RouteShield-PNT

Route Integrity & Off-Route Prevention with Resilient PNT (Position, Navigation and Timing) for Ship Bridges

Abstract

Modern ship bridges are highly dependent on Global Navigation Satellite Systems (GNSS) for track control and timing. In congested coastal waters and ports, deliberate GNSS jamming and spoofing have moved from rare anomalies to a persistent operational risk, with documented incidents affecting hundreds of vessels at once and contributing to near-misses and groundings in constrained waterways.

At the same time, regulators and standardisation bodies are pushing toward resilient multi-sensor navigation. The IMO's Guidelines for Shipborne Position, Navigation and Timing (PNT) Data Processing call for central processing units that fuse GNSS with onboard sensors such as radar, echo sounders and logs to provide integrity information to bridge teams and applications. New cyber requirements (IACS UR E26/E27) demand that onboard systems be secure and resilient against cyber threats.

RouteShield-PNT is a bridge-network module that implements this "resilient PNT" vision as a product. It continuously checks whether GNSS position and time are consistent with independent shipboard evidence by:

1. Automatically aligning marine radar video to the ENC shoreline.
2. Running dead-reckoning / INS innovation tests against GNSS.
3. Comparing echo-sounder depth to charted soundings, tide-corrected.

4. Verifying GNSS time against an independent reference.

A fusion layer applies timers and confidence weighting, then emits BAM-compliant alerts over IEC 61162-450/-460 to any connected bridge HMI. When confidence in GNSS degrades, RouteShield-PNT de-weights GNSS and guides track-control using dead-reckoning bounded by radar evidence, preserving route integrity until GNSS recovers.

This white paper describes the threat landscape, regulatory context, RouteShield-PNT architecture, key use cases and evaluation plan. It is intended for ship operators, OEMs, class/flag societies and insurers interested in practical, interoperable measures to mitigate GNSS manipulation and silent off-route drift.

Keywords: maritime safety, resilient PNT, GNSS spoofing, route integrity, radar-ENC registration, dead-reckoning, BAM alerts, IEC 61162-450/460, IACS UR E26/E27.

1. Introduction

Maritime transport carries around 80% of global trade. The majority of that tonnage relies on GNSS as the primary input to Electronic Chart Display and Information Systems (ECDIS), Integrated Navigation Systems (INS) and track-control. When GNSS works as intended, it delivers metre-level accuracy and seamless timing. When it does not, the bridge can be left navigating on a beautifully rendered but silently wrong picture.

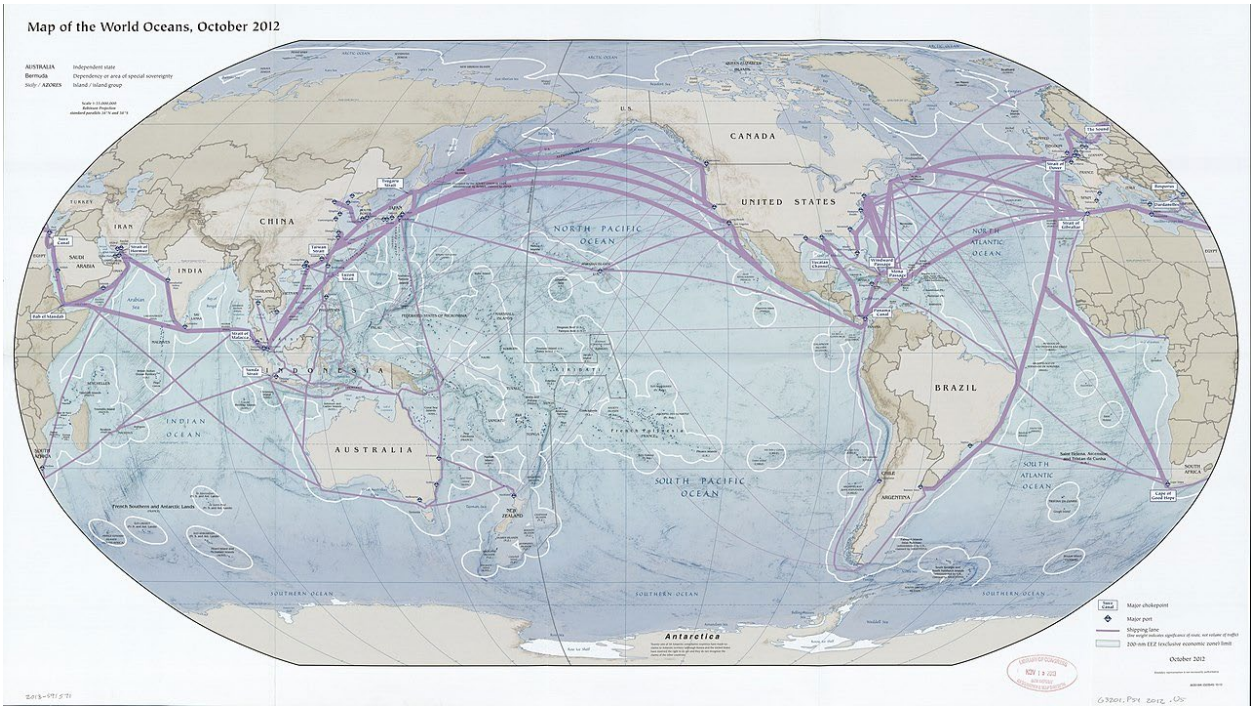

Figure 1 – Global shipping lanes and major ports.

World map showing major shipping routes and ports, illustrating how maritime traffic is concentrated along a limited set of corridors and chokepoints where GNSS disruption has disproportionate impact (image: U.S. Central Intelligence Agency, public domain).

Reports over the last decade have documented GNSS jamming and spoofing around conflict zones, major ports and chokepoints such as the Black Sea and Strait of Hormuz. Ships have appeared hundreds of kilometres inland on their ECDIS, or shown impossible "teleporting" tracks before colliding in restricted waters.

Despite this, the typical mitigation on a busy bridge remains:

- Manual eyeballing of radar overlay versus ENC,
- Occasional dead-reckoning sanity checks, and
- GNSS receiver flags such as RAIM and C/N_0.

These measures are necessary but not sufficient in high-workload harbour and coastal operations. They depend on continuous human vigilance, and they struggle with subtle "carry-off" or time-push spoofing where GNSS remains plausible but wrong.

RouteShield-PNT aims to close this gap with an **automated, vendor-agnostic integrity function** that runs on the bridge LAN, fuses independent sensors and delivers simple, standardised alerts and guidance to the bridge team.

2. Regulatory and Technical Context

2.1 IMO PNT Data Processing Guidelines

In 2017, the IMO issued MSC.1/Circ.1575 – *Guidelines for Shipborne Position, Navigation and Timing (PNT) Data Processing* – which defines the concept of a shipborne PNT data processing (PNT-DP) unit. The guidelines recommend that ships:

- Combine information from multiple PNT sources (GNSS constellations, terrestrial systems),
- Use additional onboard sensors such as radar, echo sounders and logs to verify consistency, and
- Provide a PNT solution together with an integrity flag and status information to bridge systems (ECDIS, AIS, INS, etc.).

RouteShield-PNT can be viewed as a concrete implementation of a PNT-DP unit for existing bridges, with a strong focus on route-integrity alerts and fail-safe behaviour rather than replacing existing GNSS receivers.

Early research on the ship-side PNT Module
Before the IMO issued PNT-DP guidelines, Ziebold et al. proposed an integrated maritime PNT Module as the on-board part of a wider PNT system. The core "PNT Unit" fuses multi-system GNSS/DGNSS with logs, gyro, echo sounder, IMU and potential terrestrial systems (e-Loran, R-Mode) to provide PNT data together with integrity information to the INS and other applications. Their integrity concept uses a three-stage structure: (1) individual sensor self-checks, (2) compatibility checks between similar outputs (e.g. SOG from different sensors), and (3) Kalman-filter-based innovation/residual tests and parallel sub-filters inside the integration algorithm. First sea-trial results on the survey vessel **DENEB** demonstrate this architecture and highlight practical issues such as sensor mounting positions.

RouteShield-PNT can be seen as a product-oriented continuation of this integrated PNT Module idea, with a different sensor emphasis (radar↔ENC registration, depth-vs-ENC, GNSS-independent time checks) and an explicit focus on bridge-wide BAM alerting and route-integrity behaviour.

2.2 Cyber Resilience Requirements: IACS UR E26 and E27

The International Association of Classification Societies (IACS) has introduced UR E26 "Cyber Resilience of Ships" and UR E27 "Cyber Resilience of On-Board Systems and Equipment", which become mandatory for newbuilds contracted from 1 July 2024.

These requirements:

- Treat cyber resilience as a design requirement, not an afterthought.
- Demand asset inventories, network diagrams and configuration guidelines.
- Require onboard systems to implement defence-in-depth and support secure operation throughout the vessel's life.

RouteShield-PNT has been designed with these requirements in mind, including:

- A hardened, minimal host OS image,
- Strict network exposure (unprivileged IEC 61162-450/460 emitter, no open generic services),
- Signed builds and integrity-protected logs, and
- Documentation that fits into ship-wide cyber resilience plans.

2.3 Authenticated GNSS and Alternative PNT

The European Galileo programme is introducing OSNMA (Open Service Navigation Message Authentication), which allows receivers to verify the authenticity of navigation messages and detect certain spoofing attacks. Testing concluded in 2024, and an initial operational service has now been declared.

Authenticated GNSS is a crucial step, but:

- It requires receivers that implement OSNMA, which will take time to roll out across existing fleets.
- It does not protect against all forms of interference (e.g. jamming, meaconing, multi-path effects).
- It still leaves ships dependent on space-based signals as a single point of failure.

RouteShield-PNT is complementary: it assumes GNSS can be wrong or absent, and uses **shipboard reality** – radar, depth, own-ship motion and independent time – to validate or replace GNSS for route-keeping.

3. Threat Landscape: GNSS Jamming and Spoofing at Sea

GNSS interference is no longer limited to niche cases:

- In 2017, over twenty vessels near Novorossiysk reported being spoofed, appearing inland on charts while physically at anchor.
- Dataset analyses in 2024–2025 show large-scale interference events impacting hundreds or thousands of ships in the Eastern Mediterranean and other hotspots.
- Similar trends are observed in aviation, with a steep rise in GPS jamming and spoofing events over conflict zones.

For ship operators, the main concerns are:

- **Silent off-route drift** in constrained waters (ports, straits, wind farms),
- **Misleading time** fed into bridge networks and safety systems,
- **Crew overload** when they suddenly realise the position picture is untrustworthy.

Most bridges already have the raw sensors needed to detect these problems: radar, echo sounders, gyrocompass, speed log, and in some cases independent time sources. What is missing is an automated, standardised way to put these together.

4. Current Practice and Gaps

Today, GNSS integrity on many bridges is “checked” by:

- Visual comparison of radar overlay vs ENC,
- Manual dead-reckoning calculations by the OOW,

- Built-in GNSS receiver alerts (loss of satellites, RAIM warnings, low C/N_0), and
- Generic alarms in INS/ECDIS when position jumps or updates stop.

Limitations include:

1. **No continuous automated radar↔ENC registration.** Overlays may drift out of alignment over time, and many systems rely on manual tweaking.
2. **No systematic fusion of DR, depth and independent time.** These sensors are observed, but not continuously combined into a quantitative integrity state.
3. **Fragmented, vendor-specific alerts.** Each OEM signals GNSS issues in its own way; few map them cleanly onto IMO Bridge Alert Management (BAM) categories.
4. **Poor coverage of time-push attacks.** Even when position is plausible, manipulated time can destabilise networked systems and PNT-dependent applications.

RouteShield-PNT is designed to address these gaps without replacing existing navigation equipment.

Figure 2 – Radar and ECDIS displays on a merchant ship bridge.
Close-up view of radar and ECDIS consoles on a merchant vessel. Today, consistency between these PNT-driven views is largely verified by the officer of the watch, not by a dedicated integrity function (photo: Michael Krahe, CC BY-SA 4.0).

5. RouteShield-PNT Concept

5.1 High-Level Architecture

RouteShield-PNT is a **bridge-network appliance** (or OEM-embeddable module) that connects to the existing bridge LAN and consumes:

- GNSS position and time (e.g. NMEA RMC/GGA/ZDA),
- Marine radar video or features via vendor SDK,
- Gyro heading (HDT), speed log (VHW),
- Echo sounder depth (DPT), and
- An independent reference time (e.g. LF terrestrial time service, network time, or eLoran where available).

The module runs four continuous monitors and a fusion/decision layer, then outputs:

- A current best-estimate PNT solution with integrity flags,
- BAM-compliant ALF/ALC alert messages over IEC 61162-450/460,
- Optional guidance cues to track-control/autopilot, and
- Audit-ready logs for replay and investigation.

5.2 Core Monitors

5.2.1 Radar↔ENC Registration

The radar monitor:

- Extracts stable shoreline and fixed structures from radar video,
- Compares them to ENC-derived coastline masks in the vessel's vicinity,
- Estimates the translation and rotation between "GNSS-based own-ship position" and "radar-observed world", expressed as (Δx, Δy, $\Delta\theta$), and
- Outputs a **quality score** between 0 and 1 indicating confidence in the alignment.

At a conceptual level, this is radar-to-chart matching. In practice, RouteShield-PNT uses proprietary registration workflows designed to be:

- Low-compute, suitable for fanless industrial PCs,
- Robust against clutter and partial occlusion, and
- Stable over time so that minor geometry changes do not constantly produce alarms.

Large, sustained mis-registration at high quality strongly suggests a position or heading error.

5.2.2 Dead-Reckoning / INS Innovation Test

The DR/INS monitor runs an extended Kalman filter (EKF) on:

- Gyro heading and speed log (optionally augmented with IMU),
- Generating a continuously propagated estimate of own-ship movement.

Incoming GNSS updates are treated as measurements. The filter computes an **innovation**, the difference between predicted and received position. If this innovation persistently exceeds statistically expected bounds, GNSS is considered inconsistent with the ship's own motion model.

This monitor is effective against:

- Slow "carry-off" spoofing (GNSS path diverges from inertial trajectory),
- Mis-configured GNSS offsets,
- Certain multipath and partial jamming scenarios.

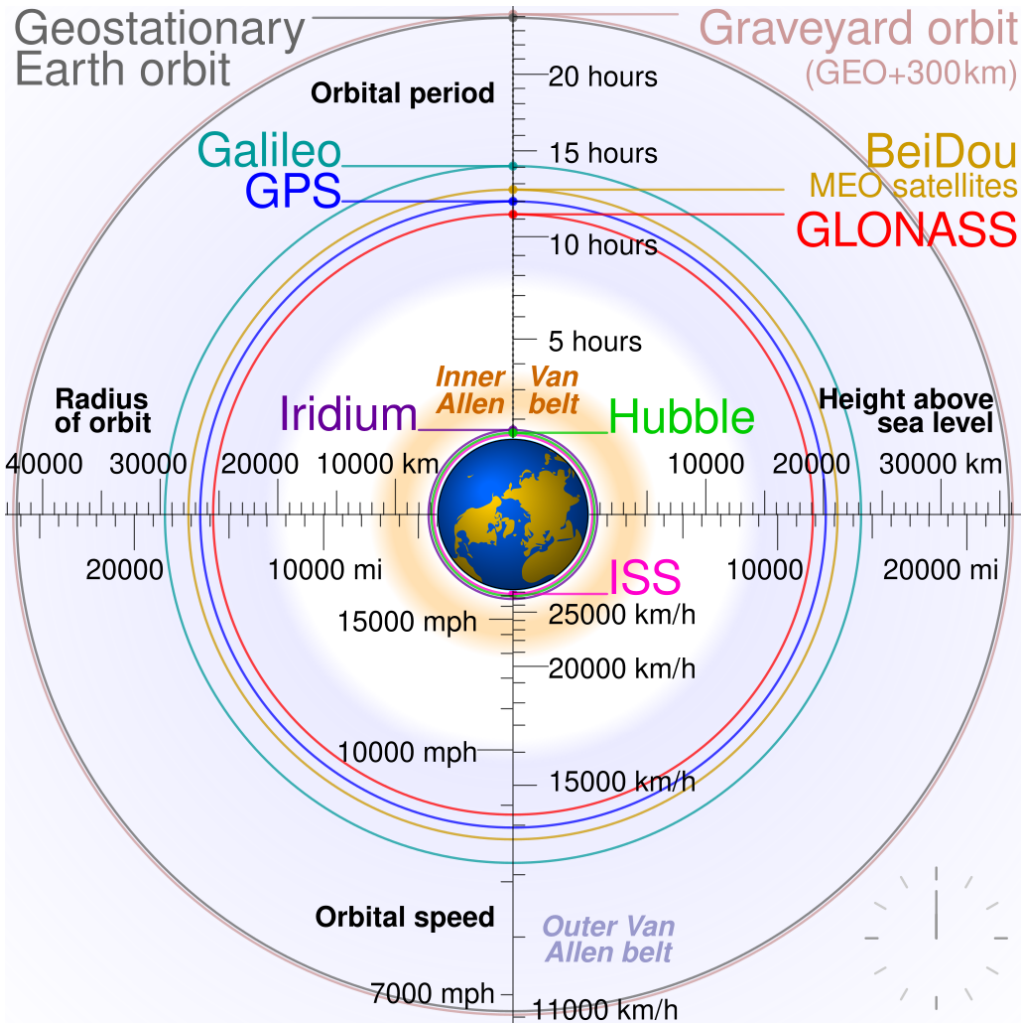

Figure 3 – GNSS constellations in Earth orbit.
Diagram comparing the orbits of GPS, GLONASS, Galileo and BeiDou (medium Earth orbit) with low-Earth-orbit platforms and geostationary orbits. The figure highlights the shared space-segment infrastructure on which maritime PNT depends (diagram: cmglee, CC BY-SA 3.0 / GFDL).

5.2.3 Depth vs Chart Consistency

The depth monitor:

- Reads real-time depth from the echo sounder,
- Corrects charted soundings for tide, where tidal information is available, and
- Computes a residual between measured and expected depth at the current GNSS position.

When the vessel is in an area with good hydrographic survey coverage, a large residual can indicate that the **horizontal position is wrong** or that tidal assumptions are invalid. This concept mirrors terrain-referenced navigation and has been proposed for spoofing detection in other domains.

RouteShield-PNT uses depth checks opportunistically:

- They are damped or disabled where chart confidence is low or tide uncertainty is high.
- They are treated as corroborating evidence rather than single-point tripwires.

5.2.4 Time Integrity

The time monitor compares GNSS-derived time with an independent reference:

- Terrestrial LF time services with disciplined oscillators,
- eLoran or other terrestrial PNT where available, or
- Certified network time solutions with traceability to UTC.

It tracks:

- Absolute time difference $|\Delta t|$,
- Stability and jitter of the reference,
- Duration of divergence.

Small, brief deviations may be tolerated; persistent divergence beyond a few milliseconds, especially when combined with spatial inconsistencies, is treated as strong evidence of GNSS time manipulation.

6. Fusion and Alerting

6.1 Decision Logic

The fusion layer ingests the four monitors and applies:

- **Confidence weighting** based on monitor quality scores and environmental context (e.g. reliable radar coverage vs open sea),
- **Timers and hysteresis** to avoid flickering alerts,
- **Multi-evidence concurrence rules** – for example, requiring agreement between at least two independent monitors for high-priority alarms.

The goal is to:

- Detect genuine integrity problems quickly (target median detection latency ≤ 10 s in coastal waters),
- Keep false alarms low enough (≤ 1 per 12-hour watch) to preserve crew trust, and
- Provide a clear, explainable rationale for each decision in the logs.

6.2 BAM-Compliant Alerts

Alerts are encoded according to IMO Bridge Alert Management (BAM) semantics and transported over IEC 61162-450/460 so that any compliant HMI can display them without custom integration.

Typical alert semantics include:

- **Caution / Advisory**
  - *"PNT consistency degraded – GNSS under review; check radar/ENC"*
- **Warning / Alarm**
  - *"GNSS position inconsistent with radar / ENC"*
  - *"GNSS time inconsistent with reference – PNT degraded"*

Alerts carry:

- Category and priority (per BAM),
- A textual description suitable for the bridge team,
- References to which monitors contributed (for evidence and debugging).

6.3 Fail-Safe Guidance

When the fusion layer classifies GNSS as untrustworthy:

1. GNSS is **de-weighted or frozen** for track-control inputs.
2. Dead-reckoning, bounded by radar corrections where possible, is used to maintain route.
3. The OOW is informed of the system state and expected limitations via alert text and optional cue cards.

This behaviour aims to avoid both extremes:

- Blindly trusting bad GNSS, and
- Abrupt “all stop” disengagement that leaves the bridge without clear guidance.

7. Use Cases and Scenarios

This section outlines representative scenarios RouteShield-PNT is designed to handle.

7.1 Harbour Approach with Carry-Off Spoofing

A tanker is approaching a confined harbour. An attacker introduces a slowly varying spoofed signal that gradually displaces the GNSS position lateral to the fairway while keeping speed and heading plausible.

- **Radar monitor:** notices shoreline features no longer align with ENC; (Δx, Δy, $\Delta \theta$) grows while quality remains high.
- **DR monitor:** innovation between predicted and GNSS positions increases over time.
- **Depth monitor:** starts to see inconsistency between charted and measured depth as the ship drifts toward shallower water.

Fusion interprets this as a high-confidence integrity failure and raises a BAM alarm, de-weighting GNSS and keeping the ship in the fairway using DR plus radar-bounded corrections.

7.2 Time-Push Attack on Coastal Transit

A ferry on a coastal route experiences a GNSS time-push without large spatial errors (e.g. for use in electronic warfare elsewhere).

- **Time monitor:** detects a growing Δt between GNSS and reference time.
- **DR and radar monitors:** initially see no major spatial inconsistency.

Fusion interprets this as a *degraded but not catastrophic* state:

- Issues a cautionary alert about time inconsistency,
- Flags PNT as degraded to bridge systems,
- Provides logs suitable for later analysis.

If time divergence grows or correlates with positional inconsistencies, the alert escalates and GNSS is de-weighted.

7.3 GNSS Outage in Coastal Waters

A tug loses GNSS entirely while manoeuvring near a wind farm.

- **Radar monitor:** still has strong returns from turbines and shoreline; alignment remains good.
- **DR monitor:** continues propagating motion.

RouteShield-PNT continues to support route-keeping on DR bounded by radar and signals a clear “GNSS unavailable – operating on DR / radar bounded” advisory to the bridge team.

8. Evaluation and Key Performance Indicators

RouteShield-PNT is being developed and evaluated with a three-tier protocol:

1. **Tier 1 – Bench tests**
    - Replay labelled interference and spoofing scenarios on recorded radar/NMEA logs.
    - At least 10 core scenarios × multiple repeats to quantify robustness.
2. **Tier 2 – Harbour pilot**
    - Short-run harbour approaches with strong radar returns and clutter.
    - Measure detection latency, true-positive rate (TPR), false alarm rate (FAR) and install time during normal operations and controlled perturbations.
3. **Tier 3 – Coastal pilot**
    - Longer coastal transits with variable geometry and radar visibility.
    - Focus on generalisation, stability and nuisance-alert suppression.

8.1 Key Metrics

- **Detection Latency (s):** time from first observable divergence to BAM alert.
- **True Positive Rate (%):** fraction of interference/spoofing intervals correctly raising alarms.
- **False Alarm Rate:** spurious alarms per 12-hour watch in radar-evaluable waters.

- **Install Time (h):** dockside hours from “box delivered” to “first valid ALF/ALC on 61162-450”.
- **Time-Offset Sensitivity (ms):** minimum sustained GNSS-vs-reference time drift detected within a defined time window.

Typical design targets (for harbour/coastal routes) are:

- Detection latency ≤ 10 s (median),
- TPR ≥ 95%,
- FAR ≤ 1 per 12-hour watch,
- Time-offset detection of ≈ 5–10 ms within ≤ 10 s.

9. Implementation Considerations

9.1 Integration with Bridge Systems

RouteShield-PNT is designed to integrate with existing equipment via standard interfaces:

- **Inputs:** IEC 61162-1 serial or 61162-450 UDP multicast; radar SDKs; independent time modules.
- **Outputs:** IEC 61162-450/460 alert and status messages; optional serial outputs; syslog-style logs.

No dedicated HMI is required; alerts are meant to appear on existing CAMs, ECDIS and INS displays.

9.2 Cybersecurity and Safety

As a safety-related system, RouteShield-PNT follows a cyber baseline aligned with IACS UR E26/E27 and relevant IEC standards:

- Hardened OS images, signed updates, least-privilege services,
- Strict network exposure and access control,
- Defensive coding practices with watchdogs and bounded queues,
- Pre-compliance testing for IEC 61162-450/460 transport, IEC 62923 BAM behaviour and IEC 60945 environmental/EMC when delivered as an appliance.
- Pilots are planned to run in advisory mode first, with any connection to track-control remaining under the Master’s authority and following fail-safe principles.

9.3 Data Management and Privacy

Most data handled are technical (radar features, NMEA messages, timing metrics). Where human feedback is collected (e.g. OOW perception of alerts), it is:

- Based on informed consent,
- Anonymised and aggregated in reporting, and
- Managed under a Data Management Plan aligned with FAIR and GDPR principles.

Synthetic and anonymised datasets, together with evaluation scripts, will be published on Zenodo or similar repositories to support reproducibility while protecting sensitive information.

10. Positioning vs Related Work

10.1 Integrated PNT Modules and IMO PNT-DP

The closest conceptual predecessor to RouteShield-PNT is the *on-board maritime PNT Module* introduced by Ziebold et al. (DLR). In that work, the PNT Module is the ship-side front-end of an integrated PNT system, with a central **PNT Unit** that fuses multi-system GNSS/DGNSS, logs, gyro, echo sounder, IMU and potential terrestrial systems such as e-Loran and R-Mode. The authors propose a three-stage integrity scheme:

1. **Individual sensor checks** (plausibility/validity tests),
2. **Compatibility checks** between similar outputs (e.g. SOG from different sensors), and
3. **Fault detection and identification in the integration algorithm**, using Kalman-filter innovations, residuals and parallel sub-filters that omit one sensor or signal at a time.
   First experimental results from the survey vessel **DENEB** in Rostock show how such checks work in practice, for example comparing rate-of-turn from an IMU vs gyro and SOG from different logs and GNSS antennas. The key conclusion is that robust PNT requires combining all available sensors and explicitly modelling integrity, not relying on any single source.

The IMO PNT-DP Guidelines later formalized a similar idea at regulatory level, defining a **PNT data processing (PNT-DP) unit** that combines multiple PNT sources and onboard sensors (including radar and echo sounder) and outputs PNT with integrity and status to bridge systems. RouteShield-PNT implements this “PNT-DP / PNT Module” concept as a deployable bridge-LAN product rather than as a research demonstrator.

10.2 RouteShield-PNT's focus and differences

While the DLR PNT Module and IMO PNT-DP describe the right *class* of function, they leave several aspects open that RouteShield-PNT addresses explicitly:

- **Sensor emphasis and behaviour:**
  - The DLR work focuses on multi-GNSS, terrestrial radio navigation (e-Loran, R-Mode), IMU and logs; radar map-matching is acknowledged only as a conceptual input in the architecture.
  - RouteShield-PNT instead centers on **radar↔ENC registration**, **depth-vs-ENC residuals**, **DR/INS innovation tests** and **GNSS-independent time checks** as the main integrity evidence for route-keeping in harbour and coastal waters.
- **Bridge-wide alerting and fail-safe route integrity:**
  - Ziebold et al. discuss integrity in terms of internal filter metrics (innovations, residuals, parallel sub-filters), not in terms of how the bridge team is alerted or how track-control should behave under degraded PNT.
  - RouteShield-PNT defines a concrete **fusion and alerting state machine**, mapped onto IMO Bridge Alert Management semantics and transported over IEC 61162-450/460, with explicit fail-safe behaviour (de-weighting or freezing GNSS, continuing on DR bounded by radar, and informing the OOW).
- **Productization and interoperability:**
  - The PNT Module paper reports early **measurement campaigns and compatibility tests** on a single research vessel. It does not specify commercial deployment, multi-vendor SDK integration, or pre-compliance with IEC 62923/61162/60945.
  - RouteShield-PNT is explicitly engineered as a **vendor-neutral bridge-network appliance / OEM module**, with KPIs for detection latency, TPR/FAR and install time, multi-vendor radar/GNSS integration, and a pre-compliance pack for BAM and bridge-LAN transport.

In that sense, RouteShield-PNT is best described as a **product-level, standards-aligned implementation of the integrated PNT Module / PNT-DP vision**, specialized for:

- **route-integrity and off-route prevention** in harbour/coastal waters,
- **automated radar↔ENC registration and depth-vs-ENC checks** as primary geometry evidence,
- **GNSS time-integrity monitoring**, and
- **BAM-compliant, vendor-agnostic alerts** on the existing bridge network.

10.3 Complementary developments

RouteShield-PNT also complements:

- **Alternative-PNT boxes** that compare GNSS to a second, space-based PNT source,
- **Hardened GNSS receivers** with anti-jam antennas and RAIM, and
- **Procedural and training measures** that encourage manual radar/ENC and DR checks.

Those measures remain necessary, but they either depend on additional external infrastructure or on continuous human vigilance. RouteShield-PNT adds a bridge-side integrity function that uses the ship's own sensors and existing standards to detect and mitigate GNSS manipulation in real time.

11. Roadmap and Future Work

Near-term development priorities include:

- Completing core algorithms and fusion logic and validating them in bench tests,
- Integrating with multiple radar and GNSS vendors,
- Executing harbour and coastal pilots with early-adopter operators, and
- Producing a pre-compliance pack for IEC 62923, 61162 and 60945.

Longer-term directions:

- Extending the concept to **Maritime Autonomous Surface Ships (MASS)** and remote control centres,
- Integrating terrestrial ranging systems (e.g. VDES-R-Mode, eLoran) where deployed,
- Feeding integrity information into shore-side VTS and fleet monitoring,
- Leveraging OSNMA and other authenticated services as additional inputs rather than sole defences.

12. Conclusion

GNSS jamming and spoofing are no longer theoretical threats for shipping. They are daily operational realities in several regions, eroding the trust that bridge teams can place in their primary positioning source. At the same time, bridges already carry most of the independent sensors needed to detect and mitigate these issues.

RouteShield-PNT proposes a practical way to turn those existing sensors into a coherent **resilient PNT and route-integrity function**, delivering:

- Automated multi-sensor integrity checks,

- Standardised BAM alerts over IEC 61162-450/460, and
- Fail-safe guidance that keeps ships on track when GNSS misbehaves.

By implementing the IMO PNT-DP vision in a vendor-neutral, cyber-hardened product, RouteShield-PNT aims to reduce the risk of silent off-route drift, support incident investigation and strengthen European strategic autonomy in maritime PNT.

Authored by:
Hrvoje Mihovilović
Founder & CEO, ELNAV.AI d.o.o., Split, Croatia

Date: December 2nd, 2025

Public Disclosure and Prior Art Statement:
All concepts, methods, and designs related to the RouteShield-PNT described herein are openly disclosed as prior art, effective 02.12.2025, to prevent exclusive patent claims by third parties. Collaboration and further innovation are welcomed.

References

1. IMO, *MSC.1/Circ.1575 – Guidelines for Shipborne Position, Navigation and Timing (PNT) Data Processing*, 2017.(International Maritime Organization)
2. "R. Ziebold, Z. Dai, T. Noack, E. Engler, *"The on-board maritime PNT Module – Integrity monitoring aspects and first experimental results,"* German Aerospace Center (DLR), Institute of Communications and Navigation, 2011.(The on-board maritime PNT Module)
3. IACS, *Unified Requirements E26 and E27 – Cyber Resilience of Ships and On-Board Systems*, various revisions.(Safer and Cleaner Shipping - IACS)
4. European GNSS Service Centre, *Service Notice #20 – Galileo Open Service Navigation Message Authentication (OSNMA) – Initial service declaration*, 2025.(gsc-europa.eu)
5. P. Zalewski, *Integrity Concept for Maritime Autonomous Surface Ships*, *Sensors*, 2020.(PMC)
6. Various reports on GNSS jamming and spoofing incidents impacting maritime navigation (Black Sea, Eastern Mediterranean, Strait of Hormuz, etc.).(sony-semicon.com)