STRIKE3

GNSS-Interferenzen beobachten – erkennen charakterisieren – reduzieren

M. Pattinson, M. Dumville, Y. Ying
Nottingham Scientific Ltd
Nottingham, UK

M. Zahidul H. Bhuiyan, H. Kuusniemi
Finnish Geospatial Research Institute
National Land Survey of Finland
Helsinki, Finnland

B. Gabrielsson, Å. Waern
Swedish Defence Research Agency (FOI)
Stockholm, Schweden

M. Pölöskey
Automotive & Rail Innovation Center (ARIC)
der AGIT mbH
Aachen, Germany

S. Hill
Satellite Applications Catapult Limited
Harwell, UK

N. Shivaramaiah, S. Kibe
GNSS Labs
Bengaluru, Indien

S. Lee
ETRI
Daejeon, Republik Korea

J. Reyes Gonzalez
European GNSS Agency (GSA)
Prag, Tschechische Republik

STRIKE3 ist eine neue europäische Initiative, um den wachsenden Einsatz von globalen Satelliten-Navigationssystemen (GNSS) auch für sicherheitskritische, strategische, wirtschaftliche oder behördliche Anwendungen zu unterstützen. STRIKE3 hat zum Ziel, internationale Standards zur Erfassung der Bedrohungen durch Interferenzen und Störquellen sowie für die Testspezifikationen für Satelliten-Navigations-Empfänger zu entwickeln.

Erreicht wird dies durch den Aufbau und den Betrieb eines internationalen Netzwerkes zur Beobachtung und Erfassung von Sat.Nav.-Interferenzen, durch das die Ausmaße und die Dynamik der Jammer-Problematik erfasst werden. Durch die Zusammenarbeit der internationalen GNSS-Partnern werden die notwendigen Standards zur Störquellenerfassung sowie für die Empfängertests erarbeitet, veröffentlicht und anschließend implementiert.

Der aktuelle Stand im STRIKE3 Projekt wird dargestellt und die ersten Erkenntnisse aus dem internationalen STRIKE3 Netzwerk werden aufgezeigt.

Schlüsselbegriffe: Interferenzen; Jammer; GNSS Störungen,

I. MOTIVATION

Durch den immer weiter verbreiteten Einsatz von GNSS im Sicherheitsbereich, in Geschäftsabläufen sowie auch in strategischen und sicherheitskritischen Anwendungen nimmt die Abhängigkeit von GNSS ständig zu. In vielen kritischen Teilen der Infrastruktur spielen Sat.Nav.-basierende Funktionen eine wichtige Rolle und die europäische Wirtschaft ist abhängig von einem ununterbrochenen Zugang zu GNSS-basierenden Positionen, Zeitnormalen und Navigation.

Gleichzeitig wird jedoch die Anfälligkeit und Verwundbarkeit von GNSS aufgezeigt und durch diese real existierenden Bedrohungen wächst die Ablehnung gegenüber GNSS-basierten Funktionen und Diensten. Berichte über Störungen oder einen Ausfall von GNSS-Diensten sind heute keine Seltenheit mehr und um den Schutz von GNSS zu gewährleisten, muss nun auf internationaler Ebene reagiert werden. Dazu muss sowohl ein gemeinsamer Standard für die Erfassung und Dokumentation der Störungen und Bedrohungen erreicht

werden, als auch einen weltweit einheitlichen Standard zum Testen und Bewerten der Sat.Nav.-Empfänger und Anwendungen unter Störeinflüssen. Dies wird die führende Rolle von GNSS als Rückgrat für die Bestimmung von Positionen, Zeitnormale und Navigation gewährleisten, insbesondere, wenn daran sehr hohen Anforderungen gestellt werden.

Das STRIKE3-Projekt wird im Rahmen des Forschungsprogramms Horizon 2020 durch die Agentur für das Europäische GNSS (GSA) gefördert, um die Bedrohungen für GNSS-basierte Applikationen, Dienste und Serviceleistungen zu erkennen, zu erfassen, zu charakterisieren und abzuschwächen oder ganz auszuschalten. Das Projekt kann mit den Anfängen der Anti-Virus-Software verglichen werden. Durch die wirtschaftliche und soziale Abhängigkeit von GNSS besteht eine große Notwendigkeit, die Bedrohungslage und die „Störer-Szene“ durchgängig zu beobachten, zu identifizieren und zu charakterisieren. Mit den daraus gewonnen Informationen und Daten ist dann ein „Anti-Virus“ zu entwickeln und insgesamt ist dafür zu sorgen, dass das GNSS ein robustes und gegen alle Angriffe – ob absichtlich oder unabsichtlich hervorgerufen – unempfindliches und stabiles System ist.

STRIKE3 wird Standards durch internationale Partnerschaften schaffen. Diese Standards sind zum einen für die Aufzeichnung und Auswertungen der Störungen sowie deren Erfassung und Dokumentation notwendig, damit eine internationale Datenbank zur Ermittlung der Angriffe und der Erfassung der Bedrohungslage entwickelt werden kann. Zum andern sind Standards zum Testen und Bewerten der Sat.Nav.-Empfänger notwendig, damit die realisierten Anwendungen als robust gegen die neuesten Bedrohungen validiert werden können. Beide Standards fehlen in allen Bereichen der zivilen Anwendungen. Dies ist eine wichtige Barriere zur weiteren Verbreitung von GNSS und dem Einzug in Märkten mit hohen Stückzahlen.

STRIKE3 wird stetig und nachhaltig die internationale Bedrohungslage verfolgen, das Ausmaß und die Dynamik der Probleme erfassen und in der Zusammenarbeit mit internationalen GNSS-Partnern die notwendigen Standards entwickeln und implementieren. Dies wird durch den Aufbau und den Betrieb eines internationalen GNSS-Netzwerks zur Erfassung der Interferenzen erreicht.

II. Understanding the Threat

GNSS-Signale wie bei GPS oder Galileo sind sehr schwach und daher sehr empfindlich gegenüber Interferenzen, die dann dafür sorgen, dass ihre Erfassung und Nachverfolgung durch den GNSS-Empfänger äußerst schwierig oder im schlimmsten Fall gar nicht möglich ist und damit die gesamte GNSS-Funktionalität ausfällt.

Es gibt sehr viele potentielle Ursachen für auftretende Interferenzen, die nicht immer absichtlich hervorgerufen sein müssen. Unabsichtliche Interferenzen können z.B. durch Naturphänomene entstehen („Weltraumwetter“ wie Sonnensturm, Magnetfelder, atmosphärische Störungen) oder werden durch den Betrieb von falsch eingestellten oder fehlerhaften elektrischen Geräten erzeugt. Auch diese Interferenzen können den Empfang der GNSS-Signale stören und führen im schlimmsten Fall dazu, dass der GNSS-Empfänger keine Position mehr bestimmen kann.

Dagegen entstehen absichtlich hervorgerufene Interferenzen durch speziell dafür hergestellte Geräte und verursachen, je nach Ausführung und Sendeleistung, Empfangsstörungen (Jamming), absichtliche Verfälschungen der berechneten Positionen (Spoofing) oder Signalverfälschungen wie sie z.B. durch Repeater hervorgerufen werden (Meaconing). Jedoch werden dabei nicht nur die „angegriffenen“ Geräte gestört oder beeinflusst, sondern auch weitere GNSS-Geräte in der Umgebung. Im STRIKE3-Projekt liegt der Fokus bei den Jammern.

Abhängig von der Ursache der Störung und der Feldstärke des Interferenzsignals sind die Auswirkungen unterschiedlich. Beim Empfänger können z.B. durch Laufzeitfehler oder durch Überlagerungen oder, wenn z.B. nur ein Teil der Satellitensignale gestört ist, durch die dann entstehende ungünstige geometrischen Konstellation der empfangbaren GNSS-Satelliten vermehrt fehlerhafte Positionsbestimmungen auftreten. Auf der funktionalen Applikations- oder Dienste-Ebene können die Auswirkungen aber, abhängig vom Grad der Störung oder der vorhandenen Rückfallebene des Gesamtsystems, von kleinen Abweichungen ohne Folgen bis hin zu folgeschweren wirtschaftlichen oder sicherheitskritischen Schäden reichen.

Es gibt jedoch eine ganze Reihe von Gegenmaßnahmen, um die (mutwilligen) Störungen und deren Auswirkungen zu vermindern. Diese beinhalten:

- Gesetzgebung um die Verbreitung, den Besitz und den Einsatz von Jammern zu unterbinden
- Schulungsmaßnahmen zur Aufklärung über die Gesetzeslage und zur Sensibilisierung, dass die Verwendung von Jammer für den „persönlichen Schutz“ oftmals weitreichende Auswirkungen und Konsequenzen hat.
- Hoheitliche Maßnahmen (Polizei, Regulierungsbehörde, etc.):
    - Detektieren, Auffinden und Einzug der Jammer oder sonstigen Quellen der Interferenzen
    - Indirekte Aufdeckung mittels Berichte oder Dokumente über die Beeinflussung oder den Ausfall von GNSS-Systemen.

- Geräteseitige Maßnahmen (Hardware, Software), um die Auswirkung der Interferenzen abzuschwächen oder zu unterdrücken
    - Antennentechnologie
    - Empfängertechnologie
    - Hybridlösungen, um zusammen mit anderen Sensoren und Verfahren eine kontinuierliche Funktionalität des Gesamtsystems zu erreichen
- Entwicklung von Verfahren und Prozessen, um im Falle des Abbruchs der GNSS-Signale eine sichere funktionale Rückfalleben zu erreichen

Jedoch hängt der Erfolg dieser Gegenmaßnahmen davon ab, möglichst viele technische Details über Funktionsweisen und Parametern der Störquellen zu kennen und zu analysieren. Dabei geht es sowohl um die Art der Störungen (Funktionsprinzip) als auch um die Häufigkeit ihres Auftretens.

Um diese Kenntnisse zu erlangen und um dieses Wissen dann auch up-to-date zu halten ist es notwendig, die auftretenden Interferenzen und Störsender und deren Einflüsse auf die Gerätefunktionen durchgehend zu erfassen und auszuwerten.

Diese Erfassung, Dokumentation und Berichterstattung (Monitoring) ist neben den technischen Auswertungen auch dafür notwendig, um die Stakeholder, wie Institutionen und Behörden, über die real existierenden Bedrohungen zu informieren. Dies führt dann zu der Veranlassung von Maßnahmen durch Polizei und Regulierungsbehörden, um die Jammer zu erkennen, aufzufinden und einzuziehen. Zum andern fließen die Erkenntnisse über die verschiedenen Funktionsweisen der Jammer in die Testspezifikationen für die Empfängertests mit ein. Damit können dann auch die durch die angepassten Antennen- und Empfängertechnik verbesserten Schutzmechanismen geprüft und getestet werden.

III. Frühere Initiativen

GSA und ESA (sowie EU-Mitgliedsstaaten) haben längst die Bedrohungen durch die Jammer auf die kontinuierliche Verfügbarkeit von GNSS erkannt. Daher wurden innerhalb der EU bereits mehrere Initiativen zur Erkennung von GNNS-Jammern und zur Abschwächung ihrer Störeinflüsse durchgeführt. Die wichtigsten Projekte dabei sind das GSA DETECTOR Projekt, die GSA PROTECTOR Studie und das ESA Interference Monitoring System (IMS). Nachfolgend eine Übersicht:

- DETECTOR, GSA, [1], [2]
- PROTECTOR, GSA, Studie, [3]
- STRIKE3 Projekt
- IMS - Interference Monitoring System, ESA, [4]
- InCarITS, Universität der Bundeswehr/DLR, [5]
- JLOC - Jammer Detection and Location System, USA, [6]
- Patriot Watch, Patriot Shield, Patriot Sword, USA, [7]
- GAARDIAN, Sentinel, beide UK, [9], [10], [11]
- MAGIC – Management of Galileo Interference and Counter Measurement, GJU, [12]
- USA, Russland und China zeigen Interesse an Standards zur Erfassung von GNSS-Interferenzen [13], [14]

IV. Der Ansatz von STRIKE3

Das Grundprinzip von STRIKE3 ergibt sich aus verschiedenen Beobachtungen und Ergebnissen aus bereits früher durchgeführten Monitoring-Aktivitäten. Die erste Erkenntnis daraus ist, dass die Störungen und Bedrohungen nicht statisch sondern mit sehr hohen dynamischen Schwankungen auftreten – selbst an einem einzelnen Ort. Die nachfolgenden Ergebnisse aus diesen früheren Aufzeichnungen zeigen die Anzahl der erfassten „Chirp“-Jammer (ein Funktionsprinzip, das typisch für kleine Jammer in Fahrzeugen ist), die an einem Ort während eines Zeitraums von zwei Jahren erkannt und erfasst wurden. Nachfolgend sind die Gesamtzahlen pro Monat dargestellt.

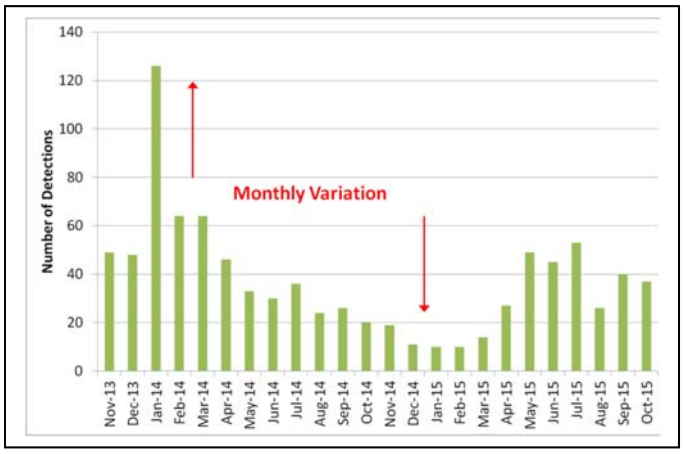

Fig. 1. Monatliche Anzahl der erfassten Jammer in “Chirp”-Technologie an einem Ort innerhalb von zwei Jahren

Die starke Varianz innerhalb dieses Zeitraumes reicht von einem Minimum von 10 Jammer in einem Monat bis zu über 120 Jammer in einem anderen Monat. Diese hohen Schwankungen zeigen, dass Langzeitmessungen und Beobachtungen absolut notwendig sind, um das Maß der Bedrohung richtig einzustufen. Kurzzeitmessungen können kein zuverlässiges Ergebnis liefern.

Die zweite Erkenntnis ist, dass das Gefährdungspotential sehr stark vom Ort abhängt. Selbst vergleichbare Orte in der gleichen Region können mit einer stark unterschiedlichen Anzahl von Interferenz-Vorfällen betroffen sein. Die nachfolgende Abbildung zeigt die Resultate aus einem Monat (Oktober 2015), aufgenommen an zwei unterschiedlichen Orten. Beide Messpunkte lagen jeweils in der Nähe einer Bundesstraße in

vergleichbaren Regionen, die Messungen wurden mit der gleichen Messausrüstung durchgeführt. Wie leicht ersichtlich ist, ist die Anzahl der erfassten Fälle sehr unterschiedlich. Am Ort A wurden insgesamt 1.436 Fälle erfasst, davon wurden z.B. 37 von „Chirp"-Jammern verursacht. Am Ort B waren es dagegen lediglich 250 Fälle, davon wurden 10 durch „Chirp"-Jammer verursacht. Dies zeigt deutlich, dass man die Informationen und Ergebnisse flächenmäßig bei verschiedenen Orten erfassen und vergleichen muss, um ein allgemeines Bild über die Gefährdung durch Jammer zu erhalten.

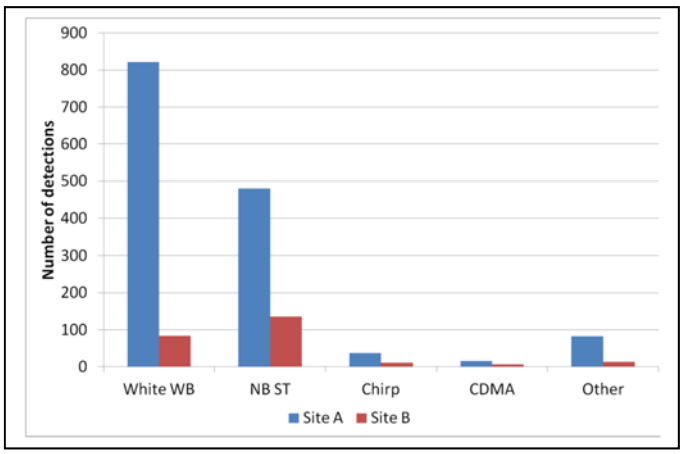

Fig. 2. Anzahl der detektierten Jammer-Ereignisse mit unterschiedlichen Funktionsweisen an zwei Orten über einen Zeitraum von einem Monat

Die dritte Erkenntnis ist, dass mit zunehmender Anzahl der Beobachtungsstationen und zunehmender Länge des Beobachtungszeitraums auch die Typenvielzahl der erkannten Jammervarianten zunimmt. Messungen über eine Woche an einem Ort mögen vielleicht 20 verschiedene Jammervarianten aufzeigen. Durch die Ausdehnung der Beobachtungszeit und durch Messungen an zusätzlichen Orten erhöht sich die Anzahl der erfassten Jammervarianten um ein Vielfaches. Die so erfassten Interferenzen werden ausgewertet und analysiert und als Signaturen in einer Datenbank abgelegt. Diese Datenbank wird laufend mit neu auftretenden Signaturen aktualisiert, womit wieder die Analogie zur Erfassung von Computerviren deutlich wird.

Diese Datenbasis ist ein Abbild der real auftretenden Interferenzen und stellt somit eine validierte Quelle zum Test der Störfestigkeit von Antennen, Empfängern sowie von Algorithmen zur Störunterdrückung dar. Darüber hinaus können diese Daten zur Entwicklung weiterer Verfahren zur Erhöhung der Störfestigkeit in Hard- und Software herangezogen werden.

Daher gehört zum Ziel des STRIKE3-Projekts die Entwicklung eines Standards für das Monitoring und Testen, um damit den größtmöglichen internationalen Nutzen zu schaffen.

STRIKE3 umfasst auch die Definition, Entwicklung und Demonstration eines kostengünstigen GNSS-Interface als Basis für einen Jammer-Detektor, um damit die Betreiber von Infrastrukturen, Anbieter von GNSS-basierten Dienstleistungen sowie Institutionen und Behörden in ihrem Kampf gegen den mutwilligen Einsatz von Jammern bei Verbrechen und organisierter Kriminalität zu unterstützen. Der Lösungsansatz von STRIKE3 setzt sich aus verschiedenen Innovationen zusammen:

- Innovation 1: Standard für die Erfassung und Dokumentation der GNSS-Störungen und Bedrohungen

  Im Projekt gibt es zwei grundsätzliche Innovationen, mit denen auch eine globale Aufmerksamkeit erreicht wird. Die erste ist die Entwicklung eines internationalen Standards zur Erfassung und Dokumentation der auftretenden GNSS-Störungen und Bedrohungen. Eine Standardisierung ist notwendig, um Daten und Ergebnisse aus unterschiedlichen Systemen und Ländern übergreifend auswerten und daraus dann Statistiken und Rückschlüsse ziehen zu können. Damit stehen dann einheitliche und konsistente Daten- und Berichtsformate über Störsignale und erfasste Attacken auf GNSS-Dienste zur Verfügung.

- Innovation 2: Testen der Störfestigkeit

  Die zweite Innovation bezieht sich auf die Erstellung von Teststandards. Im März 2015 veröffentlichte die GSA ihren vierten Marktreport [15]. Kein Hersteller von GNSS-Empfänger gibt an, dass sein Produkt auch unter Störeinflüssen noch arbeitet. Daher ist die Verfügbarkeit von validen Störmustern und internationalen Teststandards für die Entwicklung der nächsten Empfängergeneration äußerst wichtig, damit sie auch bei hochwertigen und sicherheitskritischen Systemen eingesetzt werden können.

- Innovation 3: Internationales Netzwerk zur Beobachtung und Erfassung von GNSS-Interferenzen und Störsignale

  Mit STRIKE3 wird ein internationales Beobachtungsnetzwerk aufgebaut, durch das die Partner – aber auch die Europäische Kommission, die Behörden und die GSA – die erfassten GNSS-Störungen und die daraus abgeleiteten Trends über alle Kontinente aus ausgewählten (Teil-)Netzwerken erkennen und beurteilen können. Neu auftretende Störsender werden aufgezeichnet und mit bereits erfassten Ereignissen weltweit verglichen. Damit entsteht ein reales Bild über die zeitliche Verteilung – die Dynamik – der auftretenden Störungen und Attacken.

- Innovation 4: Zentrale Datenbank der GNSS Störgrößen

  Alle im STRIKE3-Netzwerk erfassten Ereignisse werden in einer zentralen Datenbank in einem standardisierten Datenformat abgespeichert. Somit lassen sich Analysen bzgl. Trends, Muster, Signalformen, etc. sehr

einfach über alle Datensätze durchführen, unabhängig davon, durch welche Sensorstation das Ereignis erfasst wurde.

- Innovation 5: “System von Systemen”

  Durch die einheitlichen Standards ermöglicht es STRIKE3, dass eine Gruppe von unterschiedlichen Detektoren von verschiedenen Herstellern zu einem „System von Systemen“ zusammengefasst werden können. Dieses Zusammenspiel ermöglicht die kontinuierliche Erfassung von GNSS-Störungen an weltweiten Schlüsselpositionen, motiviert durch das gemeinsame Ziel, GNSS durch gemeinsam aufgebautes Wissen zu verbessern.

- Innovation 6: Neue Technologien

  Die Datenbank aus STRIKE3 wird zukünftig auch dazu dienen, dass durch neue Technologien und noch zu entwickelnde Gegenmaßnahmen das Gefährdungspotential durch die Störsender abnehmen wird. Das übergeordnete Ziel muss sein zu gewährleisten, dass die nächste Generation von GNSS-Empfängern robust gegen Störsignale sein werden und dass GNSS-basierte Applikationen gegen solche Jammer-Attacken geschützt sind. Das entspricht dem langfristigen Bestreben des STRIKE3-Projekts.

In der nachfolgenden Grafik sind die Verbindungen, Verknüpfungen und Abhängigkeiten der einzelnen Innovationen in STRIKE3 dargestellt.

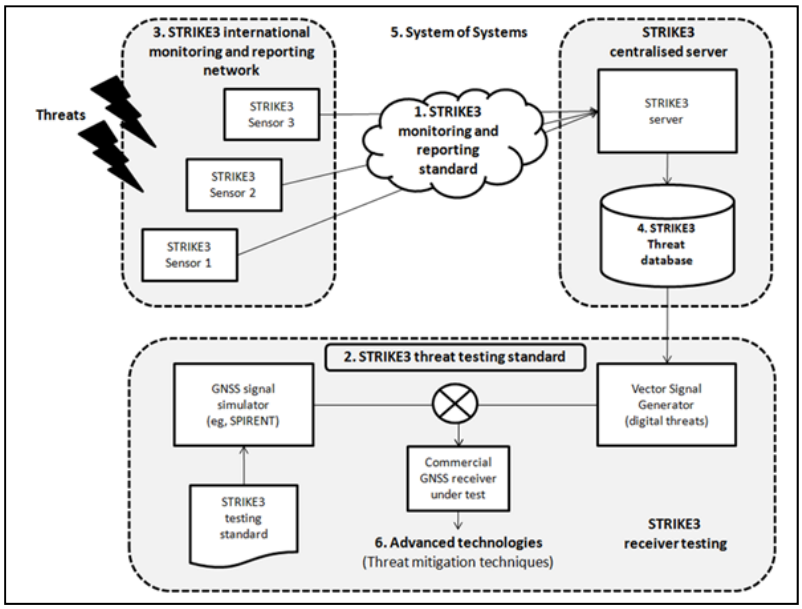

Fig. 3. Übersicht über die STRIKE3 Innovationen

Das STRIKE3-Projekt wurde im Februar 2016 gestartet. Aktuell werden Informationen über internationale Störfälle gesammelt und ein State-of-the-Art-Review erstellt. Des Weiteren begann im März der Aufbau des internationalen Monitoring-Netzwerks, das aktuell neun verschiedene Beobachtungsstationen in fünf verschiedenen europäischen Ländern umfasst. Der weitere Ausbau mit zusätzlichen Stationen in und außerhalb Europas geht weiter. Bis Anfang 2017 wird ein erster Entwurf der Reporting- und Teststandards entwickelt. Die anschließende Validierung dieser Standards führt dann längerfristig zu einheitlichen Datensätze aus dem Monitoring und zu einheitlichen Spezifikationen für die Empfängertests.

V. RESÜMEE

Durch die zunehmende Abhängigkeit von GNSS ist es wichtig, deren Störanfälligkeit, wie z.B. verursacht durch Interferenzen, zu kennen und zu erfassen. Im STRIKE3-Projekt wird dem in vielfältiger Weise Rechnung getragen, so zum einen durch die Entwicklung von Standards sowohl für die Erfassung der Störgrößen (Reporting) als eauch für die zukünftigen Empfängertests. Des Weiteren durch den Aufbau eines weltweiten Beobachtungsnetzwerks in Verbindung mit der Erstellung einer Datenbank zur Erfassung der Signaturen realer Störungen und Interferenzen. Darüber hinaus auch durch die Entwicklung einer Testspezifikation für Empfänger auf

Basis realer Störsignale, die durch das Beobachtungsnetz erfasst wurden.

Damit werden auf internationaler Ebene die Voraussetzungen geschaffen, um zukünftig die Störfestigkeit von Antennen, Empfängern, Komponenten und den gesamten Systemen testen und verbessern zu können.

Danksagung

Die in diesem Fachartikel vorgestellte Arbeiten werden durch die Agentur für das Europäische GNSS (GSA) im Rahmen des Forschungsprogramms Horizon 2020 gefördert. Der Originaltitel des Projekts lautet: „Standardization of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation“

Referenzen

[1] K. Sheridan, Y. Ying and T. Whitworth, “Pre- and Post-Correlation GNSS Interference Detection within Software Defined Radio”, Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012), Nashville, TN, September 2012, pp. 3542-3548

[2] “GSS100D Detector, GPS/GNSS Interference Detector”, http://www.spirent.com/Products/GSS100D-Detector

[3] N. Davies, C. Schäfer, B. Vauvy and M. Schoenhuber, “PROTECTOR, Protecting European GNSS Services”, GNSS Interference, Detection & Mitigation Conference, National Physical Laboratory, Teddington, London, 10 March 2011

[4] Wendel, J., Kurzhals, C., Houdek, M., Samson, J., "An Interference Monitoring System for GNSS Reference Stations," Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013), Nashville, TN, September 2013, pp. 3391-3398

[5] D. Fontanella, R. Bauernfiend and B Eissfeller, “In-Car GNSS Jammer Localization Using Vehicular Ad-Hoc Networks”, Inside GNSS, Working Papers, May/June 2013

[6] A. Brown, D. Reynolds, D. Roberts and S. Serie, “Jammer and Interference Location System – Design and Initial Test Results”, Proceedings of the 12th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 1999), Nashville, TN, September 1999, pp. 137-142

[7] “Patriot Watch, Patriot Shield, Patriot Sword: A Proposed Solution to Address Risk to US Critical Infrastructure”, http://overlooksys.com/assets/files/Patriot%20WatchShieldSword.pdf

[8] “National PNT Advisory Board comments on Jamming the Global Positioning System - A National Security Threat: Recent Events and Potential Cures”, November 4 2010

[9] C. Curry, “GAARDIAN Project Results & Introduction to The Sentinel Project”, GNSS Interference, Detection & Mitigation Conference, National Physical Laboratory, Teddington, London, 10 March 2011

[10] C. Curry, “Sentinel Project, Report on GNSS Vulnerabilities”, Project Report 001, 04 April 2014

[11] “Signal Sentry 1000”, http://www.exelisinc.com/solutions/signalsentry/Pages/default.aspx

[12] A. Ferreol, P. Morgand and E. Rossini, “Detection, Mitigation and Isolation of Galileo Interferers”, ENC-GNSS 2008 Conference, Toulouse, France April 22-25, 2008

[13] S. Kizima, “International Interference Detection & Mitigation System for GNSS”, ICG Working Group A, 8th Meeting of the International Committee of GNSS, Dubai, UAE, November 2013

[14] W. Zhen and X Zhao, “Suggestions on Standardized Reporting Form of GNSS Interference”, ICG Working Group A, 8th Meeting of the International Committee of GNSS, Dubai, UAE, November 2013

[15] European GNSS Agency, “GNSS Market Report”, Issue 4, March 2015

Kontakt:
Martin Pölöskey
Leiter Automotive & Rail Innovation Center (ARIC)
der AGIT mbH

Tel: +49-2432-93376-11
Mobil: +49-173-2730 440
Mail to: martin.poloskey@aric-aachen.de