NAWASCAN

Navigation Warfare Scan Antenna

Programm / Ausschreibung	FORTE, FORTE, FORTE - F&E-Dienstleistungen 2021/2022	**Status**	abgeschlossen
Projektstart	01.10.2022	**Projektende**	31.03.2025
Zeitraum	2022 - 2025	**Projektlaufzeit**	30 Monate
Keywords	GNSS; Jamming; Spoofing; Navigation Warfare, Antenne		

Projektbeschreibung

Das von globalen Satellitennavigationssystemen (GNSS) bereitgestellte Service kann vor allem bei militärischen oder terroristischen Aktionen absichtlich gestört oder verfälscht werden, sodass von den weithin verwendeten GPS- oder Galileoempfängern keine oder eine falsche Positions- oder Zeitinformation erhalten wird.
Das geplante Antennensystem soll auf die hierfür relevanten Frequenzbänder optimiert, Entscheidungsgrundlagen für den aktiven (Jamming/Spoofing) und passiven (peilen/orten) Einsatz von feldverwendbaren Navigation Warfare Antennen liefern. Die theoretischen Grundlagen als auch vielleicht bereits bestehende Lösungsansätze sollen detailliert recherchiert werden und ein Trade-off zwischen theoretisch optimaler Lösung und sinnvoller, praktischer Machbarkeit soll zu den notwendigen Designentscheidungen führen.
Im Speziellen:
• Identifikation von Anforderungen an eine aktive sowie passive Spezialantenne (Antennengewinn, Beamforming, ...) im militärischen Einsatz
• Recherche zu grundlegender Theorie (elektronische vs magnetische Ausprägung, aktive vs passive Bauart, Peilverfahren, Formfaktoren, Schiebeverfahren zum Beamforming, Echtzeitverfahren und Integration in SDR, ...) und Verfügbarkeit von Technologien
Zur Falsifizierung einer theoretischen Designentscheidung im Vorfeld und als Vorbereitung einer feldverwendbaren Einsatzlösung für das ÖBH soll die Funktion mittels eines eingeschränkten Demonstrators als Proof-of-Concept gefertigt werden. So reicht es hierfür zB. mit einer geringen Anzahl an Sektoren zu zeigen, dass die gewählten Verfahren ausreichen um den, für den Einsatz erforderlichen Funktionsumfang zu erzeugen.
Dabei sollen folgende Punkte adressiert werden:
• Designentscheidungen auf konkrete Implementierungsmöglichkeiten verifizieren
• Eingeschränkten Funktionsumfang demonstrieren
• Schnittstellen zu den bereits eingeführten Sende- bzw. Empfangskomponenten bereitstellen
• Bedingte Wettertauglichkeit aufweisen

Folgende Forschungsfragen sollen in diesem Projekt erarbeitet werden:

• Wie kann eine NavWar (Secure PNT) Spezialantenne für die GNSS Frequenzbänder ausgeprägt sein um den Anforderungen an Einsatzsysteme des ÖBH zu erfüllen?

• Wie kann ein Proof-of-Concept Demonstrator aussehen?
• Können damit Aussagen gemacht werden wie eine feldtaugliche Antenne in die Infrastruktur eines NavWarTÜPLs integriert werden kann?

Abstract

The service provided by global navigation satellite systems (GNSS) can be intentionally disrupted or falsified, especially during military or terrorist actions, so that no or incorrect position or time information is received from the widely used GPS or Galileo receivers.
The envisaged antenna system should be optimized for the relevant frequency bands and provide a basis for decision-making for the active (jamming/spoofing) and passive (positioning/locating) use of navigation warfare antennas that can be used in the field.
The theoretical basics as well as possibly already existing solutions should be evaluated in detail to find a trade-off between theoretically optimal solution as well as practical feasibility.
Particularly the following tasks should be addressed:
• Identification of requirements for an active and passive special antenna (antenna gain, beamforming, ...) in military use
• Research on basic theory (electronic vs magnetic characteristics, active vs passive design, direction finding methods, form factors, shifting methods for beamforming, real-time methods and integration in SDR, ...) and availability of technologies

In order to falsify a theoretical design decision in advance and to prepare a field-usable application solution for the Austrian Armed Forces, a demonstrator should be implemented as a proof-of-concept. It is sufficient to show - with a small number of components - that the selected methods are sufficient to generate the range of functions required for the application.

The following points should be addressed:
• Verify design decisions for concrete implementation options
• Demonstrate limited functionality
• Provide interfaces to the transmission and reception components that have already been introduced
• Provide conditional weather suitability
The following research questions are to be worked out in this project:
• How can a NavWar (Secure PNT) special antenna for the GNSS frequency bands be developed in order to meet the requirements for operational systems of the Austrian Armed Forces?
• How can a proof-of-concept demonstrator look like?
• Can statements be made about how a field-compatible antenna can be integrated into the infrastructure of a NavWarTÜPL?

Endberichtkurzfassung

Die Problematik von Störern innerhalb des elektromagnetischen Spektrums besteht schon sehr lange und hat an Aktualität und Priorität in den letzten Jahren nichts eingebüßt. Störungen, ob beabsichtigt oder unbeabsichtigt, führen dazu, dass ein System in der Kommunikation oder Positionsfindung unterbrochen wird. Das, von globalen Satellitennavigationssystemen

(GNSS) bereitgestellte Service, kann vor allem bei militärischen Aktionen absichtlich gestört oder verfälscht werden, sodass von den weithin verwendeten GPS- oder Galileoempfängern keine oder eine falsche Positions- oder Zeitinformation erhalten werden kann. Um solche Störer zu lokalisieren bedarf es geeigneter Antennen, meist mit nachgeschalteter Software, basierend auf komplexen Signalverarbeitungstechnologien.

Ein Hauptziel des Projekts NAWASCAN war es, einen Antennen-Array Demonstrator zu entwickeln um geeignete Elementanordnungen und Beamforming-Algorithmen zu testen. Kommerzielle CRPA (Controlled reception pattern antennas) arbeiten ähnlich wie der entwickelte Demonstrator, haben jedoch das Ziel, die Störungen zu unterdrücken und den Antennengewinn in eine Richtung zu konzentrieren, aus der keine Störung kommt. Diese Mitigationsstrategie wurde vernachlässigt, da nur die Richtungsfindung der Störung notwendig war.

Um eine geeignete Konfiguration die sowohl Hardware als auch Software betraf, zu finden, wurden im Projekt einige Simulationsumgebungen implementiert. Damit konnte das Design der Antenne und die verschiedenen Algorithmen verifiziert werden. Die endgültige Entscheidung des Designs fiel auf ein zirkulares, planares Array mit 7 Antennen-Elementen und eine Signalverarbeitungseinheit mit 4 SDR-Plattformen. Eine Herausforderung war die Kalibration der Elemente, die für Messungen alle phasengleich sein müssen. Im Zentrum des Arrays wurde dafür ein Pin installiert, der zu Beginn der Messung ein Kalibrationssignal aussendet.

Für das Beamforming wurde der MUSIC-Algorithmus entsprechend angepasst, da dieser in der Simulation die besten Ergebnisse lieferte. Bei Testungen am Truppenübungsplatz Seetaler Alpe konnte das Array im Oktober 2024 erstmals unter realen Bedingungen getestet werden und einige Datensätze aufgezeichnet werden. Die Auswertungen im Postprocessing zeigten sehr gute Ergebnisse und eine recht genaue Richtung der Störquelle.

Der Demonstrator hatte die Aufgabe, die Funktionalität zu beschreiben und war nicht auf die Optimierung im militärischen Einsatz vorgesehen. Bei einer Weiterentwicklung wäre es unabdingbar, eine sowohl kompakte Receivereinheit als aus eine kompakte Antenne zu entwickeln. Für Echtzeit-Anwendungen ist die Verarbeitungszeit von entscheidender Wichtigkeit. Eine Verlagerung von Rechenleistung in FPGA (Field Programmable Gate Array) wäre sinnvoll.

Grundsätzlich ist die Entwicklung eines Antennen-Arrays für den Einsatz im GNSS-Testbed ein wichtiger Schritt um auch im Navigation Warfare Fähigkeiten besser zu entwickeln und Testungen und Szenarien realitätsnaher zu gestalten. Bislang wurden Testungen mit Störaussendungen (Jamming, Spoofing) mit diversen Receivern aufgezeichnet um deren Verhalten zu analysieren. Mit der Information, aus welcher Richtung eine Störung kommt, ergeben sich neue Möglichkeiten des Testens und vor allem des Entgegenwirkens und der Resilienz.

Englische Version :

The issue of jammers within the electromagnetic spectrum has existed for a long time and has not lost any relevance or priority in recent years. Interference, whether intentional or unintentional, can disrupt a system’s communication or positioning capabilities. Services provided by global navigation satellite systems (GNSS) can be deliberately jammed or spoofed, particularly during military operations, making it impossible for commonly used GPS or Galileo receivers to obtain accurate or any position or time information. To locate such jammers, suitable antennas are required, typically combined

with downstream software based on complex signal processing technologies.

A main goal of the NAWASCAN project was to develop an antenna array demonstrator in order to test suitable element configurations and beamforming algorithms. Commercial CRPAs (Controlled Reception Pattern Antennas) operate similarly to the developed demonstrator but are primarily designed to suppress interference and focus the antenna gain in a direction where no interference is present. This mitigation strategy was not the focus here, as only the direction finding of the interference was necessary.

To identify a suitable configuration involving both hardware and software, several simulation environments were implemented during the project. These allowed for the verification of the antenna design and various algorithms. The final design choice was a circular, planar array with 7 antenna elements and a signal processing unit based on 4 SDR platforms. One challenge was the calibration of the elements, which all need to be phase-aligned for measurements. To achieve this, a pin was installed at the center of the array to emit a calibration signal at the start of each measurement.

For beamforming, the MUSIC algorithm was adapted accordingly, as it delivered the best results in simulations. In October 2024, the array was tested under real-world conditions for the first time at the Seetaler Alpe military training area, where several datasets were recorded. Post-processing evaluations showed very good results and a fairly accurate estimation of the direction of the interference source.

The demonstrator was intended to demonstrate functionality and was not optimized for military deployment. For further development, it would be essential to create both a compact receiver unit and a compact antenna. For real-time applications, processing time is critical. Offloading computational tasks to an FPGA (Field Programmable Gate Array) would be a practical step.

Overall, the development of an antenna array for use in the GNSS testbed is an important step toward enhancing capabilities in navigation warfare and making tests and scenarios more realistic. Until now, tests involving jamming and spoofing emissions have been conducted with various receivers to analyze their behavior. With the added information about the direction of interference, new possibilities emerge for testing, counteraction, and resilience.

Projektkoordinator

- JOANNEUM RESEARCH Forschungsgesellschaft mbH

Projektpartner

- Bundesministerium für Landesverteidigung