When we’re in here, you’re unstoppable out there.

Trimble: The only name you need in high-precision GNSS.

In the world of high-precision OEM GNSS technology, there is only one name you need to know. One name that accepts the challenge for any and all applications. One name that is synonymous with robust precision accuracy and fully streamlined integration in autonomous navigation. One name that stops at nothing to power your solution and fuel your greatest potential. The name is Trimble, and our state-of-the-art GNSS positioning technology puts you dead center of what’s truly possible. Trimble: in. Shackles: off. Power: on.

trimble.com/Precision-GNSS | Connect direct to learn more: sales-intech@trimble.com
Integrated Positioning, Navigation & Timing Test Solutions
Performance I Reliability I Flexibility

PNT TESTING EXCELLENCE

Professional Services
Support Services
Test Scenarios Test Suites
Analysis & Reporting
Database Cloud Library
Automated Testing TestBench
Test Instruments

Go to spirent.com/pnt for links to

spirent.com/pnt
globalsales@spirent.com
SPIRENT
+44 1803 546325

spirentfederal.com/gps
info@spirentfederal.com
SPIRENT FEDERAL SYSTEMS
+1 801 785 1448
**Table of Contents**

**TECHNICAL ARTICLES**

**22** GPS Combined with Galileo to Provide Robust Timing for the Financial Sector

*Precision Timing*
Ricardo Píriz, Pedro Roldán, and Esteban Garbin

A pilot customer of this new time service is currently the Madrid Stock Exchange (Bolsa de Madrid), connected to GMV’s datacenter by a network link of around 50 kilometers.

**48** Perceived Environment Aided GNSS Single Point Positioning

*An Example using a LiDAR Scanner*
Weisong Wen and Li-Ta Hsu

Taking autonomous driving as an example, instead of simply using LiDAR odometry to provide receiver movement between two data epochs, the authors make use of the objects detected by LiDAR and describe them in the representation of relative azimuth and elevation angles to the receiver.

**COLUMNS**

**16** Washington View

*Ligado Presses For Decision on Frequencies Neighboring GPS*
Dee Ann Divis
Low Noise. High Performance.

- **Low Noise**: as low as 0.009°/sec/√Hz ~ 0.038°/√Hz
- **High Performance**: as low as 3°/hr bias stability
- **Low weight and power and small size**
- **Proven Performance** in hundreds of demanding military & commercial programs
- **Wide Product Range** for multiple applications

Inertial Systems and Sensors
Delivering Value Without Compromise

+1.425.396.0829 x1  sales@gladiatortechnologies.com  www.gladiatortechnologies.com
Working Papers

Multi-Tier GNSS Signal Authentication
Oscar Pozzobon, Andrea Dalla Chiara, Luca Canzian, Samuele Fantinato, Carlo Sarto, and Giovanni Gamba

Presenting an innovative design for GNSS authentication implementation at system and receiver level that can satisfy a large number of user requirements.

UAS & the Law

European Union UAS Harmonization Moves Forward
Oliver Heinrich and Jan Helge Mey

QuNav develops and implements sensor-fusion and software receiver solutions for GPS-challenged and GPS-denied environments.

INTRODUCING GIVE 1.0

GNSS/Inertial Vehicular Engine for Automotive Applications

GIVE is a low-cost, completely self-contained solution that maintains accurate navigation capabilities even in THE most difficult environments—urban canyons, tunnels and parking structures.

Order the evaluation kit from qunav.com/products

Download Example Test Results (www.qunav.com/products)
GPS Networking Inc. is the first company to specialize in providing GPS (Global Positioning System) products and solutions to enable you to effectively distribute the GPS/GNSS (Global Navigation Satellite System) signal in your facility. With over 20 years experience, GPS Networking Inc. has been the world leader and your GPS source for providing GPS/GNSS products such as:

- Antenna Splitters
- Amplifiers
- Rack Mount Splitters
- Re-Radiating Kits
- Fiber Optic Antenna Link System

**For more information call 800-463-3063 or email salestech@gpsnetworking.com**

**PLEASE VISIT US OCTOBER 14-16TH**

**AT THE 2019 ASSOCIATION OF THE US ARMY ANNUAL MEETING BOOTH #557**

**AND OCTOBER 22-25TH AT GSMA MWC19 LOS ANGELES BOOTH #S2907**

WWW.GPSNETWORKING.COM
HIGH ACCURACY AND HIGH INTEGRITY ASSURED POSITIONING TERMINAL

Powered by GMV’s PPP service available globally and SBAS DFMC service available in Australia and New Zealand, other regions coming soon.

Built-in integrity functions providing real-time positioning error bounding, based on GMV’s patented technology.

GMV
www.gmv.com magicgnss.gmv.com/userterminal

www.facebook.com/infoGMV
@InfoGMV
https://www.linkedin.com/company/gmv/
Failure to Communicate
A Black Swan has landed...right on top of the Galileo program.

The weeklong outage of Galileo services in mid-July seems like a textbook example of black swan theory: a surprise event that has a major effect and is often rationalized after the fact.

To date, official notifications of Galileo’s outage and its causes have been tardy and ambiguous, but the essential sequence of events is this:

The European GNSS Service Center (GSC) website posted a Notice Advisory to Galileo Users (NAGU) at 14:45 UTC (coordinated universal time) on July 11. The NAGU indicated that users might experience “service degradation” due to an “event” that had begun nearly 13 hours earlier, at 01:00 UTC.

Satellite signals apparently using outdated ephemerides—orbital positions of the spacecraft—or erroneous system time data were producing large errors in receiver calculations based on Galileo. For a prolonged period, however, the Galileo navigation messages identified the signals as healthy.

When Inside GNSS published the first news report on the outage (July 12), a source at the European GNSS Agency (GSA) indicated that Galileo system operators expected to have the problem resolved within 48 hours or no later than the July 13–14 weekend. The GSA is the European Union (EU) agency responsible for Galileo services.

In the event, the GSC did not post a NAGU announcing restoration of service until 08:20 UTC on July 18, although research centers, manufacturers and experienced users detected a gradual improvement in satellite signal quality beginning late on July 16.

In a July 18 announcement, the GSA attributed the signal anomalies to an equipment malfunction in Galileo’s dual Italian and German control centers that calculate time and orbit predictions, and which are used to compute the navigation message. The next day, an amended GSA statement attributed that malfunction to a more vaguely worded “ground infrastructure equipment.”

The Positives of Galileo
Now, before going any further, let me emphasize that the Galileo program has produced many benefits, not only for Europe, but also for users worldwide. These advantages include the training and employing of engineers, and significant advances in related sciences.

The program pioneered the use of passive hydrogen maser atomic clocks on board the Galileo In-Orbit Validation Element (GIOVE) satellites, first launched in 2005.

Galileo has introduced innovative services such as piggybacking search and rescue capabilities onto Galileo satellites and offering an encrypted service available to law enforcement, customs agencies and first responders, as well as to military users.

Politically, Europe introduced full civil control of a GNSS system from the outset, and the Galileo program has been crucial in helping forge closer strategic ties between the EU, the program manager and the European Space Agency, the technical lead.

And Yet...
Program managers have defended as useful redundancy what many consider an expensive system overbuilt to accommodate the political expectations of the large number of Galileo member-states. But that redundancy has apparently not eliminated all failure modes in the Galileo system.

In any case, the “technical incident,” as Galileo leaders characterize the outage, is not unprecedented. Any complex physical infrastructure will experience blips in performance. Russia’s GLONASS suffered a systemwide failure in April 2014 that took most of a day to resolve.

Even the Global Positioning System, the self-described “gold standard” of GNSS services, has experienced satellite signal anomalies, such as the SVN49 signal anomaly in 2008 as well as clock rollovers that throw some receivers off the track. However, part of what makes GPS “golden” is the high trust level invested in the system by users—due in no small part to the transparency and alacrity with which the U.S. Air Force and Coast Guard Navigation Center respond to such incidents.

The immediate practical consequences of the lengthy Galileo malfunction appear to have been small, because of the existence of other GNSS systems and their integration into multi-GNSS receivers that crosscheck the validity of the various signals.

In the longer term, however, the Galileo program faces trust issues for its failure to communicate the situation, its cause and its consequences in a prompt, clear and thorough manner.

Perhaps the larger lesson here is that it’s not a GPS world, or a Galileo world, or a GLONASS or BeiDou world—it’s a GNSS world. And we’re all the better for it.

GLEN GIBBONS
EDITOR EMERITUS
Positioning Performance Evaluation
Support development of high performance solutions

GNSS Sensor Characterization
Perform test & simulation to assess GNSS sensor performances (Tracking, PVT, Vulnerabilities)

System Integration
Perform hardware-in-the-loop system testing

contact@m3systems.eu • +33 (0) 5 62 23 10 89
TOULOUSE—FRANCE
Visit our website www.m3systems.eu
PNT Advisory Board Has New Chairman, Members and Renewed Charter

The leading U.S. panel of satellite navigation experts, the National Space-Based Positioning, Navigation, and Timing Advisory Board (“PNT Advisory Board”) opened its June meeting with a renewed charter, a new chairman and seven new members.

CYGNSS, which is NASA’s first Earth science small-satellite constellation, will help improve hurricane intensity, tracking, and storm surge forecasts, the agency said.

Established in 2004 the board provides “independent advice to the U.S. government on GPS-related policy, planning, program management, and funding profiles in relation to the current state of national and international satellite navigation services.” It undertakes research and submits recommendations and reports to the National Executive Committee for Space-Based PNT (ExCom)—a joint civil/military policy body comprising eight federal agencies and the Joint Chiefs of Staff. The board tackles tasks at the request of the ExCom and addresses issues it identifies itself as needing attention.

The board has a new charter that was just signed in May. That charter only extends to September, however, because the board is expected to be chartered again with a designation as one of the President Donald Trump’s key advisory groups. Special designation within the executive branch gets the board additional attention and focus, explained a source familiar with the process.

“I guess that means we get a promotion,” quipped Admiral (Ret.) Thad W. Allen, the board’s new chairman.

Allen served as commandant of the U.S. Coast Guard from 2006-2010 leading the service through a major modernization program and an effort to explore the changing Arctic as well as a number of significant national and international incidents, including hurricanes, floods, search-and-rescue cases, oil spills and other environmental incidents. He is now an executive vice president of Booz Allen Hamilton.

The immediate past board chairman John Stenbit, who previously served as assistant secretary of defense, will stay on the board as deputy chairman.

The new members bring the board up to its full compliment of 25. Allen noted that this might be the largest contingent of new members the board has ever had. The new members are:

- Patrick Diamond, Diamond Consulting
- Frank van Diggelen, Google
- Dorota Grejner-Brzezinska, Ohio State University
- Terry Moore, University of Nottingham (UK)
- Jeffrey Shane, International Air Transportation Association (IATA)
- Gary Thompson, North Carolina Emergency Management/Geodetic Survey
- Todd Walter, Stanford University

The other board members are:

- Bradford Parkinson (1st Vice Chair), Stanford University
- James E. Geringer (2nd Vice Chair), Environmental Systems Research Institute (ESRI)
- Penina Axelrad, University of Colorado
- John Betz, MITRE
- Gerhard Beutler, International Association of Geodesy (Germany)
- John Stenbit, who previously served as assistant secretary of defense, will stay on the board as deputy chairman.
- Joseph D. Burns, Airo
- Scott Burgett, Garmin
- Jeffrey Shane, International Air Transportation Association (IATA)
- Ronald R. Hatch, private consultant (retired John Deere)
- Matt Higgins, International GNSS Society (Australia)
- Larry James, Jet Propulsion Laboratory
- Timothy A. Murphy, The Boeing Company
- T. Russell Shields, Ygomi
- Refaat M. Rashad, Arab Institute of Navigation (Egypt)

The National Space-Based Positioning, Navigation, and Timing Advisory Board recently named a new chairman and added seven new members.

Washington, D.C.

See Additional News Stories at www.insidegnss.com/news

- UltraWideband Proposal Could Impact GPS Users
- GPS Interface Control Working Group To Meet in September
- Second Lockheed Martin-Built GPS III Satellite Ready for July 25 Liftoff
- Maritime Groups Call for International Resolution Against Jamming & Spoofing

…and more.
In every business, there are watershed moments when a technology is introduced that elevates the performance of an entire industry. The new Phantom™ and Vega™ OEM boards driven by all-new Lyra™ II digital ASIC and Aquila™ wideband RF ASIC next-generation technology will literally rewrite the standards for precision and best-in-class performance.

- Low-power, high-precision position and heading OEM boards
- Multi-GNSS receiver that processes more than 1,100 channels
- Platform tracks all BeiDou Phase III signals, new GLONASS signals, Galileo E6, and QZSS LEX
- Provides access to Hemisphere’s Atlas® GNSS Global Corrections network

Give your products a performance advantage and specify the all-new Phantom and Vega OEM boards. Together we can achieve brand dominance for your products.

Go to www.hgnss.com/PhantomVega to learn more.
Launched on a Long March-3B carrier rocket, China sent a new satellite of the BeiDou Navigation Satellite System (BDS) into space from the Xichang Satellite Launch Center in Sichuan Province at 2:09 a.m. Tuesday, June 25, according to the Chinese news agency Xinhua.

The satellite was sent to the inclined geosynchronous earth orbit and is the 46th satellite of the BDS satellite family and the 21st satellite of the BDS-3 system. The design of the BDS constellation is unique, including medium earth orbit (MEO), geostationary earth orbit (GEO) and inclined geosynchronous earth orbit (IGEO) satellites.

Currently there are 18 MEO BDS-3 satellites, one GEO BDS-3 satellite, and two IGEO BDS-3 satellites sent into space.

After in-orbit tests, the new satellite will work with those BDS satellites already in orbit to improve the coverage and positioning accuracy of the system, Xinhua stated. The new satellite and the carrier rocket were developed by the China Academy of Space Technology and the China Academy of Launch Vehicle Technology under the China Aerospace Science and Technology Corporation.

Beijing, China

**BeiDou Constellation Expands**

**GNSS Hotspots**

---

**Penguin-Spoting Drones**

**Antarctic Peninsula, the northernmost part of the mainland of Antarctica**

Using imagery from satellites, drones and ground surveys, a team of researchers has discovered about 1.5 million penguins living in the Danger Islands, an archipelago of nine remote islands at the northwestern tip of the Antarctic Peninsula. According to a study last year, the Adélie penguin colonies on the east side of the Antarctic Peninsula are holding strong, after researchers spotted never-before-seen communities thanks to direct ground counts and computer-automated counts of unmanned aerial vehicle (UAV) imagery.

**Smart Mailboxes**

**Naperville, Illinois, USA**

According to Valqari, a Chicago area-based start-up, it has created the only drone delivery solution that has solved the last inch logistic problems with its patented Smart Drone Delivery Mailbox, or RCVR-PAD (Remote Communicating Vault Receiver—Personal Automated Delivery). With utility patents in 13 countries, the company is ahead of major players when it comes to the end process of a drone delivery. The RCVR-PAD is Valqari’s patented landing pad featuring communication technology that will allow for an entirely automated drone delivery that will allow drones to land and release packages into the secured and lockable device to help prevent theft or damage to the items delivered.

**WasteShark**

**Rotterdam, Netherlands**

Created in 2016 by RanMarine, the water drone WasteShark is being used to collect garbage present at sea. The machine has been in testing for a year, through a partnership with EcoCoast. It is controlled remotely and has the ability to collect waste in the water by the “shark mouth” species in front of you. The Dutch manufacturer claims that it supports up to 159.6 kilograms of waste and has a battery life of up to 16 hours running. It features laser imaging technology to avoid collisions.

**NASA, GPS and Artemis**

**Washington D.C., USA**

GPS could be used to pilot in and around lunar orbit during future Artemis missions. A team at NASA is developing a special receiver that would be able to pick up location signals provided by the 24 to 32 operational Global Positioning System satellites. GPS is operated by the U.S. military about 12,550 miles above Earth’s surface, and is open to anyone with a GPS receiver. These same GPS signals provide location data used in vehicle navigation systems, interactive maps, and tracking devices of all types, among many other applications. Such a capability could soon also provide navigational solutions to astronauts and ground controllers operating the Orion spacecraft, the Gateway in orbit around the Moon, and lunar surface missions.

---

**Find out more at GNSS Hotspots online!**
VectorNav sets the standard for high-performance inertial navigation solutions. The VectorNav range of IMU/AHRS, GPS/INS and GPS-Compass solutions provide industry leading performance and best-in-class size, weight and power.

**INDUSTRIAL SERIES**
- 0.3° heading
- 0.1° pitch & roll
- 5°/hr in-run gyro bias
- < 30 grams
- Made in USA and ITAR-free

**TACTICAL SERIES**
- < 0.1° heading
- < 0.03° pitch & roll
- < 1°/hr in-run gyro bias
- IP 68 rated enclosure
- Made in USA and ITAR-free
Ligado Networks is pushing spectrum regulators to make a decision on its request to allow satellite frequencies near the GPS band to also be used for terrestrial 5G networks.

To support their appeal for a waiver to the license—and perhaps boost the likelihood of a sooner-than-later response—the company is casting its plan as part of an on-going 5G controversy that needs to be resolved before a crucial fall negotiation. Moreover, Ligado is insisting that a decision is long overdue under legal requirements set out in Section 7 of the Communications Act.

What does all this add up to? That’s hard to say, at least in the near term. That urgent spectrum controversy is not about the mid-band frequencies Ligado is licensed to use. In fact it’s not about mid-band frequencies at all. As for Section 7, even though it has been in place since 1983, it’s so far been applied in an ad hoc manner—until now that is. Regulators are in the middle of crafting rules to implement the section and it is at least possible that the process may delay a response to Ligado’s request.

Background

Ligado is the successor company to LightSquared, which sought a license modification in 2010 to allow frequencies designated for satellite communications to be used for a high-powered, nationwide terrestrial network to serve the surging broadband market. Tests later showed that the network’s signals would overload the vast majority of GPS receivers. (A $2 billion lawsuit filed in December 2017 alleges that the interference problem was known before LightSquared made its request but was fraudulently concealed from LightSquared’s backers (see box, page 20).

After tests were completed in 2011 the results went to the National Telecommunications and Information Administration (NTIA), a Department of Commerce agency that coordinates government use of spectrum. In February 2012 the NTIA sent a letter to the Federal Communications Commission saying the GPS interference that would be caused by LightSquared’s network could not be mitigated and the FCC immediately put a hold on LightSquared’s request; the firm filed for bankruptcy shortly thereafter. LightSquared soon sued the federal government and a number of GPS firms and interest groups. The firm emerged from bankruptcy in 2015, dismissed or settled its lawsuits and adopted a new name and a new plan created to help address the GPS interference issues. More recently it’s been proposing that its L-band spectrum would be a highly useful component of the new wireless networks being built to the emerging and very promising 5G standards, which will ultimately enable wireless networks to handle far greater amounts of data at

Ligado Networks’ Spectrum

Ligado’s L-band spectrum is at 1526-1536 MHz, 1545-1555 MHz (this 10 MHz band is now set aside as part of a guard band to protect GPS), 1627.5-1637.5 MHz, and 1646.5-1656.5 MHz.

Should Ligado prevail regarding an upcoming spectrum auction, it would also be able to use 1670-1680 MHz. The firm leases 1670-1675 MHz. The auction would be for 1675-1680 MHz.
ALL WARFARE IS BASED ON DECEPTION.

SUN TZU

We are experienced Navigation Warfare professionals, protecting military forces around the world on land, at sea and in the air. Contact us for proven, mission ready technology assuring Position, Navigation and Timing (PNT) that can be defending your people right now.

Autonomy & Positioning – Assured | www.novatel.com/deception

NAVWAR SUPERIORITY
faster speeds.

**Politics**

Ligado has been stressing that a decision on its request needs to be made quickly if it is to add its spectrum to the national push to deploy 5G. In recent statements, including a June 26 FCC filing, the firm has insisted that the delay in approval of its request is anchored in Washington maneuvering and not the GPS interference issues that hamstrung the plans of its predecessor.

“For the past three-and-a-half years, Ligado Networks has worked with industry and government stakeholders on a plan that will finally unlock our lower mid-band spectrum for 5G. We have participated in testing, analysis, studies, workshops, reviews, and meetings, and time after time, we have accepted the burden to resolve concerns by modifying our plan. We have patiently waited for an FCC decision allowing our company to make additional investments that industries here in America so desperately need,” said Ligado Networks CEO Doug Smith in a June 25 statement. “But we can only wait so long—especially when we are no longer debating substance—technology led by the smartphone industry resolved that nearly a decade ago—but waiting because of politics. Industries in need of spectrum simply cannot wait any longer. Ligado cannot wait, and the U.S. will not win the 5G race by waiting.”

To help make the case that it’s being delayed by a political problem and not a technical one Ligado pointed to testimony by FCC Chairman Ajit Pai who told the Senate Commerce, Science and Transportation Committee on June 12 that the Department of Commerce “has been blocking our efforts at every single turn” to get more spectrum for 5G. The agency’s opposition, Pai said, could hamper the United States in negotiations expected at the World Radiocommunication Conference (WRC) to be held October 28 through November 22 in Sharm El-Sheikh, Egypt. Convened every four years, these vitally important WRC meetings are where nations hammer out what spectrum will be used for what purpose. The fortunes of companies, even entire industries, can turn on the decisions made there.

However, if one digs through the statements, testimony and filings it becomes clear that, while there has been an ongoing argument between the FCC and the Department of Commerce, and there is indeed concern it will impact U.S. efforts at the WRC, the matter at hand does not involve Ligado’s frequencies. The spat being discussed in the hearing had to do with spectrum in the 24 GHz band and whether broadband systems will interfere with atmospheric sensors used for weather and climate forecasting. Some of those sensors are in the neighboring 23.8 GHz band and the National Oceanic and Atmospheric Administration, which is part of Commerce, believes the impact could be severe.

Moreover, though quickly getting more spectrum for 5G is at the heart of the FCC’s 5G FAST Plan (for Facilitate America’s Superiority in 5G Technology) Ligado’s frequencies are not part of that either. The Commission held a 5G spectrum auction earlier this year for frequencies in the 28 GHz band. There are also plans to auction frequencies in other “high band” portions of the spectrum including frequencies in the 37 GHz, 39 GHz, and 47 GHz bands. Though the FCC has 5G-related plans for freeing up mid-band spectrum (the bandwidth neighborhood where GPS and Ligado spectrum reside) and low-band frequencies those efforts are focused on the 2.5 GHz, 3.5 GHz, and 3.7-4.2 GHz bands as well as the 600 MHz, 800 MHz, and 900 MHz bands. The FCC is also looking at the 3.1-3.55 GHz band at the direction of Congress.

Ligado’s spectrum and potential spectrum allocation runs from 1564 to 1680 MHz (see box). That does not mean that the matter can not come up, only that the FCC is focused elsewhere and, in fact, has its plate more than full with other 5G matters.

Ligado is trying to put “5G pixie dust on GPS interference and make it go away,” Recon Analytics analyst Roger Entner told Communications Daily in June. “I don’t think the FCC is going to be swayed by that argument at all.”

12 miles or 1 milliwatt

In fact, the GPS interference issue has not gone away, said Brad Parkinson, the vice chair of the National Space-Based Positioning, Navigation, and Timing (PNT) Advisory Board.

“Many other organizations have filed opposition to this (Ligado’s proposal) and we in the past have gone on record in writing as unanimously recommending disapproval,” Parkinson told the board at their own June 6 meeting. “Nothing has changed.”

The PNT Advisory Board comprises the nation’s leading experts on satellite navigation. They provide independent advice on GPS-related policy, planning, program management, and funding profiles to the National Executive Committee for Space-based PNT (the ExCom). The ExCom is a
A new kind of satellite has started showing up

Sensonor first started supplying its small IMUs to space applications in 2012. With our STIM210 we can offer 5 to 10 times lower weight than the next-best alternative with similar performance. As a result over 30 companies worldwide utilize our inertial products in space today.

*When size and performance matter*
$2 Billion Lawsuit Over Ligado Frequencies Discontinued

A judge has discontinued a $2 billion lawsuit alleging “massive fraud” in a deal that laid the foundation for LightSquared and its successor firm Ligado Networks.

Harbinger Capital Partners, LightSquared’s key backer, is alleging that Apollo Global Management LLC, knew or should have known that a terrestrial network built on the frequencies at the heart of the deal would interfere with GPS receivers. Those frequencies were held by SkyTerra, which Apollo Capital sold to Harbinger. Harbinger said Apollo and affiliated parties learned in 2001 after private tests were done, that voice and data signals on those frequencies would overload GPS receivers. They also knew about additional tests done by DIRECTV in 2007 that confirmed the findings. Harbinger alleges that those results were concealed, however, when Apollo sold it on a plan to buy SkyTerra and use its frequencies to support a ground network as well as satellite communications.

“We believe the suit lacks merit and we intend to defend ourselves vigorously,” said a spokesperson for Apollo Global Management in a written statement shortly after the suit was filed in December 2017.

Though Ligado was not part of the suit the issues raised before the court could make it very hard for the Federal Communications Commission to grant Ligado a modification to its license for those frequencies, ” said Tim Farrar, a technology consultant specializing in the satellite industry who has followed Ligado closely.

Nothing has come of the suit, however—at least not yet. After a series of mutually agreed to but repeated stays, the court discontinued the matter without prejudice on June 25.

Section 7

The newest and most interesting development in the Ligado controversy is the company’s June 25 request for a decision under Section 7 of the Communications Act.

Added to the Act in 1983, Section 7 has two mandates:

1) It directs that the Commission determine whether a proposed new technology or service is in the public interest within a year after a petition or application is filed.

2) It puts the burden to demonstrate that such a proposal is not in the public interest on any person or party opposing a new technology or service.
“Waiting indefinitely for any further input from another government agency would effectively grant that agency a veto—contrary to the authority vested in the Commission by the Communications Act—and would flout the direction of Congress under Section 7 that the Commission decide these kinds of applications expeditiously.”

Ligado Networks

The Upshot
So where does that leave the Ligado proposal? Ligado is pushing for a decision under Section 7 and insists that the record is complete. The firm also insists that it has addressed issues of GPS interference (despite the points noted above) and concerns raised by Iridium and INMARSAT, two other satellites firms. Ligado also refers to the NTIA in its Section 7 application, an agency of the previously mentioned Department of Commerce, asserting that it has had its input.

“Ligado also understands that during this time the Commission has held numerous discussions with NTIA staff concerning the license modification applications and how Ligado’s spectrum plan can co-exist with users in adjacent bands,” the firm wrote in its section 7 request.

But there’s more to the NTIA element than that. As noted in the background, during the LightSquared controversy the NTIA sent a letter to the FCC laying out the government’s GPS interference test results. That letter fed into the decision to deny the LightSquared request. Under government procedure the NTIA is supposed to send another letter to the FCC, as it did before, articulating the executive branch’s position. Inside GNSS has found no hint that that has happened. Given the public opposition of the PNT Advisory Board, the opposition of a number of the ExCom agencies and the data from DOT’s ABC tests, it would seem likely that a new NTIA letter would oppose approval of Ligado’s plan.

One can’t help but wonder if NTIA is the government agency Ligado may actually be taking aim at when it refers to politics—hoping its Section 7 request will speed an FCC decision, even if it’s without a recommendation from the NTIA.

“After more than 1,200 days,” Ligado wrote, “any government agency interested in this proceeding and in 5G deployment considerations has had more than enough time and opportunity to bring forth its formal views. Waiting indefinitely for any further input from another government agency would effectively grant that agency a veto—contrary to the authority vested in the Commission by the Communications Act—and would flout the direction of Congress under Section 7 that the Commission decide these kinds of applications expeditiously.”

Though that seems straightforward it is not entirely clear how the firm’s request will be handled.

The Commission has considered a handful of cases under Section 7 on an ad hoc basis, the FCC wrote in a February 2018 Notice of Proposed Rulemaking. That NPRM, however, is specifically underway to set the rules for how Section 7 will be implemented. In other words the process for handling Section 7 requests is in the middle of being changed.

Among the matters that the FCC is considering is how to decide if a technology is actually new, including how to handle things like incremental improvements. Regulators are also proposing that, given the tight 1-year deadline, applications under Section 7 include a separate section demonstrating that a new technology or service is both technically feasible and available for commercial use.

The GPS Innovation Alliance (GPSIA) said in its comments on the proposed rule that an applicant should have to demonstrate that “its innovation can successfully transition from a laboratory environment to a production environment as well as a ‘real world’ environment” and that its equipment can be produced using commercially available components and representative manufacturing techniques. This can be a real issue. During the early days of the LightSquared debate there was a problem getting the new network equipment to test to see if it caused interference to GPS receivers.

The new offerings also need to be consistent with the Commission’s spectrum management responsibilities, the GPSIA wrote.

“In the case of any proposed new service or technology that will use spectrum in or adjacent to bands that support navigation services, the public interest review must take into consideration fundamental distinctions among different services—particularly navigation and communications services and their different levels of susceptibility to potential interference,” the GPSIA said. “The Commission should therefore recognize, as part of this review and its application of core spectrum management principles, the impact that a 1 dB decrease in the carrier-to-noise density ratio ("C/N0") has on navigation services and the actions that any proponents of new transmission technologies can, and as a matter of public policy should, take to protect against these decreases.”

The new offerings also need to be consistent with the Commission’s spectrum management responsibilities, the GPSIA wrote.

“In the case of any proposed new service or technology that will use spectrum in or adjacent to bands that support navigation services, the public interest review must take into consideration fundamental distinctions among different services—particularly navigation and communications services and their different levels of susceptibility to potential interference,” the GPSIA said. “The Commission should therefore recognize, as part of this review and its application of core spectrum management principles, the impact that a 1 dB decrease in the carrier-to-noise density ratio ("C/N0") has on navigation services and the actions that any proponents of new transmission technologies can, and as a matter of public policy should, take to protect against these decreases.”
A n increasing number of applications require accurate, reliable, and traceable signals for time and synchronization. Key fields of application include banking and finance, telecom networks and electricity grids, rely heavily on accurate, reliable, and traceable signals for time and synchronization. Here, the authors address a new time service for the city of Madrid, Spain, distributed using the White-Rabbit network protocol over optical fiber, with the Madrid Stock Exchange serving as a pilot customer of the service.

GPS Combined With Galileo to Provide Robust Timing for the Financial Sector

Today, more and more integral fields of application including banking and finance, telecom networks and electricity grids, rely heavily on accurate, reliable, and traceable signals for time and synchronization. Here, the authors address a new time service for the city of Madrid, Spain, distributed using the White-Rabbit network protocol over optical fiber, with the Madrid Stock Exchange serving as a pilot customer of the service.

Clock Synchronization

CV provides the difference between the local clock and the remote UTC time scale. Currently the authors of this article are collaborating with PTB, the Physikalisch-Technische Bundesanstalt in Braunschweig, Germany, to align their clocks to PTB’s realization of UTC, called UTC(PTB). By calculating clock differences over several days it is possible to model and predict the behavior of the clock, and thus to adjust the clock frequency periodically to minimize its deviation from UTC. In our case we adjust our PHMs to UTC using a quadratic model that accounts for the clock phase offset (A0 term, ns), the mean clock frequency offset (A1 term, ns/day), and the frequency drift (A2 term, ns/day). Every day, we fit the PHM model to the CV results from the 15 previous days, we extrapolate the model to the current day at noon, and we calculate a corresponding frequency correction, that is applied to the PHM by means of a frequency stepper connected at its output. Each PHM is steered independently of the other one.
The most powerful LabSat yet, the new LabSat 3 WIDEBAND captures and replays more GNSS signals at a much higher resolution than before.

Small, battery powered and with a removable solid state disk, LabSat 3 WIDEBAND allows you to quickly gather detailed, real world satellite data and replay these signals on your bench.

With three channels, a bandwidth of up to 56MHz and 6 bit sampling, LabSat 3 WIDEBAND can handle almost any combination of constellation and signal that exists today, with plenty of spare capacity for future planned signals.

LabSat 3 WIDEBAND can record and replay the following signals:

- GPS: L1 / L2 / L5
- GLONASS: L1 / L2 / L3
- BeiDou: B1 / B2 / B3
- QZSS: L1 / L2 / L5
- Galileo: E1 / E1a / E5a / E5b / E6
- SBAS: WAAS, EGNOS, GAGAN, MSAS, SDCM
- IRNSS

www.labsat.co.uk
In nominal operations, our CV software uses the well-known iono-free combination of GPS P1 and P2 pseudoranges. In the unlikely event of a problem with this combination, for example due to jamming or interference in the GPS L1 or L2 bands, or even due to a total failure of GPS, we need to have alternative CV methods that ensure the continuity of operations. This is achieved by incorporating Galileo, and also by using SF CV in all the individual GNSS bands. An example of the results is shown in Figure 1 which depicts the PHM-A clock model versus UTC(PTB) for April 25, 2019, i.e., MJD 58598 (Modified Julian Day). The accompanying table (Figure 2) helps to understand the GNSS frequencies and pseudoranges involved.

### Figure 1
This example depicts the PHM-A clock model versus UTC(PTB) for April 25, 2019.

### Figure 2
<table>
<thead>
<tr>
<th>Carrier center frequency (MHz)</th>
<th>GPS frequency band name</th>
<th>GPS pseudorange name</th>
<th>Galileo frequency band name</th>
<th>Galileo pseudorange name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1575.420</td>
<td>L1</td>
<td>P1</td>
<td>E1</td>
<td>C1</td>
</tr>
<tr>
<td>1278.750</td>
<td>L2</td>
<td>P2</td>
<td>E6</td>
<td>C6</td>
</tr>
<tr>
<td>1227.600</td>
<td>L3</td>
<td>P3</td>
<td>E7</td>
<td>C7</td>
</tr>
<tr>
<td>1207.140</td>
<td>L4</td>
<td>P4</td>
<td>E8</td>
<td>C8</td>
</tr>
<tr>
<td>1176.450</td>
<td>L5</td>
<td>P5</td>
<td>E9</td>
<td>C9</td>
</tr>
</tbody>
</table>

In a visual way, the steering is the slope of the tangent to the model curves (Figure 1), evaluated at the extrapolated epoch. The steering is conceived to adjust to zero the instantaneous frequency offset at that epoch. An additional steering correction term is used to adjust the clock phase offset versus UTC to zero in the following 10 days, but this aspect will not be discussed here. “Error” in the A0 term and in the steering is calculated as the difference versus the nominal DF GPS solution (GPS P1/P2). “RMS of Fit” indicates the RMS of the CV data residuals after adjusting the quadratic clock model; the RMS value gives an idea of the uncertainty of the CV method. As can be seen, SF fits are in general nearly twice as noisy as DF ones.

### What the Results Indicate
Several facts can be observed from the results. In the first place you can see a relatively large dispersion in the adjusted A0 values, with maximum errors of more than 3 ns versus the nominal solution. This is explained by the combined calibration errors in the two GNSS receivers. The pseudorange delay in each receiver chain can reach a few hundred ns, considering the accumulated effect of the antenna, the antenna cable, and the receiver itself. The total delay can be calibrated with an uncertainty of 2 or 3 ns for each pseudorange signal. Since receiver chain delays are fairly stable, the error in the A0 can be considered constant, and thus it does not affect frequency transfer, but it does affect the time transfer.

The second remarkable fact from the results is that GPS and Galileo provide nearly identical steering results in DF, and that in fact the very small frequency drift of the clock (A2 term) can only be properly estimated in DF. We can observe a large dispersion in the A2 term from the SF solutions, with an opposite sign with respect to DF. Finally, we can see that the steering error in SF is roughly inversely proportional to the value of the carrier frequency, with smaller values in L1/E1 and larger values in L5/E5a. This makes sense since the ionospheric error in the pseudorange is inversely proportional to the square of the carrier frequency. We can...
Systron Donner offers the industry’s only “All-Causes” tactical-grade SDI600 MEMS IMU. The SDI600 features a breakthrough High-Bandwidth (HBW) gyro-design that is proven to significantly reduce vibration sensitivity and improve 1°/hr gyro & 1mg accel bias stability under >25Grms captive carry environments. Designed specifically for easy integration into missile and munition applications, the SDI600 is shorter, delivers full performance in 1 second, and features industry standard serial communication, TOV sync, and 95% BIT coverage. SDI600 is the better alternative to older generation optical RLG/FOG technologies.
also observe that the minimum steering error in SF is provided by Galileo in E1 ("GAL C1"), which can be explained by the superior performance of the NeQuick iono model as compared to Klobuchar. However the good SF results in L1/E1 must be taken with caution, since this is the signal most likely to be jammed. Interestingly, the E6 signal, unique to Galileo, is the one providing the second-best SF steering, after L1/E1. The worst SF steering is obtained using pseudoranges in the L5/E5 bands, with daily errors of the order of 0.3 ns/day.

Very similar facts are observed from an analogous CV processing of the PHM-B clock. In conclusion, in the worst scenario we would be able to steer the clock to UTC using SF CV in any single GNSS band, with a maximum deviation of 0.3 ns/day, equivalent to 9 ns in one month. This possibility would be very useful in case of persistent jamming or interference in any other band(s), in particular in L1/E1. So far SF steering has not been necessary in WANTime, and the nominal GPS P1/P2 combination has been used since the start of the service provision at the beginning of April 2019. Our deviation from UTC(PTB) so far is shown in (Figure 4).

Manufacturers
At GMV, the PHMs used in this project are model 1008 from Vremya, Russia, distributed in Europe by T4Science, Switzerland. The GNSS receivers are PolaRx5TR from Septentrio, Belgium. The frequency steppers are HROG-10 from SpectraDynamics, Colorado, USA. At PTB, GNSS data used in this experiment has been collected by a GTR55 receiver from MESIT, Czech Republic. White Rabbit equipment and support is provided by Seven Solutions from Granada, Spain. WANTime is a registered trademark of GMV.

Authors
Ricardo Píriz is an aeronautical engineer by the Polytechnic University of Madrid. He started his career as a Flight Dynamics engineer in the Precise Orbit Determination group at ESOC, the European Space Operations Center in Darmstadt, Germany. Later on he moved to Eutelsat in Paris, as a Mission Analysis engineer in the Satellite Procurement Division. Since 2001 he has been in the GNSS Business Unit of GMV working in several projects, in particular in the GIOVE Mission (the experimental phase of Galileo), and in the Galileo Time Validation Facility (TVF). He is currently Leader of the GNSS Time & Frequency Group.

Pedro Roldán has a Master of Science in Aerospace Engineering from the Technical University of Madrid and in Meteorology and Geophysics from the Complutense University of Madrid. He has worked at GMV since 2013, focused on the definition and development of GNSS and timing algorithms, including algorithms for precise orbit determination, precise point positioning, time transfer, steering of clocks and definition and maintenance of time scales.

Esteban Garbin is an Electronics and Telecommunication engineer who got his Ph.D. from Politecnico di Torino in 2017. His research studies focused mainly on GNSS receivers and signal processing algorithms, particularly for interference and spoofing detection and mitigation. Since June 2017 he has been working for GMV, focusing on different aspects in the GNSS Advanced User Segment solutions division, mainly developing novel concepts on GNSS timing and receivers.

FIGURE 3 The numerical values of the adjusted models.
Selected to test the GNSS receiver for the OneWeb Satellites

CONSTELLATOR

UNMATCHABLE SIMULATION PERFORMANCE FOR YOUR HIGHEST RETURN

Team Player
- Compatible with other best in class test solutions
- End-to-end system test including Hardware in the Loop

Future proof Investment
- Its core is Software ensuring upgradability & adaptability to future constellations, satellites & codes

Affordable TCO
- Easy hardware maintenance calibration & support at affordable prices providing quick ROI

Multi-frequency multi-constellation GNSS Simulator

Designed to test receivers against the demands of the future

Toulouse - New York - San Francisco

Headquarters
5 Bd. Jean-Augustes Ingres
31770 Colomiers, France

www.syntony-gnss.com
contact@syntony-gnss.com
Multi-Tier GNSS Signal Authentication
Could smartcard be an integral part of future GNSS authenticated services?

There are strong proponents for GNSS authentication implementation at the system level with all major constellations considering to adopt a solution. Here the authors present an innovative design for GNSS authentication implementation at system and receiver level that can satisfy a large number of user requirements, in terms of robustness and performances, by introducing the concept of smartcards for GNSS authentication processing.

GNSS open signals authentication has become an active discussion for implementation at system level with all major system providers considering to adopt a solution, with Europe’s Galileo the earliest system that has declared future upcoming service implementations. At the time of writing of this article, the requirements for GNSS authentication are still different for each application.

To date, the proposed solutions have considered only asymmetric schemes in order to avoid the use of secure dedicated hardware in the receiver to protect the integrity and confidentiality of the symmetric cryptographic material. However, with demanding requirements for robust PNT and authentication rising quickly, and with a lifecycle of the space sector that exceeds 20 years from design to service deployment, it is time to investigate alternative solutions.

The satellite television industry has a long track record in the use of symmetric key schemes with smartcards and hardware security modules for the purpose of data access control and user management. Indeed, it has an equally long track record of vulnerabilities, attacks and mitigations solutions that have been developed in the last 30 years.

Smartcards and commercial Hardware Security Modules (HSM) are becoming a technology available in every single device, for example televisions, mobile phones, vehicles, and recently even smart watches with eSIM. Hardware security implementation is not new in civil GNSS, as it has been demonstrated in 2009 by the TIGER trusted GNSS receiver (Figure 1), which used a hardware security supervisor to control a tamper mesh and store sensitive cryptographic information. With the modernization of signals, these type of security architectures might become a standard in some specific GNSS applications.

This article investigates if and how future GNSS authentication can offer...
Where CSWaP Matters!

EMCORE Fiber Optic Gyros, IMUs & Navigators

High-Accuracy and Affordability with the Industry’s Best SWaP

THE EMCORE ADVANTAGE:

- Closed-loop FOG technology with as low as 1/3 the SWaP and up to ten-times the performance of competing systems depending on the model
- Form, Fit and Function compatibility with legacy products, but with higher performance
- INS with stand-alone aircraft grade navigator performance at 1/3 the size of competing RLG systems
- High-bandwidth, high input rate, low-noise
- Land, sea, air and space applications
- Vertically-integrated manufacturing in Alhambra, CA

FIND OUT MORE:

Email: navigation-sales@emcore.com
Call: +1 626 293 3400
Or Visit: www.emcore.com/gnss

© 2019 EMCORE Corporation. All rights reserved.

www.emcore.com/gnss
Multiple services, integrating smartcards and HSM as part of the user segment.

One particular challenge is to identify the least common multiple requirements in a multi-application GNSS scenario. Different applications entail different requirements, particularly for these major drivers:
- Level of required Robustness;
- Security Protocol features: detection only or detection and mitigation (secure navigation);
- Security Protocol performances such as time to authentication, rekeying delay, etc.;
- Security Protocol Integrity, availability and accuracy performances;
- Achievable security, and
- Cost and performances impact at receiver.

Integrating the needs of safety critical and mass market applications with a single service and unique receiver hardware architecture can become very challenging both on system and receiver design.

This article presents an innovative concept of Multi-Tier Signal Authentication (MTSA) for GNSS, introducing different services and hardware implementations, which could leverage the integration of smartcards and HSM in the GNSS industry civilian domain.

The main objective is to attempt to define a service that can satisfy multiple user requirements for different applications. Being only a concept proposal, consolidated service implementation details as well as results are left for future work.

**Main Design Drivers**

The idea of the Multi-Tier Signal Authentication (MTSA) is to allow the implementation of different user services that can satisfy different requirements. The main requirements discrimination is:
- Authentication latency and authentication performances;
- Requirement for authentication only, or authentication and robust navigation (navigation under attack);
- Need of security module in the receiver, to support symmetric services;
- Availability of network connectivity (aiding channel), and
- Option to defer the security to an external component (e.g. smartcard), in order to maintain the current GNSS chip cost and design.

As baseline, the MTSA concept is designed to provide authentication services to three main classes of hardware (Figure 2):
- Class 1, GNSS receivers with no specific security hardware:
  - A) Unconnected devices with no security module. They use Asymmetric services or services that achieve asymmetry through delayed key release.
  - B) Connected Devices with no security module, server-side processing (transmission of RF samples to a cloud service). Server-side processing is out of the scope for this article but it is mentioned to highlight that Class 1 devices could support such service.
- Class 2:
  - Low end hardware security module (e.g. ISO7816 smartcard or chip-based HSM). They use symmetric key services, which are faster but require key protection. Connection is required for rekeying if needed or when scheduled, unless sufficient bandwidth is available in the broadcast signal.
- Class 3:
  - High end hardware security module. They allow navigation and timing in hostile (under attack) scenario. They do not need connection; rekeying can be performed over the air.

In order to achieve this broad coverage of requirements a scheme is proposed that requires two channels, one with public available pseudorandom noise (PRN) codes carrying data that can be processed by all users (as GPS C/A or Galileo OS), and, a second channel that allows all signal-based authentication services implementation at code level.

Class 2 devices assume that the signal processing of the authentication signal is performed inside the smartcard or HSM. This is achievable with modern technology, and it is expected that performances of security hardware will improve exponentially in the future. In order to send the minimum amount of data to the smartcard and reduce the processing on its side, it is assumed that the signal is acquired for example on an open signal component and there is knowledge of the authentication information location both in code phase and the signal complex arm.

For example, a hypothetical design could foresee an open signal transmitting on the in phase component, and the authentication signal on the quadrature part. Once the code phase and Doppler of the open signal are resolved by the receiver, the precise samples of the authentication code in the quadrature
The main concept is the following: the system generates master keys that are kept secret and never released. The master keys generate the operational keys, that are used for a period that shall be designed based on the security requirements. From the operational keys two other subset are obtained:

- Session keys, that are created every X minutes (for example 10 mins). The Session keys generates two types of keys:
  - Key Early Authentication (KEA) key, a key that will be used to implement a relatively fast authentication at code level with a symmetric authentication approach. The KEA will generate a short PRN sequence that will be included in the signal at high frequency, for example every second. These keys will also be available in the Class 3 receiver to achieve very low authentication latency and low time between authentications.
  - Key Delayed Authentication (KDA) key, that is generated as one time key every X seconds (for example 10s). The authentication key creates a PRN sequence that lasts some ms and is used for authentication purposes only. The key is released with a delayed approach and authenticated with some form of data authentication or Navigation Message Authentication (NMA).

- Secure navigation keys, that are used to generate the PRN sequence for robust navigation. This, differently from authentication, allows robust navigation also when the signal is spoofed by an attacker and continuous authentication of the signal.

Receiver operation for delayed authentication (Class 1 devices):
The receiver needs to acquire an open signal and get a time reference and code phase. At the time T0 of the foreseen delayed authentication sequence transmission the receiver will store the IF data (I/Q samples for example) and wait for the key to be released or connect to a cloud server and send the IF data. For signal in space availability only, as soon as the key is released and authenticated the receiver can generate the PRN sequence from the key and perform a correlation with the stored signal (at time T0). For connected services the receiver will transmit the IF data and wait for processing, or, alternatively can receive the PRN sequence or the delayed KDA via the cloud service.

Receiver operation for early authentication (Class 2 devices):
The receiver needs to acquire an open signal and get a time reference and code phase. At the time T0 of the foreseen early authentication sequence transmission the receiver will correlate the signal with a local replica generated by the KEA keys.

KEA will be generated by the session key. If session keys are compromised the Class 2 device needs to connect to a network and download the new session keys via a secure protocol (detection of attacks that can compromise the keys is not investigated in this article. One possible approach could be to use higher class receivers to detect lower class attacks).

<table>
<thead>
<tr>
<th>Service</th>
<th>Category:</th>
<th>Authentication Latency</th>
<th>Secure Navigation</th>
<th>Requires Comm link</th>
<th>Requires HSM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delayed Authentication (DA)</td>
<td>Class 1–autonomous</td>
<td>10s</td>
<td>Snapshot, 10s</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Delayed Authentication (DA)</td>
<td>Class 1–Remote Processing</td>
<td>3-5s</td>
<td>Snapshot, 3-5s</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Early Authentication (EA)</td>
<td>Class 2, low end HSM</td>
<td>1s*</td>
<td>Snapshot based</td>
<td>No**</td>
<td>Yes</td>
</tr>
<tr>
<td>Secure Navigation (SN)+ EA</td>
<td>Class 3, High end HSM</td>
<td>&lt;=1s</td>
<td>&lt;=1s</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 1: Comparison of HW categories
- Performances under evaluation
- The hardware does not require a comm-link unless a rekeying is performed by the system. This could be a comm link or a physical update of keys in the HSM.
Receiver operation for secure navigation (Class 3 devices):
The receiver needs to have a rough time estimation from the
internal hardware or a trusted source. The signal can be acquired by the receiver and local replica can be generated by the session keys. In order to track the full signal the receiver needs to combine both early and delayed authentication codes and secure navigation code. This can be achieved by a concatenation of the code generated by the authentication keys and the code generated of the secure navigation keys.

Analytical Description
The following paragraph provides an analytical description of the cryptosystem and a hypothetical protocol implementation. Again it is stressed that this is just an example and not the results of a specific design implementations of the authors in a specific activity. The details of key generations and productions are only given as reference: a system designer might implement any cryptographic primitives that are most suitable to its own environment and security or policy requirements.

A Master Key $K_{\text{Master}}$ is generated and maintained secretly at system level. It is assumed that it is generated by any Key Derivation Function (KDF) that is most relevant to the solution. $K_{\text{Master}}$ generates the operational keys and the Key Encryption base keys required to generate session keys that are changed on a specific crypto period via other KDF.

The operational keys $K_{op}$ and its Initialization Vector are valid for a crypto period $T_{op}$ and they are generated by secure hashing functions and secure random number generators at system level:

$$K_{op}(T_{op}) = H(K_{\text{Master}}, \text{Nonce}_1)$$

$$IV_{op}(T_{op}) = H(K_{\text{Master}}, \text{Nonce}_2)$$

$$K_{\text{base}_kek}(T_{op}) = H(K_{\text{Master}}, \text{Nonce}_3)$$

$$IV_{\text{base}_kek}(T_{op}) = H(K_{\text{Master}}, \text{Nonce}_4)$$

Session keys are then generated that will be used during the entire pre-defined crypto period $T_{op}$, this can be for example 1 month or 1 year. Each session key is valid only for a crypto period of the specific session crypto period (T), that is the period of the session that could last for example 10 minutes. The session keys for the entire period $T_{op}$ are pre-generated and encrypted.

$$K_{\text{session}}(T_{op}) = F(K_{op}, IV_{op})$$

$$K_{\text{session}_kek}(T_{op}) = F(K_{\text{base}_kek}, IV_{\text{base}_kek})$$

Where $F$ is a stream cipher function or equivalent capable to generate all $K_{\text{session}}$ and $K_{\text{session}_kek}$ for the period $T_{op}$. These keys remain valid for all $T_{op}$ unless a system rekeying is requested. System rekeying and key revocation is not covered in this paper and implementation options are left to the system designer. The stream cipher function $F$ will generate session keys that will be used by the system to generate the signal. The generated keys will appear as a vector of keys:

$$K_{\text{session}}(K_{\text{session}_1}, K_{\text{session}_2}, K_{\text{session}_3}, ...)$$

$$K_{\text{session}_kek}(IV_{\text{session}_1}, IV_{\text{session}_2}, ...)$$

The session keys are encrypted before transmission in space, where an encrypted key will be transmitted:

$$E_{C,K_{\text{session}}}(T_{op}) = E(K_{\text{session}[N]}, K_{\text{session}_kek}[N])$$

Where $E$ is an encryption function that encrypts all $K_{\text{session}[N]}$ vector with the $K_{\text{session}_kek}[N]$ vector keys.

All the $K_{\text{session}_kek}$ are transmitted by the system with some anticipation for every crypto period $T_{op}$ which is the period that each session last. So for example $K_{\text{session}_kek}[T_{op}]$ could be transmitted during $T_{op}$.

Authentication implementations of $K_{\text{session}_kek}$ is left to the system designer, they could be embedded on an existing Navigation Message Authentication (NMA) scheme or implement a specific authentication subsystem.

Preloading in hardware security modules
Based on the hardware security module, the keys are uploaded via a hardware authentication mechanism not discussed in this article (Public Key Infrastructure or other) directly in the devices.

For Class 2 devices (low end HSM), only encrypted keys are allowed ($E_{C,K_{\text{session}}}$) as these hardware categories are at risk of key leakage. In case they are compromised, only the session key would be revealed. These devices would require connectivity if rekeying is requested by the system.

For Class 3 devices (high end HSM), operational keys are allowed ($K_{op}, K_{IV}$) as this hardware category assumes a stronger protection from key leakage.

Generation of authentication and secure navigation functions
For every $T_p$ period, once $K_{\text{session}}$ are decrypted they can be used to generate the authentication function. Two type of keys for authentication are generated.

- Key Delayed Authentication (KDA) Keys
- Key Early Authentication (KEA) Keys

The KDA Keys are generated by:

$$K_{\text{temp}_K} = H(K_{\text{session}[N]})$$

$$K_{\text{temp}_IV} = H(K_{\text{session}_IV}[N], \text{Nonce}_1)$$

$$K_{\text{KDA}} = F(K_{\text{temp}_K}, K_{\text{temp}_IV})$$

$$K_{\text{KDA}_IV} = F(H(K_{\text{temp}_K}), H(K_{\text{temp}_IV}))$$

Similarly, The KEA Keys are generated by:

$$K_{\text{temp}_2K} = H(K_{\text{session}[N]})$$

$$K_{\text{temp}_2IV} = H(K_{\text{session}_2IV}[N], \text{Nonce}_2)$$

$$K_{\text{KEA}} = F(K_{\text{temp}_2K}, K_{\text{temp}_2IV})$$

$$K_{\text{KEA}_IV} = F(H(K_{\text{temp}_2K}), H(K_{\text{temp}_2IV}))$$

Where for both cases H is an optional secure hash function to introduce complexity against cryptanalysis and F is a stream cipher function or equivalent that generates a number of KEA and KDA keys. Both $\text{Nonce}_1$ and $\text{Nonce}_2$ are assumed to be transmitted in the broadcast messages.
The KDA keys will have a new crypto period $T_{KDA}$ that is very short, for example 10 seconds. The KDA keys are released authenticated after the $T_{KDA}$ expires for use in class 1 devices. The final KDA keys will be a vector (including the KEA IV):

$$K_{KDA}((K_{KDA_1}, K_{KDA_{IV_1}}), (K_{KDA_2}, K_{KDA_{IV_2}}), (K_{KDA_3}, K_{KDA_{IV_3}}), \ldots) \tag{19}$$

The KDA keys generate the Authentication Pseudo Random Number (PRN) sequence used for the Delayed Authentication (DA) service. It is generated by:

$$PRN_{DA} | T_{DAI} = SC(K_{KDA_{IV}}, K_{KDA_{IV}}) \tag{20}$$

Where SC is a Stream Cipher function that generates the entire PRN sequence for delayed authentication integration $T_{DAI}$ period (for example 20ms).

The KEA keys will have a new crypto period $T_{KEA}$ that can range between $T_{KDA}$ and $T_e$ at discretion of the designer. The KEA keys are never released, and are maintained secret by the security module Class 3. The final KEA keys will be a vector (including the KEA IV):

$$K_{KEA}((K_{KEA_1}, K_{KEA_{IV_1}}), (K_{KEA_2}, K_{KEA_{IV_2}}), (K_{KEA_3}, K_{KEA_{IV_3}}), \ldots) \tag{21}$$

The KEA keys generate the Pseudo Random Number (PRN) sequence used for the early authentication service. It is generated by:

$$PRN_{EA} | T_{EA} = SC(K_{KEA_{IV}}, K_{KEA_{IV}}) \tag{22}$$

Where SC is a Stream Cipher function that generates the entire PRN sequence for the early authentication integration period $T_{EA}$ period (for example 10ms).

$$PRN_{EA} | T_{EA}$$ and $PRN_{DA} | T_{DAI}$ can be interleaved at choice by the system designer. One option that is considered in this article is the transmission of $PRN_{EA} | T_{EA}$ with a frequency $f_{EA}$ and once every $N * PRN_{EA}$ transmissions substitute the code with a $PRN_{DA} | T_{DAI}$. This would allow for example a 1s $f_{EA}$ (an early authentication PRN transmitted every second) and a 10s $f_{DA}$ (every 9 seconds a delayed authentication PRN is transmitted).

Finally, operational keys generate $(K_{op}, IV_{op})$ generates the Key Secure Navigation (KSN) key that is used to generate the PRN sequence used for secure navigation. As an example, it can be generated by:

$$K_{SN} | T_{SN} = H(K_{op}, Nonce_{sym}) \tag{23}$$

$$IV_{SN} | T_{SN} = H(IV_{op}, Nonce_{sym2}) \tag{24}$$

$$PRN_{SN} | T_{op} = SC(K_{SN}, IV_{SN}) \tag{25}$$

Where SC is a Stream Cipher function that generates the entire PRN sequence and H a secure one way hashing function. The introduction of an H function is suggested to detach the implementation of the PRN generation from the operational keys in order to not expose the service to potential direct cryptanalysis of the PRN sequence. It is up to the system designer to find a strategy for the secure generation or dissemination of $Nonce_{sym}$ and $Nonce_{sym2}$ and they could be also a time-variable function.

The final PRN sequence transmitted by the satellite will be a combination of (20),(22) and (23):

Given the repetition intervals $t_{EA} = 1/f_{EA}$ and $t_{DA} = 1/f_{DA}$,

$$PRN_{EA} = \begin{cases} PRN_{SN}, & t \in [n \cdot t_{EA}, m \cdot t_{EA} + T_{EA}], n \in \mathbb{N} \\ PRN_{DA}, & t \in [k \cdot t_{DA}, km \cdot t_{DA} + T_{DA}], k \in \mathbb{N}, m = 10 \\ \text{elsewhere} \end{cases} \tag{26}$$

Meaning that $PRN_{EA}$ substitutes $PRN_{DA}$ once every 9 occurrences as for the example above.

Figure 6 shows the example of an entire key tree generation process following the approach proposed. The system designer shall adapt this example to its specific needs.

**Probabilistic Key Distribution for smart card attacks mitigation**

One interesting approach to mitigate the risk of a compromised smartcard can be achieved by using multiple session keys, each generating a specific KEA key, from which only a part of the codes associated to the KEA service can be derived. A receiver is given only a subset of all the session keys, in this way it can
generate only a part of the code associated to the KEA service. This part is meant to be enough for authentication purposes, but not enough to spoof a different receiver in case the smartcard is compromised, because another subset of all the session keys is given to a different receiver.

This approach is similar in philosophy to a Probabilistic Key Pre-distribution Scheme (PKPS), which is based on the strategy of allocating a subset of keys to each device from a set of keys, in order to be able to revoke the access privilege of a device without affecting the rest of the community. Gong and Wheeler, Mitchell and Piper, and Dyer et alia (Additional Resources) have investigated various strategies for the allocation of the subsets of keys, motivated by Erdos et alia's seminal work on uniqueness of subset intersections (Additional Resources). See again the paper by Dyer et alia, which also pointed out that complex deterministic allocation strategies can be easily replaced with simple random allocation strategies with very little penalty.

The considered PKPS-based approach for Class 2 authentication protection is based on the following assumptions/steps:

A total of *N* sessions keys are considered, \( K_{1,1}, K_{1,2}, \ldots, K_{1,N} \);

- The whole code associated to the KEA service is partitioned in \( N \) parts, each part \( i \) of length \( T = T_{KEA}/N \) (where \( T_{KEA} \) is the total length of the KEA code) can be generated through a stream cipher starting for the associated KEA key \( K_{KEA,i} \);
- Each user is given a subset of \( s \) sessions keys selected uniformly from the \( N \) keys, with \( s \leq N \);
- To perform an authentication check a user exploits its \( s \) sessions keys: first it generates the associated \( s \) KEA keys, then it generates the associated correlation interval (which is a subinterval of the whole KEA code), and finally it checks whether the correlation achieves a peak value above the authentication correlation threshold.

In case a generic user \( i \) compromises its smartcard and attempts to spoof the receiver with keys, he would have a disadvantage in power (only and in the example would
be in common to generate the KEA codes). This would result in a correlation loss that would not pass the security threshold (Figure 8).

It is denoted by $g(r,s)$ the probability that a single KEA authentication check performed by a user is successful, given that only a part of length $r \cdot T$ of the code interval of length $s \cdot T$ that the user correlates is correctly generated (it is remarked that the total KEA code interval length is $N \cdot T$, but the user correlates only the part of length $s \cdot T$ associated to its session keys). In the nominal situation, in which the user is tracking the authentic signal, $r=s$, hence $g(s,s)$ should be close to 1. Instead, if $r<s$ the KEA code is generated by an entity possessing only a part of the $s$ session keys associated to the user, hence in this case $g(r,s)$ should be lower than the possible, to avoid false authentications. More details concerning the achievable values of $g(r,s)$ are discussed in the next section of this article.

Considering that the $N$ session keys are assigned to the different users following a uniform distribution, assuming that a generic user $i$ is able to compromise its smartcard, the probability that user $i$ is able to spoof user $j$ for an interval equal to the repetition of the KEA code (i.e., a single authentication check is successful) can be computed by conditioning with respect to the number of session keys in common:

$$P[\text{spoof } 1 \text{ KEA check}] = \sum_{r=0}^{s} \left( \frac{N}{s} \right) \cdot \left( \frac{N-s}{s-r} \right) \cdot g(r,s)$$  \hspace{1cm} (27)

The term $P[r_{ij} = r] = \left( \frac{s}{r} \right) \cdot \left( \frac{N-s}{s-r} \right) / \left( \frac{N}{s} \right)$, which is defined only for $0 \leq r \leq s \leq N$ and $r \geq 2 \cdot s - N$, is the probability that users $i$ and $j$ have $r$ keys in common, given that they are each given $s$ keys uniformly selected from a pool of $N$ keys. Such a probability is depicted in Figure 9 for $N=50$, varying the values of $s$ and $r$.

From Figure 9 it is possible to observe that decreasing $s$ means decreasing the ratio $T/s$ between the average value of keys in common $T$ and $s$ (or the ratio between the maximum value of $r$ occurring with a significant probability and $s$). This is important because the smaller this ratio the easier it is to design correlation thresholds capable of correctly discriminating the reception of authentic signals from the reception of spoofed signal, as it is described later in this article.

However, it is important to remark that $s$ should not be too small, because the ratio $s/N$ represents the ratio of the total KEA code that a user can exploit for authentication purposes, hence a decrease of $s$ leads to an increase in the miss authentication probability in nominal scenario (tracking of the authentic signal). Hence, all these different trade-offs should be taken into account when designing a specific for the proposed approach.

Finally, it is also important to remark that KEA authentication checks are continuously performed by a user. The probability that a user is spoofed for a sustained time interval during which a total of $z$ KEA authentication checks are performed is equal to:

$$P[\text{spoof } z \text{ KEA checks}] = \sum_{r=\max(0,2s-N)}^{s} \left( \frac{s}{r} \right) \cdot \left( \frac{N-s}{s-r} \right) \cdot g(r,s)^z \quad (28)$$

If the term $g(r,s)$ is not too close to 1, then $g(r,s)^z$ converges quickly to 0 with respect to the number of checks $z$. For example, let’s assume that a KEA authentication check is performed every second and that the maximum value of $r$ for which $P[r]$ cannot be considered negligible is such that $g(r,s)=0.7$. Then the probability that the spoofing attack remains undetected for 30 seconds is upper-bounded by $0.7^{30}=0.00002254$.

**Preliminary Performance Analysis, Signal Distribution Considerations**

Test results on bandwidth usage and smartcard correlation performances are not available yet to date.

The authentication code can be distributed with a time division approach or, alternatively, can be spread between one authentication sequence and the next one. The second one is known also as spreading via a time-hopping approach (Figure 10).

The following paragraph indicates some preliminary analysis of both techniques, distribution of authentication data via “Time Division” (TD) or “Time Hopping” (TH), and the impact of spoofing when a Probabilistic Key Distribution approach is adopted.

**Authentication Test Model**

As detailed in the paper by Dalla Chiara et alia (Additional Resources) the authentication test is based on the correlation of the spreading sequences. Specifically, the model for the correlation is given by the following equations:

$$I(nT) = A(R(\Delta T) \sin(\pi \Delta T \omega) \cos(\Delta \Phi) + n_i) = A(R(\Delta r) \sin(\pi \Delta r \omega) \sin(\Delta \Phi) + n_q) \quad (29)$$

Where:
- $\Delta T$, $\Delta r$, $\Delta \Phi$ are the estimation errors for code delay, carrier doppler and carrier phase respectively;
- $T_{int}$ is the coherent integration time;
- $I(nT)$ and $Q(nT)$ are the In-Phase and Quadrature correlation value;
- $R(\cdot)$ indicates the autocorrelation function;
- $A$ is the signal amplitude set as $A=\sqrt{2T_{int}10^{CNO/10}}$;
- $n_i$ and $n_q$ represent the Gaussian noise for variance equal to 1.

This model partially describes the operation needed for the authentication test. In particular, for long integrations, the coherent integration may not be viable: this happens for example because of Doppler change and in general signal dynamics, or because of the channel (i.e. multipath). In harsh environment, in fact, short integrations are preferable, especially when the phase estimation is not precise: non-coherent accumulation mitigates the effect of the phase error. In for-
In this means that a given section of the code is coherently integrated for $T_{int}$ and then non-coherently accumulated $N$ times, through the squared sum. The accumulation time is therefore $T_{acc} = N \cdot T_{int}$ and the decision variable is:

$$X_{TD}(nT) = \sum_{n=1}^{N} I^2(nT)_TD + Q^2(nT)_TD$$ (30)

The threshold is therefore obtained inverting a Non-Central Chi Square variable with 2N degrees of freedom, for a given false-alarm probability.

One consideration is here necessary: in case of the “Time-Division” approach, the integration time $T_{int}$ coincides with the exact duration of the Authentication-Code integrated, because the code is continuous. In case of “Time-Hopping” approach the Authentication-Code is actually a watermarking of the Secure Navigation Code, and spread within it. For clarity, the notation $T_{int}$ indicates the length of the Authentication/Code integrated coherently, for both TD and TH approaches. This means that for a given $T_{int}$ the receiver needs to buffer a portion of signal $T_{buf} = T_{int}$ long for the TD approach. For the TH approach, a $T_{buf} = K_{TH} \cdot T_{int}$ portion of signal needs to be buffered, with $K_{TH}$ being the percentage of watermarking. $T_{buf}$ is actually the observation window in which the coherent integration can be done. The observation window $T_{buf}$ also indicates the interval adopted for code segmenting in the probabilistic key distribution approach.

**Expected Performance**

The model presented in the previous section allows to assess the expected performance of the technique, in standard AWGN channel, for the two approaches. In general terms, the two approaches are conceptually similar but their nature of packing vs spreading the chips make them differ for the following features:

- Viable coherent accumulation time. Specifically, the TD allows longer coherent integrations because the observation window is significantly shorter with respect to TH, when $T_{int}$ is the same. In other words, the channel fluctuations have a minor impact in a small observation window, and this can be effectively exploited by the TD approach.
- Processing time, or processing effort. This metric indicates the amount of time necessary to complete an authentication test. In general terms, the TH option has a processing time that increases linearly with time, under the assumption that the chips of the Authentication-Code are spread uniformly within the Secure Navigation Code. Equally, the number of operations done or the necessary buffering. Conversely, for TD, the accumulation is achieved stepwise for each code block; unless one code block is sufficient to complete one single test. In the latter case, TD can be significantly faster, ideally $K_{TH}$ times faster (with the same $T_{int}$). In more practical terms, this metric is reasonably negligible in the overall Time To Authentication (TTA), that must cope with the fact that the data necessary to reconstruct the code is broadcast with some delay.
• Time to disclosure of the secret data. This is an important feature that is actually a design parameter of the authentication approach. The Delayed authentication service (KDA) is based on a delay for the implementation of the asymmetry (e.g. the TESLA protocol [Perrig et alia, Additional Resources]). Consequently, a minimum time between the broadcast of the last chip of the Authentication-Code, and the disclosure of the data is necessary to reconstruct the same code. This minimum time must be carefully determined to guarantee sufficient protection against attacks that shift the receiver time. In fact, if the time advance of the attacker is sufficient to decode the broadcast reconstruction data, while the receiver is still receiving the chips, the attacker can effectively fake the signal in an undetectable way.

• Impact to standard tracking. The TH approach has a significant advantage: the local generation of the Secure Navigation Code has punctual error where the broadcast code has been watermarked. This happens when the receiver cannot reconstruct in run-time the Authentication-Code. In practice the punctual errors have an impact on the correlation value produced by the correlators: ideally the loss is exactly $K_{th}$. This means that the tracking remains stable, likely suffering more noise. Conversely, the TD approach necessarily introduces a gap in the spreading code. The width of this gap can be sufficient to prevent proper accumulation in the tracking correlators. In this case, the receiver should support a costing time or external aiding is necessary to properly update the loops to prevent loss of lock when the Secure Navigation Code is broadcast.

All the features presented here are reported to indicate the main parameters that should be considered for the fine configuration of the authentication approach. It is assumed that the system designer will perform a detailed requirement analysis, in order to understand clearly which are the design drivers that should be considered and coherently the features to be implemented.

Regardless the specific type of implementation, the two watermarking approaches share the same performance in terms of detection of the secret sequence. This, under the assumption that the coherent integration time and the number of non-coherent accumulations are the same (minus the residual time in the last accumulation due to different observation windows). An insight into the expected performance in terms of feasibility of the detection test is presented in Figure 11 and Figure 12.

Figure 11 shows the probability of detection for a false-alarm probability of $10^{-5}$, with a chipping rate of 1.023 MChip/s. The figure indicates the particular case in which the base interval of the watermarking sequence is 10 milliseconds (ms) and within this interval the override of the
Secure Navigation Code is the one reported in the legend. 10 ms is the total accumulation time for the TH approach, that is its observation window. Conversely, the observation time for TD in this particular case corresponds to the watermarking percentage, because the number of accumulations is 1.

Figure 12 presents the probability of detection for a false-alarm probability of $10^{-6}$, with a chipping rate of 1.023 MChip/s, with a more realistic approach. In this case the integration time $T_{int}$ is fixed to (a) 1 ms and (b) 0.1 ms, for a repetition period of 10 ms. The authentication test is done with different number of non-coherent accumulation: precisely: 1, 2, 5, 10, 50, 100, for the indicated total accumulation times. It is recalled that $T_{int}$ corresponds to the observation window for the TD approach (1ms in (a) and 0.1 ms in (b)). Conversely, the observation window for the TH approach remains 10 ms, for the spreading nature of the technique. Note: $T_{acc,tot}$ indicates the observation window necessary to complete an authentication test. It corresponds to $N_{acc} \times T_{bay}$ when all the data necessary to reconstruct the Authentication-Code is broadcast later. However, the technique can be designed in a way that the same observation window is covered by more than 1 broadcast of the reconstruction data: this could be the case for low very power components.

The analysis presented in Figure 11 and Figure 12 is derived from the analytical model, in AWGN channel. From Figure 12 it can be seen that an accumulation below one second can be well tailored with a 10% of watermarking, thus allowing quick authentication test, and comparable delay. The drawback of this approach can be found in the amount of data necessary to reconstruct 10% of the spreading code, and the corresponding bandwidth exploited. The second option of Figure 1212 relaxes the bandwidth demand, at the cost of slower authentication, and longer delay: however, being the Authentication-Code spread in a longer interval, the overall power of the secret component is weaker, thus making the solution more robust against estimation-based attacks.

The considerations above can be extended to cover the configuration with a probabilistic key distribution approach. In this case, the bandwidth consumption is less critical, since the data is already stored in the receiver. Evolving the analysis reported, a more complex partitioning policy can be adopted to increase the diversity among the subset of keys detained by a user. As described in Figure 77, the greater the number of total keys compared to the number of keys per user, the smaller is the overlapping among users. This is desirable to reduce the impact of a compromised smart card, as depicted in Figure 13. The figure considers a more realistic setup, where the session lasts 10 seconds and 100 keys are hold by the user (on a total of N); each key allows the generation of a code sequence long 100 us. Figure 13 shows the probability of passing the authentication test, when tracking a spoofing signal forged with the compromised keys (non-coherent integrations). The curves clearly show that a spoofing signal has a lower probability of being recognized as authentic, because of the penalty on the accumulated power: the reference indicates the performance on the authentic signal with all keys available. This gives the spoofers some margin to play with the transmitted power, but this can be easily detected with power monitoring thus making the attack less effective.

Conclusions

This article has presented an innovative design for GNSS authentication implementation at system and receiver level that can satisfy a large number of user requirements, in terms of robustness and performances. This is achieved via implementations in different type of receiver classes, based on the desired service. Three multi-tier services are discussed: delayed authentication service, early authentication service and secure navigation service. The use of smartcards and hardware security modules is introduced for commercial and civil applications, taking as example the maturity of digital satellite television. Finally, an innovative approach for preventing spoofing in case of key leakage is discussed.

Acknowledgments

Silvia Ceccato, Nicola Laurenti, Gianluca Caparra from University of Padova for the fruitful discussions on GNSS and authentication.

Additional Resources


pioneers of the concepts of trusted GNSS receivers, navigation message authentication (NMA) and signal authentication.

**Dr. Andrea Dalla Chiara** is currently leading the Simulation Tools Division in Qascom; formerly he has been designer and developer of GNSS/SBAS simulators and receivers focusing on authentication techniques at signal and data level. He collaborates with Qascom since 2010, where he actively participated in many projects with ESA, NASA, the European Commission and Industry. Previously he led a SME in the radio frequency identification domain and he worked for Infineon as designer and test engineer of smart power ICs. He holds a MSc degree in Microelectronics from University of Padova (Italy) and a Ph.D. in Information Technology with focus in instrumentation and measurements and RF interference.

**Dr. Luca Canzian** received the B.Sc., M.Sc., and Ph.D. degrees in Electrical Engineering from the University of Padova, Italy, in 2005, 2007, and 2013, respectively. From 2013 to 2015 he has been a PostDoc at the Electrical Engineering Department at the University of California, Los Angeles (UCLA), and at the Computer Science Department at University of Birmingham, UK. Since April 2015 he has been working in Bassano del Grappa, Italy, as a Radio Communication Engineer at Qascom, working on cybersecurity, interference localization and cryptography.

**Dr. Giovanni Gamba** is Head of Attack Detection System in Qascom. He received his Ph.D. in Telecommunication Engineering in 2010 from the University of Padova and had a post-doc fellowship for the Italian National Research Council (IEIIT-CNR) working on interference detection and mitigation in industrial applications. He joined Qascom in 2014, serving as R&D specialist and project manager for different EC/GSA/ESA and industry-funded projects related to interference detection, mitigation, geolocation, to GNSS anti-spoofing design and to GNSS robustness assessment for civil aviation.

**Samuele Fantinato** joined Qascom in 2014 and he is currently the Head of the Advanced Navigation unit. He is coordinating multiple activities related to the development of Qascom Robust and Advanced PNT Receiver technology for Space and Ground applications. He has been contributing to the definition of complex GNSS testbeds for interference, spoofing mitigation, and the assessment of authentication schemes of Galileo. He received a master’s degree in telecommunications engineering from the University of Padova in 2007.

**Carlo Sarto** works in Qascom since 2008, currently as Q&A manager. He is an expert in GNSS threats and authentication. He is currently involved in different R&D projects, leading the SimSAFE product team and he supported the European Commission in the definition of the Galileo Open Service Navigation Message Authentication (OSNMA). Sarto received a degree in computer science from the University of Padova.

**Authors**

Dr. Oscar Pozzobon is the founder and President of Qascom. He received a bachelor degree in Information technology engineering and a Ph.D. in aerospace engineering from the University of Padova, Italy, and a master degree in telecommunications engineering from the University of Queensland, Australia. Pozzobon has been involved in the area of GNSS authentication since 2001 and has been one of the pioneers of the concepts of trusted GNSS receivers, navigation message authentication (NMA) and signal authentication.

Dr. Luca Canzian received the B.Sc., M.Sc., and Ph.D. degrees in Electrical Engineering from the University of Padova, Italy, in 2005, 2007, and 2013, respectively. From 2013 to 2015 he has been a PostDoc at the Electrical Engineering Department at the University of California, Los Angeles (UCLA), and at the Computer Science Department at University of Birmingham, UK. Since April 2015 he has been working in Bassano del Grappa, Italy, as a Radio Communication Engineer at Qascom, working on cybersecurity, interference localization and cryptography.

Dr. Giovanni Gamba is Head of Attack Detection System in Qascom. He received his Ph.D. in Telecommunication Engineering in 2010 from the University of Padova and had a post-doc fellowship for the Italian National Research Council (IEIIT-CNR) working on interference detection and mitigation in industrial applications. He joined Qascom in 2014, serving as R&D specialist and project manager for different EC/GSA/ESA and industry-funded projects related to interference detection, mitigation, geolocation, to GNSS anti-spoofing design and to GNSS robustness assessment for civil aviation.

Samuele Fantinato joined Qascom in 2014 and he is currently the Head of the Advanced Navigation unit. He is coordinating multiple activities related to the development of Qascom Robust and Advanced PNT Receiver technology for Space and Ground applications. He has been contributing to the definition of complex GNSS testbeds for interference, spoofing mitigation, and the assessment of authentication schemes of Galileo. He received a master’s degree in telecommunications engineering from the University of Padova in 2007.

Carlo Sarto works in Qascom since 2008, currently as Q&A manager. He is an expert in GNSS threats and authentication. He is currently involved in different R&D projects, leading the SimSAFE product team and he supported the European Commission in the definition of the Galileo Open Service Navigation Message Authentication (OSNMA). Sarto received a degree in computer science from the University of Padova.
Europe has set out to abolish the national patchwork for drone operations. Faced with different drone rules all over the continent, the legislative bodies of the European Union have been very busy lately.

On February 28, the European Aviation Safety Agency (EASA) announced that we are “one step closer to harmonized rules for safe drones operation in Europe.”

What’s changed?
The announcement is based on a number of regulations adopted over the course of 2018 and early 2019.

Setting the grounds essential for the development was the so-called Basic Regulation of EASA (Regulation (EU) 2018/1139 on “Common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency”), adopted in July 2018. Despite the regulation’s title, the European Aviation Safety Agency was already established back in 2002 with Regulation (EC) No 1592/2002. It was, however, not before the recent amendment of the regulation in July 2018 that EASA’s rule making competence for “unmanned aircraft” was expanded to also cover unmanned aircraft with an operating mass of less than 150 kilograms.

This shift of competence from member states to the EU for practically all non-military aircraft indeed marks the basis for all future harmonization in law regarding unmanned aircraft within the Union. It provides the European Commission with the competence to propose a Delegated and an Implementing Regulation with further necessary regulatory details. Even military and other public activities may be placed under the uniform regulatory regime of the EU, if a member state makes use of the opt-in clause that also covers unmanned aircraft.

The EASA Committee, namely the committee for the application of common safety rules in the field of civil aviation, approved of the European Commission’s proposal for the Implementing Regulation also on February 28, 2019. This act regulates the operations of Unmanned Aircraft Systems (UAS) in Europe and the registration of drone operators and of certified drones.

The so-called Delegated Regulation was adopted by the European Commission on March 12, 2019 and then sent to the legislative bodies, the EU Parliament and the Council, which had two months to raise objections. It defines the technical requirements for drones brought to the EU market.

In lack of objections by the legislative bodies, it is expected that both acts will be published and will become gradually applicable within a year. By 2022, the transitional period will be completed and the legal framework for drones within the EU will be fully applicable.

What’s New?
The new legal acts are highly complex and introduce much detail for drone operations.
Join the pioneers already flying STIM210 in space

Sensonor first started supplying its small IMUs to space applications in 2012. Today STIM210 is in use in LEO CubeSat, Micro- and Nano-satellites for pointing and stabilization, flight control, and guidance – with 5 to 10 times lower weight than the next-best alternative.

When size and performance matter

sales@sensonor.com  •  www.sensonor.com
operations, in many ways exceeding the complexity of rules currently established on the member states’ level. Overarching is the principle of an operations-centric, risk-based approach. This means that basically three elements determine how an unmanned aircraft may be operated and what the operational requirements are:

(i) The technical capabilities and characteristics of the unmanned aircraft: e.g. its maximum take-off mass (MTOM); video and audio recording capabilities; guidance-, control- and safety systems; etc.;

(ii) the characteristics of the operation and operational environment, e.g. flight near or above people, residential areas, planned maximum above ground level of flight, transport of dangerous goods or people etc.; and

(iii) UAS operator’s responsibilities and remote pilot’s competencies.

As mentioned, the Basic Regulation expands the EU competence to all unmanned aircraft (UA), regardless of weight. It provides the basis and grants the legal competence for the adoption of the Implementing and Delegated Regulations, both accompanied by Annexes with more details on technical requirements. It’s to be supplemented by acceptable means of compliance (AMC) and guidance (material) currently available in a draft version.

It is also the instrument’s declared aim to establish three foundations for the upcoming development of airspace for urban UAS operations (“U-Space”), being registration, geo-awareness and remote identification.

**Open, Specific or Satisfied**

As a cornerstone of the EU UAS-rules, the Implementing Regulation defines the three main categories for UAS operations.

**“THIS SHIFT OF COMPETENCE FROM MEMBER STATES TO THE EU FOR PRACTICALLY ALL NON-MILITARY AIRCRAFT INDEED MARKS THE BASIS FOR ALL FUTURE HARMONIZATION IN LAW REGARDING UNMANNED AIRCRAFT WITHIN THE UNION.”**

**“OPEN”:** At this point of the legislative process, only the “open” category has been finalized in great detail. Under it, unmanned aircraft may be operated without authorization. For this, all three operational aspects—technical/characteristics/operator—have to comply with the requirements specified for the “open” category. To not limit access to this category too much while still applying the operation-centric and risk-based approach, three sub-categories (A1 to A3) are in turn linked to five different classes of unmanned aircraft (C0 to C4), based on their MTOM and the three operational aspects. Only if the combined requirements are fulfilled can the operation be considered to fall in the “open” category and commence without further authorization. Otherwise, the operation will be subject to the “specific” or even the “certified” category.

**“SPECIFIC”:** Authorization under this category requires the UAS operator to undertake and submit an individual risk assessment of the planned operation to the competent local authority, unless the operation can be shown to comply with a “standard scenario.” Such a declaration of compliance with this scenario then merely needs to be verified by the local authority for completeness, and operations can start right away. While anxiously awaited by the drone community, the “standard” scenarios, which also include beyond visual line of sight operation (BVLOS), are currently not published in Appendix 1 to the Annex of the Implementing Regulations. Nevertheless, already interesting is the possibility to either receive authorizations for a number of operations specified in time and/or location(s) or to make declarations based on national “standard” scenarios that may fill the lacunae for as long as this level of scenario is not adopted on the European level. Also of interest for professional drone users is the possibility for legal entities to obtain a so-called “light UAS operator certificate” (LUC) for one-time authorizations for companies that regularly use UAS in specific scenarios.

**“CERTIFIED”:** Category rules have also not yet been provided in detail, but this third category can be expected to apply to heavyweight operations, typically in high-risk scenarios comparable to current manned aviation, including the transport of people and carriage of dangerous goods. Accordingly, it will not only require certification of the UAS but also of the UAS operator and, where applicable, the licensing of the remote pilot.

**Registration Requirements**

The Implementing Regulation also introduces registration requirements.
All “UAS operators whose operation may present a risk to safety, security, privacy and protection of personal data or environment” are subject to registration. UAS operators have to register themselves—not the drone as such—when operating a UAV that weighs at least 250 grams or flies so fast that the kinetic impact energy exceeds 80 joules, or which is equipped with sensors able to capture data unless it complies with Directive 2009/48/EC on the safety of toys. The directive generally considers toys as products “designed or intended, whether or not exclusively, for use in play by children under 14 years of age.”

Accordingly, any professional UAS operator will have to undergo registration and display its registration number on every drone of its fleet. In case the UAS operator is a legal person, the principal place of business is the state of registration. Otherwise, the place of residence is decisive for determining the state of registry. A UAS operator can only be registered in one state at a time. Only drones that must be certified receive an individual registration mark in line with ICAO requirements.

The Implementing Regulation also determines a minimum age for remote pilots of 16 years, while class C0 drones that are toys according to the Directive, privately built drones of MTOM less than 250 grams and drones operated under supervision of a remote pilot aged 16 years and above may be operated without age limit. Applying the risk-based approach, member states are further allowed to lower the age limit by up to four years in the “open” category and up to two years for the “specific” category, in which case the operation of such lower-aged remote pilots is restricted to that member state’s territory. This concession to greater flexibility for member states may somewhat contravene the intended harmonization.

**Commission Delegated Regulation**

The Commission Delegated Regulation and its Annex are particularly relevant for manufacturers, importers and distributors of UAS who wish to introduce them onto the EU market. It lays down the requirements for UAS design and manufacturing. This includes conformity assessment with CE markings but also the detailed characteristics of the five classes of UAS subject to the open category, as addressed in the Regulation’s Annex. An unmanned aircraft introduced onto the EU market will have to be labeled according to its class requirements. The Annex also provides important information for professional operators and remote pilots about the drone characteristics, which are an important element for determining the boundaries for operation and thus the subcategory subject to the Implementing Regulation.

**Commercial Operations and Drone Pilots**

The Implementing Regulation holds the most relevant provisions for drone operators and remote pilots. While the class of a UAS has to be determined by the manufacturer, here the relevance of the Delegated Regulation mainly lies in referencing the exact technical details and characteristics of a drone class when determining operational requirements. Although definitions of key terms are spread out, the various Regulations, and their coherence, is preserved:

- **“UA”** means any aircraft operating or designed to operate autonomously or to be piloted remotely without a pilot on board;
- **“UAS”** means an unmanned aircraft and the equipment to control it remotely;
- **“UAS OPERATOR”** means any legal or natural person operating or intending to operate one or more UAS.

According to recital (20) of the Implementing Regulation, “UAS operators and remote pilots should ensure that they are adequately informed about applicable Union and national rules relating to the intended operations, in particular with regard to safe—

---

**Drone Classification Pictograms**

A sample of the required pictogram for drone classification, which needs to appear on the drone itself. This label shows that the drone may be used in the “open” category and, depending on the class number, also helps to determine the subcategory it may be operated under.
ty, privacy, data protection, liability, insurance, security and environmental protection.” Accordingly, it is not sufficient to be aware of the requirements subject to air law and UAS regulations. Both the UAS operator and the individual remote pilot on a case by case basis need to be aware of all legal implications of the operation. With reference to privacy and data protection, the awareness even has to expand to the purpose of the operation and the (later) processing of the data as already intended. In principle, establishing the organizational set-up and the adequate procedures and limitations for the type of operation and risk involved is allocated to the UAS operator, whereas the remote pilot is responsible for ensuring compliance when starting a specific UAS operation.

Operator Ramifications
If an operator already has a drone, he should look out for the drone’s class identification label. The drone classification should be affixed to the drone itself, recognizable by the pictograms required under the Annex of the Delegated Regulation (see figure page 44). Such labeling shows that the drone may be used in the “open” category and, depending on the class number, also helps to determine the subcategory it may be operated under.

If the drone has no such identification label, possibly because it was acquired before the Regulation was applicable, the UAS operator should be able to determine the class himself by applying the drone’s technical specifications. At the end, the class identification only serves as an easy reference point for determining the drone-related element of the categorization. If the drone is operated beyond the limitations applicable to the specified class, these should have to take precedence for determining the category of operations.

Following classification, the characteristics of the intended operation have to be determined. These will further help to identify the categorization and subcategory applicable. Depending on the outcome, the competency requirements of the remote pilot can be defined. Operation of class C0 unmanned aircraft in subcategory A1 merely requires familiarization with the user’s manual of the UAS. Any other operation of UAS and classes require the remote pilot to pass online examinations whose complexity increases with number of the subcategory. For the “specific” category, the authority determines the remote pilot’s competency requirements.

As with the lack of standard scenarios, the pilot requirements for the “specific” category are yet unknown. For subcategory A1 of the Annex of the Implementing Regulation, there are 40 multiple choice questions on the subjects relevant to operations. For subcategory A2 and A3, the remote pilot also has to hold a certificate of remote pilot competency issued by the competent authority or by an entity recognized by the competent authority of the member state of registration of the UAS operator. This requires answering additional multiple-choice questions, self-practical training and ability to fulfill certain in-flight requirements. Especially the
The EU UAS “Harmonization” Timeline

<table>
<thead>
<tr>
<th>DATE</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 2018</td>
<td>The Basic Regulation of the European Aviation Safety Agency (EASA) extends the organization’s rule-making competence for “unmanned aircraft” to cover those with an operating mass of less than 150 kg.</td>
</tr>
<tr>
<td>February 28, 2019</td>
<td>The EASA Committee approves the European Commission proposal for The Implementing Regulation, regulating UAS operations in Europe and the registration of drone operators and certified drones.</td>
</tr>
<tr>
<td>February 28, 2019</td>
<td>EASA announces being “one step closer to harmonized rules for safe drone operations in Europe.”</td>
</tr>
<tr>
<td>March 12, 2019</td>
<td>The Delegated Regulation is adopted by the European Commission and sent to legislative bodies, the EU Parliament and the Council. It defines technical requirements for drones brought to the EU market.</td>
</tr>
<tr>
<td>Summer 2019</td>
<td>The Implementing and the Delegating regulations are scheduled to be published.</td>
</tr>
<tr>
<td>2022</td>
<td>The legal framework for drones within the EU is to become fully applicable.</td>
</tr>
<tr>
<td>Summer 2022</td>
<td>Likely date for lapsing of recent operator documents based on national law, with the above EU regulations taking their place.</td>
</tr>
</tbody>
</table>

requirements for subcategory A3 are very extensive while still being subject to concretization by the member states.

Across Borders, Beyond Registration States

Given that no additional authorization is required for operations subject to the “open” category, cross-border operations within the EU complying with the requirements of the respective subcategory should also not require authorizations. According to the Annex of the Implementing Regulation, the capacity requirements are linked to the member state of registration of the UAS operator. As stated above, remote pilots that exceptionally benefit from a lowered minimum age are only then restricted to operations in this specific member state. This suggests a concept of mutual recognition in general. However, it does not excuse the remote pilot from familiarization with the local geographical and also legal requirements beyond air law. In practice, this aspect may still be a limiting factor for cross-border operations.

For operations subject to the “specific” category, the other EU member state is required to assess the operational authorization already granted by the member state of registration to the UAS operator and report back on the adequacy of the risk mitigation measures for the intended location. The UAS operator requires prior confirmation by the other member state. The Implementing Regulation suggests that such confirmation may only be refused if the mitigation measures contained in the authorization are not satisfactory or have not been updated for the intended location.

THE NEW LEGAL ACTS ARE HIGHLY COMPLEX AND INTRODUCE MUCH DETAIL FOR DRONE OPERATIONS, IN MANY WAYS EXCEEDING THE COMPLEXITY OF RULES CURRENTLY ESTABLISHED ON THE MEMBER STATES’ LEVEL.

Unfortunately, there is little guidance if and, in case, on what grounds a recognition of an existing authorization can be rejected and, in case, how such rejection may be challenged. It is difficult to conceive that a member state would recognize any authorization by another member state unless based on a standard scenario given that all national laws that may be affected by the operation have to be considered. However, if the intended operation is in line with a standard scenario, a mere declaration of compliance by the UAS operator is sufficient anyhow.

Third-Country Operators

Aside from intra-European drone operations, UAS operators from third countries may be interested in using their drones within the EU. For such cases the Delegated Regulation states that the Implementing Regulation fully applies. The competent authority for the third-country UAS operator shall be that of the first member state where the UAS operator intends to operate. In addition, the Delegated Regulation states that the competent authority for the operations within, to and out of the Union may recognize existing certificates on remote pilot competency. This, however, requires that (i) the third country asked for such recognition, (ii) the certificate of the remote pilot competency or the UAS operator’s certificate are valid documents of the state of issue and (iii) the European Commission, after consultation of EASA, has ensured that the requirements for issuance provide the same level of safety as the Delegated Regulation.

The LUC Certificate

The “light UAS operator certificate”—LUC—provides a convenient method for UAS operators to obtain a general authorization for operation scenarios under the “specific” category, which would otherwise be subject to individual authorizations. The LUC requires the presentation and upholding of a detailed management and organization structure within an undertaking, which needs to be precisely described in a LUC manual made available to all relevant personnel. Accordingly, the LUC is limited to legal persons. The LUC also has to contain the remote pilot’s capacity requirements applicable for the operation subject to the LUC.

A LUC is unlimited in duration, provided the scenarios are maintained.
The question only arises for “open” category operations, since operations in all other categories will be subject to specific authorizations requirements, anyhow. According to Article 20 of the Implementing Regulation, UAS types that do not comply with Delegated Regulation’s requirements and that are not privately built are allowed to continue operations when they have been placed on the market three years after the date of entry into force of the Delegated Regulation, when subject to subcategory A1 and MTOM less than 250 grams or subcategory A3 with MTOM less than 25 kilograms.

Harmonization Achieved?

Referencing the declaration on 28 February 2019, it can be summarized that indeed another great step towards harmonization of UAS operational rules in the EU has been made. The development has, however, not reached the finish line yet, and a number of issues still need to be successfully resolved for a “mission accomplished” verdict. Art. 56(8) of the Basic Regulation and recital (18) of the Implementing Regulation imply an opening for member states to lay down national rules covering public security, privacy protection or environmental concerns. Possibilities may range from prohibition to operational restrictions to use of equipment such as remote identification systems or geo awareness systems. Furthermore, many elements, such as the content of remote pilot competency requirements and the standards for the electronic registers to be created by member states, have to be defined. The complexity of these tasks should not be underestimated, not to mention the still unpublished standard scenarios that will form the backbone for the efficiency when applying the “specific” category. It is therefore not surprising that comments of industry stakeholders published on the Commission website support the overall aim of harmonization but also warn of national particularism that may yet contravene the effort. Analysis will continue concerning how the quite significant “white spots” in the framework of EU UAS regulations will be filled in the coming months.

Authors

Oliver Heinrich is co-founder and partner with BHO Legal, a boutique law firm based in Cologne, Germany, with a focus on aerospace and high-technology projects. Oliver studied German and Anglo-American law at the Universities of Trier and Cologne. He wrote his doctoral thesis at the Institute of Air and Space Law at the University of Cologne on national and European research funding. Prior to working as an attorney, Oliver worked in the contracts department of the German Aerospace Centre, DLR, and then as DLR’s project manager for the European Satellite Navigation System Galileo at DLR and legal manager for a joint venture of DLR, EADS Astrium (now Airbus DS), T-Systems and a Bavarian bank.

Jan Helge Mey is a partner with BHO Legal. Jan studied in Cologne and Qingdao (PR China) and specialized in air and space law at McGill University in Montréal (Canada). He went on to work at the Institute of Air and Space Law of the University of Cologne. After completion of the legal traineeship that led him to the German Aerospace Center, Jan worked as lawyer, mainly in the field of public procurement, public commercial law, foreign trade law and public-private partnerships.
GNSS positioning is strongly challenged in urban canyon areas. The signal reflection induces multipath and non-light-of-sight (NLOS). These signal blockages and reflections are caused by the obstacles of signal transmission between the satellites and receiver. The obstacles can be buildings, trees and even a high-rise vehicle such as double-decker buses. Interestingly, they are the obstacles in urban traffic scenes. Inspiring from this, the authors propose an innovative sensor integration scheme to aid GNSS single point positioning (SPP). Taking the uprising autonomous driving as an example, instead of simply using LiDAR odometry to provide receiver movement between two data epochs, we make use of the objects detected by LiDAR and describe them in the representation of relative azimuth and elevation angles to the receiver. According to this experiment’s results, the proposed perceived environment aided GNSS SPP can improve 35% comparing to conventional weighted least square (WLS).

WEISONG WEN
LI-TA HSU
HONG KONG POLYTECHNIC UNIVERSITY, HONG KONG

A

utonomous driving introduces high demand in GNSS in all driving environments. Currently, GNSS performance is heavily challenged in deep urban canyons. The positioning error can go up to even 100 meters, due to the notorious non-line-of-sight (NLOS) receptions which dominates the GNSS positioning errors in dense-building areas (see Hsu 2018 in Additional Resources). The conventional solution is to integrate GNSS with other on-board sensors including, inertial navigation systems (INS), vehicular odometry, and vehicular steering. More recently, more sensors are installed on the future intelligent vehicle as shown in Figure 1. Thus, visual odometry and LiDAR odometry are also integrated with GNSS now.

The level of integration is usually classified based on how “raw” the measurement is that is provided by GNSS. For example, the position and velocity are treated as loosely coupled, the pseudoranges and its rates are as tightly coupled, and I/Q correlator outputs are as ultratightly coupled integration. However, these integration schemes are purely considering that other sensors can only provide the system propagation in position and orientation of the vehicle.

However, one opportunity has been neglected. Other than LiDAR and vision odometry, both LiDAR scanners and cameras are also used to detect surrounding objects to avoid collisions. In the other words, they can perceive the surrounding environment of a GNSS receiver in a real-time manner. This means the vehicle can obtain the location of the surrounding objects including trees, buildings and vehicles as shown in Figure 2. This article dem-
onstrates the use of a LiDAR scanner to describe the perceived environment. According to the relative positions between the detected obstacles and ego-vehicle, their boundaries can be represented in the GNSS skyplot. Thus, we propose a new GNSS/LiDAR integration scheme to aid the GNSS single point positioning (SPP) as shown in Figure 3. Both the 3-D LiDAR and INS are employed to help the SPP.

How can this perceived environment be used to aid GNSS SPP? The intuitive idea is to exclude the NLOS affected measurements from the GNSS positioning. The exclusion of NLOS measurement is very effective in less-urbanized areas. It is not the case in deep urban canyons. The dilution of precision (DOP) will be easily distorted and enlarged if excluding all the NLOS measurements received in the urban canyons as illustrated in Figure 4. Obviously, enormous NLOS measurements are received and only five LOS measurements. If we exclude all the NLOS measurements, the GPS SPP will deteriorate from 92 to 169 meters and HDOP is increased from 0.9 to 3.15. This discussion has been well-discussed in 3-D mapping aided (3DMA) GNSS (Groves 2016, Additional Resources). In fact, the famous GNSS shadow matching is proposed to deal with the same problem. The shadow
matching faces other challenges as mentioned in (Groves 2012, Additional Resources). The recent state-of-the-art range-based 3DMA GNSS can correct most of the pseudorange measurement affected by NLOS receptions (see again Hsu 2018 in Additional Resources). However, the computational load of the ray-tracing simulation is immense as the simulations are required in each hypothesized position. In addition, an accurate prior-known receiver position is required by the 3DMA GNSS. To address these two issues, as an example, we present a novel method to detect the GNSS signal blockage caused by surrounding buildings and correct the NLOS pseudorange measurements based on the perceived environment features by the sensors installed on autonomous driving vehicles.

Methodology
To estimate the geometry and pose of the buildings relative to GNSS receiver, a surface segmentation method is employed to detect the surrounding building walls using LiDAR 3-D point clouds. The building boundaries are extracted and extended by the building height in a skyplot to identify the NLOS affected ones from all the measurements. Innovatively, the NLOS delay in pseudorange can be modelled and corrected. Weighted least square (WLS) is used to cooperate the corrected NLOS and healthy pseudorange measurements. Figure 5 shows the flowchart of the proposed method.

The steps of the proposed method are as follows:

**STEP I: Building Surface Identification and Extension**
To detect the top edges of buildings (TEBs) and obtain the corresponding distances between the GNSS receiver and buildings, a point cloud segmentation method is employed to implement the building surface detection. To distinguish the building surface from the unordered points set and determine the distance from GNSS receiver to the building surface, two steps are needed: the segmentation and building surface identification. The segmentation and surface identification are described in detail as shown in Algorithms 1 and 2 in the paper by Wen, et alia in Additional Resources, respectively. The output of Algorithm is the points clusters shown in the left-hand side of Figure 6 and we do not know which cluster belongs to the buildings class. The segmentation in Algorithm 1 clusters the points into bounding box $U_i$ which can be described as following:

$$U_i = [x_i, y_i, z_i, \text{roll}_i, \text{pitch}_i, \text{yaw}_i, d_{\text{left}}, d_{\text{right}}, d_{\text{front}}, d_{\text{back}}]$$ (1)

where $x_i$, $y_i$, and $z_i$ denote the position of the bounding box in $x$, $y$, and $z$ directions in LiDAR coordinate system, respectively; $\text{roll}_i$, $\text{pitch}_i$, and $\text{yaw}_i$ denote the orientation of bounding box in LiDAR coordinate system. $d_{\text{left}}$ is the length, $d_{\text{right}}$ is the width and $d_{\text{front}}$ is the height of the bounding box.

To effectively identify the bounding box representing the building surface which can result in GNSS signal reflection and subsequent NLOS receptions, building surface identification method is needed. By the Algorithm 2, the building surface can be identified shown in the middle of Figure 6. The height of the bounding box representing building surface can be extended to the real one. In fact, this building height extension can be omitted if a sky-pointing camera is used (Suzuki and Kubo, Additional Resources).

The bounding box is extended from rectangle ABCD to rectangle CDEF as can be seen in the right-hand side of Figure 6. Then, the boundary parameters for the bounding box $B_i$ corresponding to building surface are denoted by line segment $EF$ denoted as $B_{\text{build}}$ in the matrix of the boundary. To represent the building, two points, $E$ and $F$, are required. The $B_{\text{build}}$ is structured as follows:

$$B_{\text{build}} = \begin{bmatrix} x_{\text{left}} & y_{\text{left}} & z_{\text{left}} \\ x_{\text{right}} & y_{\text{right}} & z_{\text{right}} \end{bmatrix}$$ (2)

In this case, the TEBs of the buildings represented by the $B_{\text{build}}$.

**STEP II: Projecting the Top Edges of Buildings into a GNSS Skyplot**
To detect NLOS, visibility of satellite needs to be determined based on the extended TEBs ($B_{\text{build}}$). The relative position of the GNSS receiver to satellites and to building surfaces needs to be transformed into the same representation, the Skyplot. Satellite position can be easily indicated in the Skyplot representation based on corresponding elevation and azimuth angles. A transformation matrix should be employed for building surface boundaries transformation from 3 dimensions coordinate to 2 dimensions coordinate. The transformation is conducted as the following formula.

$$B_{\text{sky}} = B_{\text{build}} G_{\text{sky}} = \begin{bmatrix} x_{\text{sky}} \\ y_{\text{sky}} \end{bmatrix}$$ (3)
where $B_{\text{build}}$ denotes the matrix of bus boundary mentioned earlier. $G_{\text{build}}$ is a 3x2 transform matrix. After the transformation, satellites and building surface boundary can be presented in the same coordinate. Line segment $EF$ represents the building surface boundary corresponding to line segment $FP$ as shown in Figure 7. Then, the azimuth and the elevation angles for point E, and F can be calculated in the Skyplot respectively.

**STEP III: NLOS Correction Based on Detected TEBs**

Considering satellites’ elevation angle, azimuth angle and building boundary information (elevation and azimuth angles in Skyplot), satellite transmissions blocked by building are detected. Then, NLOS correction is implemented with a NLOS error model consequently. In terms of the measurements from a GNSS receiver, each pseudorange measurement $\rho_n$ is written as follows:

$$\rho_n = R_n + c(\delta \tau^r_i - \delta \tau^a_n) + I_n + T_n + \varepsilon_n \quad (4)$$

where $R_n$ is the geometric range between the satellite and the GNSS receiver. $\delta \tau^r_i$ denotes the satellite clock bias. $\delta \tau^a_n$ indicates the receiver clock bias. $I_n$ represents the ionospheric delay distance; $T_n$ indicates the tropospheric delay distance. $\varepsilon_n$ represents the errors caused by the multipath effects, NLOS receptions, and receiver noise. We focus on mitigating the NLOS errors. The NLOS error model proposed in the paper by Hsu, 2018 is expressed in Figure 8. The expected signal transmission route is expressed as dash blue line in Figure 8. The distance from receiver to the building $a$ represents the distance from receiver to the building. $\theta_{\text{ele}}$ represents the elevation angle of GNSS signal. Assuming the building is vertical to the ground and GNSS signal reflection satisfied the law of reflection. As a result, the NLOS error can be calculated based on the azimuth angle, elevation angle and the distance from the receiver to the building causing the reflection. The process of NLOS correction is summarized in detail in Algorithm 3 in Wen, et alia.

$$\varepsilon_{\text{nlos}} = a(\sec \theta_{\text{ele}} (1 + \cos 2\theta_{\text{ele}}) + \sec \theta_{\text{ele}} (1 + \cos 2\theta_{\text{ele}})) \quad (5)$$

**STEP IV: GNSS Positioning Based on Corrected Pseudorange Measurement**

In this step we implemented GNSS WLS based on the corrected NLOS and healthy pseudorange measurements. Measurements with low elevation angle and SNR are more likely to be a contaminated GNSS signal, such as the multipath or NLOS, due to the reflection, blockage, and diffraction. Thus, proper thresholds need to be set to exclude the unhealthy measurements. The weighting scheme follows the suggestions from Herrera, et alia in the paper in Additional Resources.

**Experiment Setup and Result**

Experiments are conducted in a typical urban canyon of Hong Kong, and the experimental scene is shown in Figure 9. The Skymask in the right-hand side demonstrates the degree of urbanization. In the experiment, a receiver is used to collect raw GPS and BeiDou measurements, while a 3-D LiDAR sensor is employed to provide the real-time 3-D point clouds scanned from the surroundings. Both the receiver and the 3-D LiDAR are installed on the top of an experiment vehicle, which can be seen in left-hand side of Figure 7. The data were collected...
at a frequency of 1 Hz for GNSS and 10 Hz for the 3-D LiDAR. In addition, a GNSS RTK/INS (fiber optic gyroscopes) integrated navigation system is used to provide the ground truth of positioning. All the data are collected and synchronized using the Robot Operation System (ROS) (Quigley, et alia Additional Resources). Moreover, the coordinate systems of all the sensors are calibrated before the experiments.

Two GNSS positioning methods are compared:
1) WLS: GNSS positioning using the WLS.
2) WLS-NC: GNSS positioning using the WLS and all the detected NLOS receptions are corrected.

**Result of Building Detection using LiDAR**

**Figure 10** shows the perception result using LiDAR-based perception, namely point clouds segmentation. The colored points denote the 3-D point clouds from 3-D LiDAR sensor. The 3-D bounding boxes represent the detected buildings using the proposed method presented in Section 2. The 2-D black boxes denote the surrounding dynamic objects which are manually labeled, such as the vehicles and pedestrians. In practical use, the excessive dynamic objects can pose difficulty on the accuracy of building detection. Due to the blockage from surrounding buildings, the GNSS NLOS measurements occurred, and is shown in the bottom panel of **Figure 10**.

In practices, the building can be mis-detected which can be seen in bottom panel of **Figure 11**. The bounding box that expected to be detected is B. However, the detected bounding box is A, the main reason behind this is that the excessive dynamic objects can block the field of view (FOV) of the 3-D LiDAR and only limited part of the buildings are detected by 3-D LiDAR. As mentioned in Section 2, the 3-D LiDAR play two significant roles in the proposed method: 1) detect the buildings for satellite visibility classification; 2) ranging the distance between the GNSS receiver and potential signal reflector. According to our recent research (Xiwei, Additional Resources), we make use of the camera to capture the sky view and hence the satellite visibility can be identified. As both the camera and 3D LiDAR are indispensable sensors for the realization of autonomous vehicles, we can leverage both the LiDAR-based perception and camera to help the GNSS positioning.

**Result of the Perceived Environment Aided GNSS Positioning**

**Figure 12** and **Table I** show the positioning results comparisons of the conventional LS, WLS and the proposed method (WLS-NC). As can be seen from **Table I**, GNSS positioning accuracy is gradually improved with increased constraints. **Figure 12** shows positioning error during a closed-loop test. The red line represents...
the result using WLS method with the mean positioning error of 10.23 meters. However, the positioning error can go up to more than 30 meters in some epochs which can be seen in Figure 12. After applying the proposed perception aided NLOS correction method, the mean positioning error decreases to 7.81 meters. Moreover, all the positioning errors are less than 30 meters. The trajectory during the test is shown in Figure 13. In the left-hand and right-hand side of the trajectories, the degree of urbanization is shown using corresponding skymask which presents only very limited sky visibility.

As the NLOS correction is not available all through the test, the Figure 14 shows the trajectories only when the NLOS correction is applied. We can find that majority of the NLOS corrections occurred when the experimental vehicle drives past the dense street shown in Figure 13. Table II shows the GNSS positioning results. We can find that the mean GNSS positioning error decreasing to 7.13 meters. Moreover, the standard deviation also decreases slightly with the assist of the proposed method. Interestingly, we can find that the mean positioning error using the WLS method increases slightly from 10.23 meters in Table I to 11.01 meters in Table II. This means that the applied weighting scheme performs worse in more dense urbanized scenarios (the two dense streets are shown in Figure 13). The improved GNSS positioning results shows the effectiveness of the proposed perception aided GNSS positioning method. The proposed method relies on the result of the object detection (building detection in this paper). With the increasing perception accuracy over time, more and more environmental information can be perceived with the on-board sensors of autonomous driving vehicles. The proposed method can perform better in improving the performance of GNSS positioning.

Conclusions, Future Work
In this article, the authors demonstrate the use of LiDAR perception to aid GNSS SPP. First we detect the building using the LiDAR point cloud data and extend its height according to the height list. Then,
the NLOS measurement is identified and corrected using the NLOS error model. The evaluated results show that the proposed method can improve GNSS positioning accuracy compared to that of WLS.

Table III is given to compare the proposed perceived environment aided GNSS with different state-of-the-art GNSS urban positioning methods. The methods in the first three rows make use of 3-D mapping database to improve the positioning method. Hence, all of them require the prior information of the receiver’s location to provide accurate GNSS positioning results. The proposed method requires extra sensor comparing to the 3DMA GNSS. However, these sensors are existing in most of the autonomous driving vehicles. In addition, the perception on obstacles detection is also used for the purpose online path and motion planning. The computation load for the proposed GNSS SPP is similar to that of the conventional WLS. Last but not the least, the LiDAR can provide the lateral distance which can be used to correct NLOS affected pseudorange measurement. Therefore, the HDOP remains unchanged for the proposed GNSS SPP.

The goal of this article is to raise the awareness of the perceived environment by LiDAR or camera can be used to aid positioning because the positioning sensors could be affected by the surrounding environments. Other than this demonstrated LiDAR-aided GNSS SPP, there are several setups that can use the same idea. For example, assembling the images collected from 360 degree cameras to describe the obstacles in the skyplot representation. This skyplot with obstacles can be used to identify GNSS NLOS measurement. This perceived environment aided idea can also apply to aid LiDAR positioning based on the perceived obstacles by image processing. We will work on the research of the dynamic objects removal for LiDAR positioning in the near future.

Acknowledgments
The authors acknowledge the support of Hong Kong PolyU startup fund on the project 1-ZVKZ, “Navigation for Autonomous Driving Vehicle using Sensor Integration.”

<table>
<thead>
<tr>
<th>METHODS</th>
<th>3-D MAPS</th>
<th>EXTRA SENSORS</th>
<th>NLOS CORRECTION</th>
<th>PRIOR INFORMATION</th>
<th>HDOP</th>
<th>COMPUTATION LOAD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Satellite Visibility Prediction</td>
<td>✓</td>
<td>×</td>
<td>Exclusion</td>
<td>✓</td>
<td>Increase</td>
<td>Low</td>
</tr>
<tr>
<td>GNSS Shadow Matching</td>
<td>✓</td>
<td>×</td>
<td>Do not use pseudorange</td>
<td>✓</td>
<td>Do not use pseudorange</td>
<td>Low</td>
</tr>
<tr>
<td>Ray-Tracing based 3DMA GNSS</td>
<td>✓</td>
<td>×</td>
<td>Correction</td>
<td>✓</td>
<td>Not changed</td>
<td>High</td>
</tr>
<tr>
<td>Perceived Environment Aided GNSS Single Point Positioning</td>
<td>×</td>
<td>✓“√”*</td>
<td>Correction</td>
<td>×</td>
<td>Not changed</td>
<td>Low^</td>
</tr>
</tbody>
</table>

* They are existing sensors in most of the autonomous driving vehicles.
^ The LiDAR based object detection is not considered as computation load for the proposed GNSS SPP since the object detection is essential and existed in autonomous driving vehicles.
Manufacturers
In the Experiment Setup and Result section of this article, the receiver used to collect raw GPS and BeiDou measurements, is the M8T from u-blox (Thalwil, Switzerland), while the 3-D LiDAR sensor, the Velodyne 32, is from Velodyne (San Jose, California, USA). In addition, the NovAtel SPAN-CPT, GNSS RTK/INS (fiber optic gyroscopes) integrated navigation system from NovAtel (Calgary, Canada) is used to provide the ground truth of positioning.

Additional Resources
(5) L.-T. Hsu, S. Miura, S. Kamijo Street Smart: 3D City Mapping and Modeling for Positioning with Multi-GNSS, GPS World.
(8) W. Wen, G. Zhang and L.-T. Hsu (2018), Correcting GNSS NLOS by 3D LiDAR and Building Height. ION GNSS+ 2018, Miami, Florida, USA.

Authors
Weisong Wen is currently a Ph.D. candidate at Department of Mechanical Engineering, Hong Kong Polytechnic University. In 2018, He was a visiting student in mechanical system laboratory in University of California, Berkeley. His research interests include perceived environment aided GNSS positioning and multi-sensor integrated localization for autonomous driving.

Li-Ta Hsu received B.S. and Ph.D. degree in Aeronautics and Astronautics from National Cheng Kung University, Taiwan, in 2007 and 2013, respectively. He is currently an Assistant Professor in the Interdisciplinary Division of Aeronautical and Aviation Engineering at The Hong Kong Polytechnic University. His research focus is GNSS positioning and signal processing in challenged environments.
New-Age Satellite-Based Navigation

STAN: Simultaneous Tracking and Navigation with LEO Satellite Signals

Today’s vehicular navigation systems couple global navigation satellite system (GNSS) receivers with an inertial navigation system (INS). Low Earth orbit (LEO) satellite signals are a particularly attractive INS aiding source in GNSS-challenged environments. Over the next few years, LEO satellites will be abundantly available at favorable geometric configurations and will transmit in several frequency bands, making them an accurate and robust navigation source. This article presents a framework that enables a navigating vehicle to aid its INS with pseudorange and Doppler measurements drawn from LEO satellite signals when GNSS signals become unusable, while simultaneously tracking the LEO satellites. This simultaneous tracking and navigation (STAN) framework is demonstrated in realistic simulation environments and experimentally on a ground vehicle and on an unmanned aerial vehicle (UAV), showing the potential of achieving meter-level-accurate navigation.

Resilient and accurate positioning, navigation, and timing (PNT) is of paramount importance in safety critical cyber-physical systems (CPS), such as aviation and transportation. As these CPS evolve towards becoming fully autonomous, the requirements on their PNT systems become more stringent than ever before. With no human in-the-loop, an inaccurate PNT solution; or more dangerously, PNT system failure, could have intolerable consequences.

Today’s vehicular navigation systems couple GNSS receivers with an inertial navigation system (INS). By coupling both systems, one takes advantage of the complementary properties of the individual subsystems: the short-term accuracy and high data rates of an INS and the long-term stability of a GNSS PNT solution to provide periodic corrections. However, in the inevitable event that GNSS signals become unreliable (e.g., in deep urban canyons or near dense foliage), unusable (e.g., due to unintentional interference or intentional jamming), or untrustworthy (e.g., due to malicious spoofing attacks or system malfunctions), the navigation system relies on unaided inertial measurement unit (IMU) data, in which case the errors accumulate and eventually diverge, compromising the vehicle’s efficient and safe operation.

Signals of opportunity are PNT sources that could be used in GNSS-challenged environments (See Merry et alia, and Kassas, 2013, in Additional Resources). These signals include AM/FM radio, cellular, digital television, and low Earth orbit (LEO) satellites (several papers listed in Additional Resources provide further details). Signals of opportunity have been demonstrated to yield a standalone meter-level-accurate navigation solution on ground vehicles and a centimeter-level-accurate navigation solution on aerial vehicles. Moreover, these signals have been used as an aiding source for LiDAR and INS.

LEO satellites are particularly attractive aiding sources for an INS in GNSS-challenged environments for several reasons. First, LEO satellites are around 20 times closer to Earth compared to GNSS satellites that reside in medium Earth orbit (MEO), making LEO satellites’ received signals significantly more powerful. Second, LEO satellites orbit the Earth at much faster rates compared to GNSS satellites, making LEO satellites’ Doppler measurements attractive to exploit. Third, the recent announcements by OneWeb, Boeing, SpaceX (Starlink), Samsung, Kepler, Telesat, and LeoSat to provide broadband internet to the world via satellites will collectively bring thousands of new LEO satellites into operation, making their signals abundant and diverse in frequency and direction. Figure 1 depicts a subset of existing and future LEO satellite constellations.

Figure 1 Existing and future LEO satellite constellations.
Table 1 summarizes the number of satellites and the transmission band of each constellation.

Figure 2 depicts a snapshot of the upcoming Starlink constellation, while Figure 3 is a heat map of the number of visible Starlink LEO satellites above an elevation mask of 5 degrees.

Figure 5 is a heat map showing the position dilution of precision (PDOP) for the Starlink constellation, while Figure 5 is a heat map showing the logarithm of the Doppler position dilution of precision (DPDOP).

Figure 2 through Figure 5 together with Table 1 demonstrate the potential of using LEO satellite signals for PNT and imply that the commercial space industry is inadvertently creating new PNT sources, which could be utilized by future vehicles to make the vehicle’s PNT system more resilient and accurate. For example, a Tesla connected to Starlink satellites could dually provide a passenger with internet access, as designed, while also enabling the vehicle to navigate in GNSS-challenged environments.

There are several challenges that need to be addressed to exploit LEO satellites for navigation. First, their positions and velocities must be known. The position and velocity of any satellite may be parameterized by its Keplerian elements. These elements are tracked, updated once daily, and made publicly available by the North American Aerospace Defense Command (NORAD) [see North American Aerospace Defense Command, Additional Resources]. However, these elements are dynamic and will deviate from their nominally available values due to several sources of perturbing forces, which include non-uniform Earth gravitational field, atmospheric drag, solar radiation pressure, third-body gravitational forces (e.g., gravity of the Moon and Sun), and general relativity (Vetter, Additional Resources). These deviations can cause errors in a propagated satellite orbit as high as 3 kilometers if not accounted for with corrections. Second, LEO satellites are not necessarily equipped with an atomic clock, nor are they precisely synchronized. Subsequently, their clock error must be known alongside their position and velocities. In contrast to GNSS, where corrections to the orbital elements and clock errors are periodically transmitted to the receiver in the navigation message, such orbital element and clock corrections may not be available for LEO satellites; in which case they must be estimated along with the receiver’s states. Third, ionospheric delay rates become significant for LEO satellites, particularly the ones transmitting in the very high frequency (VHF) band.

<table>
<thead>
<tr>
<th>System</th>
<th>Number of satellites</th>
<th>Frequency band</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orbcomm</td>
<td>36</td>
<td>VHF</td>
</tr>
<tr>
<td>Globalstar</td>
<td>48</td>
<td>S and C</td>
</tr>
<tr>
<td>Iridium</td>
<td>66</td>
<td>L and Ka</td>
</tr>
<tr>
<td>OneWeb</td>
<td>882</td>
<td>Ku and Ka</td>
</tr>
<tr>
<td>Boeing</td>
<td>2956</td>
<td>V and C</td>
</tr>
<tr>
<td>SpaceX</td>
<td>11943</td>
<td>Ku, Ka, and V</td>
</tr>
<tr>
<td>Samsung</td>
<td>4600</td>
<td>V</td>
</tr>
</tbody>
</table>

Table 1: Existing and future LEO constellations: number of satellite and transmission bands.
This article presents a simultaneous tracking and navigation (STAN) framework that addresses the aforementioned challenges (for more, see 2 papers from Morales, et alia). This framework tracks the states of LEO satellites while simultaneously using pseudorange and Doppler measurements extracted from their signals to aid the vehicle’s INS. The performance of the STAN framework is demonstrated in realistic simulation environments and experimentally on a ground vehicle and on an unmanned aerial vehicle (UAV), showing the potential of using LEO-based positioning: (i) satellite position and Doppler measurement model and discusses the sources of error in LEO-based positioning: (i) satellite position and Doppler measurement model and discusses the sources of error in LEO-based positioning:

Pseudorange, Doppler Measurement Model

This section describes the LEO satellite receiver pseudorange and Doppler measurement model and discusses the sources of error in LEO-based positioning: (i) satellite position and velocity errors, (ii) satellite and receiver clock errors, and (iii) ionospheric and tropospheric delay rate errors.

A. PSEUDORANGE AND DOPPLER MEASUREMENT MODEL

The LEO receiver extracts pseudorange \( \rho \) and Doppler frequency measurements \( f_D \) from LEO satellite signals. A pseudorange rate measurement \( \dot{\rho} \) can be obtained from

\[
\dot{\rho} = -\frac{c}{f_c} f_D,
\]

where \( c \) is the speed of light and \( f_c \) is the carrier frequency. The pseudorange \( \rho_m \) from the \( m \)-th LEO satellite at time-step \( k \), which represents discrete-time at \( t_k = kT + t_0 \) for an initial time \( t_0 \) and sampling time \( T \), is modeled as

\[
\rho_m(k) = \lVert r_r(k) - r_{leo}(k_m) \rVert_2 + c \lVert \delta t_r(k) - \delta t_{leo}(k_m) \rVert_2 + c \delta t_{iono}(k) + c \delta t_{trop}(k) + v_{pm}(k), \quad k = 1, 2, \ldots, \tag{2}
\]

where \( k_m \) represents discrete-time at \( t_k = kT + t_0 - \delta t_{trop} \) with \( \delta t_{trop} \) being the true time-of-flight of the signal from the \( m \)-th LEO satellite; \( r_r \) and \( r_{leo} \) are the LEO receiver’s and \( m \)-th LEO satellite’s 3-D position vectors, respectively; \( \delta t_r \) and \( \delta t_{leo} \) are the receiver and the \( m \)-th LEO satellite transmitter clock biases, respectively; \( \delta t_{iono} \) and \( \delta t_{trop} \) are the ionospheric and tropospheric delay rates, respectively, affecting the \( m \)-th LEO satellite’s signal; and \( v_{pm} \) is the pseudorange measurement noise, which is modeled as a white Gaussian random sequence with variance \( \sigma_{t_{pm}}^2 \). The pseudorange rate measurement \( \dot{\rho}_m \) from the \( m \)-th LEO satellite is given by

\[
\dot{\rho}_m = \left[ r_r(k) - r_{leo}(k_m) \right]^T \begin{bmatrix} \delta t_r(k) - \delta t_{leo}(k_m) \\ \delta t_{iono}(k) + c \delta t_{trop}(k) + v_{pm}(k) \end{bmatrix} \tag{3}
\]

where \( r_r \) and \( r_{leo} \) are the LEO receiver’s and \( m \)-th LEO satellite’s 3-D velocity vectors, respectively; \( \delta t_r \) and \( \delta t_{leo} \) are the receiver and the \( m \)-th LEO satellite transmitter clock drifts, respectively; \( \delta t_{iono} \) and \( \delta t_{trop} \) are the drifts of the ionospheric and tropospheric delays, respectively, affecting the \( m \)-th LEO satellite’s signal; and \( \sigma_{t_{pm}}^2 \) is the pseudorange rate measurement noise, which is modeled as a white Gaussian random sequence with variance \( \sigma_{t_{pm}}^2 \).

B. POSITION AND VELOCITY ERRORS

One source of error that should be considered when navigating with LEO satellite signals arises due to imperfect knowledge of the LEO satellites’ position and velocity. This is due to time-varying Keplerian elements caused by several perturbing accelerations acting on the satellite. Mean Keplerian elements and perturbing acceleration parameters are contained in publically available two-line element (TLE) file sets. The information in these files may be used to initialize a simplified general perturbations (SGP) model, which is specifically designed to propagate a LEO satellite’s orbit. SGP propagators (e.g., SGP4) are optimized for speed by replacing complicated perturbing acceleration models that require numerical integrations with analytical expressions to propagate a satellite position from an epoch time to a specified future time. The tradeoff is in satellite position accuracy: the SGP4 propagator has around 3 km in position error at epoch and the propagated orbit will continue to deviate from its true one until the TLE files are updated the following day. Figure 6 shows the accumulated position and velocity error for an Orbcomm LEO satellite (FM 112).

C. CLOCK ERRORS

In contrast to GNSS, LEO satellite clocks are not tightly synchronized and the clock errors (bias and drift) are unknown...
to the receiver. Moreover, LEO satellites are not necessarily equipped with high-quality atomic clocks. From what is known about the existing LEO constellations, LEO satellites are equipped with oven-controlled crystal oscillators (OCXOs). Practically, the navigating receiver will be equipped with a lower quality oscillator, e.g., a temperature-compensated crystal oscillator (TCXO). To visualize the magnitude of the clock errors in the satellite and receiver clocks, Figure 7 depicts the time evolution of the 1-σ bound of the clock bias and drift of a typical OCXO and a typical TCXO, obtained from the so-called two-state clock model (Brown and Hwang, Additional Resources). It can be seen from Figure 7 that the satellite and receiver clock bias and drift may become very significant; therefore, they must be accounted for appropriately.

D. IONOSPHERIC DELAY ERRORS

Most broadband LEO constellations reside above the ionosphere, which in turn will induce delays into their signals. Although LEO satellite signals propagate through the troposphere, its effect is less significant compared to ionospheric propagation. The magnitude of the ionospheric delay rate is (i) inversely proportional to the square of the carrier frequency and (ii) proportional to the rate of change of the obliquity factor, which is determined by the time evolution of the satellite’s elevation angle. Note that the ionospheric delay rates also depend on the rate of change of the total electron content (TEC) at zenith, denoted by TECV. However, TECV varies much slower than the satellite’s elevation angle; hence, its effect may be ignored. The effect of ionospheric propagation is significant on LEO satellite signals since (i) the high speed of LEO satellites translates into very fast changing elevation angles, as shown in Figure 8 and (ii) some of the existing LEO satellites transmit in the VHF band where the signals experience very large delay rates. The aforementioned factors result in large ionospheric delay rates, as shown in Figure 9 for 7 Orbcomm satellites over a 100-minute period.

In order to visualize the effect of (i) the satellite position and velocity errors, (ii) the clock drift error, and (iii) the ionospheric delay rates, the residual error between the measured pseudorange and the pseudorange rate estimated from the satellite position and velocity obtained from TLE files and SGP4 are plotted in Figure 10 for 2 Orbcomm satellites (FM 108 and FM 116).

STAN Framework

To exploit LEO satellite signals for navigation, their states must be known. Unlike GNSS satellites that periodically transmit accurate information about their positions and clock errors, such information about LEO satellites may be unavailable. The STAN framework addresses this by extracting pseudorange and Doppler measurements from LEO satellite to aid the vehicle’s INS, while simultaneously tracking the LEO satellites. The STAN framework employs an extended Kalman filter (EKF) to simultaneously estimate the vehicle’s states with the LEO satellites’ states. Figure 11 depicts the STAN framework.

Simulation Results

This section presents simulation results obtained with a realistic simulation environment demonstrating UAVs navigating via the LEO-aided INS STAN framework without GNSS signals. The first subsection evaluates the achieved performance from current LEO constellations (Globalstar, Orbcomm, and Iridium), while the second subsection evaluates the achieved performance with an upcoming LEO constellation: Starlink.

A. UAV SIMULATION WITH THE GLOBALSTAR, ORBCOMM, AND IRIDIUM LEO CONSTELLATIONS

A UAV was equipped with (i) a tactical-grade IMU, (ii) GPS and LEO satellite receivers, and (iii) a pressure altimeter. The UAV
navigates over Santa Monica, California, USA, for about 25 kilometers in 200 seconds, during which it had access to GPS signals only for the first 100 seconds. After lift-off, the UAV makes 4 banking turns. A total of 10 LEO satellite trajectories were simulated. The LEO satellite orbits corresponded to the Globalstar, Orbcomm, and Iridium constellations. The UAV made pseudorange and pseudorange rate measurements to all 10 LEO satellites throughout the entire trajectory. The LEO satellites’ positions and velocities were initialized using TLE files and SGP4 propagation. Figure 12 shows the trajectories of the simulated LEO satellites and the UAV along with the location at which GPS signals were cut off.

To estimate the UAV’s trajectory, 2 navigation frameworks were implemented: (i) the LEO-aided INS STAN framework and (ii) a traditional GPS-aided INS for comparative analysis. Each framework had access to GPS for only the first 100 seconds. Figure 13(a)-(b) illustrate the UAV’s true trajectory and those estimated by each of the 2 frameworks while Figure 13(c) illustrates the simulated and estimated trajectories of one of the LEO satellites, as well as the final 95-th percentile uncertainty ellipsoid (the axes denote the radial (ra) and along-track (at) directions). Table 2 summarizes the final error and position root mean squared error (RMSE) achieved by each framework after GPS cutoff.

8. UAV SIMULATION WITH THE STARLINK LEO CONSTELLATION WITH PERIODICALLY TRANSMITTED LEO SATELLITE POSITIONS

A UAV was equipped with (i) a tactical-grade IMU and (ii) GPS and LEO satellite receivers. The UAV navigates over Santa Monica, California, USA, for about 82 kilometers in 10 minutes, during which it had access to GPS signals only for the first 100 seconds. After lift-off, the UAV makes 10 banking turns. The simulated LEO satellite trajectories corresponded to the upcoming Starlink constellation. It was assumed that the LEO satellites were equipped with GPS receivers and were periodically transmitting their estimated position. There was a total of 78 LEO SVs that passed within a preset 35° elevation mask set, with an average of 27 SVs available at any point in time. The UAV made pseudorange and pseudorange rate measurements to all LEO satellites. The LEO satellites’ positions in the STAN framework were initialized using the first transmitted LEO satellite positions, which were produced by the GPS receivers onboard the LEO satellites. Figure 14 shows the trajectories of the simulated LEO satellites and the UAV along with
the location at which GPS signals were cut off (Ardito et alia).

To estimate the UAV’s trajectory, 2 navigation frameworks were implemented to estimate the vehicle’s trajectory: (i) the LEO-aided INS STAN framework and (ii) a traditional GPS-aided INS for comparative analysis. Each framework had access to GPS for only the first 100 seconds. Figure 15(a)-(b) illustrate the UAV’s true trajectory and those estimated by each of the 2 frameworks while Figure 15(c) illustrates the simulated and estimated trajectories of one of the LEO satellites, as well as the final 95-th percentile uncertainty ellipsoid (the axes denote the radial (ra) and along-track (at) directions). Table 3 summarizes the final error and position RMSE achieved by each framework after GPS cutoff.

EXPERIMENTAL DEMONSTRATIONS

This section describes the existing Orbcomm LEO constellation and the LEO receiver. Then, it demonstrates the performance of the LEO-aided INS STAN framework on a ground vehicle and a UAV with real Orbcomm satellite signals.

Orbcomm System Overview

The Orbcomm system is a wide area two-way communication system that uses a constellation of LEO satellites to provide worldwide geographic coverage for sending and receiving alphanumeric packets (See Orbcomm, Additional Resources). The Orbcomm system consists of 3 main segments: (i) subscriber communicators (users), (ii) ground segment (gateways), and (iii) space segment (constellation of satellites). These segments are briefly discussed next.

(i) Subscriber Communicators (SCs): There are several types of SCs. Orbcomm’s SC for fixed data applications uses low-cost VHF electronics. The SC for mobile two-way messaging is a handheld, standalone unit.

(ii) Ground Segment: The ground segment consists of gateway control centers (GCCs), gateway Earth stations (GESs), and the network control center (NCC). The GCC provides switching capabilities to link mobile SCs with terrestrial-based customer systems via standard communications modes. GESs link the ground segment with the space segment. GESs mainly track and monitor satellites based on orbital information from the GCC and transmit to and receive from satellites, the GCC, or the NCC. The NCC is responsible for managing the Orbcomm network elements and the gateways through telemetry monitoring, system commanding, and mission system analysis.

(iii) Space Segment: Orbcomm satellites are used to complete the link between the SCs and the switching capability at the NCC or GCC.

Orbcomm LEO Satellite Constellation

The Orbcomm constellation, at maximum capacity, has up to 47 satellites in 7 orbital planes A–G, as illustrated in Figure 16. Planes A, B, and C are inclined at 45° to the equator and each contains 8 satellites in a circular orbit at an altitude of approximately 815 kilometers. Plane D, also inclined at 45°, contains 7 satellites in a circular orbit at an altitude of 815 kilometers. Plane E is inclined at 0° and contains 7 satellites in a circular orbit at an altitude of 975 kilometers. Plane F is inclined at 70° and contains 2 satellites in a near-polar circular orbit at an altitude of 740 kilometers. Plane G is inclined at 108° and contains 2 satellites in a near-polar elliptical orbit at an altitude varying between 785 and 875 kilometers.

Table 2: Simulation results with Globalstar, Orbcomm, and Iridium LEO satellites for a UAV navigating 82 km in 600 seconds (GPS signals were cut off after the first 100 seconds). These results are after GPS cutoff.

<table>
<thead>
<tr>
<th></th>
<th>Unaided INS</th>
<th>LEO-aided INS STAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Final Error (m)</td>
<td>16,589.0</td>
<td>9.8</td>
</tr>
<tr>
<td>RMSE (m)</td>
<td>6,864.6</td>
<td>10.1</td>
</tr>
</tbody>
</table>

Table 3: Simulation results with Starlink LEO satellites for a UAV navigating 25 km in 200 seconds (GPS signals were cut off after the first 100 seconds). These results are after GPS cutoff.

<table>
<thead>
<tr>
<th></th>
<th>Unaided INS</th>
<th>LEO-aided INS STAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Final Error (m)</td>
<td>174.7</td>
<td>9.9</td>
</tr>
<tr>
<td>RMSE (m)</td>
<td>52.6</td>
<td>10.5</td>
</tr>
</tbody>
</table>
The LEO receiver draws pseudorange rate observables from Orbcomm LEO signals on the downlink channel. Satellite radio frequency (RF) downlinks to SCs and GESs are within the 137–138 MHz VHF band. The downlink channels include 12 channels for transmitting to the SCs and one gateway channel, which is reserved for transmitting to the GESs. Each satellite transmits to the SCs on one of the 12 subscriber downlink channels through a frequency-sharing scheme that provides 4-fold channel reuse. The Orbcomm satellites have a subscriber transmitter that provides a continuous 4800 bits-per-second (bps) stream of packet data using symmetric differential-quadrature phase shift keying (SD-QPSK). Each satellite also has multiple subscriber receivers that receive short bursts from the SCs at 2400 bps. Figure 17 shows a snapshot of the Orbcomm spectrum.

Figure 18 shows some of the internal signals of the receiver used to extract Doppler measurement from Orbcomm signals, mainly: (a) an estimate of the Doppler frequency, (b) the carrier phase tracking error, (c) the demodulated QPSK modulation, and (d) the QPSK symbol phase transitions. The Orbcomm receiver is part of the Multichannel Adaptive Transceiver Information eXtractor (MATRIX) software-defined radio (SDR) developed by the Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory (see, http://aspin.eng.uci.edu) (Autonomous Systems Perception, Intelligence, and Navigation Laboratory, Additional Resources). The receiver performs carrier synchronization, extracts pseudorange rate observables, and decodes Orbcomm ephemeris messages.

Note that Orbcomm satellites are also equipped with a specially constructed 1-Watt ultra-high frequency (UHF) transmitter that is designed to emit a highly stable signal at 400.1 megahertz. The transmitter is coupled to a UHF antenna designed to have a peak gain of approximately 2 dB. The UHF signal is used by the Orbcomm system for SC positioning. However, experimental data shows that the UHF beacon is absent. Moreover, even if the UHF beacon were present, one would need to be a paying subscriber to benefit from positioning services. Consequently, in this work, only downlink VHF signals are used in the LEO-aided INS STAN.

Ground Vehicle Navigation
An experiment was conducted to evaluate the performance of the LEO-aided INS STAN framework on a ground vehicle traversing a long trajectory. To this end, a car was equipped with the following hardware and software setup:

- A custom-built quadrifilar helix VHF antenna
- A universal software radio peripheral (USRP) to sample Orbcomm signals. These samples were then processed by the Orbcomm receiver module of the MATRIX SDR.
- An integrated GNSS-IMU, which is equipped with a dual-antenna, multi-frequency GNSS receiver and a microelectromechanical system (MEMS) IMU. A post-processing software development kit (PP-SDK) was used to process GPS carrier phase observables collected by the GNSS-IMU and by a nearby differential GPS base station to obtain a carrier phase-based navigation solution. This integrated GNSS-IMU real-time kinematic (RTK) system was used to produce the ground truth
results with which the STAN navigation framework was compared.

The experimental setup is shown in Figure 19.

The ground vehicle was driven along U.S. Interstate 5 near Irvine, California, USA, for 7,495 meters in 258 seconds, during which 2 Orbcomm LEO satellites were available (FM 112 and FM 117). Figure 20(a) depicts a skyplot of the satellite trajectories over the course of the experiment. Figure 20(b) shows the Doppler measured by the MATRIX SDR and the estimated Doppler using satellite position and velocity obtained from TLE files and an SGP4 propagator for the 2 Orbcomm satellites.

To estimate the UAV’s trajectory, 2 navigation frameworks were implemented to estimate the ground vehicle’s trajectory: (i) the LEO-aided INS STAN framework and (ii) a traditional GPS-aided INS for comparative analysis. Each framework had access to GPS for only the first 30 seconds. Figure 21(a) illustrate the trajectory the 2 Orbcomm LEO satellites traversed over the course of the experiment, Figure 21(b)-(c) illustrate the ground vehicle’s true trajectory and those estimated by each of the 2 frameworks, and Figure 21(d) illustrates the estimated trajectories of one of the Orbcomm satellites as well as the final 95-th percentile uncertainty ellipsoid (the axes denote the radial (ra) and along-track (at) directions).

Table 4 summarizes the final error and position RMSE achieved by each framework after GPS cutoff.

<table>
<thead>
<tr>
<th>Unaided INS</th>
<th>LEO-aided INS STAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Final Error (m)</td>
<td>3,729.4</td>
</tr>
<tr>
<td>RMSE (m)</td>
<td>1,419.3</td>
</tr>
</tbody>
</table>

A. UAV NAVIGATION

An experiment was conducted to evaluate the performance of the LEO-aided INS STAN framework on a UAV. To this end, the UAV was equipped with the following hardware and software setup:

- A high-end quadrifilar helix antenna
- A USRP to sample Orbcomm signals. These samples were then processed by the Orbcomm receiver module of the MATRIX SDR.
- A consumer-grade MEMS IMU, which is proprietary hardware of the UAV manufacturer and used in its flight controller. Log files were downloaded from the drone to parse the raw IMU data, which were subsequently fed to the INS of the STAN framework.
- A pressure altimeter, which is also proprietary hardware of the UAV manufacturer and used in its flight controller. Log files were downloaded from the drone to parse the altitude measurements, which were subsequently fed to the EKF of the STAN framework.

The ground truth trajectory was taken from the UAV’s onboard navigation system, which consists of a MEMS IMU, a multi-constellation GNSS receiver (GPS and GLONASS), a pressure altimeter, and a magnetometer. The experimental setup is shown in Figure 22.

The UAV flew a commanded trajectory in Irvine, California, USA, over a 155-second period during which 2 Orbcomm LEO satellites were available (FM 108 and FM 116). Figure 23(a) depicts a skyplot of the satellite trajec-
sities over the course of the experiment. Figure 23(b) shows the Doppler measured by the MATRIX SDR and the estimated Doppler using satellite position and velocity obtained from TLE files and an SGP4 propagator for the 2 Orbcomm satellites.

To estimate the UAV’s trajectory, 3 frameworks were implemented to estimate the UAV’s trajectory: (i) the LEO-aided INS STAN framework initialized using TLE files, (ii) the LEO-aided INS STAN framework that used the decoded periodically transmitted LEO satellite positions, which were transmitted by the Orbcomm satellites, and (iii) a traditional GPS-aided INS for comparative analysis. The estimated trajectories were compared with the trajectory extracted from the UAV’s onboard navigation system. Each framework had access to GPS for only the first 125 seconds. Figure 24(a) shows the trajectories that the 2 Orbcomm LEO satellites traversed over the course of the experiment. Figure 24(b)-(d) illustrate the UAV’s true trajectory and those estimated by each of the 3 frameworks. Table 5 summarizes the final error and position RMSE achieved by each framework after GPS cutoff.

Table 5: Experimental results with 2 Orbcomm LEO satellites for a UAV navigating about 1.53 km in 155 seconds (GPS signals were cut off after the first 125 seconds). These results are after GPS cutoff.

Manufacturer
In the Ground Vehicle Navigation section, the authors’ setup included an Ettus E312 universal software radio peripheral (USRP) from Ettus Research (Austin, Texas, USA) to sample Orbcomm signals; an AsteRx-I V integrated GNSS-IMU from Septentrio (Leuven, Belgium and Torrance, California, USA); a VectorNav VN-100 microelectromechanical systems (MEMS) IMU from VectorNav Technologies (Dallas, Texas, USA); and Septentrio’s post-processing observables collected.

In the experiment conducted to evaluate the performance of the LEO-aided INS STAN framework on a UAV, a DJI Matrice 600 UAV with an A3 flight controller was used (Shenzhen, China); again, the setup included an Ettus E312 USRP from Ettus Research (Austin, Texas, USA).

Acknowledgements
This work was supported in part by the Office of Naval Research (ONR) under the Young Investigator Program (YIP) award and in part by the National Science Foundation (NSF) CAREER award under Grant 1929965. The authors would like to thank Christian Ardito, Linh Nguyen, Ali Abdallah, Mohammad Orabi, Kimia Shamaei, Mahdi Maaref, and Naji Tarabay for their help in data collection.

Additional Resources

(2) Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory http://aspin.eng.uci.edu


www.insidegnss.com JULY/AUGUST 2019 InsideGNSS 65


Authors

Zaher (Zak) M. Kassas is an assistant professor in the Department of Mechanical & Aerospace Engineering and the Department of Electrical Engineering & Computer Science at the University of California, Irvine (UCI) and director of the Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory. He received a B.E. in Electrical Engineering from the Lebanese American University, an M.S. in Electrical and Computer Engineering from The Ohio State University, and an M.S.E. in Aerospace Engineering and a Ph.D. in Electrical and Computer Engineering from The University of Texas at Austin. In 2018, he received the National Science Foundation (NSF) Faculty Early Career Development Program (CAREER) award, and in 2019, he received the Office of Naval Research (ONR) Young Investigator Program (YIP) award. His research interests include cyber-physical systems, estimation theory, navigation systems, autonomous vehicles, and intelligent transportation systems.

Joshua J. Morales is a Ph.D. candidate in the Department of Electrical Engineering and Computer Science at UCI and a member of the ASPIN Laboratory. He received a B.S. in Electrical Engineering with High Honors from the University of California, Riverside. In 2016, he was accorded an Honorable Mention from the National Science Foundation (NSF). His research interests include estimation theory, navigation systems, autonomous vehicles, and intelligent transportation systems.

Joe J. Khalife is a Ph.D. candidate in the Department of Electrical Engineering and Computer Science at UCI and a member of the ASPIN Laboratory. He received a B.E. in Electrical Engineering and an M.S. in Computer Engineering from the Lebanese American University. In 2018, he received the IEEE Walter Fried Award for Best Paper at the IEEE/ION Position, Location, and Navigation Symposium (PLANS). His research interests include opportunistic navigation, autonomous vehicles, and software-defined radio.
July

JULY 15–26
ESA/JRC INTERNATIONAL SUMMER SCHOOL ON GNSS
Vila Nova de Cerveira, in the north of Portugal

The 12th edition of the ESA/JRC International Summer School on GNSS 2019 will be held in Vila Nova de Cerveira, in the north of Portugal, from July 15–26. Organized by the European Space Agency (ESA) and the Joint Research Centre (JRC), with the collaboration of Oporto University and several external sponsors, the school represents a unique chance for young satellite navigation researchers to get all the latest high-level information from renowned worldwide scientists and specialists, like the Director of the Galileo Programme and Navigation-Related Activities (D/NAV), Paul Verhoef. The program is open to postgraduate students, Ph.D. candidates, early-stage researchers and young engineers and professionals keen on broadening their knowledge. <https://insidegnss.com/esajrc-international-summer-school-on-gnss-coming-in-july/>

September

SEPT. 16–20
ION GNSS+
Miami, Florida, USA

ION GNSS+, the world’s largest technical meeting and showcase of GNSS technology, products and services, will take place at the Hyatt Regency Miami in Miami, Florida. This year’s conference will bring together international leaders in GNSS and related positioning, navigation and timing fields to present new research, introduce new technologies, discuss current policy, demonstrate products and exchange ideas.

The conference includes complimentary short courses taught by ION Masters. These courses will be provided on Monday, Sept. 16, on a complimentary basis to all paid registrants at ION GNSS+ with the compliments of the Satellite Division and the ION Master Instructors. ION Master Instructors are internationally recognized GNSS experts and educators. All of the ION Masters have generously donated their time and talents to this effort, as a service to the GNSS community, with the ION’s gratitude. Another special event, the Women in PNT: Roundtable Discussion Groups, will feature informal discussions on issues important to women at work in PNT. It will be held on Thursday, Sept. 19, from 5:30 p.m. to 7:00 p.m., in the Hibiscus Room. Join in for an informal evening of roundtable discussions moderated by leaders in the field and formatted to promote intimate thought-provoking discussions on a variety of topics important to women in PNT. These roundtable discussions will provide a relaxing space to examine important issues and collectively share information with the goal of helping you effectively manage your professional career. <https://insidegnss.com/ ion-gnss-returns-to-miami-in-sept/>

SEPT. 17–19
INTERGEO
Stuttgart, Germany

Combining a cutting-edge EXPO and CONFERENCE, INTERGEO is celebrating its 25th anniversary as a platform for innovation from September 17–19, and will take a close look at today’s data. It’s generated in huge volumes and grows by the hour—data, data, data. It stems from sensors, apps, IoT-linked devices, plants and satellites. Gathering, processing and visualizing data is particularly important in the geospatial industry.

The international trade fair INTERGEO is focusing on the core issues this raises, asking: Who needs this mass of data? How can it be turned into information? Is it the currency of the future?

As the world becomes more globalized and increasingly digital, the opportunities and challenges for the entire geoinformation sector are growing, too, since it already covers an incredibly broad spectrum, with new fields of work being added all the time. One challenge for this year’s INTERGEO CONFERENCE is to examine this from a range of perspectives.

Around 680 companies, institutions and associations from more than 40 countries are showcasing their services and innovations for the geospatial industry at INTERGEO EXPO. INTERGEO is hosted by DWV—the German Society for Geodesy, Geoinformation and Land Management.

November

NOV. 18–21
INC 2019
Edinburgh, Scotland

The Royal Institute of Navigation is pleased to announce that the Royal Institute of Navigation International Navigation Conference 2019 (INC 2019) will be held in the prestigious Edinburgh International Conference Centre (EICC), Edinburgh, Scotland beginning on November 18. A full conference web site has just been launched, so please visit www.rininc.org to find more details. INC2019 themes will include resilience and autonomy—not only technical aspects but also the neuroscience of navigation and human factors. For more information, visit https://rin.org.uk/events/EventDetails.aspx?id=11352396group=

ADVERTISERS INDEX

<table>
<thead>
<tr>
<th>Company</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAST Nav</td>
<td>67</td>
</tr>
<tr>
<td>Emcore</td>
<td>41</td>
</tr>
<tr>
<td>GMV</td>
<td>9</td>
</tr>
<tr>
<td>ION GNSS+</td>
<td>43</td>
</tr>
<tr>
<td>GPS Networking</td>
<td>7</td>
</tr>
<tr>
<td>Hemisphere GNSS</td>
<td>13</td>
</tr>
<tr>
<td>LKD Gladiator</td>
<td>5</td>
</tr>
<tr>
<td>M-3</td>
<td>11</td>
</tr>
<tr>
<td>NavtechGPS</td>
<td>45</td>
</tr>
<tr>
<td>NovAtel</td>
<td>68</td>
</tr>
<tr>
<td>NovAtel NavWar</td>
<td>17</td>
</tr>
<tr>
<td>QuNAV</td>
<td>6</td>
</tr>
<tr>
<td>Racelogic/LabSat</td>
<td>29</td>
</tr>
<tr>
<td>SBG</td>
<td>37</td>
</tr>
<tr>
<td>Sensonor</td>
<td>19</td>
</tr>
<tr>
<td>Skydel</td>
<td>55</td>
</tr>
<tr>
<td>Spirent</td>
<td>3</td>
</tr>
<tr>
<td>Syntony</td>
<td>27</td>
</tr>
<tr>
<td>Systron Donner</td>
<td>25</td>
</tr>
<tr>
<td>Topcon</td>
<td>23</td>
</tr>
<tr>
<td>Trimble</td>
<td>2</td>
</tr>
<tr>
<td>VectorNav</td>
<td>15</td>
</tr>
</tbody>
</table>

See additional listings at www.insidegnss.com/events
Complexity Made Simple

Intuitive GNSS/INS products...Because your job is already complex.

For over 38 years, CAST Navigation has delivered exactly what our customers need and value in simulation testing products. It’s why CAST has earned the reputation as the trusted GNSS/INS Simulation leader by major military and commercial clients worldwide.

Learn more at castnav.com
INNOVATE WITHOUT DOUBT.

Your job is to go further. Our job is to pave the way. We provide the advanced GNSS and GNSS+INS solutions for some of the world’s leading companies to stay in the lead. Our quality, integration support and manufacturing capability makes us the surest path to success — a path followed by countless leaders worldwide in the fields of autonomous vehicles, aviation, agriculture, defense, surveying, mining and construction. We can help you, too.

AUTONOMY & POSITIONING - ASSURED | novatel.com/innovate