

Beyond the Electronic Fog

Ship Monitor by JDS and the Quest for Uncorrupted Maritime Spectrum Data

Published by Ship Monitor by JDS GmbH, Rostock, Germany
September 2026

The first paper in this series made a simple argument: maritime data quality is not a commodity, and it is decided at the antenna. Corrupted inputs ruin everything downstream. This paper picks up where that one ends. It explains how Ship Monitor by JDS captures uncorrupted radio-frequency truth at the physical antenna, before any software layer ever sees it, and why that capability has just carried the company through the European Space Agency's incubation programme and into its first major commercial deployment.

1. Where the last article ends, this one begins

Most of the maritime intelligence industry works backwards. A vessel reports false or corrupted positions. Hours or days later, analysts examine the historical footprint of its track and apply algorithmic guesswork to reconstruct what probably happened. The damage is already done. The analysis is forensic, not preventive.

The JDS team knows this territory well. Its founders helped build the analytical baseline for classifying spoofing and jamming events during their earlier careers in maritime intelligence, with original taxonomy work dating back to 2023. They are on good terms with their former employers: former colleagues, now industry peers and complementary actors in the same field. But that experience taught them where track analysis stops. It can diagnose a corrupted trajectory after the event. It cannot see the corruption happening.

JDS's answer is to instrument the physical radio environment itself. Its shore stations measure raw signal strength, constellation-level signal-to-noise ratios, timestamp integrity and physical RF anomalies as they occur. The result is near-real-time detection. Instead of telling a client hours later that a track looked suspicious, the system detects interference in the local spectrum the moment someone attempts to corrupt vessel geolocation in a region.

“Track analysis diagnoses the damage after the event. We watch the attack happen at the antenna.”

2. Jamming shouts. Spoofing lies.

The distinction matters because the two attacks fail in opposite ways. With jamming, an attacker floods the frequency with loud radio noise. The receiver loses lock entirely and reports no GPS signal. It is an obvious, visible failure: the navigator knows immediately that systems are down.

Spoofing works differently, and its danger lies in how little it announces itself. The attacker does not block the genuine satellite signal. He counterfeits it, broadcasting fabricated data that the receiver accepts as authentic. Nothing on the bridge suggests a problem. The instruments keep showing a plausible position, the electronic chart updates smoothly, and the vessel edges away from its true course without triggering a single alarm. Because every navigation system on board draws from the same poisoned source, the crew has no independent reference point against which to test what their screens are telling them.

That is precisely the gap shore-based detection closes. Because the JDS fusion engine measures the physical spectrum independently of any vessel, it flags spatial anomalies within seconds of processing the incoming telemetry. And its primary client is not the individual navigator. It is the wider commercial ecosystem: underwriters, commodity traders, port authorities and coastal administrations, who need to know instantly when an entire sea corridor is undergoing active location manipulation. For an insurer or a port authority, knowing within seconds that a region's reported tracks are being corrupted changes risk assessment and liability attribution entirely.

3. Truth at the antenna: the hybrid station

The delivery vehicle for this capability is JDS's hybrid modular sensor station: a datalogger core with an AIS extension running multiple receivers and optimised antenna hardware, a GNSS extension, a software-defined radio spanning 9 kHz to 2 GHz, environmental sensors, and a solar off-grid option. The modularity is the commercial point. One physical installation serves many missions.

The GNSS extension constantly measures the physical reality of the satellite sky above the station: satellite counts, azimuth and elevation angles, signal power levels, and exact nanosecond timestamps across every active constellation. The detection logic looks for physical impossibilities. When a localised spoofer or jammer activates, it alters the power spectrum and geometric signature of the received signals in ways that clean sky never does. Abrupt, unnatural shifts in signal strength or elevation vectors are the fingerprint.

Temporal resolution is where the engineering has moved fastest. Conventional tracking systems rely on long-interval polling, taking snapshot samples every fifteen minutes or even hours. In a fast-moving spoofing attack that interval is an eternity: an attacker can manipulate a trajectory completely undetected between polling cycles. During development JDS compressed its collection cycle from fifteen-minute intervals to five, and now to one-minute updates, backed by nanosecond-level timestamping across all constellations. Operators get continuous visibility into signal stability rather than delayed, intermittent snapshots.

The multi-constellation view is the bedrock of the detection logic. The stations track GPS, Galileo, GLONASS and BeiDou, alongside the regional QZSS and NavIC systems, reporting satellite name, signal strength and timestamp per constellation. The reason is simple: interference rarely compromises every constellation simultaneously. In JDS's Baltic observations, commercial jammers and spoofers overwhelmingly target the standard civilian GPS frequencies. Manipulating every constellation across different orbits at once requires military-grade complexity. So when GPS deviates while Galileo and GLONASS hold true, the cross-check flags the discrepancy instantly.

“An attacker can fake GPS. Faking every constellation in the sky at once is another matter entirely.”

4. When the physics disagrees with the data

The fusion engine cross-references two independent layers in real time: demodulated AIS kinematic reports from vessels, and raw RF spectrum telemetry from the local stations. A divergence between them is a physical contradiction, and there are three tell-tale signatures.

The first is signal power against claimed range. A radio signal weakens predictably as it travels, so the transmission arriving at a shore station carries physical evidence of the distance it has covered. When a vessel's reported position places it far out at sea, but the received signal bears the unmistakable profile of a transmitter operating much closer to shore, the two accounts cannot both be true. The report says one thing. The physics says another. The physics wins.

The second is constellation drift against AIS position. A ship's transponder outputs coordinates derived from its onboard GPS receiver. If the shore station's GNSS extension detects active GPS interference in that sector, while clean Galileo or GLONASS telemetry confirms the true spatial geometry, every AIS position reported from that sector is immediately flagged as unverified or corrupted.

The third is direction of arrival. Using optimised directional antenna arrays, the system cross-checks the physical line of bearing of the incoming VHF signal against the vessel's reported coordinates. If the radio signal arrives from due south but the AIS payload places the vessel to the north-east, the track is marked as spoofed on the spot.

5. The Baltic, Bilbao and a corridor-agnostic architecture

The network is not a concept. Stations at Warnemünde and Nienhagen consistently capture high-density data across the southern Baltic, with long-range AIS reception out to 250 kilometres demonstrating the sensitivity of the antenna arrays. The stations are actively tracking structural signal degradation and recurring localised interference patterns in critical shipping lanes. The granular case studies, including coordinated regional events in which clusters of vessels are abruptly relocated to false benchmarks, are being held back deliberately: JDS is preparing a rigorous, peer-reviewed scientific publication for 2027 that will map these Baltic electronic anomalies with full empirical data.

An operational partner station in Bilbao, deployed for testing and data validation in northern Spain, proves the hardware is not tethered to the Baltic's particular conditions. The architecture is corridor-agnostic by design. Baltic electronic warfare dominates the

headlines, but GNSS vulnerabilities exist across at least six major maritime corridors worldwide, and expansion is already underway toward the Mediterranean and South America through local partner networks. Because the stations ingest raw multi-constellation data at source and enforce strict cryptographic verification of incoming feeds, the same trusted signal integrity can be delivered from any coastline in the world.

The same platform reaches beyond maritime. Because the station's software-defined radio runs to 2 GHz, capturing ADS-B aviation transmissions requires no hardware redesign at all. JDS was founded on a vision of monitoring the three pillars of global logistics: maritime, aviation and rail. Maritime remains the firm commercial focus for the coming decade, but the stations are, by design, dual-use infrastructure for national resilience and coastal surveillance, ready to deliver raw ADS-B telemetry to defence, aviation and critical-infrastructure partners that require multi-modal spectrum awareness.

6. Space-grade and European-built: the ESA chapter

None of this was funded by venture capital, and that was a deliberate choice. VC pressure for rapid returns compromises the one thing a neutral data provider cannot trade away: independence. Instead, JDS entered the ESA BIC Northern Germany incubation programme with a clear mandate: build a fully operational, European-sourced hardware sensor station capable of delivering high-integrity maritime tracking.

The programme gave the company what money alone could not. Direct integration with the scientific community, regional space clusters and public maritime authorities. Access to an ecosystem of hardware engineering firms to collaborate with rather than compete against. And the ultimate stamp of trust: ESA rigorously auditing and validating the hardware architecture, proving to clients that the station design and signal processing are grounded in space-grade engineering standards.

The grant itself funded physical R&D and hardware procurement, enabling the team to iterate through multiple configurations under strict supply-chain criteria: every component sourced directly from European Union suppliers. The hardware, in fact, came first out of necessity. Sourcing an industrial-grade receiver module capable of tracking every major constellation simultaneously was a formidable engineering hurdle in its own right. Only once the raw multi-constellation data stream was mastered did the anomaly-detection layer follow as the logical next step.

Staying strictly European after the initial ESA requirement was a strategic decision, not a box-ticking one. Post-pandemic supply shocks proved that long, opaque overseas hardware pipelines are an operational risk. Local sourcing delivers complete auditability, sovereign data integrity and supply continuity. It is a resilience and independence story first, and a strong sales argument second.

The original brief has now been completely realised. The prototype was built, deployed into the field, and has been actively collecting real-world data. JDS reached its final review with ESA in June 2026; the project was officially completed and accepted, marking formal graduation from the incubation. The station is no longer an incubator project. It is an active commercial unit in production, already handling deployment inquiries from external partners.

“Having ESA audit and validate your architecture is the ultimate stamp of trust.”

7. The economics of clean data

The commercial argument comes down to physics and economics: garbage in, garbage out. If corrupted or spoofed signals are captured at the antenna, no amount of expensive cloud processing, machine learning or brute-force cleaning downstream can fully recover the lost truth. When thousands of distorted data points flood a cloud environment, massive computing power is spent trying to filter and reconstruct dirty data after the fact. Trying to clean it there is an endless financial drain, and it is a large part of what makes this industry expensive.

JDS flips that model. By engineering high-quality hardware and filtering raw multi-constellation signals directly at the antenna, anomalies are caught before they ever enter the database. Cloud infrastructure overhead falls dramatically, and the savings pass to the client. For a buyer, better data at the antenna means higher accuracy, absolute trust and a significantly lower price point than more data in the cloud. JDS is now partnering with academic and research institutes to formally quantify those processing-overhead costs with hard empirical numbers.

The model is already proving itself commercially. Under a recently commenced deployment along the German coast, supported by federal funding from the BMWK, the Federal Ministry for Economic Affairs and Climate Action, major international technology companies are acquiring both the physical hardware stations and the raw data feeds they generate: physical control over high-integrity infrastructure in key coastal zones, plus uncorrupted, real-time multi-constellation feeds to power their own platforms. The wider network today handles up to 700 million AIS messages a day, a figure that reflects a hybrid architecture combining JDS's proprietary high-integrity coastal receiver network with aggregated partner feeds.

The business model behind it is deliberately focused. JDS is fundamentally a data-as-a-service company, and intends to remain one: delivering uncorrupted, ground-truth raw data is where the market gap is widest. Internal analytics and anomaly detection exist to validate the hardware and understand what the systems see. The long-term roadmap will eventually package that into a native regional alerting API, but only once two conditions are met: continuous station density across target corridors, so there are no coverage gaps, and enterprise clients continuing to integrate the raw telemetry into their own platforms first. JDS is comfortable letting partners build proprietary applications on top while it remains the authority on raw signal integrity.

One market watches this space with particular attention. As maritime claims grow more complex, insurers and underwriters increasingly need objective standards for verifying historical vessel movements during periods of electronic interference. JDS does not comment on specific commercial discussions or third-party claims workflows. Its position is simpler: whoever uses the data, it must be rooted in verifiable physical spectrum reality rather than unverified software assumptions.

8. The road ahead, honestly

The next step on the roadmap is fixed maritime infrastructure as reference nodes. A navigation buoy cannot move. If its onboard GNSS sensor reports even a few metres of drift, that is an immediate, indisputable calibration alarm for localised interference. The concept is

simple and bulletproof, and it is roadmap rather than product today: the prerequisite is completing primary shore-station coverage along the German coastline, with a target deployment window in the coming months.

And the honest limitation? Physical shore stations operate within line-of-sight and propagation physics. They cover target corridors with exceptional precision; they do not magically monitor every open ocean mile without a dense, expanding network. Nor is the system an oracle of intent. It is engineered toward 99 per cent accuracy in verifying legitimate, law-abiding maritime traffic, and JDS tells customers upfront not to expect a black box that guesses motives. The stations verify physical signal reality: RF anomalies, spoofing interference, telemetry discrepancies. The goal is to protect compliant maritime commerce by establishing undeniable ground truth.

“The era of treating maritime data as a cheap, unverified commodity is over.”

Five years from now, JDS intends to be exactly what it is today, at scale: an independent data-as-a-service company whose elite custom hardware and localised detection logic exist for one purpose, guaranteeing that the raw telemetry it feeds into the global maritime ecosystem is accurate, uncorrupted and physically verified. The hardware is its eyes and ears on the water. The identity is the world’s most trusted independent data feed.

That is the line in the sand this paper draws. High-integrity, uncorrupted maritime telemetry at a sustainable price does not start in the cloud. It starts at the antenna.

About Ship Monitor by JDS GmbH

Ship Monitor by JDS GmbH is an independent maritime data-as-a-service company founded in late 2024, headquartered in Rostock, Germany. All data infrastructure is located within the European Union. JDS maintains no competing analytics, trading, or downstream applications and does not accept venture capital funding. The company graduated from the ESA BIC Northern Germany incubation programme in June 2026. Contact: c.hilgenfeld@jds-monitor.com or d.piedra-garcia@jds-monitor.com