GRISMO

GNSS Risk and Service Monitoring

Programm / Ausschreibung	ASAP, ASAP, ASAP 14. Ausschreibung (2017)	**Status**	abgeschlossen
Projektstart	01.05.2018	**Projektende**	30.11.2019
Zeitraum	2018 - 2019	**Projektlaufzeit**	19 Monate
Keywords	Galileo, GNSS, Interference, Risk Management		

Projektbeschreibung

Das Ziel von GRISMO (GNSS Risiko und Service Monitoring) ist es, den Mehrwert von robusten Galileo Signalen mit Hilfe eines GNSS-Risiko-Management-Tools gegenüber GPS, EGNOS und Galileo Open Service darzustellen. Der Fokus liegt dabei auf prioritären, mit den Bedarfsträgern auszuarbeitenden Szenarien für sicherheitskritische kommerzielle Anwendungen sowie staatliche Nutzergruppen. In den letzten Jahren wurde das Bewusstsein der Nutzer für beabsichtigte Interferenzen durch praktische Demonstrationen und Publikation von Interferenzmessungen erhöht. Viele Nutzer wissen nun, dass sie von GNSS Signalstörungen betroffen sein könnten, jedoch sind sie derzeit unsicher in welchem Umfang sie bedroht sind und was sie dagegen tun können. In vielen Bereichen unseres täglichen Lebens wird Risikomanagement eingesetzt, um Risiken zu vermeiden, zu reduzieren oder zu teilen. Für fast jeden Aspekt unseres Lebens gibt es eine Risikomanagementstrategie, aber keine für GNSS-Daten. Ein umfassendes Risikomanagement erfordert nicht nur ein Monitoring der GNSS Signale, sondern ebenfalls die Identifizierung und Analyse unterschiedlicher Bedrohungsszenarien vor dem Einsatz der Anwendung, den Einsatz von Strategien zur Risikominimierung und ein Monitoring des Erfolgs dieser Strategien. Bisherige Monitoring-Konzepte basieren auf mit großem Aufwand betriebenen statischen Referenzstationen um eine Qualitätsbeurteilung durchzuführen. Sie sind dadurch einerseits lokal gebunden und andererseits auf professionelle Anwender zugeschnitten wodurch die zugrundeliegende GNSS Anwendung vernachlässigt wird. Im Rahmen von GRISMO findet eine fundierte Risikobewertung basierend auf den tatsächlichen Nutzeranforderungen, konkreten Bedrohungsszenarien und den technischen Möglichkeiten zur Datengewinnung statt. Die Beurteilung der Auswirkungen auf die Quality of Service erfolgt unter Berücksichtigung unterschiedlicher Abschwächungsstrategien bzw. unterschiedliche robuste GNSS Dienste. Dazu zählen Galileo Public Regulated Service (PRS), Galileo Commercial Authentication Service, aber auch das in Bälde zur Verfügung stehende Verfahren der Galileo Open Service Navigation Message Authentication. GRISMO ermöglicht es damit, basierend auf der jeweiligen GNSS Anwendung und des Bedrohungsszenarios eine Risikoanalyse durchzuführen und die Eintrittswahrscheinlichkeit, sowie die Auswirkungen auf den Empfänger, die Applikation und den Nutzer zu bestimmen. Darauf aufbauend werden für die konkrete Anwendung in Frage kommende GNSS Dienste aber auch Mitigationsstrategien vorgeschlagen. Für das Qualitäts- und Service- Monitoring werden unterschiedliche Monitoring- und Mitigationsstrategien untersucht und in Realität getestet. Der Fokus liegt dabei auf der Entwicklung von Strategien für Nutzer mit limitierten Datenbereitstellungs-möglichkeiten (z.B. low-cost Empfänger, Smartphones). Der Truppenübungsplatz des Österreichischen Bundesheeres Seetaler Alpe und die damit zusammenhängende Ausnahmegenehmigung für Jamming und Spoofing sind eine

im Alpenraum einzigartige Möglichkeit, Testkampagnen rund um GNSS Bedrohungen durchzuführen, die Daten zu analysieren und darauf aufbauend neue Technologien zu entwickeln. In diesem Punkt ist Österreich international gesehen federführend, in Deutschland etwa sind derlei Aktivitäten erst in Planung. Als Basis dafür dient die, von TeleConsult Austria entwickelte, Interferenz Analyse Software, welche im Rahmen des Projekts erweitert wird. Dieses Softwaretool kann in weiterer Folge als Referenz im Rahmen eines Interference Testbeds getestet und genutzt werden.

Abstract

The goal of GRISMO (GNSS Risk and Service Monitoring) is to demonstrate the added value of robust Galileo signals using a risk management tool against GPS, EGNOS and Galileo Open Service. The focus is on priority scenarios for safety-critical commercial and governmental applications. In recent years, user awareness regarding intentional interference was increased by practical demonstrations and publication of interference measurements. Many users now know that they may be affected by GNSS interference, but they are currently uncertain about the extent to which they are threatened and what they can do about it. Risk management is used in many areas of our daily lives to avoid, reduce or share risks. Risk management strategies exist for almost every aspect of our lives, but none for GNSS data. Comprehensive risk management not only requires monitoring of GNSS signals, but also identifying and analysing different threat scenarios before deploying the application, applying risk minimization strategies, and monitoring the success of these strategies. Previous monitoring concepts are based on high-static static reference stations to perform a quality assessment and are thus locally bound on the one hand and tailored to professional users on the other hand and therefore neglect the underlying GNSS application. GRISMO provides a sound risk assessment based on actual user requirements, specific threat scenarios, and the technical data provision capabilities of the users. The assessment of the effects on the quality of service takes into account different mitigation strategies and different robust GNSS services. These include Galileo Public Regulated Service (PRS), Galileo Commercial Service (CS) Authentication, but also the – soon available - Galileo Open Service Navigation Message Authentication (OS-NMA) method. GRISMO will carry out a risk analysis based on the respective GNSS application and the threat scenario to determine the probability of occurrence as well as the effects on the receiver, the application and the user. Building on this, suitable GNSS services and mitigation strategies are proposed for the specific application.
For quality of service monitoring, different monitoring and mitigation strategies are examined and tested in reality. The focus is on developing strategies for users with limited data provision capabilities (e.g., low-cost receivers, smartphones). The Austrian Armed Forces military training ground Seetaler Alpe and a valid exemption for jamming and spoofing in this area, are a unique opportunity to carry out test campaigns in the Alpine region, to analyse the data and to develop new technologies based on it. In this context, Austria is the international leader, as for example in Germany, such activities are only in planning. The basis for this is the interference analysis software developed by TeleConsult Austria, which will be expanded as part of the project. This software tool can subsequently be tested and used as a reference in the context of an Interference Testbed.

Projektkoordinator

- OHB Austria GmbH

Projektpartner

- Austro Control Österreichische Gesellschaft für Zivilluftfahrt mit beschränkter Haftung
- BRIMATECH Services GmbH
- Bundesministerium für Landesverteidigung