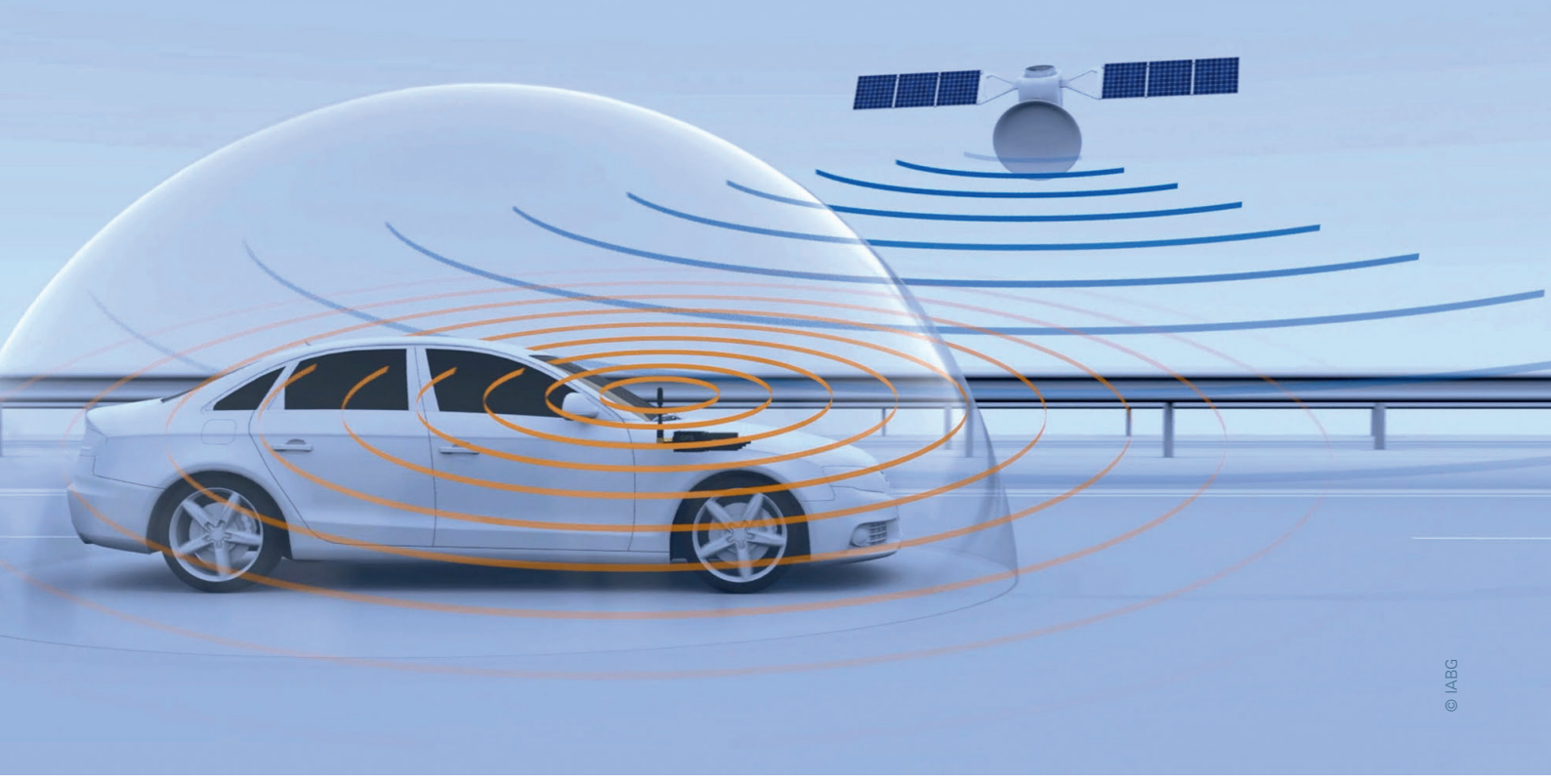

VALIDIERUNG EINER GNSS-BASIERTEN FAHRZEUGLOKALISIERUNG

Der Einfluss von **Jamming** und **Spoofing**

Beim automatisierten Fahren spielt GNSS für die Positionierung und Zeitsynchronisation des gesamten Systems eine wichtige Rolle. Die wachsende Abhängigkeit verschiedener Anwendungen von GNSS geht mit einer zunehmenden Wahrscheinlichkeit von Angriffen auf diese Informationsquelle einher. Bosch und IABG arbeiten gemeinsam an Signalangriffs- und Teststrategien, um Gegenmaßnahmen ergreifen zu können.

Aufgrund der raschen Entwicklung und der zunehmenden Verfügbarkeit mehrerer unabhängiger globaler Satellitennavigationssysteme (GNSS) in den letzten Jahrzehnten basieren immer mehr Anwendungen aus den verschiedenen Industriebereichen auf GNSS. Im Automobilsektor spielt die Satellitennavigation eine zentrale Rolle, weil diese eine globale absolute Positionsbestimmung ermöglicht. Vor allem beim automatisierten Fahren ist GNSS für die Positionierung und Zeitsynchronisation des gesamten Systems essenziell. Die wachsende Abhängigkeit verschiedener Anwendungen von GNSS geht mit gezielten Cyber-Angriffen auf die vom Satelliten frei zugänglich abgestrahlten Navigationssignale einher. Die absichtliche Verhinderung des Signalempfangs, bekannt als Jamming, ist eine ernsthafte Bedrohung, da die mit schwacher Leistung auf der Erdoberfläche eintreffenden Signale sehr leicht gestört werden können. Hinzu kommt, dass die hierfür benötigten GNSS-Störgeräte preiswert und problemlos im Internet erhältlich sind. Bleibt Spoofing, also das absichtliche Aussenden von gefälschten Signalen unerkannt, führt das zu einem Verlust der Integrität der Positionslösung. Dies stellt im Hinblick auf die Sicherheit des automatisierten Fahrens eine sehr ernstzunehmende Gefahr dar. Aus diesem Grund haben sich IABG und Bosch zusammengeschlossen mit dem Ziel, gemeinsam Signalangriffs- und Teststrategien zu entwickeln. Diese sollen es ermöglichen, die Robustheit von GNSS-Systemen in Kraftfahrzeugen gegen GNSS-basierte Cyber-Angriffe zu testen und zu bewerten. Die Testergebnisse bilden die Grundlage für die Weiterentwicklung und Umsetzung von Jamming- und Spoofing-Gegenmaßnahmen GNSS-gestützter Anwendungen im Bereich Automotive.

Zunahme von GNSS-Angriffen

Weil GNSS auf dem Gebiet des autonomen Fahrens an Bedeutung zunehmen wird, werden in Zukunft auch Angriffe

© Carl Hanser Verlag, München

auf die GNSS-Signalebene immer wahrscheinlicher. Daher ist es notwendig, die negativen Auswirkungen dieser Angriffe auf die berechnete Positions-, Navigations- und Zeitlösung (PNZ) zu analysieren und zu bewerten. Es gibt verschiedene Arten von Angriffen. Die einfachste ist Jamming, d. h. es werden Störsignale ausgesendet, um den GNSS-Signalempfang zu blockieren. Ein raffinierterer Angriff ist Spoofing, bei dem der Angreifer die PNZ-Lösung eines GNSS-Empfängers zu verfälschen versucht, ohne dass der Empfänger das bemerkt. Meaconing ist eine dritte Angriffsmethode, die sich als Unterkategorie von Spoofing einordnen lässt. Hier wird das Originalsignal vom Satelliten empfangen und mit geringfügigen Verfälschungen der Signalstruktur erneut ausgestrahlt – mit der Absicht, die PNZ des Opfer-Empfängers zu täuschen. Die Motive, GNSS-Signale zu stören, sind vielfältig. Sie reichen von der Verhinderung der Ortung durch ein auf GNSS-basiertes Flottenmanagementsystem bis hin zur Vortäuschung einer sicheren Fahrweise, um beim sogenannten „Pay-as-you-drive" Kfz-Versicherungsbeiträge zu sparen. Die Stör- und Spoofing-Bedrohungen [1, 2] zeigen, dass GNSS-Angriffe in Zukunft vermehrt auftreten werden, da die Verarbeitungsleistung der Hardware-Plattformen ständig zunimmt und die Technologie preiswerter wird, zum Beispiel durch Verwendung kostengünstiger Software Defined Radios (SDR) [3].

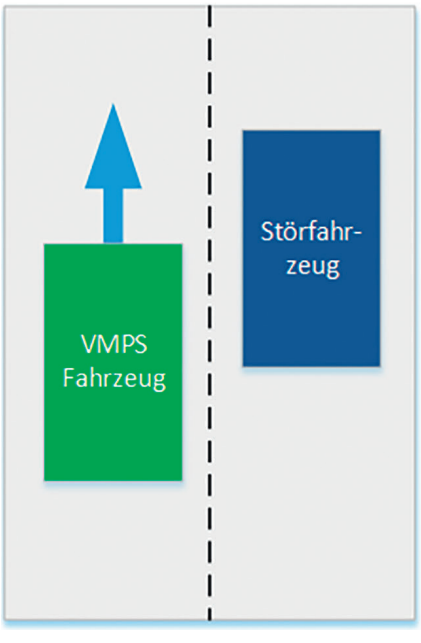

Bild 2: Schematische Darstellung des GNSS-Störszenarios mit VMPS-Testfahrzeug und Fahrzeug mit installiertem Störsender

© Bosch | IABG

Kooperation zwischen Bosch und IABG

Für das hochautomatisierte Fahren hat Bosch ein präzises und sicheres Positionierungssystem namens „Vehicle Motion and Position Sensor" (VMPS) entwickelt [4]. Der VMPS verarbeitet GNSS-Signale aus mehreren Konstellationen und in verschiedenen Frequenzbändern in Kombination mit hochgenauen und sicheren Trägheitssensormessungen. Der Empfänger wurde in Übereinstimmung mit der Sicherheitsnorm ISO 26262 und unter Berücksichtigung der SOTIF-Norm ISO/PAS 21448 entwickelt. Durch die Zusammenarbeit mit der IABG kann auf deren spezifisches Fachwissen über GNSS und Sensorfusion [5] im Hinblick auf Sicherheitsmaßnahmen zurückgegriffen werden. Das Team der IABG verfügt über einschlägige Erfahrungen im Bereich von GNSS-Cyber-Attacken sowie über effektive Methoden, um diese Bedrohungen unter kontrollierten Bedingungen in ihren Versuchseinrichtungen in Ottobrunn und Lichtenau zu testen und zu bewerten [6].

Entwicklung von Angriffsszenarien

Um GNSS-Cyber-Attacken vorzubeugen, werden als erstes Angriffsszenarien entwickelt.

GNSS-Jamming: Störszenario und Störgeräteauswahl

Typische Störsender, die in Kraftfahrzeugen eingesetzt werden können, sind sogenannte Personal Privacy Devices (PPD) [7]. Bild 1 zeigt ein PPD mit einer Antenne und einem Zigarettenanzünderanschluss für die 12-V-Gleichstromversorgung. Das Störsignal ist breitbandig und deckt das komplette obere L-Frequenzband von 1559 bis 1610 MHz ab, in dem u. a. die frei zugänglichen Satellitennavigationssignale für GPS, Galileo und GLONASS liegen.

Für die Analyse und Evaluierung des Verhaltens des VMPS wurde zunächst ein Störszenario entwickelt, bei dem das zu testende Fahrzeug mit dem integrierten VMPS das angreifende Fahrzeug mit dem installierten Störsender überholt. In Bild 2 ist dieses Szenario veranschaulicht. Es wurden mehrere Testfälle mit unterschiedlichen Relativgeschwindigkeiten definiert, um die Auswirkungen der Störung auf die PNZ-Lösung des VMPS für unterschiedlich lange Störzeiten zu analysieren.

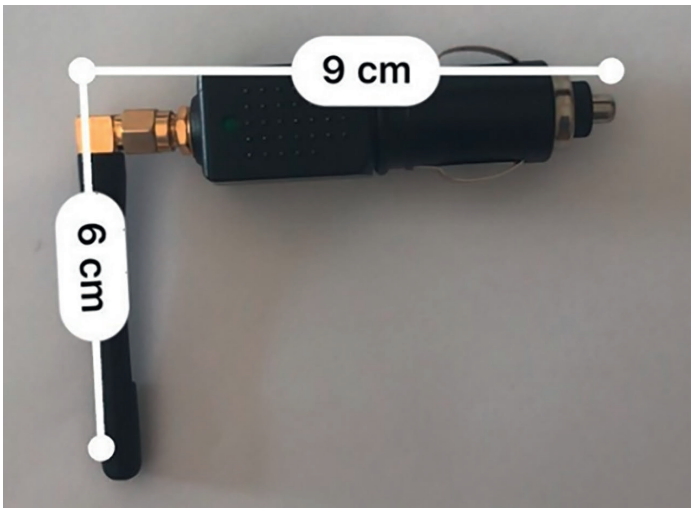

Bild 1: PPD-Störsender mit einer Sendeantenne zum Stören des oberen L-Bandes

© Bosch | IABG

GNSS-Spoofing: Szenario mit Geräteauswahl

Anstelle eines leistungsstarken Laptops mit speziellen Software-Paketen für die GNSS-Signalsimulation unter Verwendung von SDR-Hardware wurde für die Erzeugung des Spoofing-Signals ein handelsüblicher GNSS-Konstellationssimulator gewählt. Die Vorteile eines solchen Simulators im Vergleich zu einer SDR-basierten Lösung liegen in der Flexibilität bei der GNSS-Szenariogenerierung. In Bild 3 ist die Verschaltung des Simulators mit zusätzlichen externen Hardwareeinheiten zu sehen. Um die Synchronisation des gefälschten Signals mit den authentisch abgestrahlten Sa-

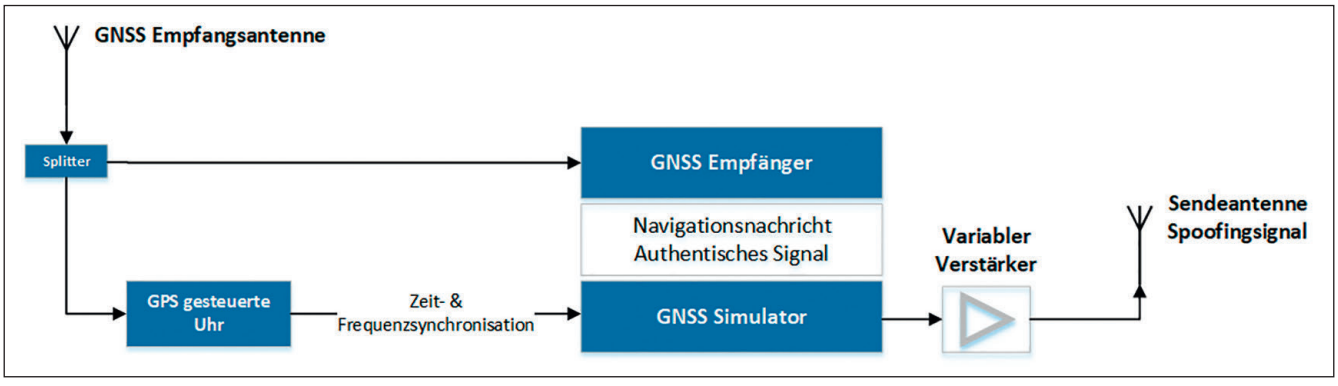

Bild 3: Komponentenübersicht mit Verbindungen zwischen dem GNSS-Signalsimulator, GPS-gesteuerter Uhr, GNSS-Empfänger zur Gewinnung der aktuell ausgestrahlten Navigationsnachricht und Verstärker sowie Empfangs- und Sendeantenne © Bosch | IABG

tellitensignalen sowohl bezüglich der Frequenz als auch der Zeit sicherzustellen, kam eine GPS-gesteuerte Uhr zum Einsatz, die auf Basis der Atomuhrgenauigkeit der Satellitenzeit ein 10 MHz Referenzfrequenz- und ein sogenanntes Pulse-Per-Second-Signal in den GNSS-Simulator einspeiste. Unentbehrlich für die Generierung des Täuschungssignals mit authentischen Navigationsdatenbits war die Verwendung eines gültigen Satzes von Satellitenbahn- und Uhrenkorrekturdaten. Diese wurden von einem separaten GNSS-Empfänger extrahiert und dem Simulator zur Verfügung gestellt. Zur Kompensation von Signalausbreitungsverlusten wurde ein HF-Verstärker mit einer einstellbaren Verstärkung von bis zu 40 dB verwendet.

Es wurde ein Spoofing-Szenario gewählt, wie es auch in alltäglichen Situationen auftreten könnte: Ein Fahrzeug steht im Stau oder wartet an der Ampel auf Grün. Ein Angreifer möchte die Position des Fahrzeugs manipulieren, indem er gefälschte Signale von einem Fahrzeug in unmittelbarer Nähe aussendet. Bild 4 stellt die Situation, bei der sich der VMPS und das angreifende Fahrzeug nebeneinander befinden, dar. Der Täuscher möchte die Position des VMPS-Fahrzeugs gezielt verfälschen und beginnt, GNSS-Signale mit einer gefälschten Trajektorie zu erzeugen, die nicht dem beabsichtigten Fahrweg des VMPS-Fahrzeugs entsprechen. Die Trajektorie des Spoofers wurde so gewählt, dass diese am Standort des anzugreifenden Fahrzeugs beginnt und mit konstanter Geschwindigkeit in einer Seitwärtsrichtung wegzieht.

Als Testgelände zur Durchführung der Angriffsszenarien wurde das Fahrtestzentrum von Bosch in Boxberg [8] gewählt. Weil das beabsichtigte Stören und Täuschen von GNSS-Signalen verboten ist, wurde für die Durchführung dieser Versuchsreihe eine Versuchsfunkgenehmigung bei der Bundesnetzagentur eingeholt.

Versuchsaufbau und Ergebnisse: GNSS-Jamming

Das mit dem VMPS versehene Fahrzeug ist mit einem hochgenauen Referenzpositionierungssystem ausgestattet, in dem neben GNSS-Sensorik eine präzise Trägheitsmesseinheit integriert ist, sodass mittels Vorwärts- und Rückwärtsfilterung im Postprocessing eine hochgenaue Referenzposition bestimmt wird. Das Referenzsystem dient als Bezugsquelle, um die Positionsfehler des VMPS zu bestimmen. Bild 5 zeigt den zeitlichen Verlauf des Positionsfehlers in seitlicher Fahrzeugrichtung und die vom VMPS ermittelte Integrität der Position. Das sogenannte Protection Level (PL) spiegelt die Obergrenze des Positionsfehlers wider und dient als Maß für die Vertrauenswürdigkeit der ermittelten Position. Je höher das PL, desto geringer die Vertrauenswürdigkeit der aktuellen Positionsausgabe. Die vertikale Linie gibt den Zeitpunkt an, an dem sich das VMPS-Fahrzeug auf gleicher Höhe mit dem Störfahrzeug befindet.

Während des Überholvorgangs beträgt der seitliche Positionsfehler weniger als 0,5 m und bleibt somit innerhalb der PL-Grenzen, d. h. der berechneten Position des VMPS kann grundsätzlich vertraut werden. Es ist hervorzuheben, dass sich der Fehler der VMPS-Position in unmittelbarer Reichweite zum Störer nicht verschlechtert, sondern eher geringer wird, u. a. durch Detektion und Ausschluss gestörter Messungen. Ein guter Hinweis darauf, dass die Qualität der GNSS-Messgrößen während der Störung abnimmt, ist der Anstieg des PLs

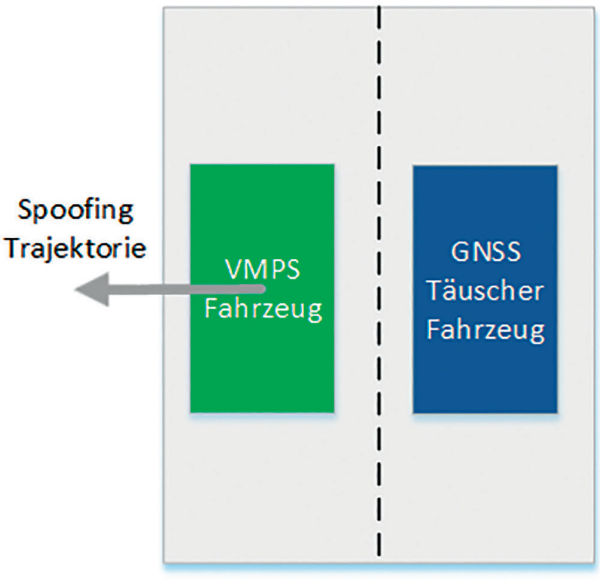

Bild 4: Schematische Darstellung des Spoofing-Szenarios mit VMPS und Angreiferfahrzeug (beide statisch) und einer dynamischen Testumgebung
© Bosch | IABG

© Carl Hanser Verlag, München

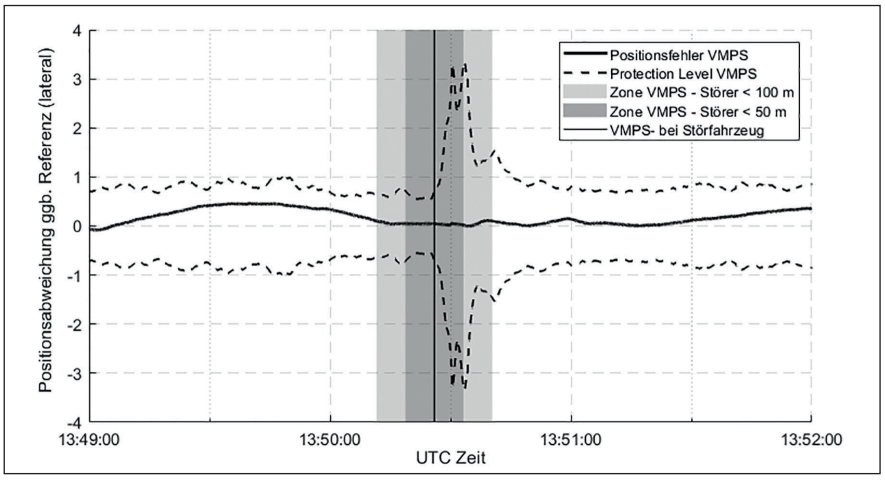

Bild 5: Positionsfehler in lateraler Fahrzeugrichtung (durchgezogene Linie) und den PLs über der Zeit für einen Überholvorgang. © Bosch | IABG

auf einen Wert von ±3,2 m. Der VMPS bewertet die Störung mit einer Abnahme der Vertrauenswürdigkeit der Positionslösung und reagiert damit auf die verschlechterten GNSS-Empfangsverhältnisse. Nach etwa 100 m Entfernung zum Störfahrzeug kehren die PLs auf ihren ursprünglichen Wert zurück, da der GNSS-Empfang vom Störer nicht mehr oder nur noch unwesentlich beeinflusst wird und der VMPS die Situation korrekterweise wieder als ausreichend sicher einstuft.

Versuchsaufbau und Ergebnisse: GNSS-Spoofing

Der Spoofer war mit einer GNSS-Richtantenne ausgestattet, die auf das VMPS-Fahrzeug ausgerichtet wurde. Der seitliche Abstand zwischen Spoofer- und VMPS-Fahrzeug betrug 5 m. In Bild 6 sind die X-, Y- und Z-Koordinaten in einem sogenannten Earth-Centered-Earth-Fixed-Koordinatensystem (ECEF) von getäuschter Trajektorie, VMPS-Position und Positionsinformation, die ausschließlich auf GNSS (GNSS only) beruht, aufgetragen. Die reine GNSS-Positionslösung ist eine VMPS-interne Information, die unabhängig vom Sensorfusionsfilter gerechnet wird. Die Positionen sind relativ zur Referenzposition des VMPS-Fahrzeugs aufgetragen.

Während der ersten 5 s war der Spoofer inaktiv. Danach setzte eine statische Spoofing-Attacke an der Position des VMPS-Fahrzeugs für die Dauer von 2,5 s ein. Nach 7,5 s wurde eine Positionsverschiebung mit einer konstanten Geschwindigkeit von 3,5 m/s eingeleitet. Beim Start des Spoofings traten keine Unterbrechungen der reinen GNSS-Position auf. Das deutet darauf hin, dass die Leistung des Spoofing-Signals nur geringfügig höher war als die der echten Signale, jedoch immer noch stark genug, um eine Wirkung auszuüben. Es ist zu erkennen, dass die reine GNSS-Position des VMPS in Richtung der verfälschten Position wandert, während die VMPS-Position der Sensorfusionslösung unbeeinflusst bleibt. Das VMPS hat den Täuschungsangriff im Prozessierungspfad der Sensorfusion somit erfolgreich detektiert und den Einfluss mitigiert.

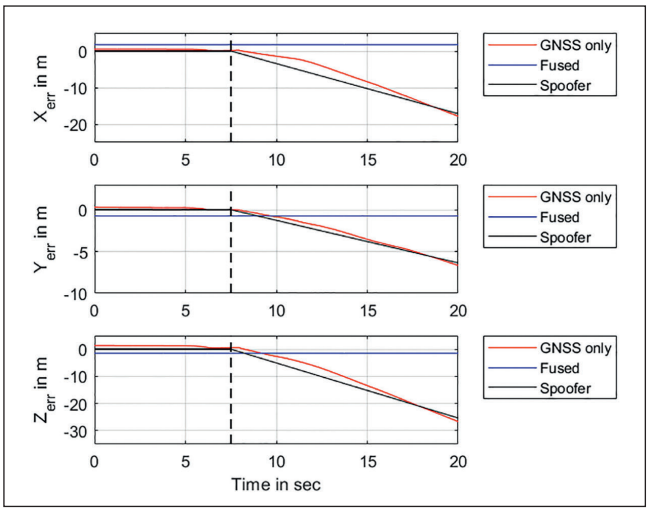

Bild 6: ECEF-Positionsabweichungen in X-, Y- und Z-Richtung von der Antenne des Opferempfängers für die reine GNSS-basierte Position (GNSS only), VMPS-Position (Fused) und Spoofer-Trajektorie in Abhängigkeit von der Zeit
© Bosch | IABG

Ausblick und Schlussfolgerungen

Die Ergebnisse der durchgeführten Jamming- und Spoofing-Tests zeigen deutlich, wie leicht GNSS-Signale gestört und getäuscht werden können. Die Fusionierung mehrerer unabhängiger Sensordaten und geeignete Plausibilitätschecks der Daten sind ein wirksames Mittel, um einen Angriff zu erkennen und den Schutz der Verfügbarkeit, Kontinuität und Integrität des Gesamtsystems zu gewährleisten. Die Tests zeigten, dass der VMPS die Integrität der Positionslösung bei GNSS-Signalverlust und -verfälschung wahrt.

In Zukunft wird die Automobilindustrie in besonderem Maße gefordert sein, Gegenmaßnahmen für GNSS-Angriffe zu entwickeln. Zum einen muss der Fokus auf die Erkennung und Mitigation von Jamming und Spoofing gelegt werden. Zum anderen wird von staatlichen Institutionen erwartet, dass sie wirksame Maßnahmen ergreifen, um potenzielle Jamming- und Spoofing-Angriffe zu unterbinden. Neben dem sofortigen Ausfindigmachen von Angreifern sollte sowohl national als auch international der Schwerpunkt auf Maßnahmen zur wirksamen Bekämpfung von GNSS Jamming- und Spoofing-Attacken gelegt werden. Eine der größten Herausforderungen ist in diesem Zusammenhang die Entwicklung eines Industriestandards für ein Test- und Freigabeverfahren, das eine sichere GNSS-Positionierung im Automobilsektor zum Gegenstand hat. Darüber hinaus müssen zukünftige Entwicklungen der Jamming- und Spoofing-Bedrohungslage ständig überwacht und gemeldet werden. Nur so können rechtzeitig neue Angriffsmethoden in Standardisierungsarbeitsgruppen diskutiert und in einschlägigen Normen berücksichtigt werden. ■ (eck)

www.bosch.de
www.iabg.de

Quellenverzeichnis

[1] C4ADS, „Above us only stars," 09 07 2021. [Online]. Available: https://www.c4reports.org/aboveusonlystars.

[2] STRIKE3 Consortium under EU-H2020 co-funded by European GNSS Agency, „STRIKE3," 09 07 2021. [Online]. Available: http://gnss-strike3.eu/.

[3] T. E. H. e. al., „Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," ION GNSS Conference, 16 – 19 09 2008.

[4] Robert Bosch GmbH, 09 07 2021. [Online]. Available: https://www.bosch-mobility-solutions.com/en/solutions/sensors/vehicle-motion-and-position-sensor/. [Zugriff am 09 07 2021].

[5] iABG mbH Reitenhardt, Matthias, Independent Testbed for Positioning, Navigation, and Timing in GNSS-denied / degraded environments for the development of cost-effective (military or commercial) sensor platforms, DEFTECH Konferenz armasuisse, August 2021.

[6] DLR Raumfahrtmanagement Abteilung Navigation, Galileo Thementag Jamming & Spoofing von GNSS-Signalen, Virtuelle Veranstaltung, 2021.

[7] Oliver Towlson (NSL); David Payne (NSL); Patrik Eliardsson (FOI);Venkatesh Manikundalam (GNSS labs), „STRIKE3 D6.2: THREAT DATABASE ANALYSIS REPORT," Galileo Space Agency, 2019.

[8] Robert Bosch GmbH, „Prüfzentrum Boxberg," [Online]. Available: https://www.bosch-mobility-solutions.com/de/loesungen/entwicklungs-services/pruefzentren/pruefzentrum-boxberg/. [Zugriff am 15 7 2021].

Dr. Marco Limberger ist SOTIF Experte und Function Owner Integrity bei der Robert Bosch GmbH. © Bosch

Michael Baus war Projektdirektor für GNSS-Positionierung und ist seit 2021 Abteilungsleiter in der Forschung und Vorausentwicklung bei Robert Bosch. © Bosch

Ann-Kathrin Eisenhardt ist Teamleiter für den System Test bei der Robert Bosch GmbH. © Bosch

Dr. Boubeker Belabbas ist Fachreferent für Satellitennavigation und Integrity bei der Robert Bosch GmbH. © Bosch

Dr. Stefan Baumann arbeitet als Programm-Manager im Fachbereich der Satellitennavigation bei der IABG. © IABG

Nikolas Dütsch ist Elektrotechnikingeneur und Fachexperte im Bereich von GNSS Jamming- und-Spoofing-Untersuchungen im Satellitennavigationsteam bei der IABG. © IABG

Matthias Reitenhardt ist Experte im Bereich der Satellitennavigation und Sensorfusion und arbeitet im Satellitennavigationsbereich der IABG. © IABG

Real-Time-Driver-Software für AUTOSAR und Nicht-AUTOSAR-Architekturen

Die Real-Time-Driver-Software (RTD) von **NXP** unterstützt alle S32-Automobilprozessoren mit Arm-Cortex-M oder Cortex-R52-Kernen. Als eines von mehreren neuen Angeboten im Rahmen der S32-Software-Enablement-Plattform unterstützt die RTD-Software die neuen S32K3- und die bestehenden S32K1/S32G-Familien mit einem Paket von produktionsreifen, sicherheitskonformen Software-Treibern. Die Software-Treiber sollen die Entwicklung von AUTOSAR- und Nicht-AUTOSAR-Anwendungen vereinfachen. Die Verwendung einer gemeinsamen Code-Basis und Software-API trägt dazu bei, die Wiederverwendbarkeit von Software über Prozessorplattformen hinweg zu maximieren.

Die Software unterstützt alle S32-Automobilprozessoren mit Arm-Cortex-M oder Cortex-R52-Kernen. © NXP

Durch die Weiterentwicklung von Autos hin zu Software-definierten Fahrzeugen ist die Automobil-Software zur zentralen Entwicklungsherausforderung geworden. Das S32K3-MCU-Software-Angebot unterstützt Kunden dabei, diese Aufgabe zu meistern. Gleichzeitig können Anwender von der gemeinsamen Architektur der S32-Automotive-Plattform und der hohen funktionalen Sicherheit bis ASIL D profitieren. Zudem ist eine Hardware-Security-Engine-Firmware und ein Inter-Platform-Communication-Framework beinhaltet. Dabei handelt es sich um eine Middleware zur Verwaltung des Kommunikationsverkehrs und Ressourcen in Multi-Core/OS-Systemen. Ein neues Safety-Software-Framework ist lizensiert erhältlich und beinhaltet Sicherheitsbibliotheken für die Fehlererkennung und Reaktionsprotokolle, die die Grundlage für die Einhaltung der ISO 26262 bilden.

www.nxp.com

© Carl Hanser Verlag, München