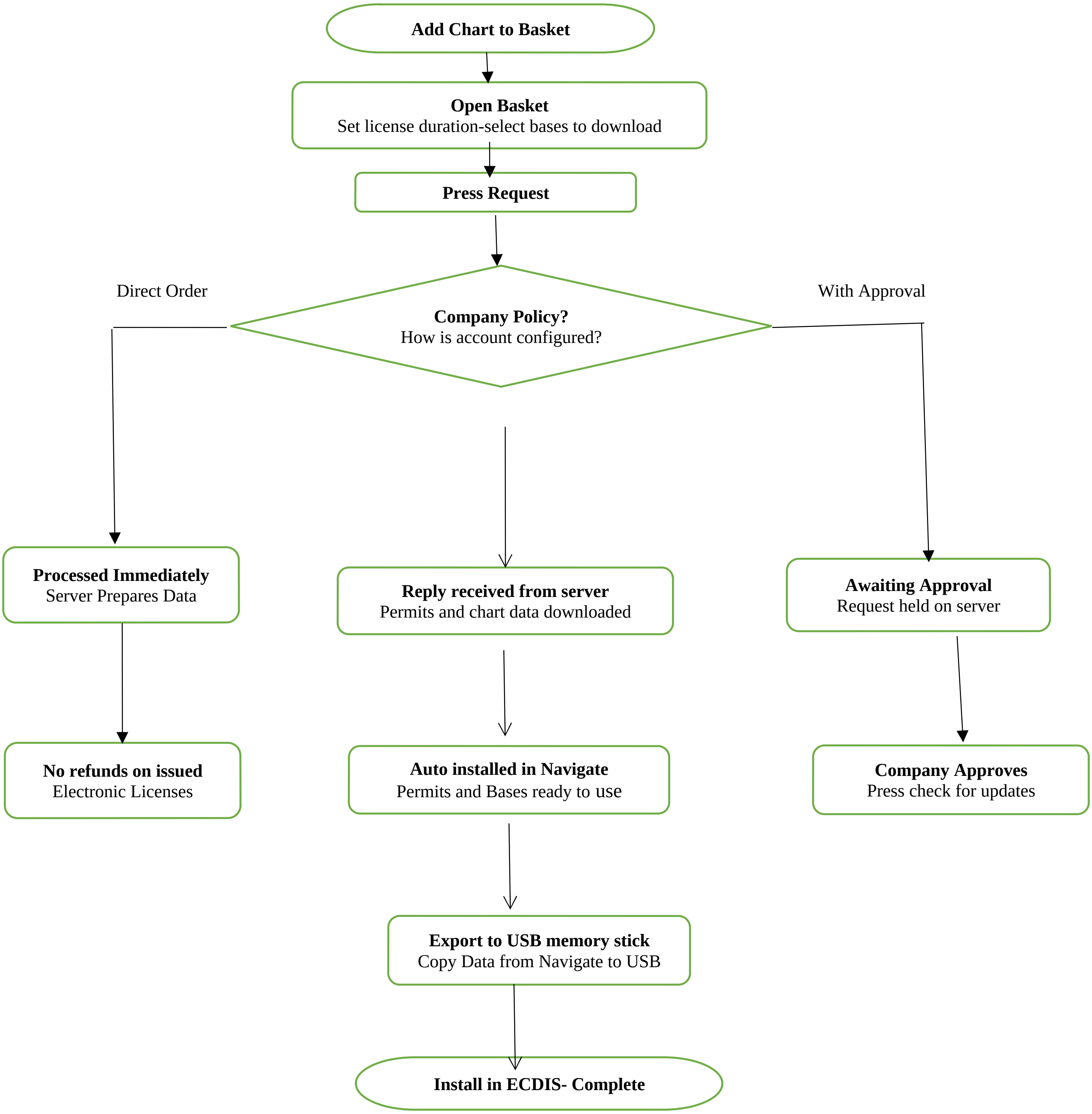

Figure 18: AVCS ordering flowchart showing the permit lifecycle (Source: CAIM Sea)

The ordering workflow involves chart selection from the Catalogue, addition to Selected Items, submission to NaviServer for approval, permit issuance from the UKHO and installation on the vessel [3]. During the internship, I processed approximately 40 to 50 chart orders through this pipeline and the most common delay was at the approval stage when shore-side approvers were unavailable or the order required commercial verification.

3.9 Pay As You Sail (PAYS) Licensing

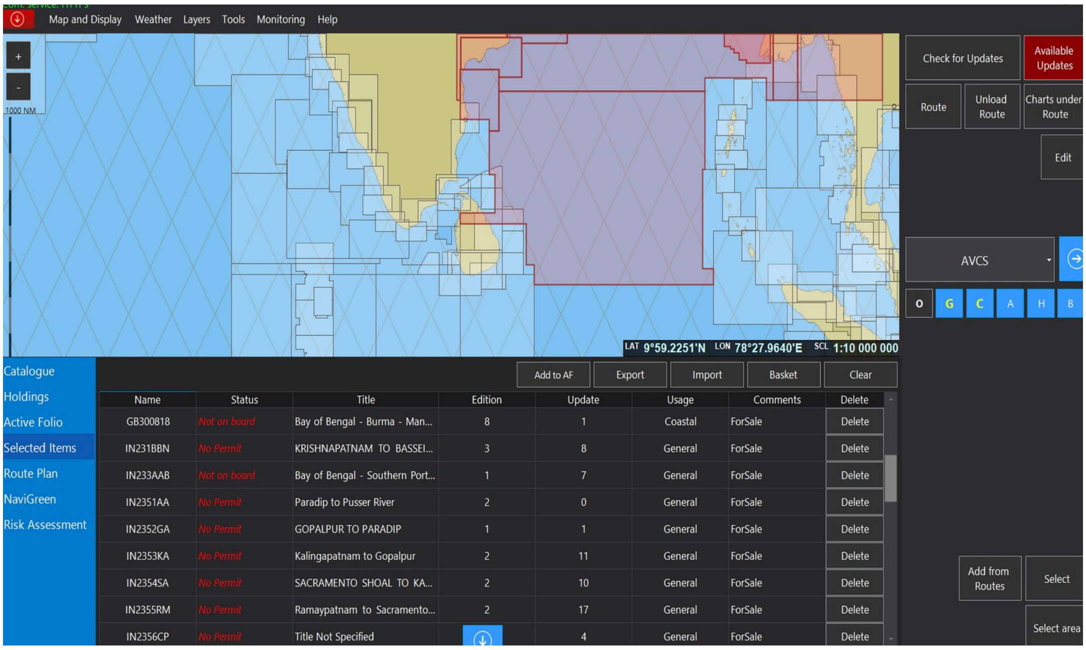

Figure 19: PAYS licensing interface with GPS tracking (Source: CAIM Sea)

PAYS allows vessels to pay only for charts actually used during navigation rather than purchasing full permits in advance [17]. The system uses GPS position tracking through NaviServer to determine which chart cells the vessel transits and billing is triggered accordingly [3]. This model reduces upfront costs for vessels with variable trading patterns but requires accurate GPS reporting and careful attention to excluded area designations. In PAYS mode, vessel tracking carries commercial significance as the mechanism through which UKHO billing is triggered. The Services section in NaviServer must have vessel tracking explicitly enabled and the station must be operating in Master mode for tracking data to be transmitted.

3.10 NGStick: Offline Chart Distribution

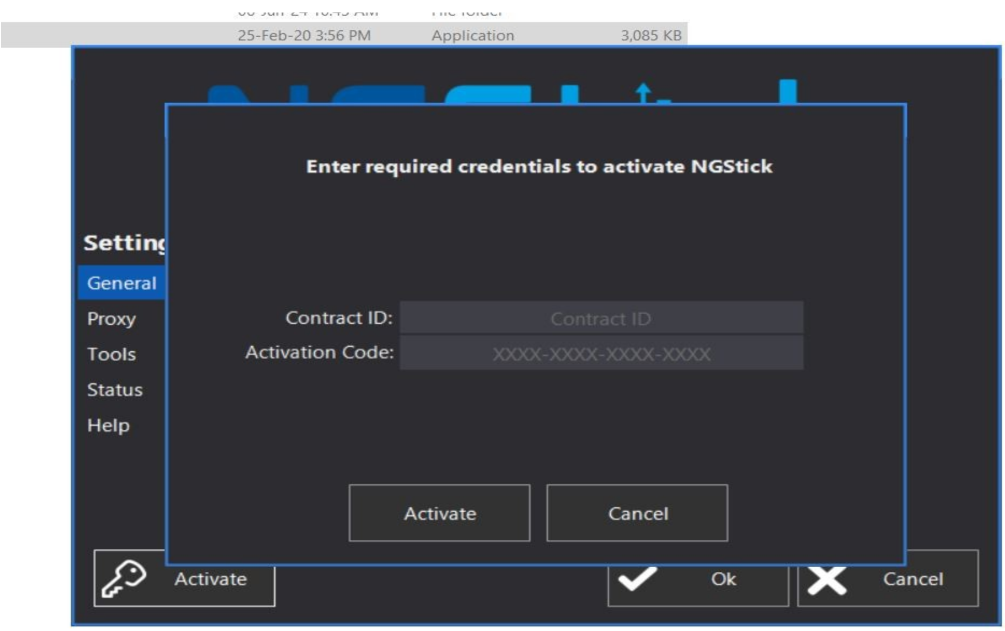

Figure 20: NGStick device and data transfer interface (Source: CAIM Sea)

The NGStick is a dedicated USB device used for transferring chart data between the shore-based system and the vessel when direct internet connectivity is not available or practical [3]. It provides a physical bridge for chart updates when the Offline email method is insufficient for the data volume involved. NGStick detection can be enabled or disabled through the AVCS section of the main status menu.

3.11 NGBox: Centralised Communication Hub

For vessels requiring enhanced cybersecurity, the nGateway service can be deployed on a separate dedicated PC on the vessel's LAN rather than on the bridge workstation itself. This configuration is called NGBox.

Because nGateway is built as a Windows Communication Foundation (WCF) service, it does not need to reside on the same computer as the user interface. In the NGBox configuration, a dedicated hardware unit on the vessel LAN hosts the nGateway service exclusively. The NaviGate application on the bridge PC connects over the LAN to the NGBox IP address to send requests and the NGBox handles all internet communications with shore servers, collects NMEA tracking data and synchronises AVCS updates.

This setup isolates the bridge workstation from direct external network handling, enhancing security and allowing multiple NaviGate stations across the vessel to use a single centralised communication hub.

3.12 NGLink: Secure AVCS Distribution

For configurations employing advanced cybersecurity architectures, the network may include an NGLink device, a secure hardware appliance hosting an RSync server. Every time the nGateway service receives new AVCS updates from shore, it automatically syncs these files directly to the NGLink device over the network. This ensures that updated ECDIS-compliant chart data and permits are staged for secure retrieval by the bridge ECDIS systems without exposing them directly to the internet [3]. NGBox and NGLink together address the IMO maritime cyber risk management requirements [11] by creating an encrypted, authenticated channel for chart distribution.

3.13 NGStick: USB Chart Distribution Device

The NGStick is a specialised USB pen drive equipped with dedicated chart updating software [3]. It serves as a physical bridge for vessels to securely retrieve, update and transfer official AVCS digital charts when direct internet connectivity is not available or practical. The workflow relies on a simple cycle: connecting to a shoreside computer with internet access to sync with the server, then physically carrying the stick to the bridge systems.

Before first use, the NGStick must be activated on a Windows PC with internet access. Activation can occur automatically if plugged into a PC with NaviGate already installed, or manually by entering a Contract ID and Activation Code from the distributor. The NGStick cannot download data unless an Active Folio is defined on the server, either through NaviGate or by contacting support.

When requesting updates, the software connects via HTTPS port 443 to maritimegate.net, checks file integrity on the stick and downloads only missing or updated data [5]. For large updates exceeding 250 chart bases, the software splits data into batches automatically. If a connection drops, partial downloads are saved and can be resumed.

Once fully updated, the USB drive is carried to the bridge. The root directory contains four folders used to update the ECDIS: PERMITS (containing the PERMIT.TXT file), AVCS (containing the vector chart data), AIO (containing the Admiralty Information Overlay layers), and Software (containing the program executable and databases). The NGStick also includes a built-in virus self-check that scans for malware each time the software launches, warning the user before plugging a potentially compromised stick into the ECDIS.

Figure 21: NGStick data preparation and update transfer process (Source: CAIM Sea)

3.14 Paper Charts Management

Although electronic navigation is now standard on most commercial vessels, paper chart management remains a regulatory requirement under SOLAS [10]. The platform tracks paper chart holdings, Notice to Mariners (NTM) correction status and provides compliance reports for port state control inspection readiness [3]. Paper chart holdings can be imported from external files in CMS format (.csf extension), typically provided by the distributor. The paper charts section includes capabilities for downloading and printing NTM corrections, generating holdings reports and displaying the weekly BA NTM documents.

3.15 Digital Publications: AENP

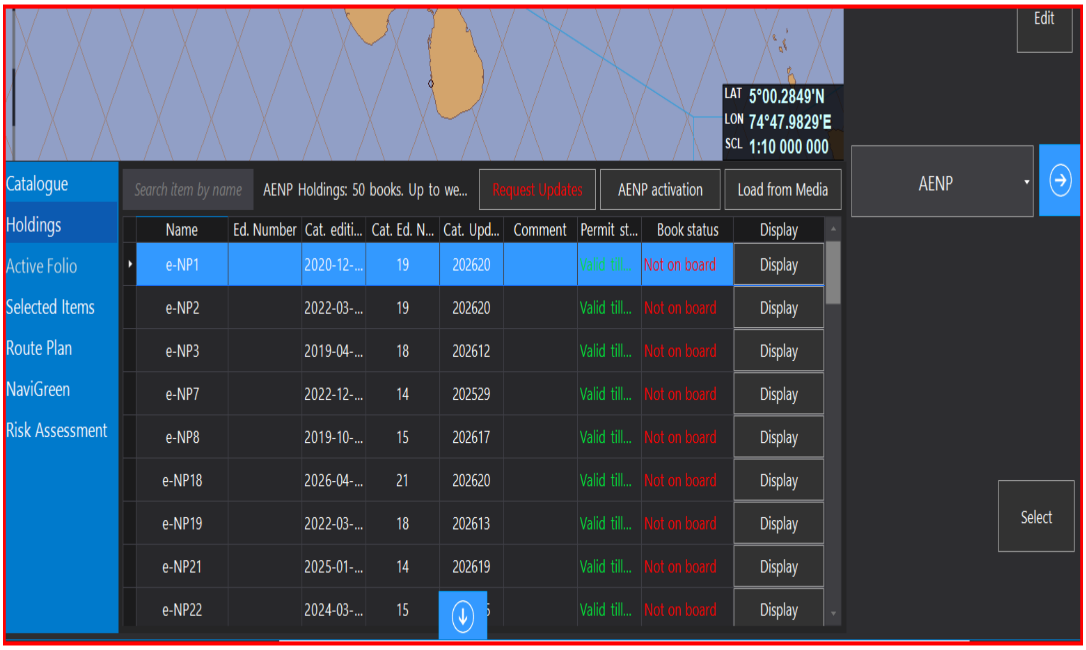

Figure 22: Admiralty e-Nautical Publications (AENP) viewer (Source: CAIM Sea)

Electronic Nautical Publications are the digital equivalents of paper sailing directions, tide tables and list of lights [16]. The AENP reader displays these on the navigation workstation and requires registration against the UKHO server, with a maximum of three registered devices per licence.

3.16 Admiralty eNP Reader

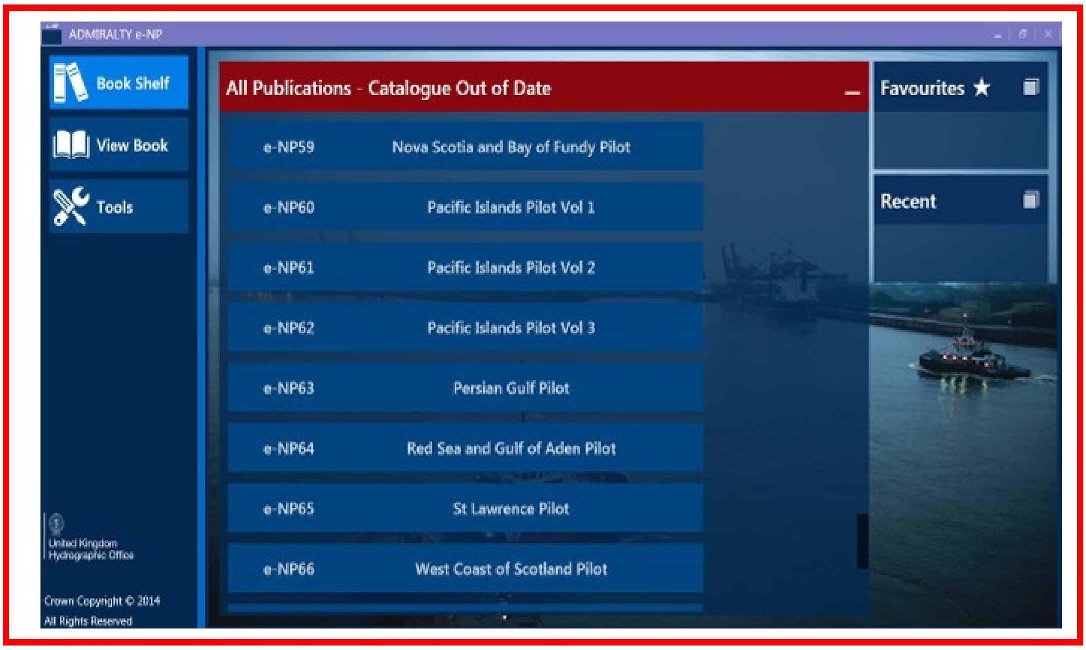

Figure 23: eNP Reader registration and interface (Source: CAIM Sea)

The eNP reader requires periodic updates downloaded through the e-Navigator application [16]. Updates are processed through e-Navigator and downloading of eNPs is through an FTP connection in PASV mode with the normal control port of 21 [5]. Device slot management becomes a recurring support task whenever vessel PCs are replaced.

3.17 Admiralty Digital Publications: ADP

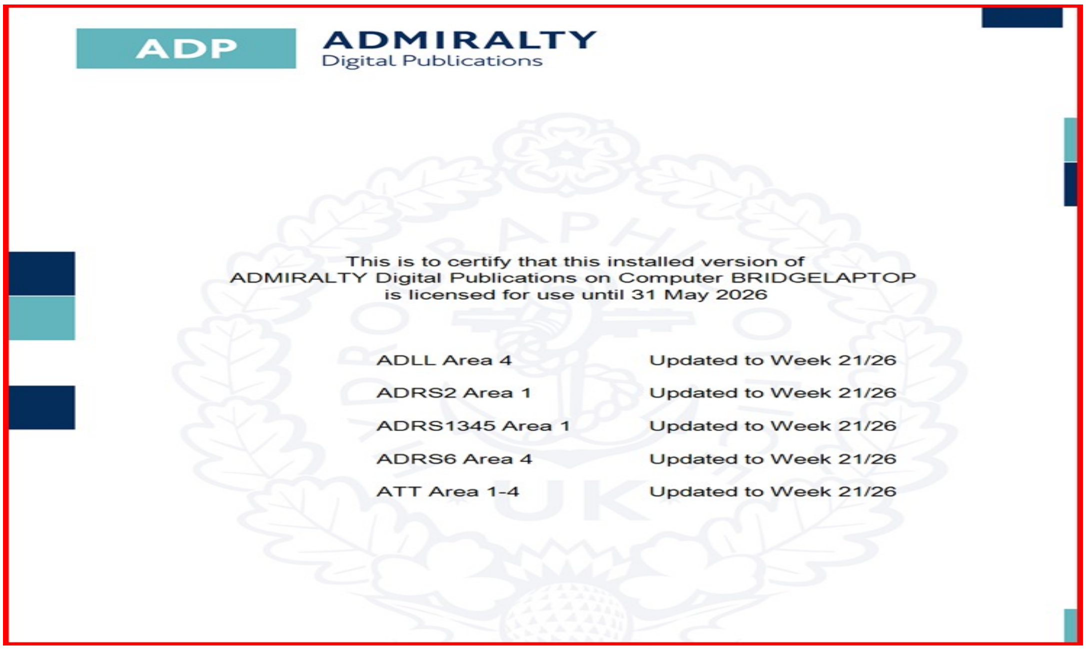

Figure 24: ADP application interface (Source: CAIM Sea)

ADP provides weekly-updating digital versions of Admiralty publications including List of Radio Signals and the Mariner's Handbook [15]. The application runs independently of the navigation platform and has its own activation and update cycle. ADP requires internet access for product activation and updates, with specific firewall whitelisting requirements as detailed in Table 2 [5].

3.18 Map and Display: Chart Management and Weather

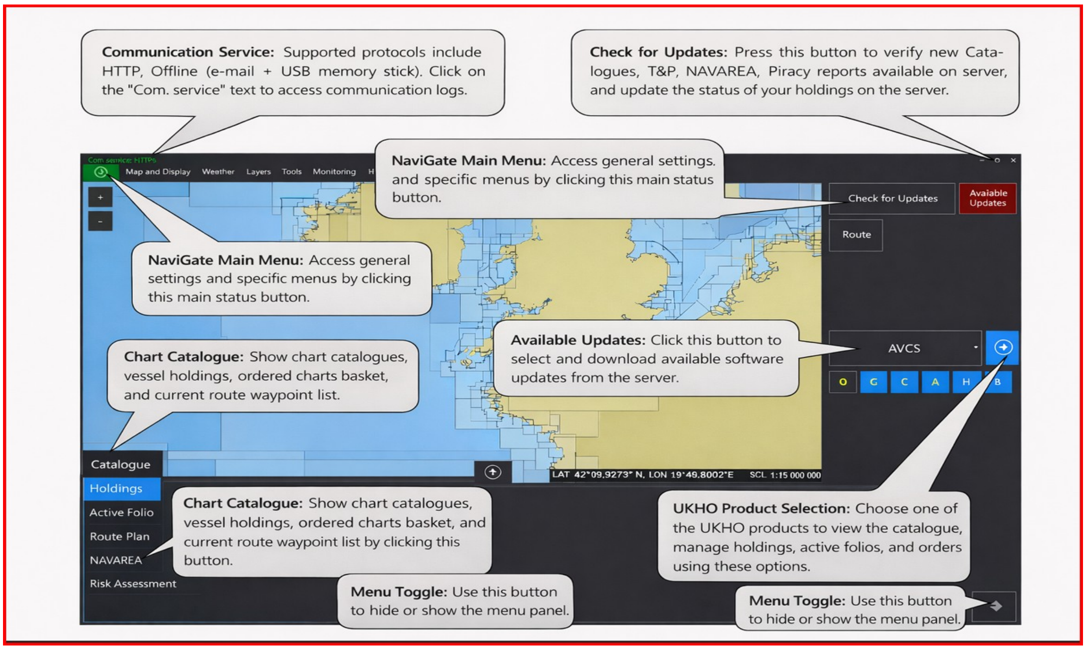

Figure 25: Map and Display interface showing chart installation and safety parameters (Source: CAIM Sea)

The Map and Display section manages AVCS chart installation within the platform and controls the chart presentation parameters [3]. the display settings allow selection between Base, Standard and Other display categories, choosing between simplified or traditional chart symbol presentation and setting the depth safety limits and contours. These parameters directly affect the visual presentation of depth information and the generation of safety warnings during route checking. Incorrect settings here can cause the system to flag false safety alarms or, more dangerously, fail to flag genuine shallow-water risks.

The Install AVCS function allows manual installation of AVCS charts and includes options to request updates from the server, install charts from DVD or USB memory stick, install permits from file and delete installed charts [3]. Night Mode activates a darker colour palette for night navigation.

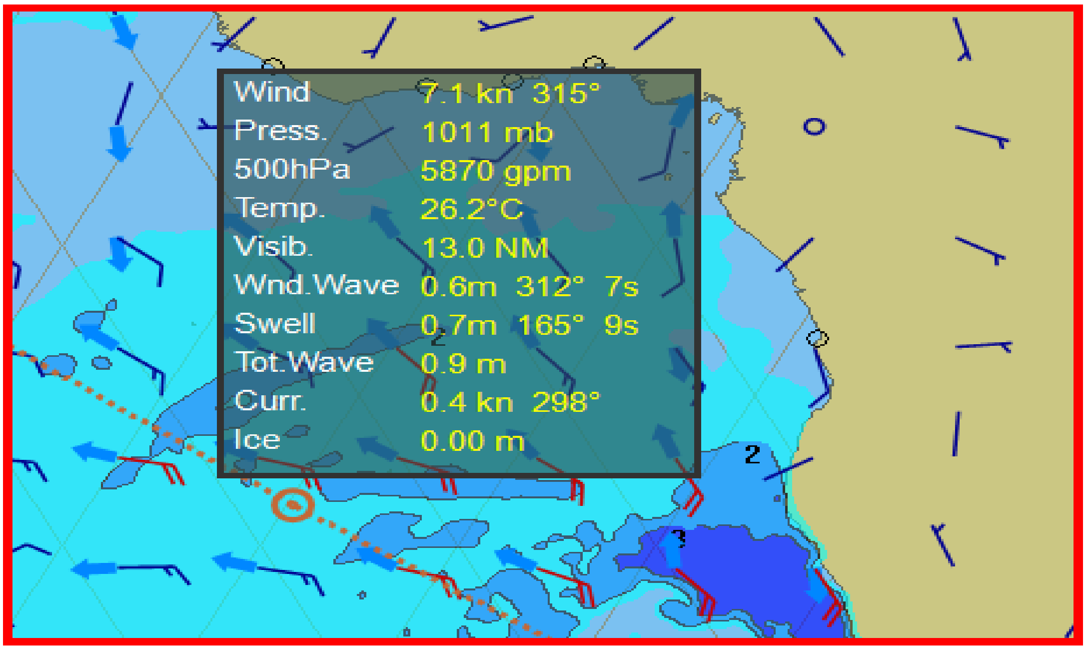

Figure 26: Weather overlay with forecast data on the chart display (Source: CAIM Sea)

The Weather module downloads and displays a six-day weather forecast for large predefined areas with 1-degree grid resolution [3]. Alternatively, the user can define a smaller custom area with more detailed forecasts at 0.5-degree grid resolution. The weather data is provided by the Sat-Ocean forecast centre, which generates new forecasts every 12 hours. Downloaded files contain Wind, Pressure, Visibility, 500hPa Geopotential Height, Total Waves, Swell, Sea Temperature and Surface Currents. An interpolation option averages the gridded weather parameters to display smoother values, though it may not fully represent the real weather situation in some locations [3].

3.19 Layers and Safety Overlays

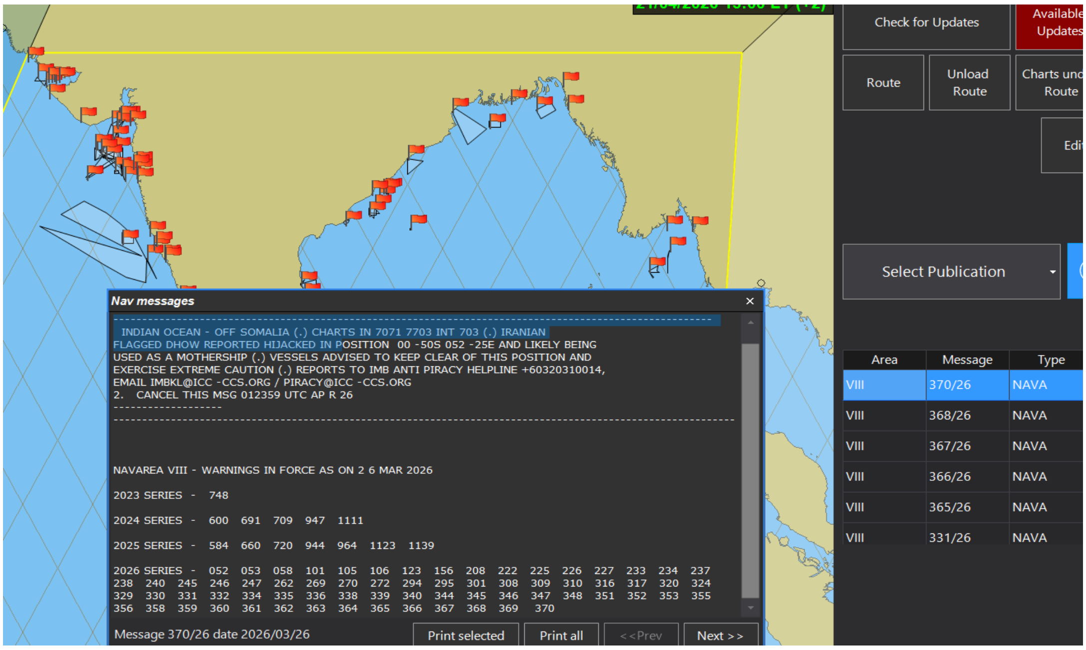

Figure 27: Layers panel showing available information overlays (Source: CAIM Sea)

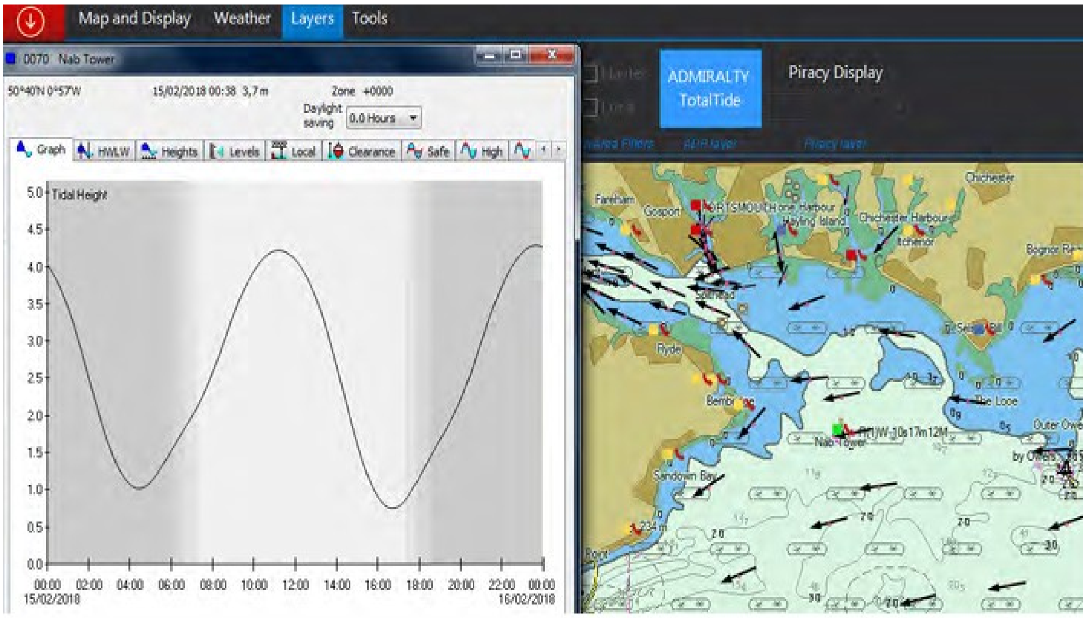

Figure 28: Safety overlays including T and P notices and NAVAREA warnings displayed on chart (Source: CAIM Sea)

The Layers function enables a comprehensive suite of information overlays on the chart display [3]. These include T and P (Temporary and Preliminary) notices, which can be shown on the map with full text accessible through right-click; NAVAREA warnings, which display regional maritime safety messages with coordinate-based positioning; TotalTide integration for tidal stream data if TotalTide is installed with a valid licence; piracy attack reports colour-coded by recency (yellow for recent reports); environmental MARPOL and PSSA area overlays; and custom layers that can import and display boundaries, limits and special areas from Google KML files, ESRI Shapefiles, or generic text files with latitude and longitude [3].

The "Under Route" functions for both T and P and NAVAREA are particularly useful during voyage planning, as they automatically compile a list of all notices found within a configurable distance of the active route, based on the Ship Data Voyage defaults settings.

The platform also includes an integrated object editor for creating custom layers, replacing the legacy text/CSV import function [3]. The editor allows creation of areas, lines and points with associated information. Objects can be qualified as "Alerts," meaning that when the Check Route function is run on a route crossing that object, an alarm will be raised. This capability supports the creation of company-specific restriction zones, whale speed reduction areas, or other operationally relevant boundaries.

3.20 Risk Assessment and Voyage Planning

3.17.1 Risk Assessment Module

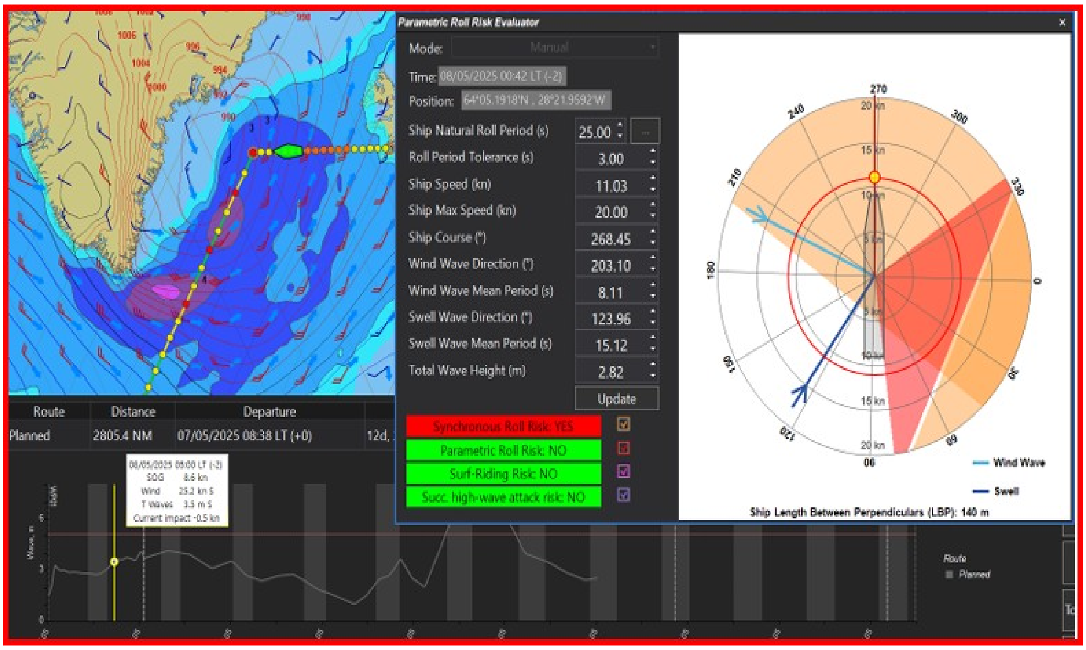

Figure 29: Risk Assessment module with weather analysis along the planned route (Source: CAIM Sea)

The Risk Assessment module evaluates weather and wave conditions along a planned route at the vessel's planned speed, using colour coding and time simulation to provide a visual indication of where conditions are likely to become challenging or operationally significant [3]. For a basic route weather check, only the vessel's draught and sea passage speed are required as input. The platform calculates expected speed adjustments for each route leg based on the wave height forecast, produces an estimated time of arrival and total fuel consumption for the passage and generates wave and wind profile charts that can be scrolled forward in time to show how conditions evolve relative to the vessel's projected position. A red threshold line on the profile indicates the sea state above which conditions are classified as rough for that vessel.

If the Roll Risk Integration flag is enabled, the platform calculates potential parametric rolling risks along the route and displays in colour the points where one or several risks are likely, with four types of alarms each colour-coded [3].

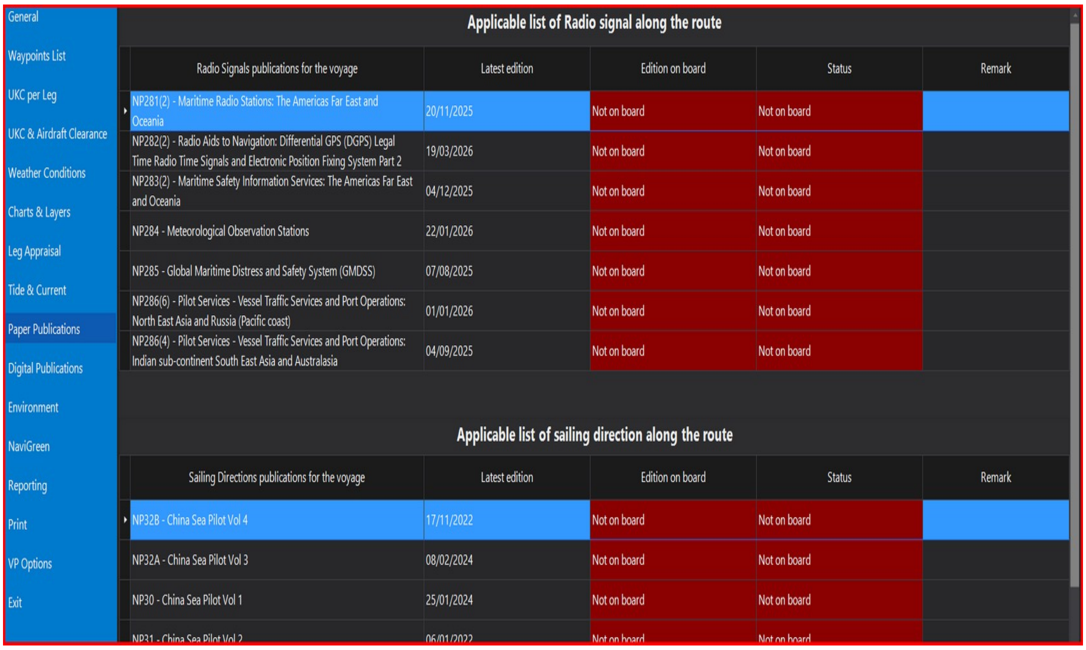

Figure 30: Risk Assessment comparing the planned route against the optimised weather routing alternative (Source: CAIM Sea)

For the full weather routing optimisation, the ship model must be correctly populated in Ship Data before the module is run [3]. The main criterion in the optimisation is safety as the number one priority, with ETA and consumption at lower priority. The platform calculates an alternative route and generates a comparison report covering both the planned and optimised routes, providing the navigator and shore management with a documented basis for the final route decision. The accuracy of all outputs is directly proportional to the quality of the ship model data. During the internship, I encountered several cases where Risk Assessment outputs appeared anomalous. In each instance, the cause was traced to incorrect or incomplete ship model entries rather than software errors.

3.17.2 Voyage Plan Module

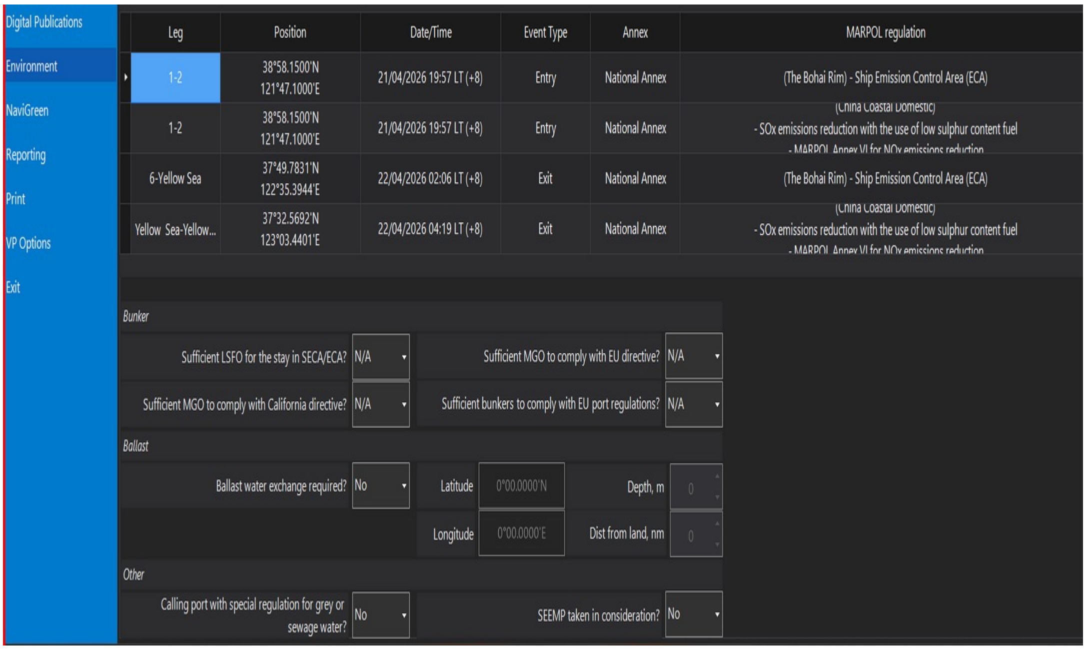

Figure 31: Voyage Plan environmental compliance sequence (Source: CAIM Sea)

The Voyage Plan module generates a comprehensive passage plan covering under-keel clearance calculations, weather conditions, chart and publication status, tidal and current data, environmental compliance events, leg appraisal parameters and paper and digital publication requirements [3]. It requires a fully prepared route with correct waypoint types, speeds and cross-track distances; accurate Ship Data with vessel dimensions and block coefficient; correctly set safety depth and contour values; a current weather forecast; and all charts for the planned route installed and up to date.

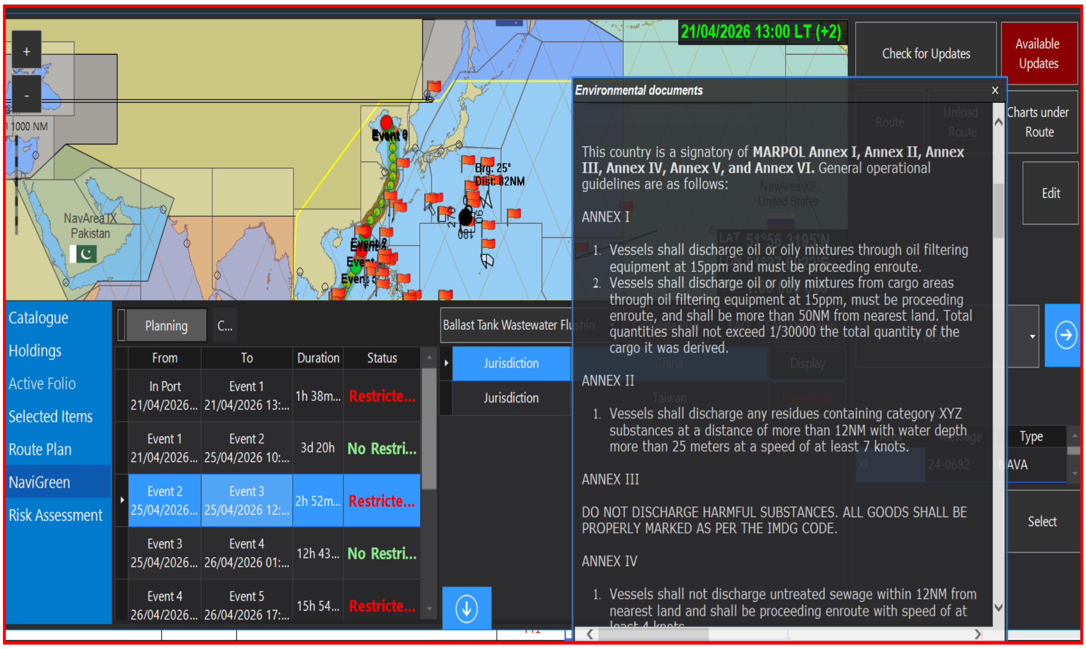

Figure 32: Voyage Plan Waypoints List showing the complete route sequence from Dalian to Singapore with ETA, speed and chart assignments per leg (Source: CAIM Sea)

The Voyage Plan outputs are organised into specific sections, each addressing a different aspect of the planned passage [3]. The Waypoints List presents the complete route sequence with position, speed, course, distance, ETA, cross-track limits and best available chart for each leg. The UKC Per Leg section calculates under-keel clearance for each leg across three voyage phases (Departure, Sea Passage and Arrival) using the vessel's static draft and block coefficient with squat allowance applied for speed through water. Negative UKC values are highlighted in red as safety-critical flags requiring resolution before departure.

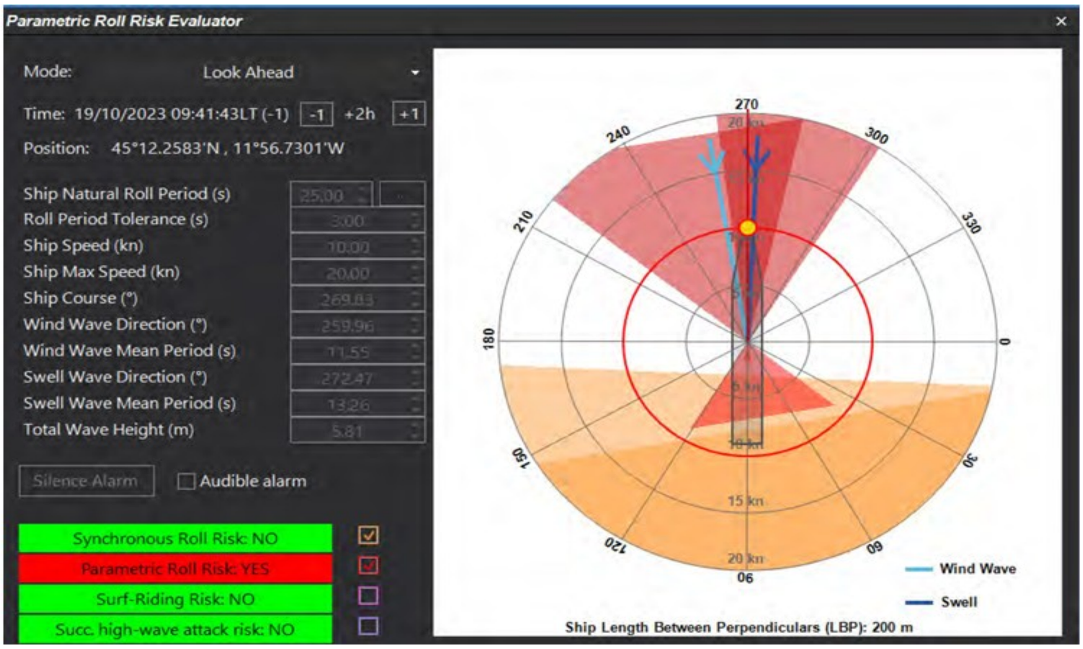

Figure 33: UKC and Air Draft Clearance section showing calculated clearances at departure and arrival berths with safety threshold comparison (Source: CAIM Sea)

Figure 34: Voyage Plan Weather Conditions section (Source: CAIM Sea)

The Charts and Layers section flags any ENCs or paper charts along the route that are not updated to the current week, with danger indicators showing where safety concerns exist due to chart currency gaps. The Leg Appraisal section records operational parameters including main engine status, position verification methods, reporting requirements, bridge and engine manning and security level for each leg [3]. Paper Publications and Digital Publications sections list the required titles for the voyage area with on-board status indicated.

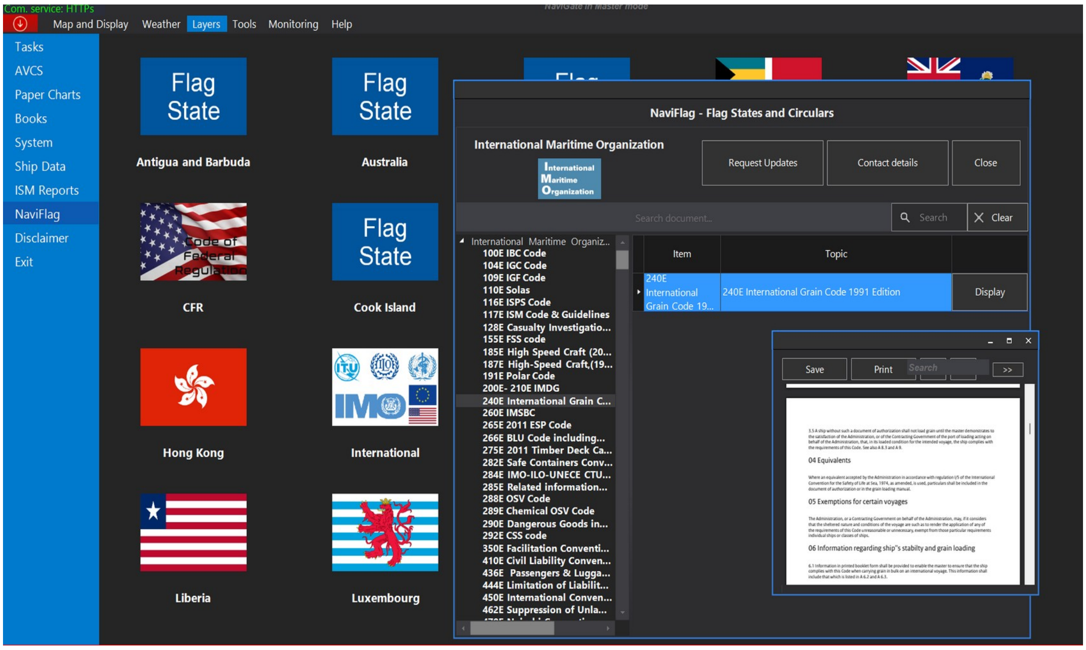

Figure 35: NaviFlag module with flag state selection, available circulars list and document access (Source: CAIM Sea)

3.21 Monitoring: MRV and Parametric Roll

EU MRV regulation, in force from January 2018, requires shipping companies to monitor and report CO2 emissions for every voyage, covering fuel consumption both at sea and alongside in port and compile this data into an annual aggregate report [7]. The platform integrates MRV reporting directly into the active voyage workflow [3]. Once a route is defined by a Voyage ID, departure and arrival ports, departure date and waypoints, and approved by the master as the Active Voyage, the MRV module records fuel consumption automatically throughout the passage including time in ice and time at anchorage. On voyage completion, the platform produces a PDF summary for crew verification and an XML file formatted for direct upload to the EMSA Thetis MRV platform [6].

The Parametric Roll Risk Evaluator assesses four rolling hazard types: parametric roll, synchronous rolling motion, surf riding and successive high wave attack, all of which have been responsible for serious casualties in commercial shipping [3]. The module uses the vessel's configured Ship Data dimensions combined with the downloaded weather forecast to assess risk at the current or a selected position and can be stepped forward hour by hour to project risk development along the planned route. Hazardous parameters are highlighted in red with an audible alarm available for watch officer notification.

3.22 NaviServer: Shore-Based Management

NaviServer is the shore-based administrative platform that underpins the entire operational ecosystem [2]. Every vessel account, every chart permit, every order approval workflow and every service configuration originates in NaviServer. For anyone working in maritime IT support, NaviServer is where the solutions to most problems that appear on board must ultimately be implemented.

Account setup requires the vessel name, company, IMO number, MMSI, flag state, vessel email address and download size limit [2]. These details define how the server identifies and communicates with the specific installation. NaviServer generates activation keys after account creation. The Ordering section routes all vessel chart orders to the designated approver before permits are issued, protecting against irrecoverable duplicate costs [17]. The AVCS module must be explicitly enabled before the vessel can access AVCS data and PAYS must be activated separately for vessels on that licensing model. The Active Folio determines which chart updates are prepared weekly; the Holdings section provides the shore team with an independent, auditable record of the vessel's chart outfit; and the Services section controls which capabilities each vessel can access. An incomplete Services configuration at setup is one of the most common sources of early post-deployment support calls.

Vessel tracking through NaviServer provides real-time fleet position visibility, transmitting GPS position data at each server connection when operating in Master mode [2]. In PAYS mode this tracking carries commercial significance as the mechanism through which UKHO billing is triggered.

3.23 UKHO Server: The Data Supply Chain

The UKHO server sits at the origin of all Admiralty Vector Chart Service data [17]. It holds the master catalogue of every existing AVCS chart cell globally, generates and issues every chart permit, produces weekly updates for all cells every Thursday night UTC and maintains the licensing records that determine what each vessel in the world fleet is legally permitted to display and navigate by.

The distribution structure is three-tiered: the UKHO server produces and validates data; NaviServer, operated by the distributor, retrieves weekly updates and distributes them with vessel-specific configurations; the platform on board retrieves its specific prepared data from NaviServer [3]. This architecture insulates the UKHO from direct management of individual vessel accounts while allowing the distributor to provide a technical support layer and apply operational customisation. Permit synchronisation between NaviServer and the UKHO server must be maintained carefully: any configuration change involving chart installations from physical media, hardware replacements, or significant Active Folio revisions may require explicit permit resynchronisation by the distributor [17].

Chapter 4: Technical Issues and Troubleshooting

This chapter provides a systematic account of the technical issues encountered throughout the internship and the diagnostic and resolution approaches developed for each category of problem. The issues are drawn directly from real support cases handled during the placement at CAIM Sea and the descriptions reflect the operational context in which they occurred: a live maritime support environment where vessels are waiting for resolution and the time available to diagnose and correct problems is measured in hours, not days.

Technical support at this level requires more than knowledge of individual error messages. It requires a systematic diagnostic methodology: the ability to read available evidence, form and test hypotheses about underlying causes and navigate efficiently through a decision tree toward resolution without being distracted by surface appearances or premature conclusions.

4.1 Communication Issues

4.1.1 nGateway Communication Failure

nGateway is a Windows background service (nGateway.exe) that handles all data exchange between the platform and the remote server [3]. It operates independently of the user interface application: the platform can be open and fully functional in appearance while nGateway has stopped, which means the system displays no indication of a communication problem until an update request is submitted and fails silently. Understanding this architectural separation is the single most important diagnostic insight for communication support.

Resolution: Close the platform. Open the nGateway Manager application. Press Stop to ensure the service has fully halted. Press Run to perform a clean restart. Reopen the platform. Pending requests will begin queuing and transmitting automatically. If the queue does not clear on the first attempt, repeat the stop/run cycle. The majority of nGateway communication failures resolve with this procedure alone.

Case example: In July 2025, a tanker operating in the Mediterranean reported that chart updates had stopped arriving. The application interface showed no errors. The communications log revealed that the last successful server exchange was four days earlier, with no entries since. Restarting the nGateway service immediately cleared the queued requests and resumed normal operation. The root cause was a Windows update that had restarted the PC without also restarting the nGateway service, a scenario that occurs because the service's automatic recovery settings do not always trigger correctly after an OS-level reboot.

4.1.2 nGateway Reconfiguration

When a service restart does not restore communication, the configuration settings in the nGateway Admin Tool must be reviewed [3]. A service that restarts without errors but with incorrect settings will immediately return to the same non-communicating state. Key areas to verify: the server address must use HTTPS on port 443 to the correct domain [5]; the protocol must be HTTPS rather than HTTP; the communication mode must match the vessel's actual connectivity situation; GPS input settings must reflect the configured hardware connection.

Once settings are corrected, stop and restart the service and reopen the platform to verify. If communication is still not restored after a full settings review and restart, the problem lies outside the platform itself, typically a firewall restriction, a satcom provider routing limitation, or a corporate network policy. These require coordination with the vessel's IT department or satcom provider.

4.1.3 Log and GPS Incoming Data

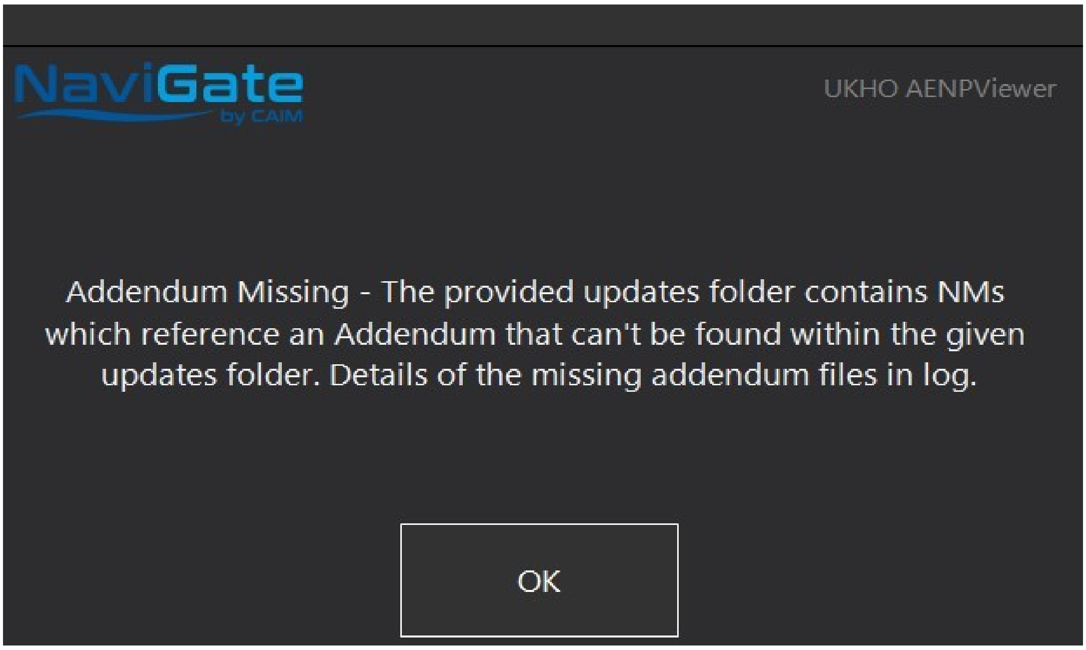

Figure 36: Communications Log and GPS Incoming Data display (Source: CAIM Sea)

The Communications Log records every server exchange with timestamps and error detail [3]. It is the primary evidence source for all communication diagnostics. The three main error categories and what each indicates, are as follows:

A timeout error in the log means the request reached the network but received no response. This points to network path issues, DNS problems, or server availability issues. The request left the vessel but never arrived at the server, or the server's response never arrived back at the vessel.

A handshake failure means the TCP connection completed successfully but TLS negotiation was rejected [12]. This points directly to TLS configuration. The server is reachable, the route exists and port 443 is open. The failure occurred during the protocol negotiation phase, after the TCP handshake but before any application data was exchanged.

A 401 or 403 response means the server received the request but rejected it due to authentication or authorisation failure. This points to account status or contract issues on the server side.

Reading the log correctly and interpreting the error types it presents, is what separates rapid diagnosis from extended guessing.

The GPS Incoming Data display confirms whether live NMEA 0183 position sentences are reaching the platform from the vessel's GPS system [8]. This confirmation is operationally important because GPS feed failure disables multiple functions simultaneously, including MRV voyage recording, NaviGreen environmental monitoring, parametric roll risk assessment and

NaviServer position tracking, without generating any visible error in the main interface. Confirming that NMEA data is arriving in the GPS Incoming Data tab should be part of every initial health verification.

4.1.4 Contract Not Found Error

The "Contract Not Found" error appears when the platform cannot locate a valid contract associated with the installation. This occurs most commonly when the activation has expired, the contract details have been changed on the server side without corresponding update on the vessel PC, or the link between the software and NaviServer has been broken by a hardware change or reinstallation [2]. The resolution requires two steps: resetting the existing contract state through the Tasks menu to clear the corrupted local record, then reactivating using a valid Contract ID and Activation Code from the distributor.

4.1.5 Contract Not Found By Token: Backup Station

This error is specific to the Backup station and appears when the token stored in the local configuration file no longer matches the token registered against the vessel account on the server [3]. This is most commonly caused by a Master station reactivation or a contract renewal that updates the server record without updating the Backup station's local configuration. The resolution involves identifying the discrepancy between the local token and the server record, locating a valid token from the server-side communication logs and restoring the correct value to the local configuration file. This procedure requires access to server-side logs and should be performed only by authorised support personnel.

4.1.6 Error 500 CryptographicException

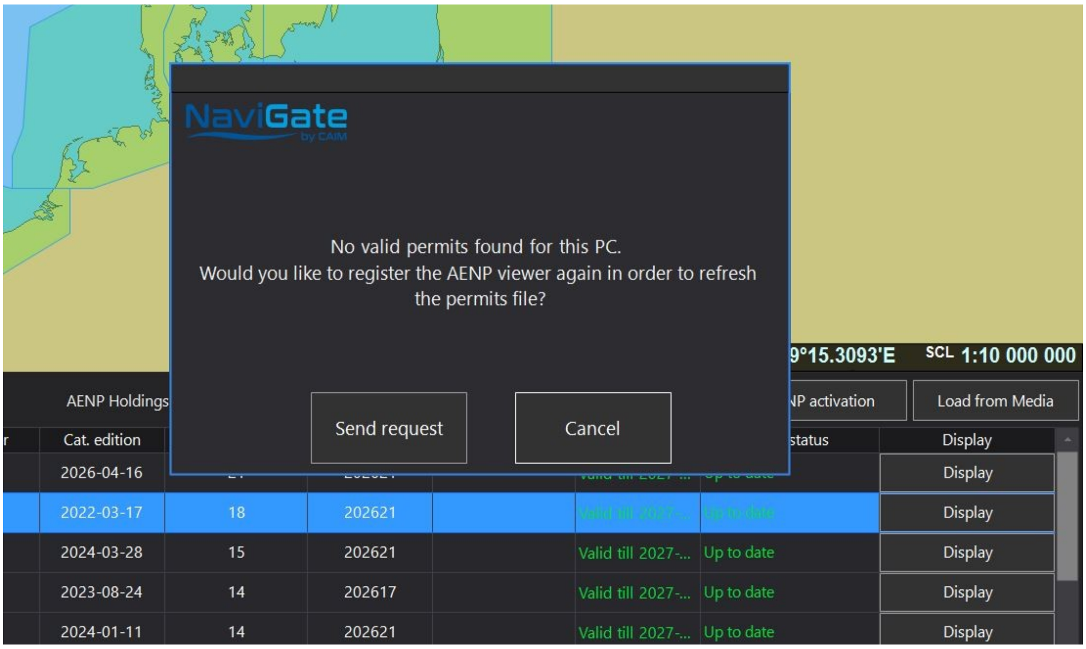

Figure 37: Error 500 CryptographicException with affected system path information (Source: CAIM Sea)

The Error 500 CryptographicException occurs when the AENP viewer encounters a corrupted or invalidated key set in the Windows Cryptographic Service Provider storage [13]. The error references a System.Security.Cryptography.CryptographicException with a keyset validity failure and identifies the specific system folder containing the problem. This is a Windows operating system level issue, not a fault in the AENP viewer or the platform software.

Resolution: Rename (do not delete) the affected cryptographic storage folder identified in the error message. Renaming rather than deleting preserves the original data as a fallback. Reboot the device. Windows will regenerate the cryptographic folders with clean key sets on restart. In most cases this single step clears the error. If it persists after the first rename and reboot, a second rename of a broader parent folder followed by another reboot resolves it.

4.1.7 Manual Installation of eNP Update Files

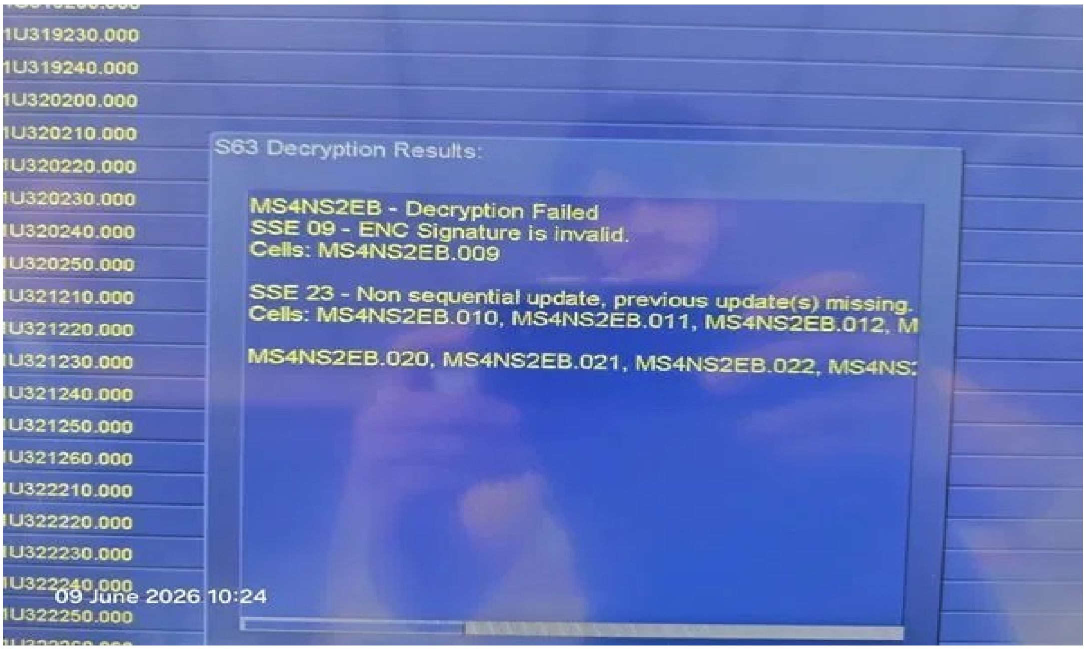

Figure 38: Manual eNP update file installation (Source: CAIM Sea)

When the automatic eNP update process fails, files must be installed manually by placing them in the eNP update directory [16]. The critical prerequisite is making the destination folder visible: it resides inside ProgramData on the C drive, which is hidden from File Explorer by default. Hidden items must be enabled through the View tab before the folder can be navigated to. Once visible, navigate to ProgramData, then to the eNPData Updates subfolder, extract the downloaded update file, copy all contents into the Updates folder and confirm the file replacement prompt.

4.1.8 Available Updates Not Clearing After Download

This issue presents as a persistent red "Available Updates" indicator after what appears to be a successful download. The cause is an update that downloaded correctly but failed to register in the system's internal update tracking database, leaving the indicator in a flagged state despite the data being present [3]. The resolution requires navigating into Holdings for each flagged product (typically ADLL, ADRS, or ATT) and submitting an update request from within Holdings even if the holdings list appears empty. This forces the system to re-evaluate the update state and register the previously downloaded data. Complete this step for every flagged product before pressing Check for Updates to verify the indicator has cleared.

4.1.9 Voyage Plan Calculation Issues

Unexpected voyage plan outputs, including incorrect ETAs, negative UKC values, missing weather data and incomplete section data, are almost always caused by missing or incorrect input data rather than software errors [3]. Systematic diagnosis requires checking Ship Data accuracy for vessel dimensions, draft and block coefficient; verifying the Route Plan table for correct waypoint types, speeds and cross-track distances; confirming safety depth and contour values are appropriate for the vessel's operational draft; and ensuring the Active Folio is current with all charts for the route installed. If problems persist, the chart data for the route should be reviewed, as missing or outdated chart cells affect depth calculations and CATZOC uncertainty corrections in ways that can produce anomalous UKC results.

4.1.10 B2B Error

The B2B error is generated when a vessel submits an order for a product that already exists in its holdings [17]. The system identifies the duplicate and blocks the submission to prevent double charging for the same licence. The resolution is to review the holdings list carefully before submitting any order and remove already-held products from the order basket. Persistent unexplained B2B errors should be referred for server-side account investigation.

4.2 AENP Issues

4.2.1 No Valid Permits Found

This error appears when the AENP viewer on the vessel PC is not registered against the UKHO server, or when the registered permit file has expired or been invalidated [16]. Publications may appear in the holdings list as current and up to date, as the holdings table reflects what the licence covers, not what can currently be opened. The fix requires pressing "Send Request" in the error popup. This sends a re-registration request to the server, which responds with a fresh permit file. The AENP licence allows a maximum of three registered devices simultaneously. If all three slots are occupied when a new machine needs to register (typically after a PC replacement), one existing slot must be cleared through the distributor before the new registration can succeed.

4.2.2 Activation Failed: Invalid Login ID or Password

The error indicates either incorrect credentials or inability to reach the activation server [16]. Credentials must be verified exactly as provided by the Chart Agent, as Login ID and Password are both case-sensitive. If credentials are confirmed correct and activation still fails, the PC's internet connection must be tested for the activation server specifically: the vessel's firewall, satcom system, or corporate network may be blocking the activation endpoint address [5].

4.2.3 eNP Update Failed: Invalid Machine Identifier

The machine identifier registered against the eNP licence on the server does not match the machine attempting to request updates [16]. The mismatch is almost invariably caused by a hardware replacement or significant component change that altered the PC's identity string. Resolution requires the distributor or the e-Navigator account administrator to clear the old machine registration and register the new machine in its place.

4.2.4 AENP Activation by Email

When direct internet activation is not possible, AENP can be activated through an email-based procedure. The activation request generates a file that the vessel officer emails to the Chart Agent, who processes it and returns an activation response file. This file is then imported into the AENP viewer to complete the activation [16]. This workflow is functionally equivalent to the Offline mode in the main platform and is used under the same connectivity constraints.

4.3 ADP Issues

4.3.1 ADP Update Download Failure

ADP updates are released weekly and must be downloaded through the application's built-in update function [15]. Failures are typically caused by firewall rules blocking IP address 137.135.243.254 [5], intermittent satellite connectivity during the download, or insufficient disk space. In September 2025, one vessel reported persistent ADP update failures that were traced to a new corporate firewall policy blocking port 443 to the update server, a change that had been applied across the fleet without notification to the navigation support team.

4.3.2 ADP Activation Failure

Similar to the eNP activation, ADP activation requires access to a specific endpoint at adpactivation.ukho.gov.uk on IP address 62.172.108.45, ports 20 and 21 [5]. The most common failure pattern is a firewall configuration that permits update downloads but blocks the separate activation endpoint. These use different IP addresses and ports, so permitting one does not automatically permit the other.

4.4 AVCS and ECDIS Issues

4.4.1 Permit Synchronisation Failures

Permit synchronisation between NaviServer and the UKHO server must be maintained at each tier of the distribution chain [17]. The most complex cases encountered during the internship involved vessels that had received chart installations from physical media during a drydock period. This creates a divergence between what the platform database believes it holds and what permits the UKHO has issued. Resolving these cases required coordinating between the vessel, NaviServer and the UKHO to reconcile the records. In one case during September 2025, a bulk carrier emerged from drydock with chart DVDs installed directly into the ECDIS, bypassing the normal distribution chain. Reconciling the Holdings record with the UKHO's permit registry took three days of coordination.

4.5 TLS 1.2 Technical Requirements and Diagnostic Significance

TLS 1.2, as defined in RFC 5246 [12], is the minimum protocol version accepted by the server. The Windows Schannel security provider handles TLS negotiation at the operating system level and its configuration is controlled through the Windows registry [13]. The NIST SP 800-52 guidelines provide the configuration standards that the server's TLS requirements align with [14].

According to the IT/ICT Reference Guide [5], without TLS 1.2 properly enabled, communication will be completely dropped. Windows 7 only supports TLS 1.2 if Service Pack 1 is installed and the KB3140245 update has been applied. Without this, TLS 1.2 will not appear in Internet Options. Editing the registry incorrectly can cause system issues, so registry keys should always be exported before making changes.

The configuration process consists of two parts [5]. Part A involves enabling TLS 1.2 via Internet Options: opening Internet Properties, navigating to the Advanced tab, scrolling to the Security section and checking "Use TLS 1.2" while unchecking older protocols for better security. Part B involves cleaning custom TLS/SSL settings in the Windows registry by navigating to the Schannel Protocols key at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols, backing up the key, removing all custom override subkeys except TLS 1.2 and rebooting Windows so Schannel reloads with default settings.

The diagnostic significance of TLS failures must be understood precisely. A TLS handshake failure means the TCP connection to the server completed successfully, meaning the server is reachable, the route exists and port 443 is open. The failure occurred during the protocol negotiation phase, after the TCP handshake but before any application data was exchanged [12]. In the communications log, this appears as an SSL_ERROR, HANDSHAKE_FAILURE, or CryptographicException entry, not as a connection timeout. A timeout means the request never reached the server. A handshake failure means it reached the server and was rejected at the protocol level. Misreading a handshake failure as a network problem directs the entire investigation incorrectly and wastes hours on checks that will not identify the cause.

Table 5: Windows Configuration Summary (Source: [5])

Windows Version	Requirements	Recommendation
Windows 7	SP1 + manual TLS setup + .NET 4.8 offline installer	NOT RECOMMENDED
Windows 8+	Verify TLS 1.2 + .NET Framework 4.8+	RECOMMENDED

Case example: In October 2025, a bulk carrier running Windows 7 reported that all server communication had stopped after a routine Windows update. The communications log showed HANDSHAKE_FAILURE errors. Investigation revealed that the Windows update had reset the TLS registry settings, disabling TLS 1.2 and reverting to TLS 1.0, which the server rejected. Re-enabling TLS 1.2 through the registry and restarting the nGateway service restored communication immediately. The total resolution time was approximately 45 minutes once the correct diagnosis was reached, but the vessel had spent two days attempting network-level fixes based on an incorrect assumption that the problem was connectivity-related.

Chapter 5: Operations and Incident Monitoring

Fleet operations monitoring and incident response were two of the most consistently demanding and professionally formative aspects of the internship. Effective monitoring prevents incidents from developing; incident response becomes necessary when monitoring has not caught a problem early enough, or when a problem arises faster than any monitoring system can detect.

5.1 Fleet Monitoring Through NaviServer

The daily monitoring routine involved systematic review of the NaviServer dashboard to identify signals requiring attention [2]. Three categories of signal were most operationally significant: vessels that had ceased communicating with the server beyond their normal schedule, suggesting a potential nGateway failure or connectivity interruption; chart permits and contract licences approaching expiry within the next thirty days, requiring renewal action before a compliance gap developed; and vessels showing pending updates that had not been downloaded within a reasonable period after publication, potentially indicating a connectivity or configuration issue.

Developing the judgment to distinguish routine signals from those requiring action took time and accumulated exposure. A vessel absent from the server for twelve hours may simply be in a scheduled communication window or a port with limited connectivity, or it may have experienced a nGateway failure that nobody on board has noticed yet because the system appears to be running normally from the interface. Reading the pattern of absences, understanding each vessel's normal communication schedule and knowing the typical connectivity profile of its operating region were all required to make that judgment accurately.

Permit management was particularly consequential. During the internship, I tracked approximately 25 vessels through their permit renewal cycles [17]. The practice of renewing permits two to three months ahead of expiry exists because the renewal process involves coordination between the vessel, NaviServer and the UKHO server and that coordination takes time. In two cases, late identification of expiring permits nearly resulted in compliance gaps that would have been flagged during port state control inspections [10].

5.2 Incident Response Process

When a support request arrived, whether through the Zoho Desk ticket queue [18], a direct email, or an escalated call, the response followed a consistent structure that became increasingly automatic as the internship progressed.

The first step was always to understand precisely what the vessel was experiencing. Officers describe problems in operational language: "the charts are not updating" or "the system has stopped working." Neither of these tells the diagnostician what they need to know. The specific symptom, the last successful operation, the communications log entries and the error messages visible on screen are the evidence that can guide diagnosis.

The second step was diagnosis. Matching the specific symptom to its underlying cause required reading the available evidence without prejudice, using the communications log, the NaviServer account status, the vessel's known configuration history and the specific error presentation to form and test hypotheses. Early in the internship this process was exploratory and often required guidance from more experienced colleagues. As the internship progressed and pattern recognition developed, the same evidence pointed more quickly and reliably to the correct diagnosis.

Case example: One specific instance stands out from late October 2025. A container vessel reported "system not working" in a single-line email. Based on the vessel's history in NaviServer, showing a last server contact three days prior, I suspected a nGateway issue, asked for a screenshot of the communications log, confirmed a timeout pattern indicating a firewall change and resolved the case within two hours of the initial report. Three months earlier, the same presentation would have taken me a full day.

The third step was resolution and documentation. When a fix could be applied directly, it was applied, verified and the ticket was updated with the complete record of what was found and what was done. Every case, regardless of complexity or outcome, was documented in Zoho Desk [18] with sufficient detail that any team member could understand the full history without a briefing.

5.3 What Operations Monitoring Taught

The central lesson from the operations and monitoring work was the practical meaning of proactive management. A shore team that checks the dashboard daily, knows the normal pattern for each vessel in the fleet and acts on deviations before they become vessel-initiated support calls is using the technology to its full effect. A team that checks weekly and responds only when vessels report problems uses the same technology to far less effect. The gap between those two outcomes is not a technology gap. It is a professional practice gap. Understanding that distinction was one of the most lasting things the internship produced.

5.4 Operational Lessons from Fleet Monitoring

Three specific operational lessons emerged from the daily monitoring routine that are worth documenting for future reference.

First, permit expiry management requires a longer lead time than the system default warnings provide. The platform generates an automatic warning approximately one month before permit expiry [3]. In practice, one month is not sufficient when the renewal requires coordination between the vessel, the shore office, the distributor and the UKHO [17]. The distributor must verify the renewal terms, the shore office must approve the commercial commitment, the UKHO must issue new permits and the vessel must download and install them. Each step in this chain can introduce delay. The effective practice at CAIM Sea was to begin the renewal process at least two months before expiry and to flag any vessel within 90 days of expiry during the daily monitoring review.

Second, connectivity patterns are diagnostic information. Each vessel in the fleet develops a characteristic communication pattern: how often it contacts the server, at what times of day and how the pattern changes with operating region. Deviations from this established pattern are early indicators of potential issues. A vessel that normally connects every six hours but has not connected for 24 hours may simply be transiting a region with poor satellite coverage, or it may have experienced a nGateway failure. Knowing the vessel normal pattern and its current operating region, is necessary to distinguish between the two possibilities.

Third, post-drydock support requires proactive outreach rather than reactive response. Vessels emerging from drydock almost always have configuration issues that need attention, whether from hardware changes, network reconfiguration, or chart data installed from physical media during the drydock period. Reaching out to vessels within the first week after drydock completion, rather than waiting for them to report problems, consistently produced better outcomes and shorter resolution times. During the internship, I monitored approximately eight vessels through post-drydock transitions and in six of those cases, proactive outreach identified issues that the vessel officers had not yet noticed.

Chapter 6: Documentation and Professional Communication

Professional communication in a maritime IT support context is governed by a requirement that sounds simple and is not: every communication must enable the recipient to take the correct action. Not to understand the situation in depth. Not to appreciate the diagnostic reasoning behind the recommendation. To take the correct action, under operational pressure, with the information and context available to them, in the time available to them.

6.1 Zoho Desk Ticket Management and Support Workflow

Every support request entering the team from vessels, shore offices, fleet managers, or technical contacts was captured in the Zoho Desk platform as a ticket the moment it arrived [18]. The platform converted incoming emails automatically into tracked tickets assigned to the appropriate queue. The queue structure reflected the operational states of support work: Unassigned for new tickets awaiting allocation; Assigned for active cases with a designated handler; Open for cases that have received a reply and are awaiting the customer's response; Escalated for cases requiring elevated priority or senior involvement; Order Approvals for chart or publication orders requiring commercial authorisation before processing.

The continuity the platform provided was its most operationally significant capability. Every ticket contained the full history of the case from first contact: the original request, all subsequent correspondence, internal comments from team members, actions taken, results observed and current status. A team member encountering a ticket for the first time could understand the complete context, the current state of the problem and the next appropriate action without any briefing or handover.

6.2 Ticket Lifecycle and Communication Discipline

The communication skills developed through working in Zoho Desk were among the most durable outcomes of the internship. The challenge was calibration: adjusting the content, depth, tone and format of every response to what would be most effective for the specific recipient in their specific operational context.

A reply to a vessel officer on a working bridge must be short enough to read in one pass, structured so that steps are numbered and unambiguous and written at a technical level that assumes operational maritime competence but not software engineering knowledge. It should tell the officer precisely what to do, in exactly which order and what to expect when each step is complete. Any information not needed to complete the resolution is noise at the moment the officer is reading the message.

A reply to a shore-side fleet manager can carry more contextual information explaining what was found, what was done and what the implications are for the vessel's chart compliance status. A reply to a technical contact at a shipping company can use more precise technical terminology and can engage with the diagnostic reasoning.

Case example: The most common early error was over-explanation. In June 2025, I wrote a detailed response to a vessel officer explaining the TLS handshake process and why their Windows 7 machine needed registry modifications. The officer's follow-up made clear that the explanation had been confusing rather than helpful. The same issue, rewritten as four numbered steps with no background explanation, was resolved on the first attempt. That pattern repeated often enough that writing concisely for the recipient became a conscious discipline.

Chapter 7: Skills Gained and Professional Development

7.1 Technical Competence

The most significant technical development was in diagnostic methodology, not in the sense of learning a fixed set of procedures for named error types, but in developing the underlying reasoning discipline that makes diagnosis effective for novel problems as well as familiar ones. Understanding the ecosystem as a connected system where the nGateway depends on the Windows TLS configuration [12], [14], which depends on the Schannel registry settings [13], which may be overridden by previous software installations, means that a communication failure is not a single diagnostic question but a structured set of possible causes arranged by likelihood and testability.

Specific technical skills acquired and exercised to professional competency during the placement include: platform installation, activation and configuration management; nGateway communication diagnosis and reconfiguration; TLS 1.2 configuration on Windows 7 including registry-level diagnosis and correction [5]; AVCS chart and permit lifecycle management through NaviServer [17]; ADP and eNP reader installation, activation and update management [15], [16]; S63 decryption error resolution; PAYS permit management and excluded area identification; voyage plan generation with UKC review; NaviServer account setup and services configuration [2]; and Zoho Desk ticket management and professional support communication [18].

7.2 Communication and Professional Standards

Communication development during the internship was more demanding and more consequential than anticipated at the outset. The writing quality was not the challenge. The challenge was the professional judgment required to produce responses that were precisely as long, as technical, as structured and as detailed as their specific recipients required and no more.

The discipline of writing short was particularly demanding. When a problem is understood clearly and the solution is confirmed, the natural impulse is to write a comprehensive response that demonstrates that understanding. For most maritime support recipients, that comprehensive response is counterproductive, as it buries the actionable steps in context they do not have time to process.

The Zoho Desk platform [18] reinforced this discipline through two mechanisms: every reply was visible to the whole team and could be reviewed, creating an implicit standard; and the follow-up questions generated by unclear replies provided direct feedback on where replies had missed the target.

7.3 Working Under Operational Pressure

The capacity to work effectively under pressure, to maintain diagnostic discipline, clear communication and professional composure when a vessel has a hard deadline and the problem is not resolving quickly, is a competency that cannot be developed except under actual pressure. Simulations and academic exercises do not carry the operational weight of a real vessel waiting for a chart update before departure.

Case example: In one case in September 2025, a car carrier preparing to depart Rotterdam reported a complete AVCS failure two hours before sailing. The diagnosis required checking three separate subsystems (nGateway status, NaviServer permit status and Active Folio configuration) before identifying that a recent Active Folio change had not been synchronised with the UKHO server [17]. The vessel departed on time. Working through that case under genuine time pressure, without skipping diagnostic steps, was a concrete demonstration that the methodology works.

The confidence that developed was not the confidence of having encountered every possible problem. It was the confidence of knowing, from demonstrated experience, that methodical thinking applied consistently under pressure produces results and that the discomfort of not knowing the answer immediately is a normal and manageable feature of professional work rather than a signal of inadequacy.

Chapter 8: Reflections and Challenges

8.1 The Immediate Challenge of Operational Pace

The most disorienting aspect of the internship in its early weeks was the pace. Support cases arrived continuously and the operational expectation, from the first day, was contribution rather than observation. There was no protected familiarisation period during which the systems could be explored and knowledge consolidated before being applied under operational conditions.

This was, retrospectively, the single most educationally valuable feature of the placement. The first two weeks produced more practical competency development than any equivalent period of supervised learning could have delivered, not because the content was more sophisticated, but because the requirement to apply it in real time, with real consequences for real vessels, forced engagement at a depth that voluntary learning cannot replicate.

8.2 Technical Complexity and the Discipline of Not Assuming

Problems that presented with elaborate error messages and multiple simultaneous symptoms sometimes turned out to have a single straightforward cause: a stopped service, an incorrect registry entry, a permission setting that had changed. Problems that appeared straightforward sometimes indicated underlying issues of significant complexity requiring careful investigation.

Case example: In August 2025, a vessel reported a communication failure that looked identical to a case I had resolved the previous week by restarting the nGateway service. I applied the same fix, told the vessel it was resolved and the problem returned two days later. The actual cause was a TLS registry conflict [13] that the restart had temporarily bypassed. The lesson was direct: confirming that a resolution has worked is not the same as confirming that the underlying cause has been corrected. Where the cause has not been positively identified, the resolution should be treated as provisional and the case kept under review.

8.3 Communication Under Frustration

The most professionally demanding communication situations during the internship were not the technically complex cases but the cases involving frustrated customers. A vessel that has been unable to receive chart updates for three days before a planned departure and whose previous contacts with the support team have not resolved the problem, does not communicate in a tone that makes clear thinking easy.

Case example: In October 2025, a fleet manager escalated three times within 24 hours over an eNP registration failure [16]. By the time the ticket reached me, the tone was hostile. I replied with a numbered list of four diagnostic steps, a specific timeline ("I expect to have the registration cleared within 4 hours"), and the contact at the UKHO I was coordinating with. The manager's next reply was professional and the case was closed that afternoon. The most reliable approach was to focus on the problem rather than on the communication tone, to be specific about what had been established and to set realistic and honest expectations about timeline.

8.4 The Value of Difficulty

The cases that were most demanding, that resisted easy resolution, that required coordination across multiple parties, were the cases that produced the most durable learning. The competencies developed through those cases were not narrowly applicable to the specific technical content of the cases themselves; they were broadly transferable diagnostic and professional orientations that will apply across any future context that presents genuine complexity.

A placement that presents only familiar problems with known solutions may feel productive in the moment but produces limited professional development. The discomfort of the difficult cases during this internship was evidence that genuine development was occurring.

Chapter 9: Conclusion and Recommendations

9.1 Key Technical and Professional Conclusions

The platform's operational effectiveness in any deployment depends entirely on the correctness of the infrastructure surrounding it: the nGateway configuration [3], the Windows TLS settings [12], [13], [14], the firewall rules [5], the NaviServer account configuration [2], and the consistency of the Active Folio management. Supporting the platform effectively requires understanding it as a distributed system with multiple potential failure points, each with characteristic symptom patterns and each requiring a different diagnostic approach. That understanding cannot be acquired from the platform documentation alone; it develops through the accumulated experience of real cases.

The AVCS chart management ecosystem, from the UKHO server through NaviServer to the platform to the ECDIS, is a chain with multiple potential points of divergence between what the system believes it holds and what is actually installed [17]. Maintaining synchronisation throughout this chain requires consistent workflow discipline: all chart management through the platform, all Active Folio changes reflected on NaviServer, all Holdings updates completed before departure. When that discipline lapses, the divergence that accumulates is not immediately visible and can produce compliance gaps that only become apparent under inspection pressure [10].

Professional communication in technical support is a discipline, not merely a skill. The difference between a response that enables the recipient to resolve their problem immediately and one that generates a clarification request is not primarily a matter of technical accuracy. It is a matter of whether the response was written for the recipient's operational context or for the writer's professional satisfaction.

9.2 Recommendations for the University Programme

The most consequential gap between the academic preparation provided by the STRATEGOS programme and the operational readiness required at the start of a professional maritime IT placement was familiarity with the actual software tools used in the industry. Arriving without prior exposure to the platform, NaviServer, or the Zoho Desk support platform meant that the first several weeks of the placement were consumed by orientation to the tools rather than by the higher-order competencies that the placement is designed to develop.

The recommendation is practical and achievable: integrate industry-standard maritime navigation software into at least one module of the STRATEGOS curriculum. Demonstration environments, screen-recorded walkthroughs of key workflows and structured exercises around the types of decisions and problems documented in Chapter 4 of this thesis would provide meaningful pre-placement familiarity. The regulatory and strategic content of the programme, including SOLAS [10], MARPOL [9], maritime cybersecurity frameworks [1], [11], and ISM management systems, proved directly applicable in the operational environment and required no further development. The gap was specifically in applied technical tool knowledge.

9.3 Recommendations for Future Interns

Arrive ready to contribute, not to observe. The placement does not begin with a protected orientation period. It begins with real cases and operational expectations from the first day. That is both the most demanding and the most valuable feature of the experience.

Ask questions without hesitation. The experienced professionals in a maritime support environment have encountered, in most cases, every problem category that will appear during the placement. Their accumulated pattern recognition and diagnostic experience is a resource of enormous value that is available only if it is actively sought.

Document everything. The habit of maintaining thorough, accurate case records [18] complete enough that any team member can understand the history and current state without a briefing is both a professional standard and a learning tool. Reviewing closed cases, particularly difficult ones, is one of the most reliable ways to consolidate diagnostic pattern recognition and communication skills.

What this placement produces is not a finished professional. Six months is not sufficient for that. What it produces is someone who understands what the work involves, has begun building the diagnostic and communication instincts that operational experience develops and is better equipped to continue developing professionally than was possible from academic preparation alone.

9.4 Future Directions in Maritime Navigation Software

Maritime navigation software is converging with broader maritime digitalisation trends. The IMO cyber risk management guidelines [11] and BIMCO standards [1] are increasingly integrated into port state control inspection frameworks. Vessels that cannot demonstrate adequate cybersecurity controls, including secure communication channels for chart and publication updates, face potential detentions. CAIM's NGBox and NGLink products address this directly by providing encrypted, authenticated communication between the ECDIS and shore-based servers.

The shift toward autonomous shipping and increased shore-based control will further increase the importance of reliable, secure communication between vessel and shore. The skills developed during this placement, including diagnostic reasoning for distributed systems, communication calibration for operational contexts and workflow management for fleet-scale operations, will remain directly applicable as these trends develop.

Appendix A: Extended Technical Reference

A.1 NaviGate System Architecture Overview

The platform may be part of architectures more complex than the standard standalone configuration [3]. These include automated collection of AVCS from shore, sending navigation data to shore and sending ENC updates to the ECDIS through an IT-secured channel using the NGBox and NGLink hardware. The standard architecture consists of the platform running on a PC connected to the Internet, communicating through the nGateway service to the maritimegate.net server on port 443 using HTTPS [5]. More advanced configurations integrate NGBox for encrypted, authenticated communication between the ECDIS and the distribution server, addressing the cybersecurity requirements that regulators are increasingly enforcing [11].

A.2 The NMEA 0183 Protocol and GPS Integration

GPS integration uses the NMEA 0183 protocol [8], with the serial device server converting the vessel's GPS serial output to a network-accessible data stream. Confirming that NMEA sentences are arriving correctly is essential for MRV voyage recording, environmental monitoring and fleet tracking through NaviServer [2]. The GPS Incoming Data display within the platform provides this confirmation. Common issues include incorrect COM port selection, baud rate mismatches and configuration errors where the serial port mode is set incorrectly.

A.3 AVCS Chart Cell Architecture and S57/S63 Standards

AVCS chart cells are distributed in S57 format (the IHO standard for electronic navigational chart data) and encrypted using the S63 standard [17]. Each cell is identified by a unique cell name and carries a specific edition number and update number. Permits are issued by the UKHO for specific cell sets and are tied to the vessel's licence. S63 decryption errors occur when the permit does not match the cell edition, when the permit has expired, or when the encryption keys have become corrupted. These errors require permit resynchronisation through NaviServer.

A.4 Environmental Compliance in NaviGate

The platform's environmental compliance features directly support MARPOL requirements [9] and EU MRV regulation [7]. ECA and SECA zones appear as overlays on the chart through the Environment layer [3]. Environmental events are recorded in the voyage plan automatically. The NaviGreen module tracks compliance in real time, recording fuel consumption, emission calculations and zone entry/exit times. Experiencing environmental regulation as a designed system feature rather than an administrative requirement changed how the regulatory framework was understood during the internship.

A.5 Cybersecurity Considerations in Maritime Navigation Software

The IMO Guidelines on Maritime Cyber Risk Management [11] and the BIMCO guidelines [1] establish the framework within which maritime cybersecurity is now assessed. Port state control authorities in several jurisdictions have begun incorporating cybersecurity verification into their inspection checklists. The use of TLS 1.2 [12] for all server communications, the requirement for dedicated navigation PCs with no cloud synchronisation [5], and the availability of NGBox/NGLink hardware encryption represent the practical implementation of these guidelines within the CAIM Sea product ecosystem.

A.6 Seasonal and Regional Patterns in Maritime Support

Maritime IT support work is not uniformly distributed across the calendar year or across geography. Vessel drydock periods, typically scheduled during quieter trading seasons, generate concentrations of support requests related to hardware replacement, system reinstallation and configuration update following shipyard work. During the internship, vessels emerging from drydock frequently required activation and reactivation, presented firewall and TLS diagnostic cases from network reconfiguration and needed database synchronisation after receiving physical chart DVDs during the drydock supply process.

Seasonal trading patterns affect the geographic distribution of support requests in predictable ways. Vessels moving into high-latitude routes for the summer season encounter connectivity constraints as satellite coverage and bandwidth quality change with position. The same vessel that has been updating charts reliably through an equatorial route may find that Offline mode becomes the only viable communication option when operating north of 70 degrees latitude. Support teams need to anticipate these transitions and ensure vessels are prepared with current charts, the Active Folio appropriately configured [2], and Offline mode procedures understood before the transition occurs.

A.7 Lessons from Failure Cases

Some of the most instructive professional experiences during the internship came from cases where the initial approach was wrong, the diagnosis was delayed, or the resolution created a new complication. These failure cases, approached honestly and analytically, produced some of the most durable learning.

One instructive failure involved premature closure on a diagnosis. In August 2025, a case where nGateway communication had been restored through a service restart appeared resolved; the vessel confirmed updates were downloading. But the underlying cause had not been identified. Two weeks later the same vessel reported the same problem. The pattern of recurrence pointed to a TLS registry conflict [13] that had been temporarily bypassed by the restart. The lesson: confirming that a resolution has worked is not the same as confirming that the underlying cause has been corrected.

Another instructive failure involved underestimating scope. A vessel presenting with an AENP permit failure turned out, on deeper investigation, to have a sequence of interconnected issues: the permit failure was caused by a corrupted registration, which was caused by a Windows cryptographic folder issue, which had been partially addressed by a previous IT intervention that was not documented. Working through each layer in sequence took longer than the initial estimate but produced a stable and complete resolution.

A.8 Summary of Key Competencies Developed

In the technical domain: platform installation, activation and reconfiguration including nGateway management and TLS configuration on Windows 7 and Windows 10 [5]; AVCS chart and permit lifecycle management through NaviServer [17] including Holdings, Active Folio and PAYS administration; ADP and eNP reader installation, activation and update management [15], [16]; S63 decryption error diagnosis; Windows system administration relevant to navigation software including TLS registry management [13]; and Zoho Desk ticket management throughout [18].

In the communication domain: calibrated technical communication to vessel officers, fleet managers, technical contacts and non-technical stakeholders; internal case documentation to a standard sufficient for seamless team handover; escalation communication with distributor technical teams, satcom providers and the UKHO; and professional management of time-pressured customers without compromising diagnostic accuracy.

In the operational domain: fleet monitoring through NaviServer [2] for connectivity status, permit expiry and update completion; proactive permit and contract renewal management; incident response process execution from symptom gathering through diagnosis, resolution and documentation; and multi-party case coordination across vessels, distributors and service providers.

A.8 NaviGate Integration with Third-Party ECDIS: Operational Procedures

The Check Route function within the Tools section performs a safety verification of the active route against the installed chart data [3]. It lists all dangers found under the route according to the safety depth and safety contour values set in Map and Display. Dangers are classified as either Alarm (safety contour dangers, which are always set as alarm) or Indication (other dangers which may be qualified as Indication or Alarm by the user). This classification is significant because it determines whether the danger generates a mandatory response or an informational notification during the voyage.

dangers can be highlighted on the chart by clicking in the results panel, but the correct chart scale must be used to see the highlighted object, as each belongs to an ENC with minimum and maximum display scales. During the internship, this function was used extensively when reviewing voyage plans before departure. In one notable case in October 2025, the Check Route function identified a shallow-water danger along a planned route through the Strait of Malacca that had not been visible at the overview scale the officer was using for planning. The danger was a recently charted wreck that appeared only at scales larger than 1:200,000.

The ERBL (Electronic Range and Bearing Line) tool displays a range and bearing measurement line on the chart for calculating distances and bearings between any two points [3]. A second ERBL can be displayed simultaneously, allowing parallel measurements. The Distance Measuring tool provides simple point-to-point distance calculation. The Time Zones tool displays the local time and UTC offset at any cursor position on the map. The Search Ports function provides a searchable database of global ports with the ability to display selected ports on the chart.

The NaviGreen Environmental Module tracks the vessel position against environmental regulation zones in real time [3]. When the vessel enters or exits an ECA, SECA, PSSA, or other regulated zone [9], the module records the event with timestamp and position. These records are compiled into environmental compliance documentation that can be presented during port state control inspections [10] or submitted as part of the company environmental management records. The module operates passively in the background and requires no manual intervention once the GPS feed is established and the environmental layers are enabled.

The Flag States module and NaviFlag database provide access to a comprehensive collection of flag state regulations, international circulars and maritime authority documents [3]. The database is organised by flag state and includes documents from major maritime authorities including Panama, Liberia, Marshall Islands and the Bahamas, as well as international organisations. During the internship, this module was used primarily by shore-side fleet managers preparing for port state control inspections in specific jurisdictions, where flag-state-specific requirements needed to be verified against the vessel documentation.

A.9 NaviGate Integration with Third-Party ECDIS Systems

The platform operates both as a standalone voyage planning tool and as an integrated component within a broader bridge navigation system [3]. When integrated with an ECDIS, the platform manages the AVCS chart permits and updates centrally, exporting permit files and chart data to the ECDIS through the AVCS section of the main status menu. The export function generates a permit file package that can be transferred to the ECDIS via USB media or, where available, through a direct network connection.

the platform manages two separate AVCS databases: the ECDIS Database (charts installed in the ECDIS) and the internal database (charts installed and displayed within the platform). When all charts and updates are managed and downloaded only through the platform, the two databases remain synchronised. However, when chart installations occur from physical media such as during drydock periods or when the ECDIS receives updates from an independent source, these databases can diverge. This divergence was encountered multiple times during the internship and represents one of the more complex diagnostic scenarios in AVCS management.

The direct network connection capability, described in the User Manual chapter on ECDIS900 integration [3], allows the platform to communicate directly with compatible ECDIS hardware over the vessel LAN. This eliminates the need for USB transfer of chart data and permits, streamlining the update workflow considerably. However, the network connection must be properly configured with correct IP addresses and port settings on both the platform PC and the ECDIS and the vessel LAN must permit traffic between the two devices.

A.10 Connecting to Ship NMEA Instruments

The platform can receive data from the vessel NMEA instruments through several connection methods [3]. The most common configuration uses a to convert the GPS serial output to a TCP/IP data stream accessible over the vessel LAN. This configuration requires setting the correct COM port, baud rate (typically 4800 for NMEA 0183), and data format (8 data bits, no parity, 1 stop bit) in both the and the platform settings.

When properly configured, the platform receives GGA, RMC and other NMEA sentence types from the GPS receiver, enabling position display on the chart, MRV voyage recording, NaviGreen environmental zone tracking and fleet position reporting through NaviServer [2]. The GPS Incoming Data display in the platform provides confirmation that sentences are being received correctly and shows the raw NMEA data for diagnostic purposes.

AIS targets can also be monitored through the platform when an AIS transponder is connected via the NMEA interface [3]. AIS target information is displayed as overlay symbols on the chart, with vessel name, MMSI, speed and course information available through right-click interrogation. This functionality supports situational awareness during voyage planning and monitoring.

A.11 IT Security: NGBox and NGLink

CAIM has developed NGBox and NGLink as hardware security solutions for the maritime navigation data chain [3]. NGBox is installed on the vessel and establishes an encrypted, authenticated tunnel between the ECDIS on the bridge and the shore-based distribution server. NGLink is the shore-side counterpart that manages the encryption keys and certificate infrastructure.

These products address a genuine and growing regulatory requirement. The IMO Guidelines on Maritime Cyber Risk Management [11] require shipping companies to incorporate cyber risk management into their Safety Management Systems. The BIMCO Guidelines on Cyber Security

Onboard Ships [1] provide detailed implementation guidance. Port state control authorities in the EU, United States and Asia-Pacific region are increasingly incorporating cybersecurity verification into their inspection checklists. Vessels that cannot demonstrate adequate cybersecurity controls face potential detentions.

NGBox operates transparently within the existing architecture. Chart updates and permit data flow through the encrypted channel without requiring changes to the platform configuration or the ECDIS settings. The encryption uses current cryptographic standards and the certificates are managed centrally through NGLink, reducing the burden on vessel IT staff. During the internship, I assisted with the configuration of NGBox on two vessels as part of a pilot deployment programme. The process required careful coordination between the vessel IT setup, the NGBox hardware installation and the NGLink shore-side configuration, but once operational, the system required no ongoing intervention.

A.12 Voyage Plan Compliance and Port State Control Readiness

The Voyage Plan module generates outputs that directly support port state control inspection readiness [10]. The UKC calculations, chart currency status, publication holdings and environmental compliance records produced by the module constitute the documented evidence that inspectors review when assessing a vessel compliance with SOLAS Chapter V requirements.

During the internship, I assisted with the preparation of voyage plans for approximately 15 departures where the vessel master specifically requested a compliance check against port state control requirements. In each case, the process involved verifying that the Active Folio covered the planned trading area [17], confirming that all charts along the route were updated to the current week, checking that safety depth and contour values were correctly set for the vessel draught and ensuring that environmental compliance zones were properly displayed and recorded in the voyage plan [7].

The most common compliance issue identified during these checks was chart cells in the Active Folio that had not been updated because the vessel had been operating in Offline mode and the email-based update files had not been imported in the correct sequence. This resulted in charts that were technically held but not current to the latest weekly update, a condition that would be flagged during an inspection.

A.13 Managing the Transition from Legacy to Current Systems

Several vessels supported during the internship were in various stages of transitioning from older software configurations to the current platform version. These transitions presented unique challenges because they involved not only software installation but also the migration of chart holdings, permit records, route libraries and ship model data from the previous system.

The migration process typically followed a sequence: backup of the existing installation using the System menu backup function [3], clean installation of the current version, activation using new credentials from the distributor, restoration of backed-up data where compatible and full catalogue recovery followed by Check for Updates. The most common complication was permit incompatibility between the old and new installations, requiring permit resynchronisation through the UKHO [17].

On Windows 7 machines, the migration also provided an opportunity to address legacy TLS configurations [13]. Several vessels had registry entries from previous software installations that explicitly disabled TLS 1.2 or forced older protocol versions, configurations that would have caused immediate communication failures on the current platform. Identifying and cleaning these legacy registry entries, using the procedure described in the IT/ICT Reference Guide [5], was a standard part of the migration workflow.

A.14 Knowledge Management and Institutional Learning

The Zoho Desk platform [18] served not only as a ticket management system but also as an institutional knowledge base. The accumulated closed tickets, spanning several years of support operations, constituted a searchable archive of precedent cases that made recurring issue types faster to recognise and resolve. When encountering an unfamiliar error or symptom pattern, searching the closed ticket archive frequently revealed a previous case with the same presentation, including the diagnosis that was reached and the resolution that was applied.

This institutional knowledge was complementary to the individual pattern recognition that developed through personal case experience. Where personal experience provided speed and confidence in recognising familiar patterns, the ticket archive provided access to patterns encountered by other team members at different times, on different vessel types and under different operational conditions. Together, these two knowledge sources, personal experience and institutional archive, formed the diagnostic foundation that support work relied on.

A.15 Communicating Technical Complexity to Non-Technical Stakeholders

A recurring professional challenge was explaining technical situations to stakeholders who had no technical background but had direct operational or commercial interest in the outcome. Fleet managers, company directors and vessel owners are regularly involved in decisions about maritime IT systems, whether to renew a licence, whether to upgrade a PC, whether to invest in NGBox infrastructure, without having the technical foundation to evaluate the options on technical grounds alone.

The most effective approach observed was to anchor technical explanations in operational consequences rather than technical mechanisms. A fleet manager does not need to understand what a TLS handshake failure is or how the Windows Schannel registry tree is structured [13]. They need to understand that the vessel cannot receive chart updates while this problem exists, that this creates a compliance risk if the vessel departs without current charts [10], and that the resolution requires a specific sequence of steps that will take a specific amount of time. Framing technical complexity in terms of operational impact and resolution timeline provides the information the stakeholder needs to make informed decisions without requiring them to understand the underlying technical content.

This translation between technical and operational language required conscious development. Early attempts were too technical, explaining the mechanism when the stakeholder needed the impact. Developing sensitivity to whether a communication had produced the understanding needed for a decision and the flexibility to reformulate explanations quickly when it had not, was one of the more valuable communication skills the six months produced.

A.16 Operational Detail: Paper Charts, ISM Reports and Ship Data

The platform approach to paper chart management goes beyond simple inventory tracking. The NTM corrections module downloads the latest Notice to Mariners corrections from the server and provides tools for printing correction overlays, marking corrections as applied and generating compliance reports that document the correction status of every paper chart in the vessel holdings [3]. This is particularly relevant for vessels that maintain a dual chart outfit, electronic and paper, as required by some flag state regulations and certain trade routes where electronic-only navigation has not yet been approved [10].

The ISM Reports function generates three categories of compliance report: AVCS holdings reports showing the current status of all electronic chart cells; paper chart currency reports documenting the NTM correction status; and publication status reports listing all required publications with their current update status [3]. These reports are formatted for direct inclusion in the vessel ISM documentation and can be presented to port state control inspectors as evidence of compliance with SOLAS Chapter V requirements. During the internship, I generated ISM reports for approximately 20 vessels, typically in preparation for port state control inspections.

The Ship Data section stores the vessel physical characteristics that underpin all computational functions throughout the platform [3]. The data includes vessel dimensions (length, beam, draft), block coefficient, default sea passage speed and search range parameters. The accuracy of Ship Data entries directly affects the reliability of UKC calculations, Risk Assessment outputs, MRV fuel consumption estimates and weather routing optimisations. Incorrect Ship Data is the single most common root cause of anomalous computational outputs, as identified during the internship across multiple support cases.

A.17 The MRV Reporting Workflow in Detail

The MRV emission reporting workflow integrated into the platform follows the requirements of EU Regulation 2015/757 [7]. The workflow begins with the creation of a voyage record defined by a unique Voyage ID, departure and arrival ports, departure date and the active route. Once the master approves the voyage as Active, the MRV module begins automatic recording of fuel consumption throughout the passage [3].

The recording covers multiple operational phases: fuel consumption at sea during the passage, fuel consumption at anchorage, fuel consumption alongside in port and time spent in ice conditions where applicable. The system uses GPS position data to determine the vessel operational state and the applicable fuel consumption recording mode. On voyage completion, the platform produces two outputs: a PDF summary document for crew verification and signature and an XML file formatted for direct upload to the European Maritime Safety Agency THETIS MRV platform [6].

During the internship, supporting the MRV workflow involved verifying that GPS data was being received correctly, confirming that the Active Voyage had been properly configured, troubleshooting cases where MRV recording had stopped unexpectedly (typically due to GPS feed interruption), and assisting with the generation and export of final voyage reports. In one case in August 2025, a tanker reported that MRV data was incomplete for a 12-day passage across the Atlantic. Investigation revealed that the GPS feed had been interrupted for three days when the device [8] lost its network configuration after a power fluctuation. The missing data had to be reconstructed manually from the vessel deck log and entered into the MRV record through a correction procedure.

A.18 Weather Module: Operational Use and Limitations

The Weather module provides six-day weather forecasts from the Sat-Ocean forecast centre, with new forecasts generated every 12 hours [3]. The module supports two resolution levels: predefined large areas at 1-degree grid resolution and user-defined custom areas at 0.5-degree resolution. The downloaded weather files contain multiple parameters including Wind speed and direction, Atmospheric Pressure, Visibility, 500hPa Geopotential Height, Total Wave height and direction, Swell height and direction, Sea Temperature and Surface Currents.

The data interpolation option smooths the gridded forecast data to display averaged values at any point on the map, providing a more visually continuous representation. However, as noted in the User Manual [3], the interpolation is a mathematical average of the original forecasted gridded data and may not fully represent the real weather situation in some locations, particularly in areas with complex coastal effects or strong local weather patterns.

The Pick Report function, when enabled during weather display, provides a detailed numerical readout of all weather parameters at the cursor position for the selected time. This is particularly useful during voyage planning discussions with the master and shore management, as it provides specific numerical values rather than relying on the colour-coded visual representation alone.

The METAREA display function shows the coverage of each METAREA region and provides access to the last received navigational warnings and weather messages for each area [3]. These messages are received through the regular Check for Updates process and complement the gridded forecast data with text-based warnings from the responsible maritime authority.

Older weather files are automatically moved to a Historical Weather archive, maintaining a record of previous forecasts that can be useful for post-voyage analysis and MRV reporting verification. During the internship, the weather module was used primarily in support of voyage planning and Risk Assessment calculations, where the quality of the weather data directly affects the accuracy of the route optimisation and the ETA calculations.

References

[1] BIMCO et al., "The Guidelines on Cyber Security Onboard Ships," Version 4, BIMCO, Copenhagen, Denmark, 2021. [Online]. Available: https://www.bimco.org

[2] CAIM Sea, "NaviServer Platform Documentation and Internal Support Procedures," CAIM Sea, Genova, Italy, 2025. [Online]. Available: https://caim.it

[3] CAIM Sea, "NaviGate," Version 1.2.7.3, CAIM Sea, Genova, Italy, 2025. [Online]. Available: https://caim.it

[4] CAIM Sea, "Company Overview and Product Information," CAIM Sea, Genova, Italy, 2025. [Online]. Available: https://caim.it

[5] CAIM Sea, "NaviGate, ADP and eNP IT/ICT Department Reference Guide," Version 1.0, CAIM Sea, Genova, Italy, 2025. [Online]. Available: https://caim.it

[6] European Maritime Safety Agency, "THETIS MRV: EU MRV Reporting Platform Technical Documentation," EMSA, Lisbon, Portugal, 2024. [Online]. Available: https://www.emsa.europa.eu

[7] European Parliament and Council of the European Union, "Regulation (EU) 2015/757 on the Monitoring, Reporting and Verification of Carbon Dioxide Emissions from Maritime Transport," Official Journal of the European Union, 2015. [Online]. Available: https://eur-lex.europa.eu

[8] International Electrotechnical Commission, "IEC 61162-1: Maritime Navigation and Radiocommunication Equipment and Systems, Digital Interfaces, Part 1: Single Talker and Multiple Listeners," IEC, Geneva, Switzerland, 2016. [Online]. Available: https://www.iec.ch

[9] International Maritime Organization, "International Convention for the Prevention of Pollution from Ships (MARPOL), as amended," IMO, London, United Kingdom, 1973/1978. [Online]. Available: https://www.imo.org

[10] International Maritime Organization, "International Convention for the Safety of Life at Sea (SOLAS), as amended," IMO, London, United Kingdom, 1974. [Online]. Available: https://www.imo.org

[11] International Maritime Organization, "Guidelines on Maritime Cyber Risk Management," IMO, London, United Kingdom, 2021. [Online]. Available: https://www.imo.org

[12] Internet Engineering Task Force, "RFC 5246: The Transport Layer Security Protocol Version 1.2," IETF, 2008. [Online]. Available: https://www.ietf.org/rfc/rfc5246

[13] Microsoft Corporation, "Windows TLS Protocol Support Documentation," Microsoft, Redmond, Washington, United States, 2023. [Online]. Available: https://docs.microsoft.com

[14] National Institute of Standards and Technology, "Guidelines for the Selection, Configuration and Use of Transport Layer Security Implementations," Special Publication 800-52 Revision 2, NIST, Gaithersburg, Maryland, United States, 2020. [Online]. Available: https://www.nist.gov

[15] United Kingdom Hydrographic Office, "ADMIRALTY Digital Publications User Guide," UKHO, Taunton, United Kingdom, 2017. [Online]. Available: https://www.admiralty.co.uk

[16] United Kingdom Hydrographic Office, "ADMIRALTY eNP Reader User Guide," Versions 1.2 and 1.3, UKHO, Taunton, United Kingdom, 2020. [Online]. Available: https://www.admiralty.co.uk

[17] United Kingdom Hydrographic Office, "Admiralty Vector Chart Service Technical Documentation and User Guidance," UKHO, Taunton, United Kingdom, 2024. [Online]. Available: https://www.admiralty.co.uk

[18] Zoho Corporation, "Zoho Desk: Customer Support Software Documentation and User Guide," Zoho Corporation, 2025. [Online]. Available: https://www.zoho.com/desk