# TACTIC

CreaTing Awareness of Galileo PRS at CriTical InfrastruCtures

| | | | |
|---|---|---|---|
| **Programm / Ausschreibung** | ASAP, ASAP, ASAP 12. Ausschreibung (2015) | **Status** | abgeschlossen |
| **Projektstart** | 01.04.2016 | **Projektende** | 31.12.2018 |
| **Zeitraum** | 2016 - 2018 | **Projektlaufzeit** | 33 Monate |
| **Keywords** | Galileo PRS, anti-spoofing, anti-jamming, kritische Infrastrukturen | | |

## Projektbeschreibung

Das globale Navigationssatellitensystem (GNSS) nutzt die Zeitdifferenz zwischen einem gesendeten und einem empfangenen Signal aus um daraus für eine Vielzahl an Benutzern Positions-und Zeitdaten zu bestimmen. Aufgrund der großen Distanz zwischen den Satelliten und den Empfängern, kann das Systems beeinträchtigt werden wenn entsprechende Signale im selben Frequenzbereich, wie sie auch für GNSS verwendet werden, in beabsichtigter Weise übertragen werden. Obwohl bereits zahlreiche Erkenntnisse zu dieser Thematik in der Vergangenheit gewonnen werden konnten, besteht nach wie vor der Bedarf ein Bewusstsein für die Gefahren, die sich aus gezieltem Spoofing ableiten, in den GNSS Nutzergruppen zu schaffen. Spoofing zielt darauf ab, den Empfänger gezielt zu täuschen und somit eine falsche Lösung für die Navigationsdaten zu generieren, durch die Verwendung GNSS ähnlicher Signale. Ein sogenannter Spoofer schöpft dabei den gesamten Umfang der Open Service (OS) GNSS Signale aus und ist in der Lage perfekte Täuschsignale zu senden.
Eine gewisse Robustheit gegenüber Spoofing ist teilweise bereits in die Open Service GNSS Empfänger oder Anwendungen integriert (z.B.: autonome Integritätskontrollen), dennoch ist eine Überprüfung dieser Schutzmaßnahmen mittels einer realistischen Spoofing-Attacke noch ausständig. Im Gegensatz zu den OS Signalen, sind verschlüsselte GNSS Signale, wie etwa das Galileo Public Regulated Service (PRS) Signal, inhärent unempfindlicher gegenüber solcher Angriffe, da die Signalstruktur von PRS geheim gehalten wird. Die Gefahren beabsichtigter falscher oder beschädigter GNSS Signale werden ebenfalls zur Bewusstseinsbildung bei kritischen Infrastrukturen beitragen. Zudem gibt es kaum Berichte über Experiment zu Spoofing-Angriffen zum Wohl der Gesellschaft (wie z.B. Schutz vor Anschlägen mit UAVs).
Die in TACTIC durchgeführten Versuche beinhalten einen realitätsnahen Aufbau mittels eines GNSS Zielempfängers und eines OS/GPS L1/E1 Spoofers. Kommerzielle Jammer werden ebenfalls berücksichtigt. Als Spoofing Fall ist die erzwungene Landung einer Drohne angedacht, weiters die Täuschung eines Smart-Phone Benutzers, und die Beeinträchtigung der Synchronisation eines Stromnetzes. Gleichzeitig wird ein PRS-ähnliches Signal von einem terrestrischen Testsender gesendet und zusammen mit dem Open Service Signal und dem Spoofing Signal empfangen, um die Vorteile eines PRS Empfängers zu verstehen. Das Projektteam verfügt über sämtlich notwendige Expertise um solch fordernde Experiment zu planen, aufzubauen und durchzuführen. Selbstverständlich aber wird dieses Forschungsprojekt die Kompetenz des Projektteams weiter stärken, ebenso die Position in der Wissenschaftsszene und im Marktsegment. Der Nutzen des TACTIC Projekts für die GNSS Anwender aber ist ein erhöhtes Bewusstsein für Bedrohungen und eine bessere Einschätzung der Wahrscheinlichkeit solcher Fälle. In enger Zusammenarbeit mit den entsprechend Betroffenen sollen die Ergebnisse von TACTIC optimal

veröffentlicht werden.
Bezüglich technischer Weiterentwicklung im Projekt ist die software-basierte Aussendung von GNSS Signalen zu erwähnen, die später als Spoofer kommerzialisiert werden kann oder als terrestrischer Sender (Pseudolites) oder GNSS-RF-Simulator.

## Abstract

Global Satellite Navigation Systems (GNSS) utilize the time difference of arrival (TDOA) principle to provide position and time information to a multitude of users. Due to the large distances between satellites and users, the system may be compromised if suitable signals are broadcast on the same frequencies as used by the GNSS. One distinguishes between spoofing and jamming signals, if those interfering signals are broadcast intentionally. Whereas many research and evidence of jamming has been gained in the past, the awareness about spoofing threats may still further be stressed for the navigation community and GNSS user groups. Spoofing aims at deceiving the GNSS receiver's estimate of position and timing information, by broadcasting GNSS-like signals. A spoofing device exploits the full documentation of the open service GNSS signals and is able to broadcast a perfectly modified signal. Resistance against spoofing is partly intrinsically present in open service GNSS user receivers (e.g. receiver autonomous integrity monitoring) or applications, but those counter-measures have never been tested under a realistic spoofing attack. In contrast to open service signals, encrypted GNSS signals, like the Galileo PRS service are inherently more robust against spoofing, as the detailed signal structure of PRS is kept secret. The threats of intentionally falsified or disrupted GNSS signals may still bring further awareness in the GNSS user community of critical infrastructure entities. Also there are hardly any experiments with spoofing attacks for the benefit of the society (e.g. protection against hostile UAVs).
The experimentation includes a realistic setup of target GNSS receivers and an open-service GPS/Galileo L1/E1 spoofing device transmitting the spoofing signal over the air. Commercial off-the-shelf jammers are also considered. Envisaged spoofing cases are controlled landing of an UAV, deceiving a user navigating with a smart phone and impacting the time synchronization of an electrical power network. In parallel a PRS-like signal will be broadcast from a pseudolite and received simultaneously with the open service satellite + spoofing signal. This will allow assessing the benefit of future Galileo PRS receivers against those threat scenarios. The project team has all required expertise to design, implement and execute such demanding experiments. Certainly, as a mutual benefit, such research work will further increase the project team's competence and will strengthen their position in the related scientific community and market. The benefit of the TACTIC project for the GNSS user community is an increased awareness of this threat and a better assessment of the likelihood of such cases. By close cooperation with respective stakeholders, the dissemination of TACTIC results is maximized. From the technology point of view, software-defined GNSS signal transmission technology is developed, which can be commercialized later in terms of a spoofing device, a GNSS pseudolite or for a GNSS RF simulator. An existing GNSS receiver is tested for its robustness against spoofing and recommendations can be given how a spoofing/jamming attack can be identified and what counter measures are most useful.

## Projektkoordinator

- JOANNEUM RESEARCH Forschungsgesellschaft mbH

## Projektpartner

- IGASPIN GmbH