



*Philipp Berglez und Bernhard Hofmann-Wellenhof*

## **Galileo und Grafarend unterwegs zu GNSS**

### **Zusammenfassung**

Das europäische Satellitennavigationssystem Galileo erlebte in seiner bisherigen Entwicklung mehrfach Verzögerungen, die auch zur Frage führen, ob der Wettbewerb mit den anderen Global Navigation Satellite Systems (GNSS) noch erfolgreich bestanden werden kann. Eine besondere Herausforderung für Galileo in letzter Zeit stellten die beiden Satelliten dar, die im August 2014 von einer russischen Trägerrakete in ihre Umlaufbahnen gebracht werden sollten, diese aber nicht erreichten. Ist dadurch Galileo in Frage gestellt, kommt es zu weiteren Verzögerungen? Gibt es für Galileo positive Perspektiven, die gerade jetzt in dieser kritischen Phase Vorteile gegenüber anderen GNSS bieten?

### **Einleitung**

Am 22. August 2014 fand der erste Start von zwei „Galileo FOC (Full Operational Capability)“-Satelliten statt. Auf Grund von Problemen, die 35 Minuten nach dem Start der Trägerrakete auftraten, gelang es nicht, die Satelliten in ihre nominellen Umlaufbahnen zu bringen. Wie später analysiert werden konnte, führte ein Fehler im Entwurf der Fregat-Raketenoberstufe, welche bei Sojus-Trägerraketen zum Einsatz kommt, zu diesen Problemen und veranlasste eine Fehlstellung der Steuerdüsen [1].

Entgegen der ursprünglich geplanten nahezu kreisförmigen Umlaufbahn (Exzentrizität nahezu 0) mit einer Inklination von  $55^\circ$  und einer großen Halbachse von 29.600 km befanden sich die beiden Satelliten in einer Umlaufbahn mit einer Exzentrizität von 0.23 und einer Inklination von  $49.8^\circ$  [2]. Dadurch ergab sich eine viel zu elliptische Umlaufbahn, welche die Satelliten durch den Van-Allen-Strahlungsgürtel führte und somit eine Gefahr für die Lebensdauer der Satelliten darstellte. Die Satellitenbahn verursachte auch Schwierigkeiten bei den Sensoren in den Satelliten, die für eine genaue Ausrichtung der Antennen in Richtung Erde zuständig sind [3]. Ein weiteres Problem – für die Navigation – ergab sich im Bereich der Navigationsnachricht. Die Bahnparameter konnten auf Grund der gestiegenen Wertebereiche teilweise nicht in der binären Navigationsnachricht abgebildet werden. Auch bewirkte der elliptische Orbit eine fast doppelt so hohe Dopplerverschiebung des Signals, die unter gewissen Umständen den Empfängern Probleme bereiten könnte.

Die beiden im August 2014 gestarteten Galileo-Satelliten wurden in den vergangenen sechs Monaten in eine höhere Umlaufbahn gebracht [4]. Dadurch ist es gelungen, die Satelliten aus der Gefahrenzone des Van-Allen-Strahlungsgürtels zu manövrieren und somit die Lebenszeit sowie Verlässlichkeit zu steigern. Obwohl die Umlaufbahnen noch immer nicht den nominellen Parametern entsprechen, gelang es damit, die Orbit-Wiederholrate auf 20 Tage zu setzen. Somit ist eine einfachere Synchronisation mit den übrigen Galileo-Satelliten, die eine Wiederholrate von 10 Tagen aufweisen, möglich. Ob und wie diese beiden Satelliten in Zukunft für Navigationsanwendungen verwendbar sind, wird derzeit von der European Space Agency (ESA) noch genau untersucht. Nach Abschluss der Analysen wird eine entsprechende Entscheidung getroffen werden [4].

Abbildung 1 zeigt einen Vergleich der Umlaufbahnen im raumfesten Koordinatensystem (links) sowie in der Orbitalebene (rechts). In Blau dargestellt ist die nominelle Galileo-Umlaufbahn. Der auf Grund des Problems bei der Fregat entstandene Orbit (im September 2014) ist in Rot dargestellt. Die

Umlaufbahn nach erfolgter Korrektur ist in Grün dargestellt.

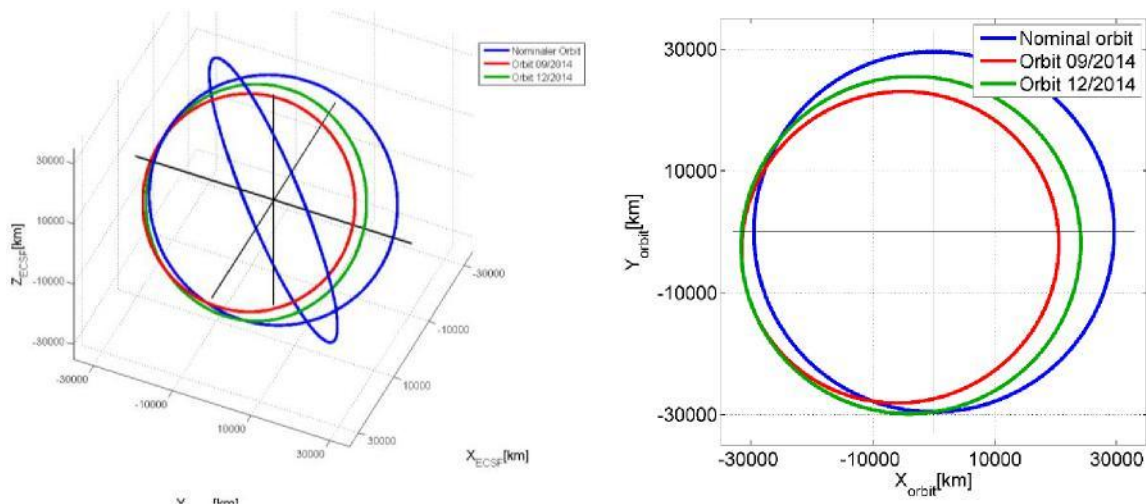


Abbildung 1: Vergleich der Galileo-Umlaufbahnen (blau nominelle Umlaufbahn; rot anfängliche Umlaufbahn im September 2014 und grün korrigierte Umlaufbahn im Dezember 2014)

Können diese Satelliten trotz ihrer noch immer leicht elliptischen und zu „tiefen“ Bahnen für GNSS mitverwendet werden? Gibt es für Galileo positive Perspektiven, die gerade jetzt in dieser kritischen Phase Vorteile gegenüber anderen GNSS bieten?

### Ist Galileo in Frage zu stellen?

Die Antwort auf diese Frage kann nur mit „Nein“ beantwortet werden, dazu genügt es schon, das nutzerorientierte Konzept von Galileo als Argument einzubringen. Auch durch die Betrachtung der aktuellen Bedürfnisse und Anforderungen der Nutzer resultiert ein klares Bekenntnis zu Galileo. Während andere GNSS, wie zum Beispiel das amerikanische GPS, das russische GLONASS oder das chinesische Beidou, unter militärischer Kontrolle stehen, ist Galileo auf eine primär zivile Nutzung unter ziviler Kontrolle ausgelegt. Galileo als eines der wichtigsten europäischen Weltraumprojekte hat in den vergangenen Jahren neue technische Maßstäbe im Bereich GNSS gesetzt und ist derzeit mehr denn je von strategischer Bedeutung für die Unabhängigkeit (bezüglich anderer Systeme) und die Wirtschaft der Europäischen Union.

In den vergangenen Jahren wurde die Praxistauglichkeit von Schlüsseltechnologien erforscht und erfolgreich getestet. So ist es zum Beispiel gelungen, eine außergewöhnlich stabile passive Wasserstoff-Maser-Uhr – die fortschrittlichste Uhr, die bisher für Navigationszwecke verwendet wurde – an Bord eines Satelliten zu betreiben. Die erste Positionslösung, die nur unter Verwendung von Galileo-Satelliten gemacht wurde, gelang der ESA am 12. März 2013. Die erste Galileo-Positionslösung in Österreich wurde am 21. März 2013 in Graz erzielt [5]. Am 27.

März 2015 wurden zwei weitere Galileo FOC-Satelliten erfolgreich vom Europäischen Weltraumbahnhof in Französisch-Guyana gestartet. Derzeit (Mai 2015) befinden sich diese beiden Satelliten in der Kommissionierungsphase [6]. Vier weitere Galileo-Satelliten befinden sich derzeit in der finalen Testphase und sollen noch im Jahr 2015 gestartet werden [7]. Das Ziel der Europäischen Kommission ist es, bis Ende 2016 erste Services (Open Service, Public Regulated Service und Search and Rescue Service) den Nutzern zur Verfügung zu stellen. Bis zum Jahr 2020 soll dann die volle Konstellation, mit 24 Satelliten und 6 Reservesatelliten, von Galileo erreicht werden. Bis dahin soll der verschlüsselte Commercial Service ebenfalls operationell sein [7]. Wenn dieser Zeitplan eingehalten werden kann, ist Galileo im internationalen Wettbewerb um eine gute Marktposition wieder im Rennen.

## GNSS-Verwundbarkeit und Bedrohungen

In Zukunft kommen neue Herausforderungen im Bereich der satellitengestützten Positionierung und Navigation auf die Nutzer zu. Globale Satellitennavigationsysteme haben mittlerweile eine wichtige Rolle in unserem Alltag eingenommen. Je wichtiger eine Technologie für unsere Gesellschaft wird, desto mehr steigt auch das Gefahrenpotential hinsichtlich Störattacken. Speziell in den letzten Jahren wurden Anwendungen von GNSS vermehrt Ziel von Störattacken. Studien belegen, dass durch absichtliche Störattacken beträchtliche wirtschaftliche, aber auch materielle Schäden entstehen können. Störsignale können den Betrieb von GNSS-Empfängern signifikant beeinflussen. Dies kann von einer schlechteren Positionsgenauigkeit bis hin zu einer falschen Position oder zum totalen Ausfall der Positionierung führen. Dies hätte fatale Auswirkungen auf das Transportwesen, die Telekommunikation, sowie standortbezogene Dienste (Location-Based Services).

GNSS-Empfänger stellen abgesehen von der geographischen Breite und Länge sowie Höhe eine vierte wesentliche Dimension – die Zeit – zur Verfügung. Mit Hilfe der von den Satelliten abgestrahlten Signale ist es möglich, die Zeit mit einem GNSS-Empfänger zu bestimmen [8]. Dies ermöglicht es den Nutzern, eine hochgenaue Zeitinformation jederzeit, global und mit einer Genauigkeit von besser als 1 Nanosekunde zu erhalten.

Präzise Zeitbestimmung ist von entscheidender Bedeutung für eine Vielzahl von Anwendungen und Verfahren weltweit. Abbildung 2 zeigt anhand einiger Beispiele die Abhängigkeit von GNSS in unserer heutigen Gesellschaft. Kommunikationssysteme, Stromnetze und Finanznetzwerke verlassen sich alle auf präzise Zeitinformation für die Synchronisation. Die freie Verfügbarkeit einer GNSS-Zeit bedeutet für Unternehmen Kosteneinsparungen und Vorteile hinsichtlich der Effizienz. So verwenden beispielsweise Mobilfunknetzwerke eine GNSS-Zeit, um alle Basisstationen zu synchronisieren. Dies ermöglicht eine effizientere Nutzung des begrenzt verfügbaren Frequenzspektrums [9]. Weltweit nutzen Finanzdienstleister GNSS-Zeitstempel, um Transaktionen zu koordinieren, zu protokollieren und nachvollziehbar zu machen. Verteilte Netzwerke von Sensoren, die koordiniert werden müssen, um genaue Ergebnisse zu erzielen, bedürfen einer Zeitquelle, die an allen Stellen eine hohe Genauigkeit garantieren kann. GNSS-basiertes Timing ist für Anwendungen von Bedeutung, bei denen genaue Zeitpunkte von Geräten, die über weite geographische Gebiete verteilt sind, erforderlich sind. So ermöglicht beispielsweise die Verwendung von GPS-Zeit in seismischen Messnetzwerken Forschern, schnell und präzise die Epizentren von Erdbeben zu bestimmen.

Energieversorgungsunternehmen haben hohe Anforderungen an Zeit und Frequenz, um eine effiziente Energieübertragung und -verteilung zu ermöglichen. Wiederholte Stromausfälle haben in der Vergangenheit die Notwendigkeit einer besseren Zeitsynchronisation in Versorgungsnetzwerken demonstriert. Die Analyse dieser Blackouts haben viele Unternehmen veranlasst, GPS-basierte Zeitsynchronisation in Kraftwerken und Umspannwerken zu verwenden. Durch die zeitliche Analyse von Ausbreitungsanomalien ist es möglich, die genaue Lage eines Defekts zu verfolgen [9].

Beispiele aus der jüngeren Vergangenheit zeigen, wie real die Bedrohung durch Störattacken ist. Im Jahr 2010 kam es am Flughafen in Newark in New York im Bereich des bodenbasierten Augmentierungssystems (GBAS) zu Ausfällen, so dass das System zeitweise heruntergefahren werden musste. Die Störungen wurden von Jammern (Störsendern), welche an der nahegelegenen Autobahn in vorbeifahrenden LKWs zum Einsatz kamen, verursacht. Die Jammer wurden mutmaßlich dazu verwendet, um die Fahrtroute der Fahrer zu verschleiern. Am Flughafen Kaohsiung in Taiwan wurden im Zeitraum von August bis September 2011 im Rahmen einer Studie 117 Störevents pro Tag festgestellt [10]. In San Diego (USA) sorgte eine unabsichtliche Störattacke, hervorgerufen durch die US Marine, mehrere Stunden für Verwirrung bei der Bevölkerung. Notfallpager, Geldautomaten und weitere Infrastruktur fielen während des Zwischenfalls aus [11].

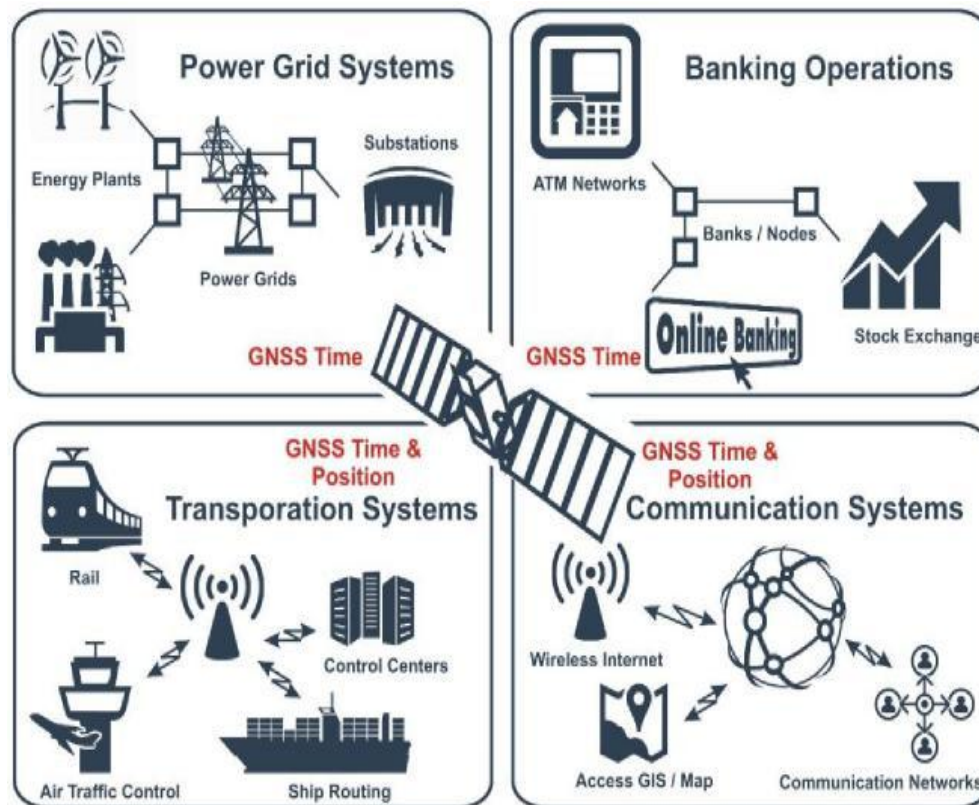


Abbildung 2: Abhängigkeit von GNSS

Im Rahmen des Forschungsprojekts „GAIMS – GNSS Airport Interference Monitoring“ wurde im vergangenen Jahr im Raum Graz in Österreich während eines Feldtests bereits in der ersten Stunde ein GNSS-Störsender (Jammer) detektiert [12]. Der Jammer konnte am 19. August 2014 um 11:24 in der Nähe des Flughafens Graz detektiert werden. Abbildung 3 zeigt die örtlichen Gegebenheiten der Messpunkte sowie die Nähe zur Autobahn A2.



Abbildung 3: Feldtests im Rahmen des GAIMS-Projekts in der Nähe des Flughafens Graz Thalerhof und der Autobahnen A2 und A9

In Abbildung 4, welche die spektrale Leistungsdichte darstellt, erkennt man den Jammer, der das GNSS-L1/E1-Band stört. Da das Störsignal über einen Zeitraum von ca. 7 Sekunden vorhanden war, kann davon ausgegangen werden, dass es sich um ein sogenanntes "Personal Privacy Device" handelt, welches mit dem Zigarettenanzünder in einem LKW/PKW betrieben werden kann. Die schnell

ansteigende und dann wieder abfallende Leistung unterstützt die These eines vorbeifahrenden Jammers.

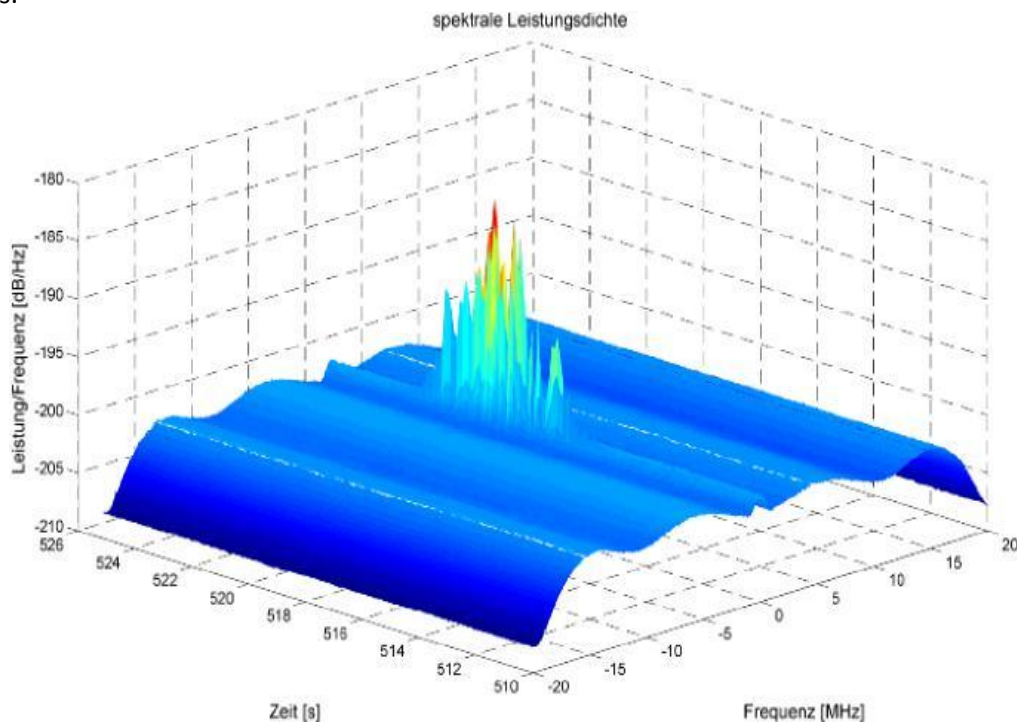


Abbildung 4: Spektrale Leistungsdichte des GNSS-L1/E1-Bandes zum Zeitpunkt der Störattacke

Der Effekt des Störsenders wird auch am Signal-Rausch-Verhältnis (SN<sub>0</sub>R) der Satelliten deutlich. In Abbildung 5 sind die theoretischen SN<sub>0</sub>R-Werte der Satelliten den gemessenen gegenübergestellt. Deutlich sichtbar ist der Abfall der empfangenen Signalleistung während der Störattacke.

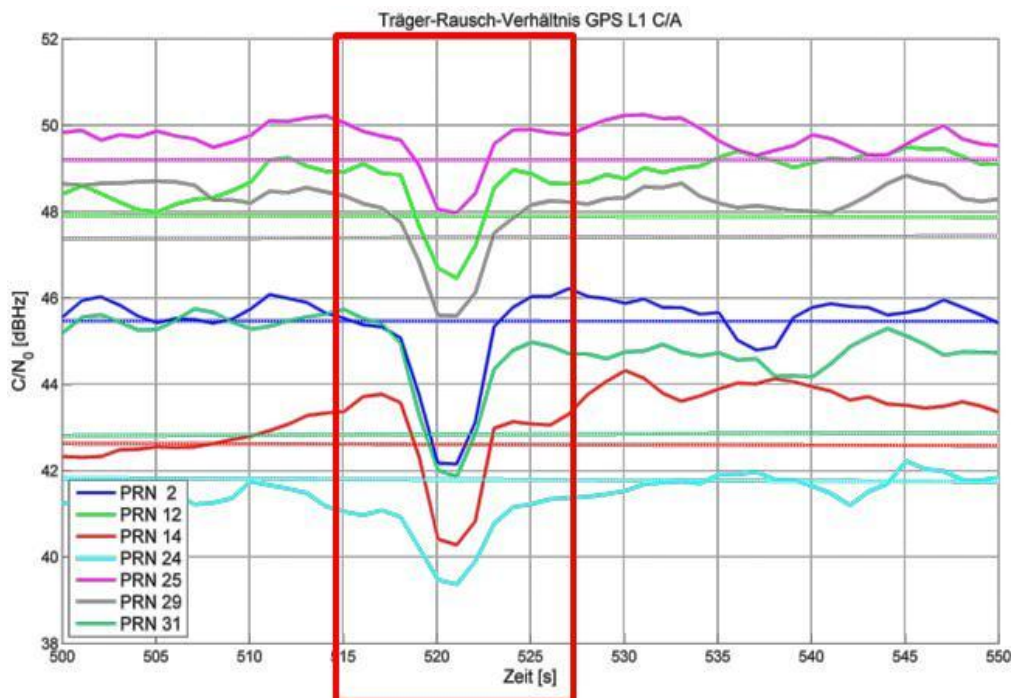


Abbildung 5: Signal-Rausch-Verhältnis zum Zeitpunkt der Störattacke

Die Störsignale des Personal Privacy Device, welches in einem Auto oder LKW verwendet wurde, können den Betrieb von GNSS-Empfängern im Umkreis von bis zu 1000 m signifikant beeinflussen. Auf die Landesysteme des Flughafens hatten die Störsignale in diesem konkreten Fall keine Auswirkung. Personal Privacy Devices gibt es bereits für unter 50 Euro zu kaufen und sie sind in ihrer Verwendung denkbar einfach. Der Betrieb eines solchen Gerätes ist jedoch strengstens verboten.

Neben den Jammern, die das Frequenzband stören, gibt es eine weitere Methode – Spoofing genannt –, das GNSS-Signal absichtlich zu verfälschen. Im Gegensatz zu Jamming (Störung des GNSS-Signalspektrums) löst Spoofing keinen Alarm im GNSS-Empfänger aus, da von einem Spoofer verfälschte GNSS-Signale ausgestrahlt werden, die nicht von den originalen Signalen unterschieden werden können. Dadurch ist es gezielt möglich, die aus den Messungen mit einem GNSS-Empfänger resultierende Position von der tatsächlichen Position abweichen zu lassen. Das Herzstück eines Spoofers ist ein GNSS-Simulator, wie er in der GNSS-Empfängerentwicklung eingesetzt wird. GNSS-Simulatoren können, wenn sie in falsche Hände gelangen, bereits mit relativ geringem Aufwand und niedrigen Kosten für illegale Zwecke verwendet werden. Speziell durch das Aufkommen von software-basierten Simulatoren [5] ist dieses Risiko weiter gestiegen. Eine Alternative zu Simulatoren wäre das Aufzeichnen und Abspielen von realen GNSS-Signalen. Spoofing ist derzeit, im Vergleich zu Jamming, noch keine große Gefahr. Jedoch zeigen erfolgreiche Experimente die Auswirkung einer Spoofing-Attacke sehr deutlich.

So wurde im Juni 2013 eine 65-m-Yacht im Rahmen eines Feldversuchs von der Universität von Texas in Austin durch eine Spoofing-Attacke von ihrem Kurs abgebracht. Dabei kam ein von der Universität von Texas entwickelter GNSS-Spoofers zum Einsatz, der die Größe einer Aktentasche besitzt. Es gelang, die Yacht um mehrere hundert Meter vom Kurs abzubringen, ohne dass die Besatzung Verdacht schöpfte [13]. Auch gelang es durch Spoofing, Drohnen (UAVs) vom Kurs abzubringen oder die Zeitsynchronisation in einem Energieversorgungsnetz zu verfälschen [14]. Diese Experimente zeigen deutlich die Schwäche der GNSS-Empfänger, solche Spoofing-Attacken zu detektieren.

Galileo bietet hier, im Unterschied zu den anderen derzeit verfügbaren Systemen, auch zivilen Nutzern in Zukunft eine Lösung, da die Signalstrukturen von einigen Galileo-Services resistenter gegenüber Störattacken und, wenn auch eingeschränkt, für zivile Anwender nutzbar sind.

### **Mehrwert von Galileo PRS**

Während das militärische GPS-Signal (P(Y)- und M-Code) ausschließlich militärischen Nutzern zur Verfügung steht, wurde der Galileo Public Regulated Service (PRS) für autorisierte zivile Nutzergruppen konzipiert. Durch eine Verschlüsselung des übertragenen Signals wird der Zugang zum PRS von der EU und ihren Mitgliedstaaten eingeschränkt. Die primären Nutzer werden Exekutive (z.B. Polizei, Zoll) sowie öffentliche Notdienste (z.B. Rettung, Feuerwehr) und Katastrophenschutz sowie Betreiber von kritischer Infrastruktur (z.B. Telekommunikationsanbieter und Energieversorger) sein. Dadurch wird ein wesentlich breiteres Nutzerspektrum von den Vorteilen verschlüsselter GNSS-Signale profitieren. Der PRS wird durch zwei verschlüsselte Signale realisiert, welche in zwei unterschiedlichen Frequenzbändern (E1 und E6) liegen. Bewusst wurde bei der Konzeptionierung darauf geachtet, dass zumindest ein Frequenzband (E6) von keinem anderen GNSS verwendet wird.

Diese Aufteilung unterstützt das Konzept der selektiven Störung – andere GNSS-Signale können gestört werden, aber das PRS-Signal bleibt dennoch verfügbar. Auch wurden die PRS-Signale hinsichtlich ihrer Signalparameter und Eigenschaften so konzipiert, dass der Dienst eine widerstandsfähige, verlässliche und kontinuierliche Positions- und Zeitinformation, sogar unter schwierigen Bedingungen und vor allem auch im Fall von Störattacken, dem Nutzer zur Verfügung stellen kann [15].

Im Rahmen des Forschungsprojekts "PURSIT – Galileo Public Regulated Service Signal Simulation and Position, Velocity, and Time Calculation" wurden die Leistungsfähigkeit und der Mehrwert der PRS-Signale im Vergleich zu den zivilen Signalen untersucht. Um Einschränkungen durch Vertraulichkeit und Sicherheit von PRS-Informationen vorzubeugen, wurden das PRS-Signal sowie die PRS-Verschlüsselung durch öffentlich zugängliche Informationen und Verschlüsselungsmethoden ersetzt. Die

Leistungsfähigkeit wurde mit Hilfe von Simulationen untersucht, wobei ein GNSS-Signalsimulator verwendet wurde.

Der Simulator – GNSS Multisystem Performance Simulation Environment (GPSIE®) [16] – ermöglicht es, GNSS-Signale mit all ihren Eigenschaften und Fehlereinflüssen möglichst realitätsnahe zu simulieren. Der Simulator wurde von der TeleConsult Austria GmbH entwickelt und im Rahmen von PURSIT um PRS-ähnliche Signale erweitert. Für die Auswertung kam ein softwarebasierter Mehrfrequenz-GNSS-Empfänger, welcher ebenfalls von TeleConsult Austria entwickelt wurde, zum Einsatz [15].

Ein Vergleich zwischen den zivilen Signalen von GPS und Galileo mit dem PRS-ähnlichen Signal im Fall einer Jammer-Attacke soll exemplarisch den Mehrwert und die Leistungsfähigkeit zeigen. Für die Simulation wurde ein kombiniertes GPS- und Galileo-Szenario benutzt. Im Verlauf des Szenarios wurde eine Störattacke von einem „Swept Continuous Wave (SCW)“-Jammer, so dieser in Graz detektiert wurde, simuliert. Abbildung 6 zeigt das Signalspektrum der Simulation. In Blau dargestellt ist das Spektrum der simulierten GNSS-E1/L1-Signale. Das Spektrum des SCW-Störsenders (rot) überlagert die Zentralfrequenz des E1/L1-Bands. Die schwarze Linie symbolisiert das thermische Rauschen.

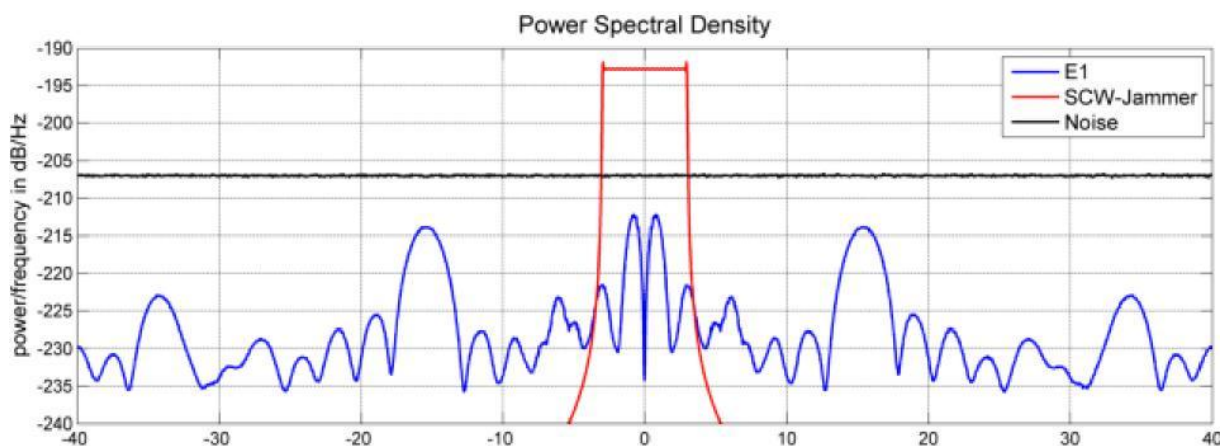


Abbildung 6: Signalspektrum der simulierten E1/L1-GNSS-Signale (blau) und des SCW-Jammers (rot)

Abbildung 7 zeigt einen Vergleich der Positionslösungen unter Verwendung unterschiedlicher GNSS-Signale im Fall einer Störattacke. Wie zuvor beschrieben, wurde ein am Empfänger vorbeifahrender SCW-Jammer im Zeitraum von Epoche 12 bis 27 simuliert. Deutlich ist zu erkennen, dass bei Verwendung des GPS-C/A-Signals (grüne Linie) keine Positionslösung möglich ist. Dies ist darauf zurückzuführen, dass in diesem Fall der Jammer das gesamte Frequenzspektrum des C/A-Signals überdeckt. Im Fall von Galileo OS ist eine deutliche Verschlechterung der Positionslösung (blaue Linie) während der Störattacke sichtbar. Dass dennoch eine Positionslösung möglich ist, ist auf die Galileo-OS-E1B-Signalmodulation zurückzuführen. Das Galileo-E1B-Signal verwendet eine „Composite Binary Offset Carrier (CBOC)“-Modulation, welche im Frequenzspektrum Signalenergie außerhalb des gestörten Bereichs besitzt. Dies bedingt allerdings, dass der Empfänger in der Lage sein muss, das gesamte CBOC-Signalspektrum verarbeiten zu können. Im Fall von kostengünstigen Empfängern ist dies jedoch nicht sichergestellt. Die Positionslösung, die unter Verwendung des PRS-ähnlichen Signals erzielt wurde (rote Linie), bleibt von der Störattacke vollkommen unbeeinflusst.

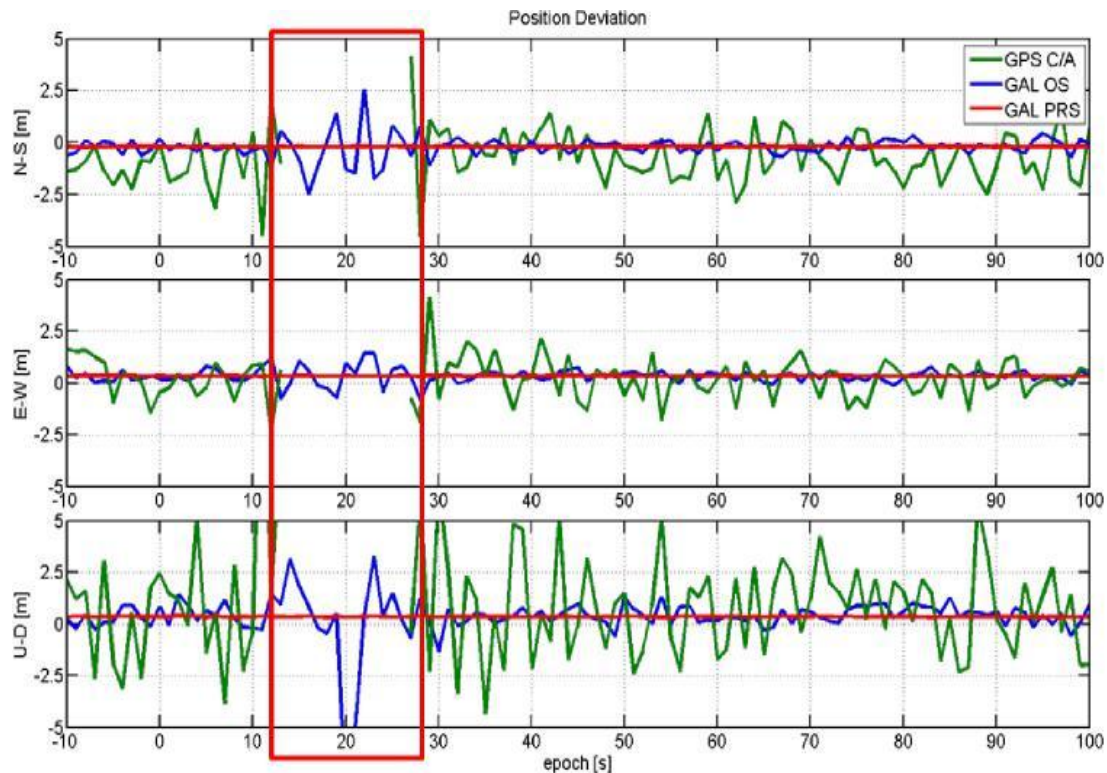


Abbildung 7: Vergleich der Positionslösungen im Fall einer Störattacke

Die Untersuchungen zeigten allerdings auch, dass PRS nicht komplett resistent gegenüber Störungen ist. Aus derzeitiger Sicht ist jedoch der Aufwand, der betrieben werden müsste, um PRS unbrauchbar zu machen, zu hoch. Da aber, wie zuvor beschrieben, PRS nicht allen Anwendern zur Verfügung stehen wird, ist es notwendig, Gegenmaßnahmen zu ergreifen. Derzeitige Gegenmaßnahmen umfassen sowohl Signalverarbeitungsalgorithmen als auch Datenverarbeitungsalgorithmen, die in den GNSS-Empfängern zum Einsatz kommen. Einen wesentlichen Beitrag liefert dabei die verbesserte Galileo-Signalstruktur. Die derzeitigen Entwicklungen sind allerdings nur in der Lage, Störattacken von Jammern zu detektieren. Dass die Bedrohung ernst genommen wird, zeigen die zahlreichen Entwicklungen, Forschungsergebnisse und Publikationen der letzten Jahre.

In diesem Zusammenhang ist die Detektion und Lokalisierung von Jammern und Spoofern derzeit gerade Gegenstand von weiteren Untersuchungen und Entwicklungen bei der TeleConsult Austria. So wird gegenwärtig ein System zur Detektion und Lokalisierung von Jammern und Spoofern im Rahmen des Forschungsprojekts GAIMS-2 entwickelt und getestet.

Positiv betrachtet bieten die derzeitigen Herausforderungen und Probleme bei Galileo auch Potential für Innovation und neue technische Ansätze im Bereich von GNSS. Es werden Beiträge aus unterschiedlichsten Fachbereichen notwendig sein, um innovative Lösungen zu entwickeln. Die dabei gewonnen Erkenntnisse werden dann in Zukunft wieder dem Galileo-Nutzer zu Gute kommen.

### Brücke zu Prof. Erik W. Grafarend

Die Brücke zwischen diesem Beitrag und Erik W. Grafarend ist leicht zu schlagen. Dieser Beitrag wurde aus Anlass seines 75. Geburtstags geschrieben. Der Zweitautor dieses Beitrags blättert in seinen persönlichen Erinnerungen:

Meine erste, persönliche Begegnung mit Erik W. Grafarend liegt lange zurück. Ich war noch Student, und es muss wohl in den Jahren zwischen 1973 und 1975 gewesen sein, also vor rund vierzig Jahren, als Grafarend von Helmut Moritz nach Graz zu einem Vortrag eingeladen worden war. Als Student war ich unter den Zuhörenden, und vom ersten Augenblick faszinierte mich der junge Vortragende, der selbstbewusst und redegewandt das Publikum in seinen Bann zog. Vor allem nach dem Vortrag, als es zu Fragen aus dem Publikum kam, war ich von der Sicherheit beeindruckt, mit der



Grafarend die Fragen beantwortete und demonstrierte, wie sehr er thematisch mit dem komplexen Gebiet vertraut ist.

Später, als ich selbst begann, internationale Tagungen zu besuchen, kam es immer wieder zu Begegnungen. Grafarend war inzwischen in der Geodäsie zu einer allgemein respektierten Persönlichkeit gereift. Und vielleicht ist es eine von Grafarends schönsten Eigenschaften, dass er trotz seines ungeheuren Wissens und seiner Reputation nie den Eindruck von Überheblichkeit erweckte. Er war stets für alle ansprechbar und offen für Fragen und Probleme!

Ein besonderes Ereignis muss ich erzählen, obwohl ich nicht selbst in den Genuss des Erlebens gekommen bin, sondern es nur tradiert bekam: Sommerschule in Erice! Wer eine Reise nach Sizilien plant, sollte einen Besuch der kleinen Bergstadt nahe Trapani unbedingt einplanen. Die malerischen Gassen laden zu einem Spaziergang vor. Und jetzt lassen wir es ganz romantisch werden, wir lassen Gitarrenklänge ertönen. Wir wandern also durch die Gassen und hören die Gitarrenmusik. Als wir näher kommen, sehen wir in einem Fensterrahmen lässig sitzend den Gitarrenspieler, es ist Erik W. Grafarend!

Abbildung 8 zeigt Grafarend als Gitarrespieler, allerdings nicht in Erice, sondern am Stuttgarter Institut anlässlich einer Weihnachtsfeier.



Abbildung 8: Grafarend und die Musik

Die Kunst spielt im Leben von Grafarend zusammen mit der Wissenschaft eine überragende Rolle. In der wunderbaren Schrift der Technischen Hochschule Darmstadt anlässlich der Ehrenpromotion von Grafarend gehört die Musik zu Grafarends „Clausthaler Glücksmomenten“. Hier heißt es: „... die Vorlesungen über Musik von Professor Boetticher/Göttingen, die umfangreiche Arbeit über `Zahlensymbolik bei J.S. Bach´ mit Ulrike Büttner, meiner späteren Frau, die Gründung einer studentischen Musikvereinigung ...“ Kann es etwas Schöneres geben, als über die Kunst, die Musik aus Glücksmomenten mehr zu machen, nämlich mit Ulrike Büttner das ganze weitere Leben gestalten zu können? Wie heißt es bei Franz von Schober so treffend: „Du holde Kunst, ich danke dir dafür!“ Letztlich ist alles im Leben vergänglich, aber manchmal ist es möglich, die Vergangenheit wieder aufzuwecken. Früher, als bei den Veranstaltungen Vorträge mit handgeschriebenen Overheadfolien abgehalten wurden, konnte man viel über didaktischen Konstruktivismus erfahren. Mich haben Grafarends Vorträge immer fasziniert, das Bild seiner Folien, die stets sehr umfangreich gefüllt waren, ist mir noch in bester Erinnerung. Ein Beispiel ist in Abbildung 79 zur Veranschaulichung gegeben. Leider hat mir der

Autor nur eine Schwarz/Weiß-Abbildung zur Verfügung gestellt, aber auch uncoloriert kann sie einen guten Eindruck vermitteln, wie Grafarend schwierige Theorie verständlich zu machen versucht.

white box  
←

Discussion of the eigenspace

CHARACTERISTIC     The characteristic equation of the eigen values  $(\lambda_1, \lambda_2, \lambda_3)$   
 IS determined the characteristic equation

WRITE  
 →  
 BOX

$\lambda^3 - \lambda^2 I + \lambda II - III = 0$

subject to the invariants

$I = \text{tr } J = J_{11} + J_{22} + J_{33} = J_1 + J_2 + J_3$   
 $II = (J_{11}J_{22} - J_{12}^2) + (J_{22}J_{33} - J_{23}^2) - (J_{33}J_{11} - J_{31}^2) = J_1J_2 + J_2J_3 + J_3J_1$   
 $III = \det J = J_{11}J_{22}J_{33} - J_{11}J_{23}^2 - J_{12}J_{23}^2 - J_{33}J_{12}^2 - 2J_{12}J_{23}J_{31} = J_1J_2J_3$

Abbildung 9: „Discussion of the eigenspace“ - Vortragsfolie von E.W. Grafarend

Allein diese Darstellung zeigt, wie der Autor auch langwierigen Herleitungen von Formeln nicht aus dem Weg geht. Als Leser profitiert man ungemein von dieser Ausführlichkeit, insbesondere bei schriftlichen Beiträgen, weil der Weg zum Ziel Schritt für Schritt dargestellt wird.

Die breit gestreute Themenvielfalt in Grafarends ungemein reichhaltiger Publikationsliste grenzt zumindest im Bereich der Geodäsie an Universalität. So ist auch die eingangs dieses Abschnitts erwähnte Brücke von Grafarend zu GNSS über seine Publikationstätigkeit leicht zu schlagen. Ich erwähne nur zwei Arbeiten. Die erste stammt aus dem Jahr 1985 und wurde in *manuscripta geodaetica* publiziert: „The critical configuration of satellite networks, especially of Laser and Doppler type, for planar configurations of terrestrial points“ (Koautor V. Müller). Das Summary zu dieser Arbeit lautet: “Consider a threedimensional range (Laser) or range difference (Doppler) satellite network in its minimal point configuration. E. Tsimis (1973 p. 102) claims that a planar configuration of terrestrial points is not critical, while computer simulations of N. Schatz (1980) have shown a strong critical configuration once the terrestrial points approach a plane. K. Killian and P. Meissl (1980) studied the corresponding twodimensional problem and gave arguments in favor of a singularity. Here the analytical proof for a threedimensional singularity is given.”

Das volle Zitat des Summary habe ich gemacht, um einerseits zu zeigen, wie es Grafarend (in Kooperation mit Müller) mit wenigen Sätzen gelingt, das Wesentliche auszusagen, und andererseits, weil mit Karl Killian und Peter Meissl zwei Wissenschaftler zitiert werden, die mir Glücksmomente in meinem wissenschaftlichen Leben geschenkt haben.

Die zweite Arbeit zitiere ich, weil im Titel das Global Positioning System (GPS) vorkommt, das zusammen mit dem russischen Global Navigation Satellite System (GLONASS) den Ursprung von GNSS bildet: „GPS Solutions: Closed Forms, Critical and Special Configurations of P4P“ veröffentlicht im Jahr 2002 in der Zeitschrift *GPS Solutions* mit Jeffrey Shan als Koautor. Diese beiden Beiträge erklären den Titel dieser Publikation „Galileo und Grafarend unterwegs zu GNSS“ – Galileo als System noch auf dem Weg dorthin, Grafarend als Wissenschaftler schon angekommen.

## Zusammenfassung und Ausblick

Den Vergleich mit anderen globalen Navigationssatellitensystemen braucht Galileo, trotz der bisherigen Verzögerungen und Probleme, nicht zu scheuen. Durch die Betrachtung der aktuellen Bedürfnisse und Anforderungen der Nutzer resultiert nach wie vor ein klarer Vorteil, besonders im Hinblick auf die zivile Nutzung unter ziviler Kontrolle. Galileo als eines der wichtigsten europäischen Weltraumprojekte hat in den vergangenen Jahren neue technische Maßstäbe im Bereich GNSS gesetzt und ist derzeit mehr denn je von strategischer Bedeutung für die Unabhängigkeit (bezüglich anderer Systeme) und die Wirtschaft der Europäischen Union. In den vergangenen Jahren wurde die Praxistauglichkeit von Schlüsseltechnologien erforscht und erfolgreich getestet.

In Zukunft kommen neue Herausforderungen im Bereich der satellitengestützten Positionierung und Navigation auf die Nutzer zu. Globale Satellitennavigationssysteme haben mittlerweile eine wichtige Rolle in unserem Alltag eingenommen. Je wichtiger eine Technologie für unsere Gesellschaft wird, desto mehr steigt auch das Gefahrenpotential hinsichtlich Störangriffen. Speziell in den letzten Jahren wurden Anwendungen von GNSS vermehrt das Ziel von Störangriffen. Galileo bietet hier, im Unterschied zu den anderen derzeit verfügbaren Systemen, auch zivilen Nutzern in Zukunft eine Lösung, da die Signalstrukturen von einigen Galileo-Services resistenter gegenüber Störangriffen und, wenn auch eingeschränkt, für zivile Anwender nutzbar sind.

Die Galileo-Konstellation soll in diesem Jahr noch um weitere vier Satelliten erweitert werden, so dass bis Ende 2016 erste Services den Nutzern zur Verfügung gestellt werden können. Bis zum Jahr 2020 soll dann die volle Konstellation von Galileo erreicht werden.

Dieser Beitrag wurde als eingeladener Vortrag anlässlich des 75. Geburtstags von Erik W. Grafarend präsentiert. Dem Jubilar ist daher auch diese schriftliche Version gewidmet. Die Feier fand als Kolloquium der Leibniz-Sozietät zum Thema „Geodäsie – Mathematik – Physik – Geophysik“ am 13. Februar 2015 in Berlin statt. Zwei Fotos, die der Zweitautor im Rahmen dieser Feier machte, bilden einen würdigen Abschluss und öffnen Wünsche für die Zukunft. Auf dem linken Foto ist Erik W. Grafarend in Diskussion mit Helmut Moritz. Ob Grafarend sich in diesem Augenblick an einen seiner Glücksmomente „Helmut heuert mich als jungen Spund als Lecturer der legendären ‘Summer School in the Mountains’ an“ erinnerte? Das rechte Foto zeigt Grafarend mit zwei Gitarren am Revers. Mögen seine Gitarrenklänge noch oft ertönen!



## Danksagung

Die Projekte GAIMS, GAIMS-2 und PURSIT wurden vom österreichischen Bundesministerium für Verkehr, Innovation und Technologie im Rahmen des Austrian Space Application Programme der österreichischen Forschungsförderungsgesellschaft gefördert. Für die zur Verfügung gestellten Projekter-

gebnisse bedanken sich die Autoren bei den Mitarbeitern der TeleConsult Austria, Herrn Dipl.-Ing. Stefan Hinteregger und Herrn Dipl.-Ing. Sascha Bartl.

## Literaturverzeichnis

- [1] GPS World: The System: Fregat Design Ambiguity Steered Galileo Wrong. [www.gpsworld.com/the-system-fregat-design-ambiguity-steered-galileo-wrong/](http://www.gpsworld.com/the-system-fregat-design-ambiguity-steered-galileo-wrong/) (1. November 2014).
- [2] GPS World: Galileo Satellites Not in Expected Orbit. [www.gpsworld.com/galileo-satellites-not-in-expected-orbit/](http://www.gpsworld.com/galileo-satellites-not-in-expected-orbit/) (25. August 2014).
- [3] ESA Press Release #44-2014: Galileo satellite recovered and transmitting navigation signals. [www.esa.int/For\\_Media/Press\\_Releases/Galileo\\_satellite\\_recovered\\_and\\_transmitting\\_navigation\\_signals](http://www.esa.int/For_Media/Press_Releases/Galileo_satellite_recovered_and_transmitting_navigation_signals) (3. Dezember 2014).
- [4] Inside GNSS: Second Galileo FOC Satellite Reaches Corrected Orbit. [www.insidegnss.com/node/4429](http://www.insidegnss.com/node/4429) (13. März 2015).
- [5] Berglez Philipp: Development of a multi-frequency software-based GNSS receiver. Doktorarbeit, Technische Universität Graz, 2013.
- [6] Inside GNSS: Successful Galileo FOC Launch Brings Relief to Europe's GNSS Program. [www.insidegnss.com/node/4471](http://www.insidegnss.com/node/4471) (28. März 2015).
- [7] ESA: Two new satellites join the Galileo constellation. [www.esa.int/Our\\_Activities/Navigation/The\\_future\\_Galileo/Launching\\_Galileo/Two\\_new\\_satellites\\_join\\_the\\_Galileo\\_constellation](http://www.esa.int/Our_Activities/Navigation/The_future_Galileo/Launching_Galileo/Two_new_satellites_join_the_Galileo_constellation) (28. März 2015).
- [8] Hofmann-Wellenhof Bernhard, Lichtenegger Herbert, Wasle Elmar: GNSS – Global navigation on satellite systems: GPS, GLONASS, Galileo, and more. Springer, Wien New York, 2008.
- [9] [GPS.gov: Applications:Timing.](http://www.gps.gov/applications/timing/) [www.gps.gov/applications/timing/](http://www.gps.gov/applications/timing/) (8. Mai 2015).
- [10] Isoz Oscar, Akos Dennis, Lindgren Tore, Sun Chih-Cheng, Jan, Shau-Shiun: Assessment of GPS L1/Galileo E1 Interference Monitoring System for the Airport Environment. In: Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011), Portland, Oregon, 20. -23. September, 2011: 1920 - 1930.
- [11] Hambling David: GPS Chaos: How a \$30 box can jam your life. New Scientist Magazine, Issue 2803, 6. März 2011.
- [12] PresseBox: TeleConsult Austria detektiert GPS-Störsignal in Graz.
- [13] [www.pressebox.de/pressemitteilung/teleorbit-gmbh/TeleConsult-Austria-detektiert-GPS-Stoersignal-in-Graz/boxid/703455](http://www.pressebox.de/pressemitteilung/teleorbit-gmbh/TeleConsult-Austria-detektiert-GPS-Stoersignal-in-Graz/boxid/703455) (23. September 2014).
- [14] Zaragoza Sandra: UT Austin Researchers Successfully Spoof an \$80 Million at Sea. [www.utexas.edu/news/2013/07/29/ut](http://www.utexas.edu/news/2013/07/29/ut) (8. Mai 2015).
- [15] Sathyamoorthy Dinesh: Global Navigation Satellite System (GNSS) spoofing: A review of growing risks and mitigation steps. Defence S&T Tech. Bull., 6(1), 2013: 42-61.
- [16] Baumann, Stefan, Stadler, Christoph: The Galileo Public Regulated Service (PRS) A Certified GNSS Service for Security-relevant Users in Europe. In: Proceedings of the International Symposium on Certification of GNSS Systems and Services 2014 (CERGAL 2014), Dresden, Deutschland, 7. – 8. Juli, 2015.
- [17] Hinteregger Stefan, Berglez Philipp, Leontyeva Olga: Multi-frequency, multi-constellation IF software simulator including Galileo PRS-like signals. In: Proceedings of the European Navigation Conference 2013 (ENC2013), Wien, Österreich, 23. – 25. April, 2013.

Adressen der Verfasser:

Philipp Berglez, TeleConsult Austria GmbH, Schwarzbauerweg 3, 8043 Graz, Österreich;  
Bernhard Hofmann-Wellenhof, Technische Universität Graz, Institut für Geodäsie, Steyrergasse 30, 8010 Graz, Österreich