Fraunhofer CML

Maritime Security

Special Edition Newsletter

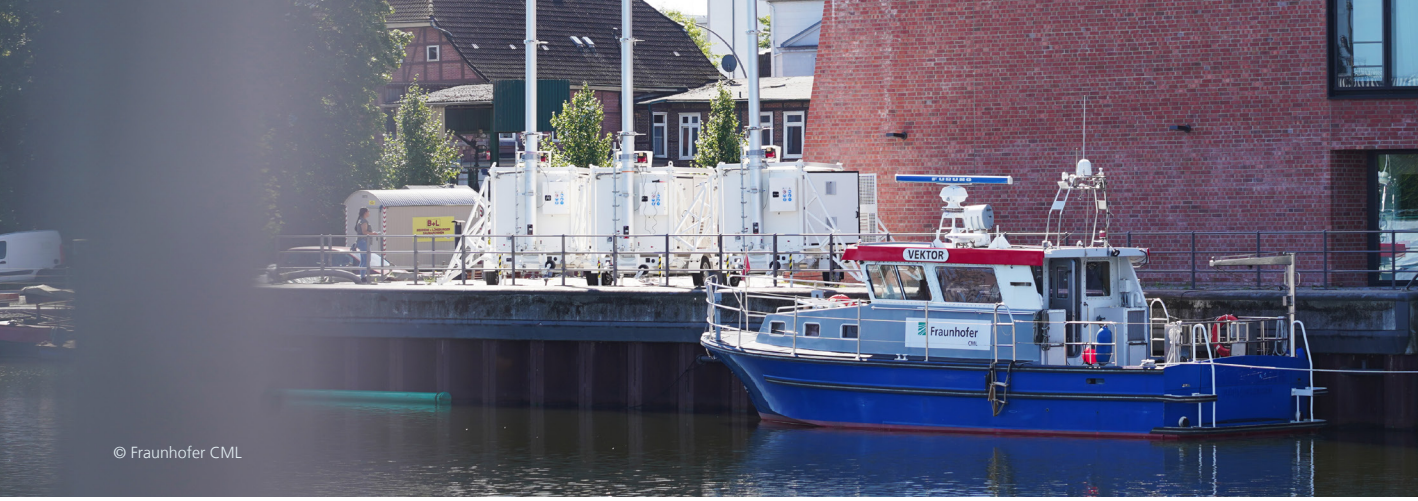
Dear readers,

Ensuring maritime security is essential in light of global challenges and hybrid threats. This special edition of our newsletter shows how innovative research approaches at Fraunhofer CML already address concrete application needs today and strengthen the resilience of maritime infrastructures. Among other things, you will learn how AI-supported, mobile multi-sensor networks and data-sovereign security pictures detect threats at an early stage, evaluate sensor data in real time, and support well-founded decisions. Our forecasting methods, multisensory navigation, and digital technologies make supply chains more resilient and help identify disruptions early on. We also introduce our maritime cybersecurity lab MaCy and the research vessel VEKTOR as practice-oriented test environments.

Please feel free to contact us – our know-how and expertise can be flexibly applied to your requirements, new partnerships, and applications. We hope you enjoy this informative read!

Yours, **Dr. Ole John, MBA**
Head of Department Ship and Information Management
Fraunhofer CML

Newsletter Maritime Security



The VEKTOR and three Cells on Wheels as central components of the KIRMES system.

Mobile Sensor Technology Protects Ports from Hybrid Threats

Critical maritime infrastructures such as ports, offshore facilities, or underwater pipelines are increasingly targeted by hybrid threats. In addition to physical attacks, cyberattacks, GNSS spoofing, or manipulated vessel data also complicate reliable situation assessment. The research project KIRMES, supported by the Fraunhofer Zukunftsstiftung's funding program „Transfer for Global Challenges", is therefore developing an AI-supported overall system that captures and analyzes maritime security situations flexibly, intelligently, and in real time. The aim is to support operators and authorities in detecting risks at an early stage and making well-founded decisions to protect critical infrastructures.

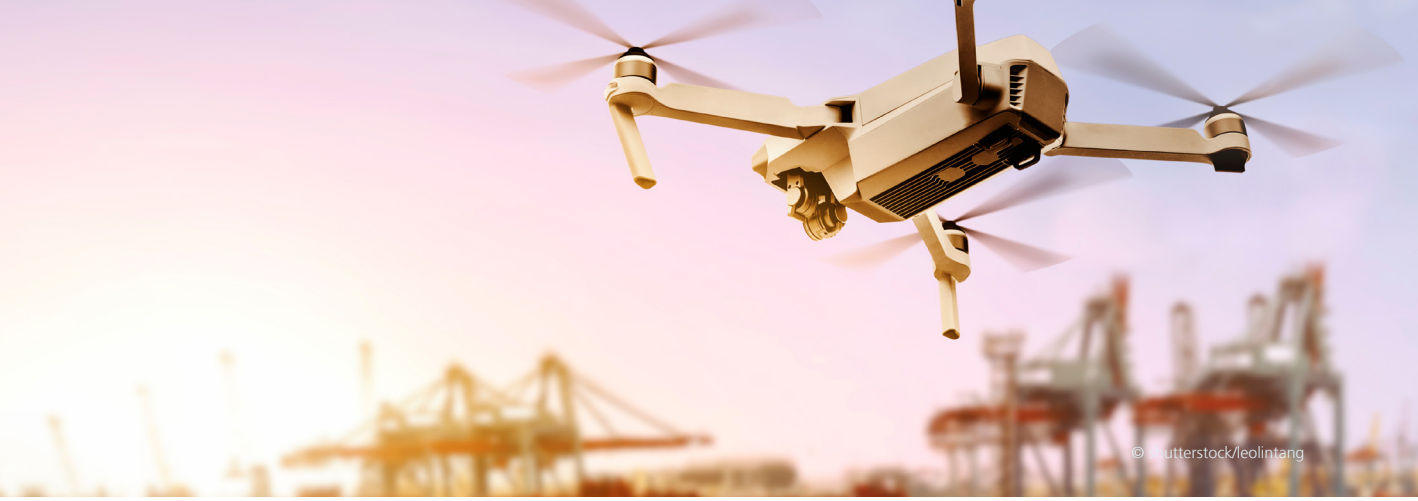
At the core is a mobile sensor network consisting of three Cells on Wheels – transportable multi-sensor platforms for flexible use on land – as well as Fraunhofer CML's research vessel VEKTOR. The system can be set up at a wide range of deployment sites within a few hours. The collected data is brought together on a central data platform, fused in real time, and evaluated using AI-based analysis methods. This creates a comprehensive cyber-physical situational picture that automatically detects anomalies such as GNSS interference, unusual traffic patterns, or security-relevant events and visualizes them clearly. Thanks to a modular microservice architecture, the system can also be flexibly extended with additional sensors or analysis methods.

In KIRMES, Fraunhofer CML draws on its long-standing expertise in developing intelligent maritime assistance and analysis systems. Proven technologies – for example for the automated transcription of maritime radio, ETA forecasts, and traffic analyses – are integrated into a powerful overall system. This allows new AI methods to be transferred into practice more quickly and complex threat scenarios to be assessed holistically.

Port operators, security authorities, maritime critical infrastructure operators, and research institutions alike benefit from this. The mobile solution enables the use of state-of-the-art sensor technology without elaborate stationary infrastructure and creates a robust data basis for safe decisions – even in remote areas and acute deployment situations. This makes KIRMES a key contributor to strengthening the resilience of maritime infrastructures.

Contact

Christoph Martius, M. Sc.
Email: christoph.martius@cml.fraunhofer.de
Phone: +49 40 271 646 - 11406



DIEB uses intelligent data linkage to detect threats at an early stage (symbolic image).

DIEB Connects Data for Greater Maritime Security

Ensuring the security of maritime infrastructures requires new, data-based approaches in light of complex security risks. Cyberattacks, sabotage, and espionage can significantly affect ports, energy supply, and supply chains. The research project DIEB (Data-driven Identification, Evaluation, and Addressing of threats to LNG terminals) by Fraunhofer CML and Niedersachsen Ports (NPorts), funded by the Federal Ministry of Research, Technology and Space, is developing an intelligent security picture for this purpose: it combines data from various sources, detects threats at an early stage, and supports decision-makers in responding quickly and effectively.

The relevance of this topic is reflected in the circle of associated partners: with Deutsche Energy Terminal GmbH as LNG terminal operator, the Lower Saxony State Criminal Police Office, the Lower Saxony State Authority for Road Construction and Traffic as port security authority, the German Federal Waterways and Shipping Administration, the German Navy at its Wilhelmshaven site, and UAV DACH e.V., operators, security agencies, and federal authorities accompany the project and contribute their practical requirements directly to its development.

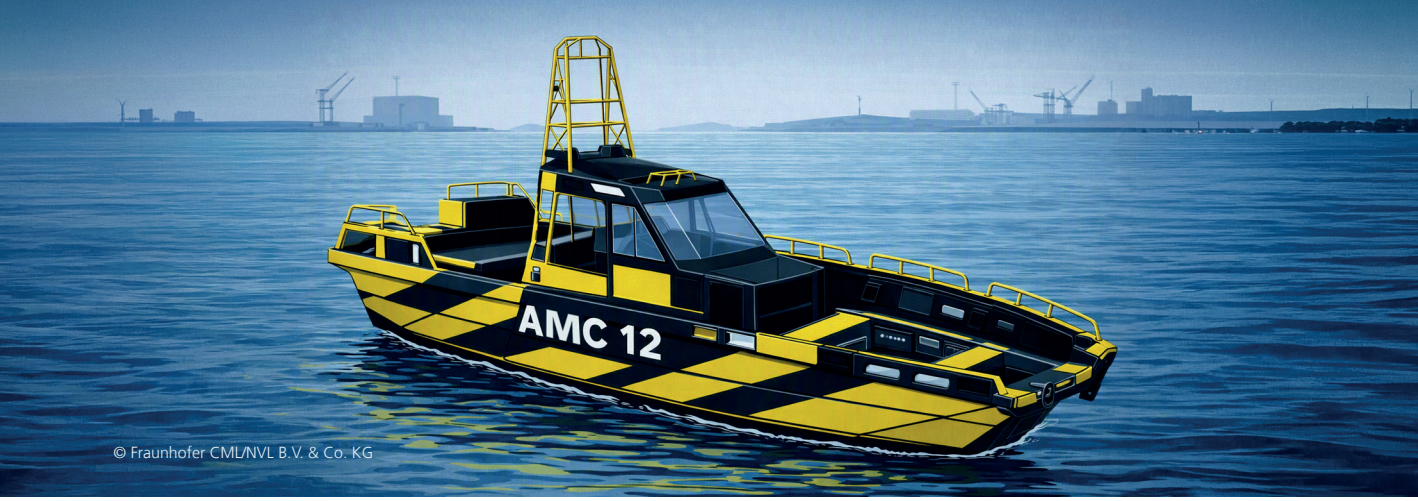
DIEB relies on a modular, data-sovereign system that combines local and mobile sensor data in real time and evaluates it using AI-supported big data analyses. This creates a situational picture that automatically identifies and assesses threats and forwards them in a targeted manner to the responsible bodies via an integrated decision-support and alert system. The scalable architecture also allows the system to be applied to other maritime fields of application.

Fraunhofer CML holds technical leadership and is responsible for the system architecture as well as methods for multisensory data integration, pattern recognition, and AI-supported risk assessment. Together with NPorts, Fraunhofer CML conducts field tests with mobile Cells on Wheels and the research vessel VEKTOR to demonstrate practical suitability.

DIEB lays the foundation for data-based collaboration among infrastructure operators, security authorities, and other stakeholders. Faster situation assessments and shorter response times help detect risks early on – opening up new perspectives for resilient maritime security.

Contact

Maximilian Reimann, M. Sc.
Email: maximilian.reimann@cml.fraunhofer.de
Phone: +49 40 271 646 - 11409



Graphical representation of NVL's 12-meter autonomous test platform AMC12 for port surveillance.

Unmanned on Patrol: Better Protection for Ports from the Sea

Port security today poses a challenge to critical maritime infrastructure (CRITIS), which is essential for both national and international flows of goods. The AMC12 project, carried out jointly by Fraunhofer CML, Naval Vessels Lürssen NVL, and Hamburg University of Technology, focuses on developing a modular, autonomous surface system for monitoring these sensitive areas. Through the use of state-of-the-art sensor technology and communication solutions, threats from the sea are to be detected at an early stage, described in detail, and prevention measures improved.

The project's core innovation is the autonomous test vehicle AMC12 – a twelve-meter, highly adaptable test platform that serves as a basis for sensor networks and AI-supported data analysis. Complemented by novel ultra-low-power underwater communication technologies, extensive environmental data can be continuously captured and analyzed in challenging port environments. The modular design facilitates the installation of specialized sensors that capture highly precise data – ranging from pipeline monitoring to the analysis of ambient noise levels.

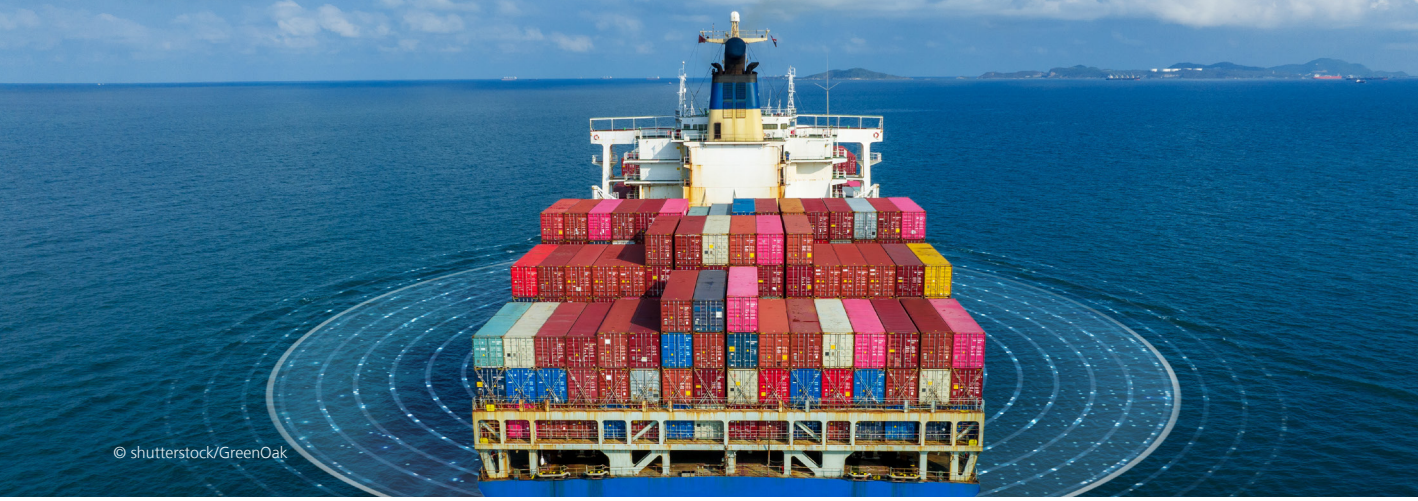
With its extensive expertise in maritime security research, Fraunhofer CML makes a key contribution to the project, supported by its diverse test infrastructure, including the research vessel VEKTOR and its own Maritime Cybersecurity Lab. Building on previous research experience, Fraunhofer CML is further advancing data-driven anomaly detection and adaptive monitoring solutions. State-of-the-art analysis methods are used to generate actionable information from heterogeneous sensor data in real time.

For partners from industry and public institutions, the AMC12 concept offers substantial benefits: it reduces operational costs, minimizes risks to personnel, and allows for flexible deployment – ideal for dynamic crisis situations. It also raises the technical responsiveness of security authorities to a new level by complementing traditional monitoring structures with adaptive, mobile systems.

The AMC12 project thus impressively demonstrates how innovation can address technical and strategic challenges in the maritime domain.

Contact

Maximilian Reimann, M. Sc.
Email: maximilian.reimann@cml.fraunhofer.de
Phone.: +49 40 271 646 - 11409



The MuSensPos project develops holistic navigation approaches to secure vessel traffic.

Resilient Navigation: Secure Position when GPS Fails

Ensuring precise and secure navigation is essential for shipping, but hazards such as GNSS spoofing and jamming mean that purely satellite-based navigation systems and ECDIS are increasingly reaching their limits. In the joint project MuSensPos (Multi-sensor approach for detecting GPS spoofing attacks and satellite-independent positioning) – carried out by Fraunhofer CML together with Lange-Electronic GmbH and coordinated by Thales Deutschland GmbH – a forward-looking solution is being developed that makes navigation systems more resilient through multisensory approaches. The goal of the project, funded by the Federal Ministry of Research, Technology and Space, is satellite-independent positioning that detects GNSS interference, employs alternative technologies, and ensures seaworthy resilience.

The project uses a combination of four independent positioning systems: inertial navigation systems (INS), magnetic field mapping, bathymetric matching, and radio-based navigation methods. Through this integration strategy, MuSensPos offers reliable localization even in GNSS-disrupted scenarios.

At the same time, robust fusion software ensures real-time evaluation of sensor data as well as automatic switching between technologies in the event of GPS outages.

Fraunhofer CML's technical expertise and equipment play a key role: the systems are tested in realistic environments – whether on the stationary ship's bridge or the research vessel VEKTOR. This allows the interaction of all sensors to be tested in real time, while user-friendly navigation interfaces are developed to provide the crew with clear recommendations for action in critical situations.

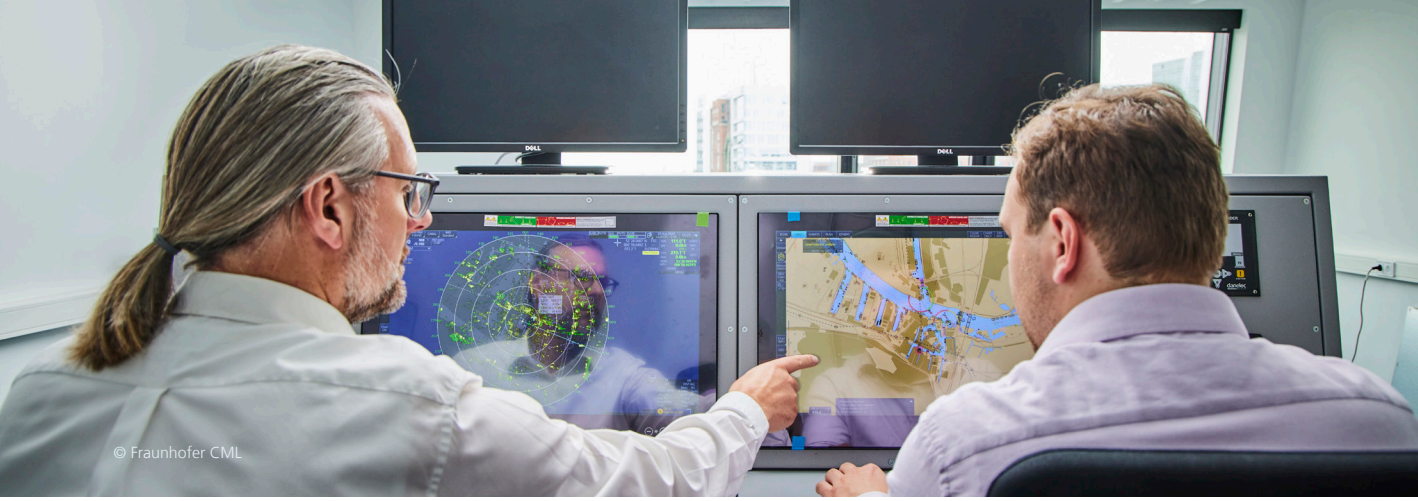
In addition to navigation safety, the project enables comprehensive situational pictures through advanced sensor data fusion. This allows maritime stakeholders to respond quickly and effectively to critical incidents and make strategic decisions.

For shipping companies and security authorities, MuSensPos offers clear benefits: it strengthens operational safety, protects supply chains, and reduces dependence on satellite systems. Particularly in the face of hybrid threats, the system marks a milestone in maritime technology development, safeguards global supply chains, and enhances resilience in maritime transport.

Contact

Dr. rer. nat. Valeria Bartsch
Email: valeria.bartsch@cml.fraunhofer.de
Phone: +49 40 271 646 - 11465

Navigation Warfare: Protection Against Cyber Attacks



The radio and bridge lab creates a realistic environment for assessing maritime cyber risks.

Cyber Attacks on the Ship's Bridge – Safe Testing in the Lab

Increasing digitalization on board ships opens up new possibilities for more efficient and automated maritime processes – but it also raises the demands on cybersecurity. Connected navigation, communication, and automation systems can present potential attack surfaces, the effects of which extend far beyond individual components. The Maritime Cybersecurity Research and Development Environment (MaCy) at Fraunhofer CML provides a unique test environment for analyzing maritime systems under realistic conditions and making them more resilient.

The radio and bridge lab replicates a complete ship's bridge with certified navigation technology (including radar and ECDIS), communication systems, and an antenna platform supplied with real-time data. This allows typical on-board environments and various network topologies to be reproduced. Using software-based tools, controlled cyberattacks can be simulated, vulnerabilities identified, and security concepts developed and validated for individual components or entire bridge systems.

In the MaCy lab, Fraunhofer CML combines its maritime systems expertise with extensive know-how in digitalization and IT security. The researchers develop structured methods for assessing maritime cyber risks, examine technical, regulatory, and organizational requirements, and support partners in implementing holistic security concepts. This includes penetration testing, analysis of network configurations, the development of response plans, and training for the personnel involved.

Manufacturers of maritime hardware and software, shipyards, shipping companies, and fleet operators can use the test environment to check the security of new devices and applications before they are integrated on board. Existing systems can be assessed for their resilience and optimized in a targeted manner.

In addition, the lab enables the development and testing of suitable security strategies for different operating scenarios. The MaCy lab helps companies and authorities meet regulatory requirements, detect risks at an early stage, and sustainably increase the security of digitally connected ships. It thus contributes to safe and future-proof maritime operations.

Contact

Philipp Sedlmeier, M. Sc.
Email: philipp.sedlmeier@cml.fraunhofer.de
Phone: +49 40 271 646 - 11413

Navigation Warfare: Protection Against Cyber Attacks

With marFM® Mobile, radio messages are transcribed in real time and digitally documented directly on board (symbolic image).

Mobile Speech Recognition for Shipping

Safety at sea depends significantly on clear and traceable communication. This is exactly where Fraunhofer CML's projects marFM® and marFM® Mobile come in. While marFM® has already been successfully deployed as a stationary solution in control centers and on bridges, marFM® Mobile brings proven maritime speech recognition to mobile devices for the first time – closing the last analog gap on board.

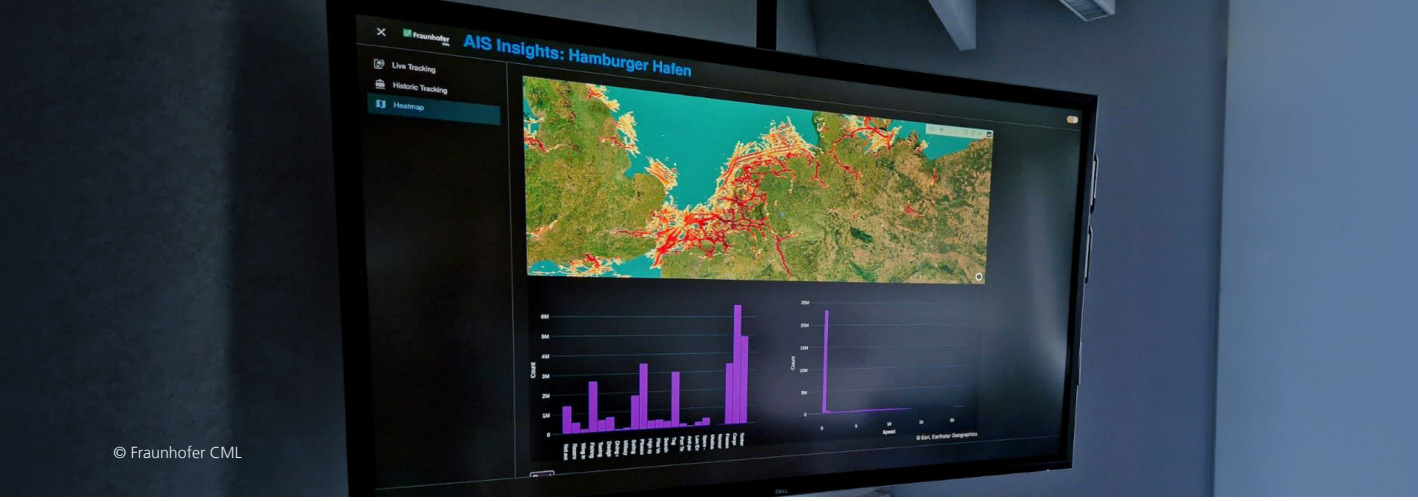
marFM® Mobile enables radio messages to be transcribed in real time, time-stamped, and digitally stored in loud, dynamic environments such as ports, response boats, or even regattas. Unlike the stationary marFM® solution, which relies on fixed installations and professional hardware, marFM® Mobile works flexibly on any smartphone or tablet – without additional infrastructure. This allows smaller vessels, training boats, or coast guards to also benefit from digital radio documentation. Especially in the context of maritime security, marFM® Mobile offers decisive advantages: misunderstandings caused by noise or accents are minimized, and radio messages are immediately visible as text and available for analysis, incident reports, or compliance requirements. The German Sailing Association (DSV) actively supports the project and provides real-world deployment environments for practical testing.

With long-standing expertise in maritime speech recognition and digitalization, Fraunhofer CML is shaping the future of safe shipping. Get in touch with us – together, we will continue to advance the mobile radio communication of the future.

Contact

Emin Nakilcioğlu, M. Sc.
Email: emin.nakilcioglu@cml.fraunhofer.de
Phone: +49 40 271 646 - 11408

Infrastructure & Solutions: Efficient, Digital, Connected



© Fraunhofer CML

Demonstrator in Fraunhofer CML's bridge lab for visualizing and analyzing AIS data.

Turning 7 Billion AIS Data Points into Vessel Behavior

The AISaaS project (AIS context provided as Software as a Service) addresses a key challenge in the maritime industry: while the enormous volume of raw AIS (Automatic Identification System) data provides position information, automated context enrichment that makes actual vessel behavior and interactions understandable has so far been lacking. This is essential particularly for maritime security, port logistics, and operational management, in order to detect risks at an early stage and design processes efficiently.

AISaaS addresses this by developing an intelligent AIS context engine, built on a self-managed database of more than 7 billion AIS data points as well as strategic partnerships providing access to historical data. Using machine learning and expert rules, semantic events are derived from the raw data – such as port calls, pilot assistance, bunkering operations, or security-relevant anomalies. This creates a detailed event history for each vessel, which can be used for both historical analyses and real-time assessments and forecasts.

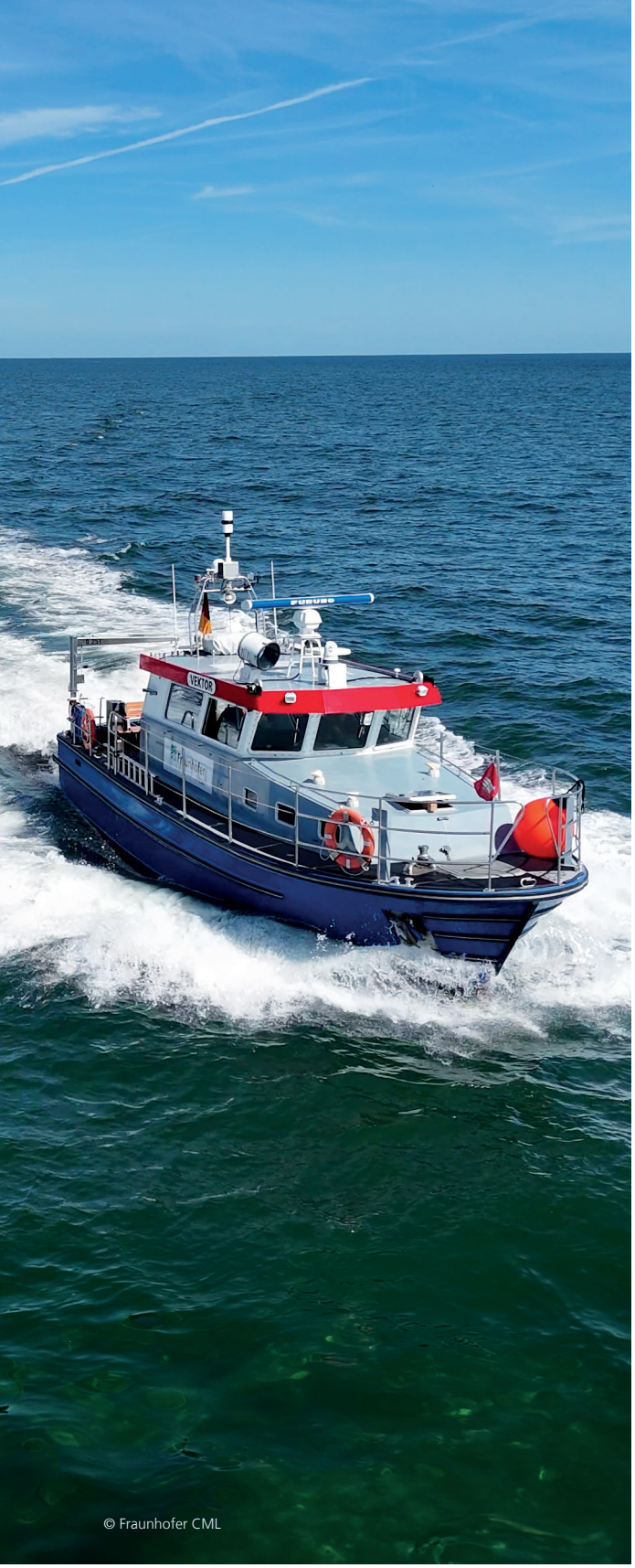
Fraunhofer CML contributes its extensive expertise in processing, analyzing, and visualizing AIS data and provides the technical infrastructure for persistent storage and API-based access. The solutions are demonstrated and further developed under practical conditions in Fraunhofer CML's bridge lab. Collaboration with strategic partners Soft-Park and Sleipner Maritime enables distribution to a broad target group: shipping companies, port authorities, pilotage and towage services, offshore companies, logistics platforms, security organizations, and research institutes all benefit from the context-rich data basis, which significantly improves operational decisions, planning processes, and security assessments.

AISaaS provides the crucial analytical layer that enhances existing systems and enables process automation. Users benefit from more efficient deployment planning, an improved security picture, less manual evaluation effort, and more reliable forecasts.

Contact us to jointly develop new solutions for your challenges in security, logistics, and operational management. We look forward to hearing from you and shaping the future of maritime intelligence.

Contact

Christoph Martius, M. Sc.
Email: christoph.martius@cml.fraunhofer.de
Phone: +49 40 271 646 - 11406



© Fraunhofer CML

Protecting Critical Maritime Infrastructure

The security of maritime infrastructures increasingly depends on the ability to develop and validate new technologies under realistic conditions. With the research vessel VEKTOR and the mobile sensor platforms Cells on Wheels (CoWs), Fraunhofer CML has powerful infrastructure assets at its disposal, enabling practice-oriented monitoring scenarios on inland and coastal waters.

As a floating lab, VEKTOR provides ideal conditions for monitoring in maritime environments. Complemented by the flexibly deployable CoWs, mobile test and measurement infrastructures are created that can be quickly adapted to different deployment scenarios. The combination of state-of-the-art sensor technology, communication systems, and modular equipment enables the collection of high-quality data as well as the validation of innovative technologies under controlled yet realistic conditions. With these research platforms, Fraunhofer CML combines its expertise in maritime systems, digitalization, sensor technology, and data analysis. VEKTOR and the CoWs support, among other things, the development of autonomous systems, intelligent assistance solutions, and data-based situational pictures for maritime security applications.

Companies, authorities, and research partners benefit from flexible testing and trial opportunities for individual research and development tasks. In this way, Fraunhofer CML accelerates the transfer of innovative technologies into maritime practice.

◂ *VEKTOR in action.*

Experience the VEKTOR up close!
In this video, Jan Solle presents the equipment of this state-of-the-art research vessel.

QANCOMFIN:
Quantum Technologies for Resilient Materials in Defenses

With QANCOMFIN (Quantum Computing with Finite Elements for crack propagation in defence applications), the project partners Impetus AS (coordinator), Forsvarets Forskningsinstitutt, Multiverse Computing SL and Fraunhofer have launched a pioneering research project in the field of maritime and land-based security under the European Union's EDF (European Defence Fund), which is financed by the European Union. The aim is to improve the simulation and prediction of crack propagation in safety-critical materials. A key challenge in simulating crack propagation in materials is that no single numerical and physical model simultaneously offers high accuracy, computational efficiency, scalability and robustness in predicting crack initiation, crack growth and fragmentation under extreme dynamic loading conditions.

QANCOMFIN will serve as a starting point for making the European defense ecosystem quantum-ready, leading to future strategic, technological and operational benefits: improved and accelerated material development and performance, cost reduction as well as increased safety and operational reliability. By being integrated into a commercially available simulation package to predict crack propagation in materials, the project aims to minimize downtime and enhance combat readiness.

Interested companies and institutions are welcome to contact Dr. Valeria Bartsch (valeria.bartsch@cml.fraunhofer.de) to learn more about the work of Fraunhofer CML in the project.

Innovation thrives on dialogue. Fraunhofer CML works with industry and the public sector to develop pioneering technologies. If you are looking for practical solutions for maritime security, resilient supply chains or the protection of critical infrastructure, we will support you from the initial idea through to application. We look forward to talking with you!

Fraunhofer CML

Fraunhofer Center for
Maritime Logistics and Services CML

Blohmstr. 32 · D-21079 Hamburg · www.cml.fraunhofer.de
Phone: +49 40 271 646 0 · Email: pr@cml.fraunhofer.de

YouTube LinkedIn