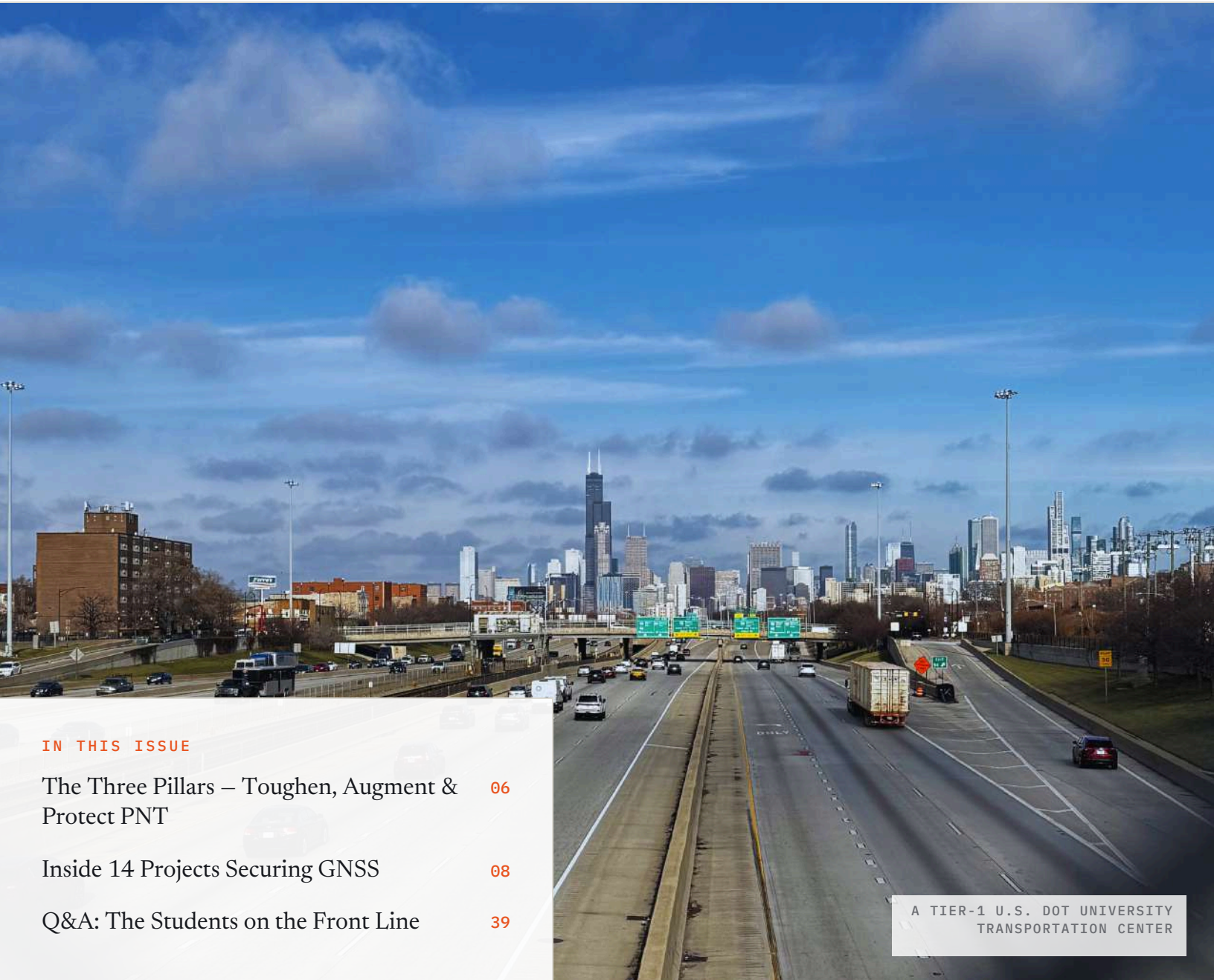
CARNATIONS
Center for Assured & Resilient Navigation in Advanced Transportation Systems
A Tier-1 U.S. DOT University Transportation Center

ISSUE 02
2026

THE ANNUAL RESEARCH MAGAZINE

Navigate.

Resilient positioning, navigation & timing for a contested world.



IN THIS ISSUE

A TIER-1 U.S. DOT UNIVERSITY TRANSPORTATION CENTER

ISSUE 02 — 2026

Contents

Navigate.

CARNATIONS — Center for Assured & Resilient Navigation in Advanced Transportation Systems, Illinois Institute of Technology, Chicago.

DIRECTOR
Boris Pervan

ASSOCIATE DIRECTOR
Mathieu Joerger

PROGRAM MANAGER
Aashish Narang

CONSORTIUM
Illinois Tech · Stanford · Virginia Tech · UC Riverside · Chicago State

A TIER-1 U.S. DOT UNIVERSITY TRANSPORTATION CENTER

01 Foreword

A letter from the Director on a year of resilient-PNT research — and the people behind it.

Boris Pervan
DIRECTOR, CARNATIONS

FROM THE DIRECTOR

“Protecting GPS is critical to both the economic and physical security of the United States — and that’s what this Center is all about.”

Modern transportation runs on signals from space. The trucks that move freight, the aircraft sequencing into busy airspace, the connected vehicles entering our streets — all depend on position, navigation and timing data that is faint, predictable, and increasingly contested.

CARNATIONS was established as a Tier-1 U.S. DOT University Transportation Center to confront that vulnerability head-on. Across five partner universities, our researchers pursue resilient PNT and the communications that connect it, so that a single point of failure never becomes a systemic one.

This second issue of Navigate gathers a year of that work — fourteen projects, eighty-three peer-reviewed papers, and a growing community of students carrying the field forward. I hope it conveys both the urgency of the problem and the optimism of the people solving it.

Boris Pervan
DIRECTOR, CARNATIONS · ILLINOIS INSTITUTE OF TECHNOLOGY

02 The three pillars

Toughen, augment, protect – the strategy that shapes every project in the Center.

THE MISSION

The Three Pillars of Our Mission

CARNATIONS pursues a three-pillar strategy to toughen, augment and protect the PNT systems behind multimodal surface transportation.

01

Toughen

We enhance the resilience and robustness of GNSS receivers and transportation systems so they can withstand interference, jamming, and spoofing attacks without loss of function.

02

Augment

We expand the capabilities of existing navigation infrastructure by integrating backup PNT systems — including LEO satellites, inertial sensors, and distributed RF sensing — to provide redundancy when GPS is disrupted.

03

Protect

We safeguard critical transportation infrastructure by detecting threats, developing countermeasures, and building the testing frameworks that will define industry standards for resilient navigation.

> *No single point of failure should ever become a systemic one — that principle runs through every project in the Center.*

03 Research highlights

Fourteen projects across five universities — toughening, augmenting and protecting the signals that move a nation.

THE PORTFOLIO

Fourteen projects, one mission

The research portfolio flows from device to network — antenna → receiver → multi-sensor system → connected network — spanning five partner universities.

01 **GNSS Anti-Jam and Anti-Spoof Antenna Technology for Multimodal Transportation**
Stanford · Virginia Tech

02 **Receiver Signal Processing to Resist GNSS Jamming and Spoofing Attacks**
Illinois Tech

03 **Defending Against GNSS Jamming and Spoofing by Multi-Sensor Integration**
Illinois Tech

04 **Radio-Frequency Signal Augmentation to Reduce PNT Jamming and Spoofing Risks**
Virginia Tech

05 **Towards Resilient V2X Communications over 5G/6G Networks: Sensing and Cooperative Perception**
Virginia Tech · UC Riverside

07 **Threat Models and Use Cases for Multimodal Transportation**
Stanford

08 **R-PNT Virtual Conflict Simulation**
Virginia Tech

09 **Comprehensive Testing and Evaluation of Resilient PNT Systems**
Illinois Tech · Virginia Tech

10 **Improving GNSS Resiliency Using Edge AI Solutions**
Chicago State

11 **Development of a Generalized Integrity Monitoring Framework for Connected and Automated Vehicle Applications**
UC Riverside

12 **Examining and Enhancing Vehicle Spoofing Detection Capabilities in CAV Applications: Real-World Testing**
UC Riverside

13 **Resilient V2X Communication for Cooperative Autonomy**
UC Riverside

14 **Develop and Test Optimal Speed Control Strategies for Connected and Automated Vehicles under GPS Jamming and Spoofing**
Chicago State · Virginia Tech

NEW THIS YEAR

The REACH initiative joins the portfolio with strong industry backing, bringing the Center to **14 active projects**.

01

GNSS Anti-Jam and Anti-Spoof Antenna Technology for Multimodal Transportation

UNIVERSITY PARTNER
Stanford University · Virginia Tech

PRINCIPAL INVESTIGATORS
Sherman Lo · Mark Psiaki

This project is advancing multi-element antenna architectures — Controlled Reception Pattern Antennas (CRPAs), Dual Polarization Antennas (DPAs), and distributed patch arrays — to detect, localize, and mitigate GNSS jamming and spoofing across ground, maritime, and aviation domains. Progress this year spans two closely coordinated efforts at Stanford and Virginia Tech, each attacking the problem from a different angle.

At Stanford, DPAs were successfully integrated with commercial receivers including the Trimble BX992 and Novatel PwrPk7D, and low-cost CRPA development continued using KrakenSDR arrays — proving that credible anti-spoof capability doesn't require exotic, expensive hardware. Distributed non-synchronized receiver techniques were validated using real interference data from Jammertest 2024 and 2025 in Norway, including blind spoofing test statistics that clearly flagged spoofing attacks in September 2024 Norway data and in July 2024 Israel data featuring two simultaneous spoofers. An ARAIM-based solution-separation approach was developed enabling spoofing detection with two or more receivers over both short and long baselines, with applications spanning ground, maritime, and aviation domains. Spoofer localization methods using time-difference-of-arrival measurements were implemented to estimate spoofer position through hyperbolic positioning, and dual-polarization antenna (DPA) data from field and controlled tests were analyzed to improve interference mitigation and direction-of-arrival estimation, with particular focus on resolving ambiguity in signal direction.

01

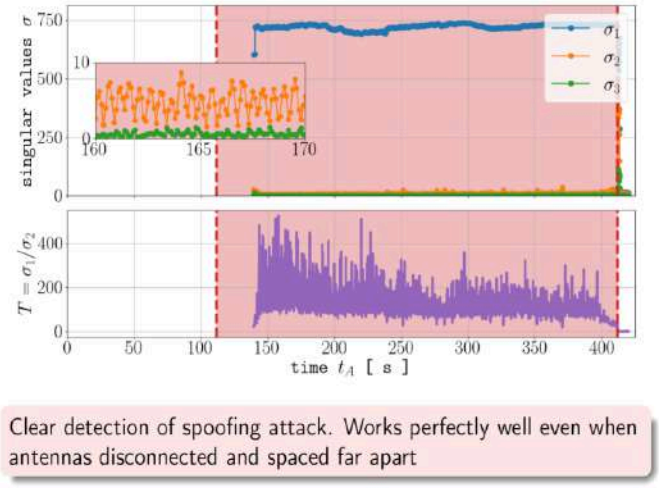
UNIVERSITY PARTNER
Stanford University · Virginia Tech

PRINCIPAL INVESTIGATORS
Sherman Lo · Mark Psiaki

An application for Jammertest 2026 has been submitted, extending the team's multi-year track record of live, adversarial field testing in some of the world's most realistic jamming environments.

At Virginia Tech, blind multi-antenna nulling techniques were evaluated using both simulated datasets and recorded live data, focused on steering antenna-array nulls toward spoofing sources and then recovering the authentic underlying signal. Extensive analysis assessed performance under measurement noise and uncertainty, and additional work addressed multipath-like correlation patterns and timing offsets introduced by the nulling process itself — a subtle side-effect the team had to characterize before it could be corrected for. Methods are now under development to separate these distortion components and estimate accurate pseudoranges for authentic signals. Results demonstrate that signal nulling is effective under practical field conditions, with ongoing work focused on improving signal separation and automating the identification of spoofed versus authentic signals — a step toward a fully autonomous onboard detection capability.

Key remaining challenges across both institutions include limited CRPA sensitivity in low-cost hardware, phase inconsistencies in DPA measurement results, and intermittent data dropouts during extended field trials — practical engineering hurdles the teams are actively working through as they push toward field-deployable, low-cost hardware.



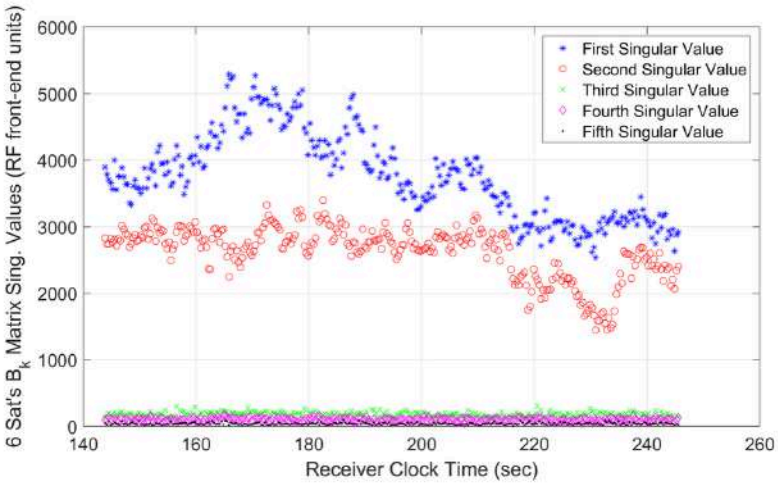


Figure:Blind spoofing test statistics indicate spoofing attacks in September 2024 Norway data (left-hand panel) and in July 2024 Israel data that features 2 spoofers (right-hand panel)

IMPACT

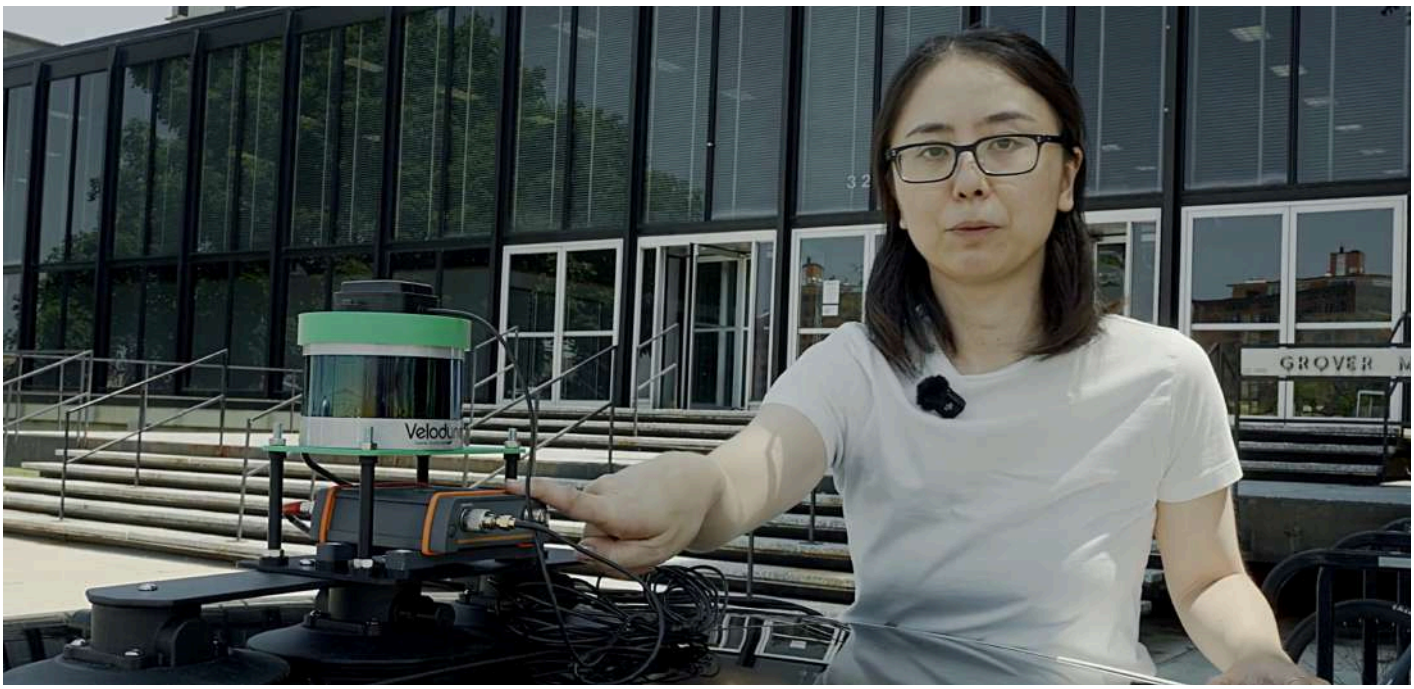
This work strengthens navigation resilience across aviation, autonomous vehicles, and intelligent transportation systems by enabling low-cost, scalable detection and mitigation of GNSS interference — technology directly transferable to commercial receiver platforms and validated in two consecutive years of live, internationally recognized jamming trials in Norway.

02

Receiver Signal Processing to Resist GNSS Jamming and Spoofing Attacks

UNIVERSITY PARTNER
Illinois Institute of Technology

PRINCIPAL INVESTIGATORS
Boris Pervan · Samer Khanafseh · Aashish Narang



This project is developing receiver-based methods for GNSS spoofing detection and improving signal tracking under interference using IMU-aiding — strengthening the security of the receiver itself rather than relying solely on external sensors or antennas, so the protection travels with every device that uses it.

The team's signature contribution, a receiver-based spoofing detection method built on decomposition of the Complex Cross Ambiguity Function (CCAF) using full complex I/Q measurements, was matured and rigorously validated over the past year. The method exploits carrier-phase inconsistencies to separate authentic and counterfeit signals — including closely aligned, power-matched attacks that are especially difficult to detect because they mimic genuine signal strength almost perfectly — and applies a new error-decorrelation process to improve performance under thermal noise and multipath interference. Results from multiple satellites are combined using inverse RAIM (iRAIM) to form separate, independent navigation solutions, enabling identification and continued tracking of authentic signals even while under active attack. The approach was validated with both simulation and live RF data, presented at IEEE/ION PLANS 2025 in Salt Lake City, formed a core part of Sam Ahmed's Ph.D. dissertation defense in May 2025, and was published in IEEE Transactions on Aerospace and Electronic

02

UNIVERSITY PARTNER
Illinois Institute of Technology

PRINCIPAL INVESTIGATORS
Boris Pervan · Samer Khanafseh · Aashish Narang

Systems in October 2025 (Vol. 61, No. 5) — one of the field's most rigorous peer-reviewed venues and a major milestone for the Center this year.

In parallel, the team initiated new work on IMU-aided GNSS pilot-signal tracking to sustain positioning under broadband jamming. Kalman filter–based carrier tracking on GPS L1C and L5 signals showed that tracking could be maintained at signal levels as low as 4 dB-Hz using an industrial-grade IMU, and down to a striking 0 dB-Hz with a tactical-grade IMU — meaning meaningfully better jamming resistance is achievable simply by upgrading sensor grade, with no change to the underlying algorithm. Early findings were presented by Nagai et al. at the ION International Technical Meeting in Anaheim in January 2026. While still early in development, this work represents an important step toward next-generation GNSS receivers capable of maintaining reliable positioning in contested and complex signal environments.

Reflecting the project's growing scope, Aashish Narang joined this year as an additional Principal Investigator — supporting system-level integration, coordinating data activities, and tracking progress across algorithm development, testing, and reporting to ensure consistency as the team's work matures toward field deployment.

IMPACT

By enabling GNSS receivers to independently detect sophisticated attacks and keep tracking authentic signals through severe jamming, this research delivers receiver-level protection with a direct path to commercial and government deployment — reinforced this year by a landmark peer-reviewed journal publication and a successful Ph.D. defense.

03

Defending Against GNSS Jamming and Spoofing by Multi-Sensor Integration

UNIVERSITY PARTNER
Illinois Institute of Technology

PRINCIPAL INVESTIGATORS
Boris Pervan · Samer Khanafseh · Aashish Narang

This project fuses GNSS with inertial and other onboard sensor data to detect and mitigate spoofing and jamming — building resilience through redundancy, so that no single point of failure can take down a vehicle's navigation.

An INS-aided spoofing monitor was developed and refined this year, exploiting temporal patterns in INS/GNSS Kalman filter innovations to catch sophisticated, power-matched attacks that don't follow real platform dynamics — attacks that are otherwise very difficult to distinguish from authentic signals because they are engineered to look convincing. Initial results were presented at ION GNSS+ 2025 in Baltimore (Kujur, Khanafseh & Pervan), and the method was evaluated under demanding jamming-then-spoofing scenarios, demonstrating continued detection capability even after periods of GNSS denial and degraded IMU performance — precisely the compound, real-world attack sequence adversaries are most likely to attempt. Validation using real FAA live-flight spoofing data further confirmed the monitor's ability to detect deceptive, low-magnitude attacks under genuine operational aviation conditions, building directly on earlier work validating the monitor against live spoofing data presented at ION ITM 2025.

03

UNIVERSITY PARTNER
Illinois Institute of Technology

PRINCIPAL INVESTIGATORS
Boris Pervan · Samer Khanafseh · Aashish Narang

Complementary work evaluated a tightly coupled DME/INS architecture as an alternative aviation positioning approach supporting RNP 1.0 navigation standards — published as “Integrated DME/INS Alternative PNT System for RNP 1.0” at ION GNSS+ 2025 in collaboration with industry co-authors Vitan, Berz, and Osechas. The team also completed a comprehensive assessment of LiDAR spoofing threats, examining integrity risks from laser-injection attacks and physical scene tampering that could compromise feature-based localization — work presented at PLANS 2025 and expanded into a full review, “Fundamental Architectures for High-Integrity Georeferenced Lidar Positioning,” published in NAVIGATION journal (Winter 2025) with co-authors Rife, Wassaf, Khanafseh, and Pervan.

Results collectively show that multi-sensor integration meaningfully improves detection capability across attack types. Key remaining challenges include managing inertial error growth during extended GNSS outages — since inertial sensors alone drift over time — and extending integrity-monitoring methods to a wider range of sensor types beyond the ones already validated.

IMPACT

By combining GNSS with inertial, DME, and LiDAR sensing, this project reduces reliance on any single navigation source — strengthening safety and operational continuity for aviation, connected vehicles, and autonomous platforms operating in contested or GNSS-degraded environments, with results already validated against real FAA flight data and published in a leading navigation journal.

04

Radio-Frequency Signal Augmentation to Reduce PNT Jamming and Spoofing Risks

UNIVERSITY PARTNER
Virginia Tech

PRINCIPAL INVESTIGATORS
Mathieu Joerger · Mark Psiaki

This project explores alternative radio-frequency signals — including Low Earth Orbit (LEO) satellite constellations such as Starlink and dedicated PNT constellations like Xona Space Systems' "Pulsar" — to provide backup positioning, navigation, and timing when traditional GNSS is disrupted, and to assess their real-world applicability to transportation systems.

Working closely with industry partner Xona Space Systems, the team developed recursive integrity-evaluation methods integrating GNSS and Xona satellites, created new time-correlated measurement error models, and defined navigation performance requirements for uncrewed air vehicles and automated ground systems. Worldwide accuracy, integrity, and availability were analyzed for GNSS-only, Xona-only, and combined constellations — establishing, for the first time, quantitative integrity requirements for Xona's emerging PNT constellation, a genuinely novel contribution supporting the design of a next-generation commercial satellite system. In parallel, Doppler-only Signal-of-Opportunity (SoOP) filters were designed to operate efficiently with fewer than eight LEO signals, supported by new geometric dilution of precision (GDOP) analysis for accuracy evaluation, building on earlier time-diverse Doppler-only LEO PNT work by Moore, Psiaki, and Buehrer.

04

UNIVERSITY PARTNER
Virginia Tech

PRINCIPAL INVESTIGATORS
Mathieu Joerger · Mark Psiaki

The team also successfully collected and processed live Starlink Ku-band signal data, reverse-engineering repeatable signal features — including edge pilots and T-codes — to enable precise Doppler-shift measurements without requiring any cooperation from the satellite operator. A nonlinear navigation filter was developed to improve performance under large initial position uncertainties, addressing a key limitation of standard extended Kalman filters. This body of work culminated in a paper, “Pilots and Other Predictable Elements of the Starlink Ku-Band Downlink” (Qin, Psiaki, Bowman & Humphreys), submitted for journal peer review in February 2026 in collaboration with a fellow USDOT University Transportation Center — identifying predictable signal structures that support improved processing for opportunistic PNT applications going forward. The project has supported three Ph.D. students (one now graduated, with a completed dissertation on Advanced Receiver Autonomous Integrity Monitoring for Multi-Constellation and LEO-Augmented GNSS) and a postdoctoral researcher over the year, resulting in multiple publications and continuing knowledge exchange with industry experts at Xona and beyond.

IMPACT

This research is building the technical foundation for LEO-based backup PNT that can protect transportation networks when traditional GNSS is disrupted — pairing academic rigor with direct industry collaboration on a live commercial constellation to accelerate a truly resilient, multi-constellation national navigation infrastructure.

05

Towards Resilient V2X Communications over 5G/6G Networks: Sensing and Cooperative Perception

UNIVERSITY PARTNER
Virginia Tech · University of California, Riverside

PRINCIPAL INVESTIGATORS
Walid Saad · Hang Qiu

This project is building resilient, low-latency communication systems for connected and automated vehicles operating over emerging 5G and 6G networks, spanning both network-level resilience and next-generation sensing-communication integration.

Early in the year, the team developed a two-phase resilience framework for cellular V2X networks operating under imperfect channel-state information, achieving up to a 56% reduction in delay and a 16% improvement in throughput compared to baseline approaches — a substantial gain for safety-critical, latency-sensitive vehicle messaging. A neuro-symbolic AI detection method was also demonstrated against emerging 6G Integrated Sensing and Communication (ISAC) security threats, improving attack-identification accuracy by more than 50%, with related work published as “Sensing Safety Analysis for Vehicular Networks with ISAC” at IEEE GLOBECOM 2025 (Shui, Saad & Chen). A semantic-communication microservice was also built to preserve message meaning even during degraded connectivity, expanded upon in a completed Virginia Tech M.S. thesis by DeRieux on AI-based semantic communications with multimodal data.

05

UNIVERSITY PARTNER
Virginia Tech · University of California, Riverside

PRINCIPAL INVESTIGATORS
Walid Saad · Hang Qiu

Building on this foundation, the team shifted focus to modeling transmission delay jitter in vehicle-to-vehicle communication as a function of inter-vehicle distance and nearby interference — published as “Resilient Vehicular Communications with Minimal Jitter” at the 59th Asilomar Conference (Paul, Saad & Burger, November 2025). Results show that increasing the number of transmit antennas improves performance against distance effects but can reduce performance under interference — an important, non-obvious design trade-off for V2X hardware designers to weigh. An adaptive power-allocation method was implemented and shown to reduce recovery time compared to fixed allocation, supporting more stable communication under varying real-world traffic conditions.

Work also began on integrated sensing and communication (ISAC) using mmWave radar hardware. After limited access to suitable mmWave equipment slowed early progress — a genuine hardware-availability constraint the team openly flagged — the team identified a Texas Instruments radar platform to move proof-of-concept implementation forward in the coming period.

IMPACT

This project strengthens the communications backbone that connected and automated vehicles depend on — cutting network delay by over half in tested scenarios and hardening emerging 6G sensing systems against next-generation security threats before they ever reach the field.

07

Threat Models and Use Cases for Multimodal Transportation

UNIVERSITY PARTNER
Stanford University

PRINCIPAL INVESTIGATORS
Todd Walter · Sherman Lo · Sam Pullen

This project develops the comprehensive threat models and realistic test scenarios that let the rest of the transportation industry understand and prepare for GNSS spoofing and jamming — turning raw interference data into structured, usable knowledge that other CARNATIONS teams and outside industry can build on directly.

Using the Stanford GPS Laboratory's Automatic Dependent Surveillance-Broadcast (ADS-B) based RFI localizer and a network of low-cost GNSS RFI monitors (LCMs), the team expanded rfi.stanford.edu's global mapping and analysis of spoofing and jamming incidents, including documented observations of GNSS spoofing in Russia (2023–2024) presented by Lo et al. at ION ITM 2025. Analysis revealed a clear trend toward multi-frequency, “tiered” attacks in which jamming and spoofing occur concurrently, along with spoofing patterns that appear to specifically target different classes of users. Receiver testing at Jammertest 2024 and in Stanford's labs — published as “Combining ADS-B, LCM, and DPA for GNSS Jammer Detection” and “Interference Detection in Massive GNSS Jammer Test” (Chen, Liu, Kriezis, Lo & Walter, ION ITM 2025) — showed that commercial off-the-shelf receivers such as the ublox F9 series use cross-signal and cross-frequency aiding that shapes how interference actually manifests, a finding with direct implications for how realistic test scenarios should be built.

07

UNIVERSITY PARTNER
Stanford University

PRINCIPAL INVESTIGATORS
Todd Walter · Sherman Lo · Sam Pullen

This year, the team formalized this knowledge into a structured spoofing-attack taxonomy, drawing on both ADS-B data documenting real-world global aviation spoofing incidents in 2024–2025 — published as "Global Incidents of Aviation Spoofing in 2024-2025 Detected with Automatic Dependent Surveillance Broadcast" (Lo, Liu, Ibrahim, Chen, Akos & Walter, ION ITM 2026) — and expanded Jammertest 2025 datasets covering multiple simultaneous spoofers and varied attack trajectories, published as "Determining Protection Levels Using Multiple Antennas Under Spoofing Conditions" (Blanch, Lo, Chen, Kriezis & Walter, PLANS 2025) and "TDOA-Based Spoofing Source Localization Using Multi-Constellation Unsynchronized Receivers" (Babcock-Chi, Lo, Chen, Blanch & Walter, ION GNSS+ 2025). The team coordinated directly with Jammertest organizers to help define advanced multi-directional spoofing scenarios for the 2026 event, and developed a new modeling tool to assess how spoofing affects autonomous aircraft with varying degrees of GNSS reliance. Work to align the taxonomy with RTCA industry standards is ongoing, complicated by continually evolving official definitions of interference types — a genuine standards-development challenge the team is working through directly with RTCA stakeholders.

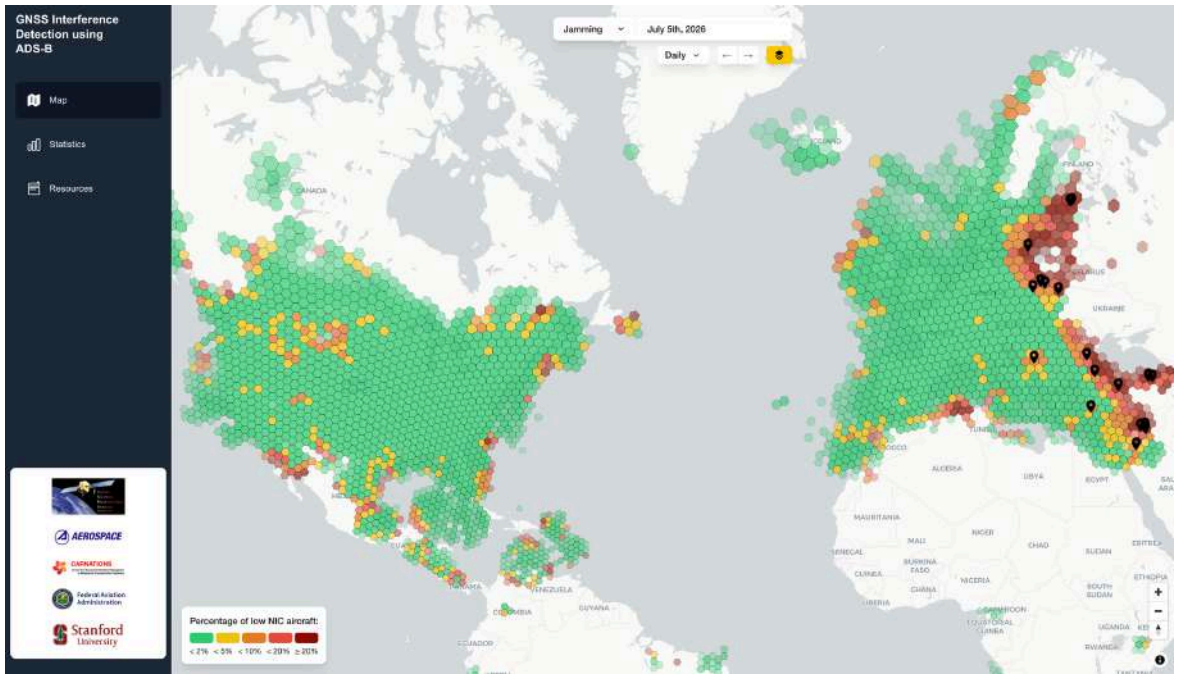


Figure: Map of identified spoof events and ADS-B locations (before spoofing) relevant to the RFI from rfi.stanford.edu

IMPACT

This project strengthens the communications backbone that connected and automated vehicles depend on — cutting network delay by over half in tested scenarios and hardening emerging 6G sensing systems against next-generation security threats before they ever reach the field.

08

R-PNT Virtual Conflict Simulation

UNIVERSITY PARTNER
Virginia Tech

PRINCIPAL INVESTIGATORS
Hesham Rakha · Mark Psiaki

This project examines how GNSS spoofing cyberattacks affect transportation networks at a system-wide level — moving beyond single-vehicle impact to ask how falsified navigation data reshapes traffic patterns across an entire region, using both offensive (“red-team”) and defensive (“blue-team”) simulation strategies.

Earlier simulations on the QNET corridor road network showed that spoofed routing data diverting vehicles from a freeway onto parallel arterials produced cascading congestion effects across 46 origin-destination trips spanning 10 network zones — not just the directly targeted trip. Percentage changes in travel time ranged from -35.7% to +6.9% at low traffic demand and up to +20% at full demand, with some trips actually benefiting from redistributed freeway traffic even as most degraded — a nuanced finding showing that spoofing impact is not uniform across a network.

This year, the team applied the same rigorous methodology to the I-66 corridor as a new case study, using both synthetic transportation networks and real-world roadway data. Simulations focused on freeway segments of 100–200 meters — the physical range needed to realistically spoof a moving vehicle's receiver — and confirmed that targeting just three selected road segments (IDs 298, 197, and 1335) increased total network delay from a 43.46-second baseline to as much as 48.18

08

UNIVERSITY PARTNER
Virginia Tech

PRINCIPAL INVESTIGATORS
Hesham Rakha · Mark Psiaki

seconds, a roughly 11% increase, while average travel time rose by up to 1.6% and introduced perceived congestion that triggered unnecessary rerouting across the network.

A web-based tool is now in development to help identify which candidate road segments are most vulnerable to spoofing attacks based on constraints such as segment length and speed limit, giving transportation agencies a practical, ready-to-use vulnerability-assessment capability rather than a one-off academic exercise.

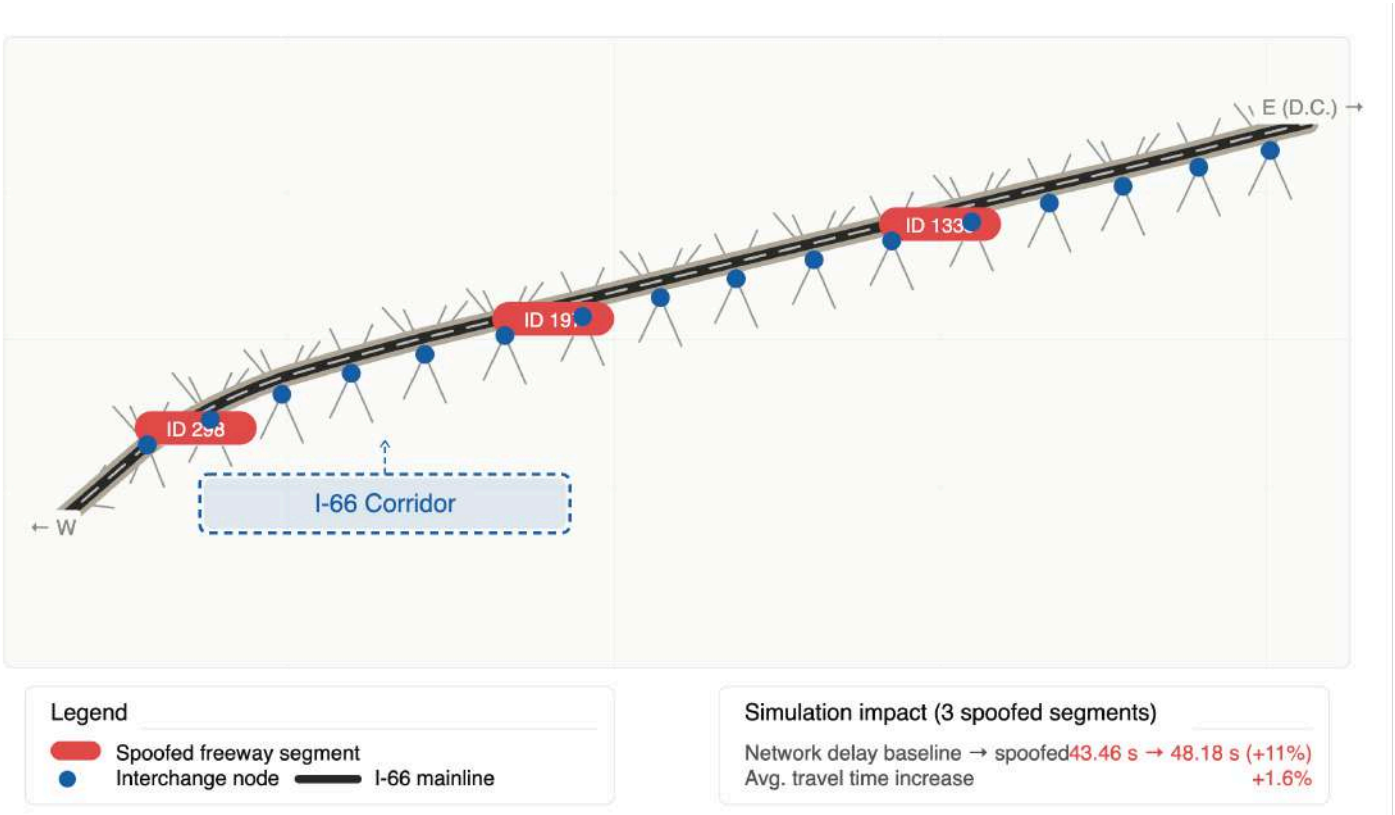


Figure: The I-66 road network used to simulate how targeted spoofing at specific freeway segments cascade into network-wide delay.

IMPACT

This pioneering, network-level analysis gives transportation agencies concrete, quantified evidence of how a single spoofed road segment can cascade into system-wide delay — directly informing infrastructure hardening priorities and mitigation strategy for real-world traffic operations centers nationwide.

09

Comprehensive Testing and Evaluation of Resilient PNT Systems

UNIVERSITY PARTNER
Illinois Institute of Technology · Virginia Tech

PRINCIPAL INVESTIGATORS
Mathieu Joerger · Matthew Spenko

As the Center's primary testing and evaluation platform, this project analyzes real radio-frequency interference (RFI) data and experimentally evaluates the anti-jamming and anti-spoofing technologies developed across CARNATIONS — serving as the connective tissue that validates work from across the entire consortium.

The team automated a live jamming-prediction method using data from more than 900 U.S. Continuously Operating Reference Stations (CORS) and redeployed its public alert web application — now hosted on OracleWS at rfi.aoe.vt.edu — with improved detection sensitivity, event-duration estimation, and interactive visualization tools for tracking RFI activity by time and location, both nationally and internationally. Field tests conducted in collaboration with Inertial Labs confirmed that GNSS can be effectively augmented with inertial navigation systems (INS), LiDAR, and vehicle-to-vehicle motion sharing to sustain navigation performance under interference. Industry partnerships deepened with TUALCOM and Spirent, the latter contributing a GSS 9000 GNSS simulator as a cost-share contribution to the Center — real hardware that expands what the team can safely test.

09

UNIVERSITY PARTNER
Illinois Institute of Technology · Virginia Tech

PRINCIPAL INVESTIGATORS
Mathieu Joerger · Matthew Spenko

This year, experimental evaluation expanded to collaborative multi-sensor PNT architectures combining (1) GNSS with INS, LiDAR, and vehicle-to-vehicle data sharing, and (2) INS with shared motion constraints and vehicle-to-vehicle scalar or vector cross-links — demonstrating that combining multiple sensing modalities supports consistent navigation performance under real interference conditions. A major structural challenge for the entire field is that broadcasting at GNSS frequencies is illegal, which limits what can be tested in open-sky conditions; a new anti-RFI testbed is under active development at Virginia Tech's Smart Roads, with contributions from industry partners including simulation and sensing equipment, giving the Center a safe, controlled environment to work within this legal constraint. A major outcome of this year's work is the demonstrated validation of RFI monitoring using actual operational data alongside multi-sensor navigation approaches — connecting theoretical detection methods to real-world evidence.

IMPACT

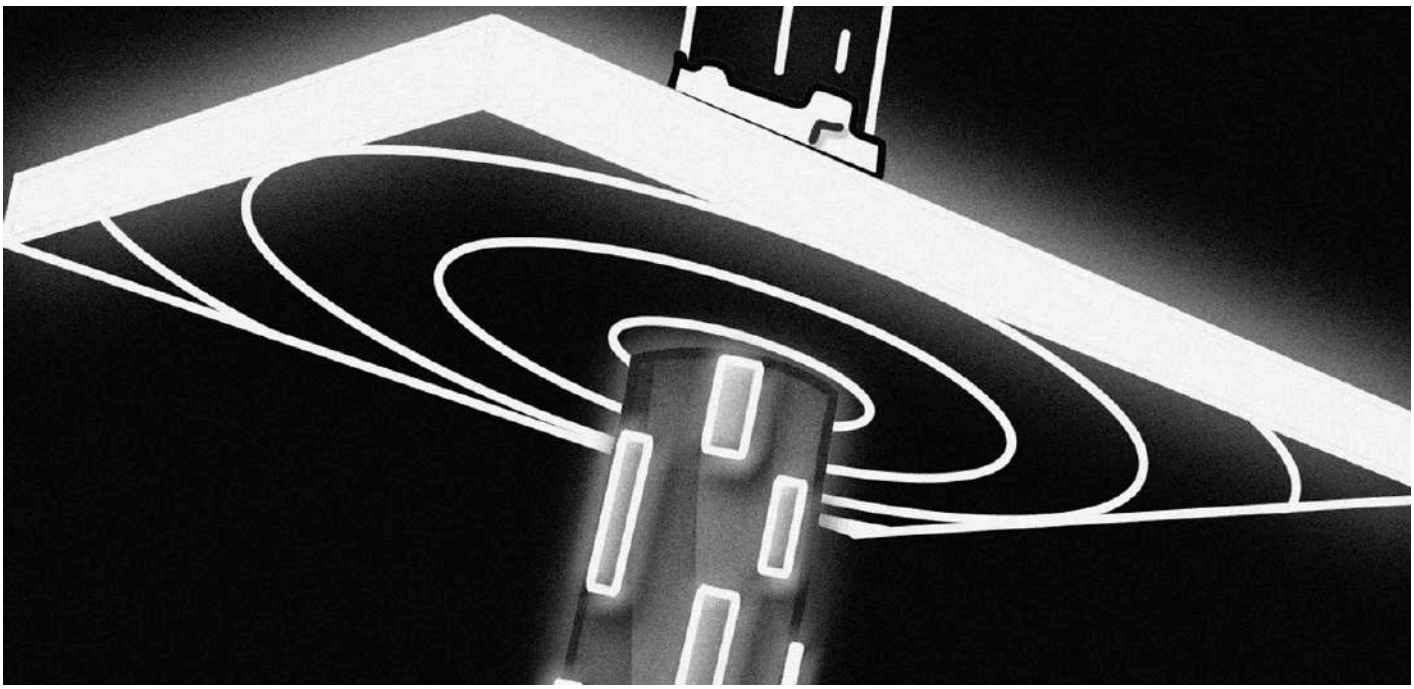
By converting nationwide, real-world interference data into an operational monitoring and prediction platform used by the public, this project accelerates validation of anti-jamming and anti-spoofing technologies and gives transportation stakeholders early warning of RFI events across the country.

10

Improving GNSS Resiliency Using Edge AI Solutions

UNIVERSITY PARTNER
Chicago State University

PRINCIPAL INVESTIGATORS
Moussa Ayyash



This project combines artificial intelligence, distributed sensing, and advanced networking to improve navigation reliability in urban and GNSS-challenged environments — bringing the power of edge computing directly to the point of navigation failure, rather than relying on cloud processing that can itself be disrupted.

Earlier work proposed a Reinforcement Learning and Factor Graph Optimization (RL+FGO) framework to mitigate multipath and non-line-of-sight disruptions in urban canyons, and developed a Deep Neural Network (DNN) model for GNSS resilience against spoofing and jamming — published as “Enhancing GNSS Resiliency Against Spoofing and Jamming Employing Deep Neural Networks” (Gandhi, Shah, Singh & Ayyash) at the 2025 IEEE World Forum on Public Safety Technology. The team also began exploring Distributed Acoustic Sensing (DAS) for signal-integrity assessment, an emerging sensing modality not widely applied to GNSS resilience.

This year, that early exploration matured into a full Edge AI framework integrating GNSS with Distributed Acoustic Sensing, federated learning for cooperative positioning across distributed nodes, and decentralized algorithms for task allocation and

10

UNIVERSITY PARTNER
Chicago State University

PRINCIPAL INVESTIGATORS
Moussa Ayyash

data consistency — work presented as “An Augmented GNSS-DAS Architecture for Continuous and Robust Positioning” (Wang, Zhong, Singh, Jaber & Ayyash), accepted for publication at IEEE ICC 2026 in Glasgow.

Predictive models were developed to mitigate non-line-of-sight and multipath effects using environmental features and spatial correlations, while reinforcement learning was further integrated with factor graph optimization to improve urban positioning, alongside deep-learning-based multi-sensor data fusion. A new composite metric was introduced to track GNSS resiliency over time — giving the team, and eventually deployers, a single number to benchmark performance against. Validation is ongoing across diverse operational environments including tunnels and dense urban areas, with results shared through both conference publications and journal submissions.

IMPACT

This work extends reliable navigation into the GNSS-challenged urban environments where positioning is currently weakest — directly supporting autonomous vehicles, smart-city infrastructure, and emergency-response operations navigating tunnels, canyons, and dense downtown corridors, with a growing international publication record to match.

11

Development of a Generalized Integrity Monitoring Framework for Connected and Automated Vehicle Applications

UNIVERSITY PARTNER
University of California, Riverside

PRINCIPAL INVESTIGATORS
Matthew Barth

This project is building a comprehensive framework for evaluating positioning integrity in Connected and Automated Vehicle (CAV) applications, grounded in a realistic, physically accurate digital twin of a real intersection rather than a generic simulated environment.

The team designed a high-fidelity digital twin of the Iowa–University Avenue intersection in Riverside, California, incorporating accurate lane geometry and calibration to map virtual coordinates to real-world geodetic positions. The CARLA driving simulator was integrated with the NS-3 network simulator to establish a full Vehicle-to-Everything (V2X) communication framework, enabling joint analysis of communication metrics — latency, packet loss, throughput — alongside vehicle positioning performance. This culminated in the initial release of CAV TESTS V1.0, a combined SUMO, CARLA, and NS-3 co-simulation platform capable of testing both nominal and safety-critical scenarios such as illegal pedestrian crossings and occluded vehicle movements — exactly the edge cases that matter most for real-world safety certification.

11

UNIVERSITY PARTNER
University of California, Riverside

PRINCIPAL INVESTIGATORS
Matthew Barth

This year, the team refined the intersection digital twin toward greater photorealistic and metrically accurate fidelity, and began developing data-driven methods to introduce controlled variations into sensor data, enabling systematic comparison between reference and modified datasets for integrity evaluation. While key goals were achieved, challenges remain in managing the complexity of multi-platform synchronization across SUMO, CARLA, and NS-3 simultaneously. A current limitation is the absence of real-time GNSS measurement generation, since existing tools operate offline; the team is now developing methods to generate GNSS measurements dynamically from simulated vehicle states, which will substantially expand the platform's testing capability and move it closer to real-time, hardware-in-the-loop testing.

IMPACT

This realistic, physically grounded co-simulation environment gives researchers and industry a repeatable way to evaluate CAV positioning integrity and communication performance before real-world deployment — establishing the scientific foundation needed for trustworthy autonomous vehicle navigation at a real, mapped intersection.

12

Examining and Enhancing Vehicle Spoofing Detection Capabilities in CAV Applications: Real-World Testing

UNIVERSITY PARTNER
University of California, Riverside

PRINCIPAL INVESTIGATORS
Matthew Barth · Hang Qiu

This project investigates how GNSS spoofing and jamming affect Connected and Automated Vehicle (CAV) systems — not just the targeted vehicle, but surrounding vehicles and critical subsystems such as sensors and communication modules — and develops real-time detection and mitigation strategies grounded in live field testing.

The team modified its MK6 Vehicle-to-Vehicle (V2V) communication hardware to sustain operation under GNSS-denied conditions and developed a custom Basic Safety Message (BSM) Part 2 structure carrying GNSS time-loss indicators, last-valid timestamps, and inconsistent-data flags to improve resilience during spoofing and jamming events. This system was field-tested at the APEX25 experiment at White Sands Missile Range over five nights of live jamming and spoofing conditions — a rare, genuinely adversarial government test range opportunity most academic teams never get access to. Data analysis showed reliable communication performance via C-V2X sidelink and effective clock-drift estimation under real interference, though extended Department of Defense data-release review timelines limited how quickly full results could be analyzed — a bureaucratic, not technical, constraint the team is working through.

12

UNIVERSITY PARTNER
University of California, Riverside

PRINCIPAL INVESTIGATORS
Matthew Barth · Hang Qiu

This year, the team processed the resulting CAV dataset and developed a detection approach that integrates GNSS data, onboard sensors, and V2V communication to identify abnormal positioning behavior in real time, including LiDAR-based awareness — published in part as “Sensor- and Communication-Based GNSS Spoofing and Jamming Detection Framework for Connected and Automated Vehicle Applications” (Stas, Nguyen, Snyder, Mo & Barth, ION Pacific PNT 2026). Development also began on a factor-graph-based tightly coupled inertial navigation system (INS) to support fault detection and maintain continuous positioning. With continued limited access to live field environments, validation is proceeding through a controlled, repeatable post-processing approach using simulated spoofing and jamming scenarios overlaid on real vehicle data, enabling controlled and repeatable evaluation of system performance without requiring another expensive range booking.

IMPACT

Field-validated at a live government test range under real jamming and spoofing conditions, this detection capability — fusing vehicle sensors, LiDAR, and V2V data — moves CAV spoofing defense from theory toward deployable, real-world-tested systems ready for industry adoption.

13

Resilient V2X Communication for Cooperative Autonomy

UNIVERSITY PARTNER
University of California, Riverside

PRINCIPAL INVESTIGATORS
Hang Qiu

This project addresses critical vulnerabilities in cooperative autonomous transportation by strengthening Vehicle-to-Everything (V2X) communication for both cooperative driving — where vehicles share sensor data — and remote driving, which allows human intervention when needed, both of which depend on secure, low-latency, high-bandwidth communication.

The team released the world's first public C-V2X direct-communication dataset, SEE-V2X, documenting real throughput, latency, and channel performance in an application-centric approach (Mo, Wu & Qiu, ACM SenSys, May 2025), and expanded it into CooperScene, a multi-agent, multi-modal CAV dataset with integrated C-V2X communication targeted for submission to a top-tier conference. A new calibration method, BEVCalib, improving multi-modal LiDAR-camera sensor alignment via geometry-guided bird's-eye-view representations, was published at the Conference on Robot Learning (CoRL) in September 2025 (Yuan, Li, Yue, Shah & Qiu) — setting the stage for future research in GNSS-denied environments.

13

UNIVERSITY PARTNER
University of California, Riverside

PRINCIPAL INVESTIGATORS
Hang Qiu

This year, the team developed R'CV2X, a coordination framework that improves channel utilization and message exchange between vehicles and roadside units, and built a simulation-based prototype of a flooding-based synchronization protocol to sustain communication continuity in environments with no GNSS signal at all — with results (Mo, Tan & Qiu, “R'CV2X: RSU Coordinated Cooperative Perception via C-V2X Direct Communication”) prepared for submission to the 32nd Annual ACM MobiCom conference, one of the field's premier venues, in Austin this October. A standard-compliant C-V2X interface was also built using software-defined radios and the open-source srsRAN platform, giving the team flexible timing control that addresses the restricted programmability of commercial C-V2X hardware — an open-source workaround the team is actively expanding.

Collaboration was also established with Virginia Tech to explore semantic communication for enhancing PNT resilience in cooperative and remote driving, connecting this project's communication expertise directly with Project 5's sensing and semantic-communication work.

IMPACT

By open-sourcing benchmark datasets used industry-wide and building GNSS-independent synchronization tools, this project accelerates development of resilient cooperative and remote-driving communication for the corner-case, limited-visibility scenarios where autonomous vehicles need it most.

14

Develop and Test Optimal Speed Control Strategies for Connected and Automated Vehicles under GPS Jamming and Spoofing

UNIVERSITY PARTNER
Chicago State University · Virginia Tech

PRINCIPAL INVESTIGATORS
Moussa Ayyash · Hesham Rakha

As the Center's newest research initiative, this project is developing robust, physics-informed and AI-enhanced frameworks for positioning, navigation, and vehicle control under adversarial GNSS conditions — deliberately extending CARNATIONS research from detection into active vehicle response, closing a gap in the Center's portfolio.

The project was formally initiated in late November 2025 following required USDOT approvals, with active technical work beginning in February 2026. Initial efforts focused on coordinating roles, scope, and research direction across the two participating university teams — an essential first step for any new multi-institutional collaboration — alongside a literature review to support development of vehicle-control approaches under positioning uncertainty. The team is now designing initial system concepts, combining multi-source positioning, integrity monitoring, cooperative vehicle control, terrain fingerprinting, and adaptive spectrum management into a single, unified implementation approach. This phase establishes the foundation for the development and testing activities to follow, with the team building toward evaluating how connected and automated vehicles should adjust speed and following behavior in real time when their positioning confidence drops due to jamming or spoofing.

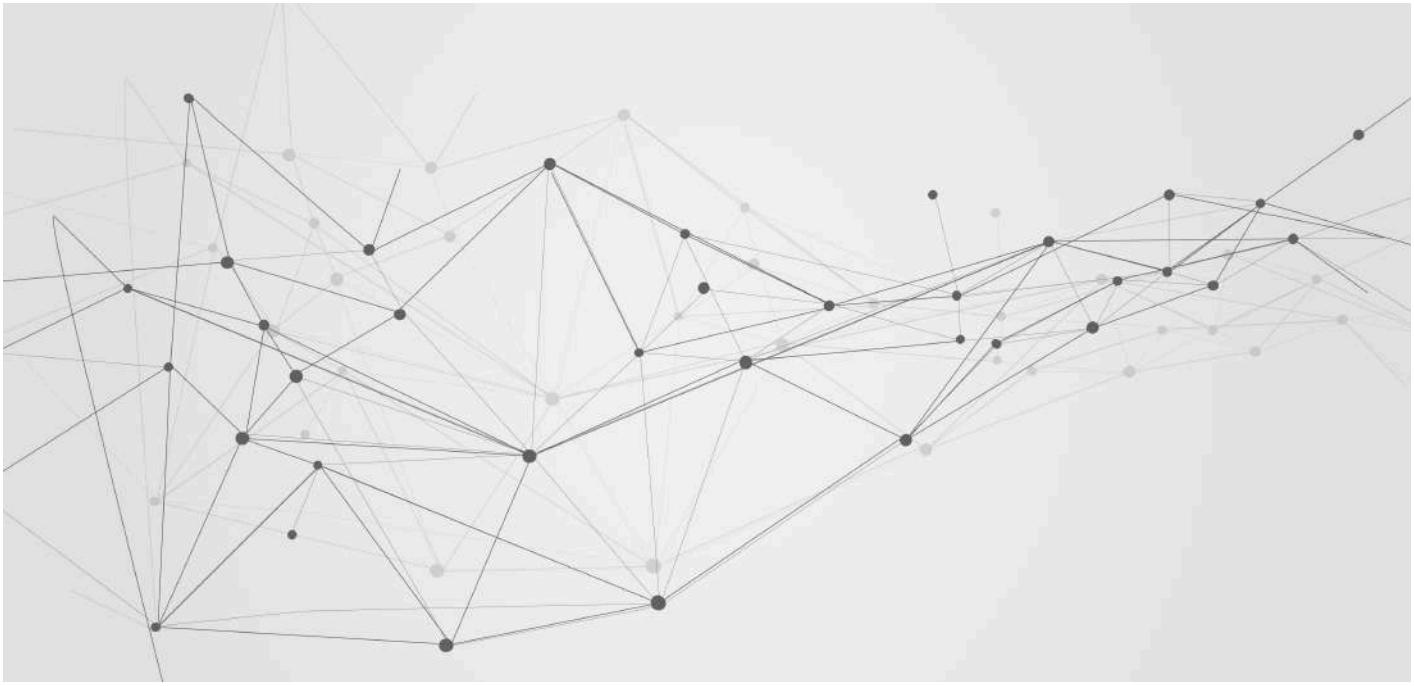
IMPACT

As one of the Center's newest initiatives, this project positions CARNATIONS to directly address vehicle control — not just detection — under GNSS attack, closing the loop between spoofing awareness and safe, automated driving response for the CAVs of the near future.

NEW INITIATIVES

The REACH Program

EXPANDING OUR REACH & CAPABILITIES



CARNATIONS has launched the REACH program, a new initiative gaining significant momentum and industry support. REACH expands the Center's engagement with broader transportation stakeholders, connecting our research outputs with partners, practitioners, and policymakers who can act on our findings. With one new project added through this initiative, our active portfolio has grown to 14 projects — a milestone that reflects the increasing demand for CARNATIONS' expertise.

04 By the numbers

A year of resilient-PNT research, measured — output, partners and recognition.

IMPACT

The year in numbers

14
ACTIVE RESEARCH PROJECTS

5
PARTNER UNIVERSITIES

83
PEER-REVIEWED PAPERS

2
BEST-PRESENTATION AWARDS · ION GNSS+

3
TRANSPORT MODES — AIR, SURFACE, SEA

1
PODCAST LAUNCHING — WAYPOINT

PROJECT INVOLVEMENT BY UNIVERSITY

CENTER-WIDE IMPACT SNAPSHOT

The year at a glance

April 2025 – March 2026

42
LEADERSHIP POSITIONS HELD

26
NEW INSTITUTIONAL COLLABORATIONS

40+
INDUSTRY & GOVERNMENT PARTNERS

87
STUDENTS IN CARNATIONS COURSES

12
OUTREACH EVENTS

1
IEEE FELLOW ELECTED

YEAR-DEFINING MILESTONES

- ★ Director Boris Pervan elected IEEE Fellow (Jan 2026) for contributions to satellite-navigation integrity.
- ★ TruNav-CARNATIONS Tech-transfer partner advanced through the final 4 out of 448 submissions of the DOT ARPA-I Ideas Challenge; patent application filed.
- ★ Ph.D. student Liam Carey named DOT Outstanding Student and CARNATIONS Student of the Year.
- ★ Two new testbeds online — Virginia Tech Smart Roads anti-RFI site and the UC Riverside Smart Intersection.
- ★ Research field-tested under live jamming & spoofing at APEX25 (White Sands) and Jammertest 2025, Norway.
- ★ Publications grew 64 → 83, incl. IEEE T-AES and a NAVIGATION journal review.
- ★ The Waypoint podcast launched; first full episode May 12, 2026, with a new documentary series.
- ★ CARNATIONS Days 2025 drew 67 participants to Virginia Tech, keynoted by DOT's Dr. Andrew Hansen.
- ★ AI knowledge tool CARNATIONS Navigator entered testing; two Best Presentation Awards at ION GNSS+ 2025.
- ★ Deepened ties with 40+ partners — Xona, Inertial Labs, Spirent, MITRE and StarNAV.
- ★ Chicago State advanced a joint PNT partnership with the University of North Texas and a new IEEE committee.
- ★ Ahead: CARNATIONS Days 2026 at UC Riverside (Jul 15–16) and the Transportation Cybersecurity Summit, D.C.

05 People & Culture

The students and faculty carrying the field forward — in their own words.

JADE BABCOCK-CHI

ABOUT

Jade Babcock-Chi is a student researcher at Stanford University and a member of the CARNATIONS University Transportation Center

STUDENT PROFILE

Jade Babcock-Chi

STUDENT MEMBER · STANFORD UNIVERSITY

Q. What is your travel story?

This past September, our team traveled to Bleik, Andøya, Norway to participate in Jammertest 2025: a unique, government-coordinated RF interference testing event now in its fourth year. Organized by a consortium of Norwegian government agencies - including the Norwegian Space Agency, the Norwegian Public Roads Administration, and the Norwegian Defense Research Establishment - Jammertest brings together roughly 300 - 400 participants from government and industry worldwide to stress-test technology against real-world GNSS jamming and spoofing scenarios.

Q. What makes your team special?

Our team was proud to be among a small handful of U.S. universities invited to attend. We deployed a distributed network of stationary GNSS monitoring receivers positioned throughout the town and surrounding area, designed to simultaneously observe the same interference sources and enable source localization. We also conducted mobile data collection, mounting receivers on vehicles and driving survey routes during live RFI events. The scheduled, controlled nature of the tests provided an invaluable research environment that is nearly impossible to replicate outside of a coordinated event like this, and the data collected will directly advance our work in GNSS resilience and interference detection.

Jammertest offers a scheduled, controlled environment for observing live GNSS interference — one that is nearly impossible to replicate anywhere else.

LIAM CAREY

RECOGNITION

Best Presentation Award, ION GNSS+ 2025 · DOT Outstanding Student Award 2025. Advised by Dr. Mathieu Joerger.

STUDENT PROFILE

Liam Carey

PH.D. CANDIDATE · RESILIENT NAVIGATION

Q. What problem are you trying to solve?

My research is on how to best leverage multi-sensor augmentation intended for transportation applications to detect subtle attacks that may consistently alter all measurements of a subset of sensors. The objective is to achieve more resilient PNT. I develop algorithms at the observables level: for GNSS, I am using range and range-rate as inputs. In tight collaboration with the MITRE Corporation' Steve Langel, who has been mentoring me under CARNATIONS REACH (the Research Engagement and Collaboration Hub), I focus on the Cumulative Vector Sums (CVS) monitor to detect faults and bounding the impacts of undetected faults on the navigation solution. Specifically, the CVS monitor aims to improve detection of subtle shifts over time in the mean of the measurement errors. My work presented at ION GNSS+ 2025 evaluated this monitor for an example GNSS/INS scenario where a GNSS spoofer attempted to slowly pull the vehicle off course. Now I'm working on applying the monitor to a more general set of faults and analyzing the performance against realistic faults models found in GNSS standards for aviation.

Q. What does a typical week look like

Most of my time in the week is spent creating the MATLAB simulations used to evaluate the performance of the monitors. We focus on determining what scenarios and performance metrics would best compare the performance of the detection algorithms and build the simulation for that analysis. After completing the simulation, we compare the results with what we expected to see based on our understanding of each monitor.

"I focus on the Cumulative Vector Sums (CVS) monitor to detect faults and bounding the impacts of undetected faults on the navigation solution."

Q. Where do you want this to go?

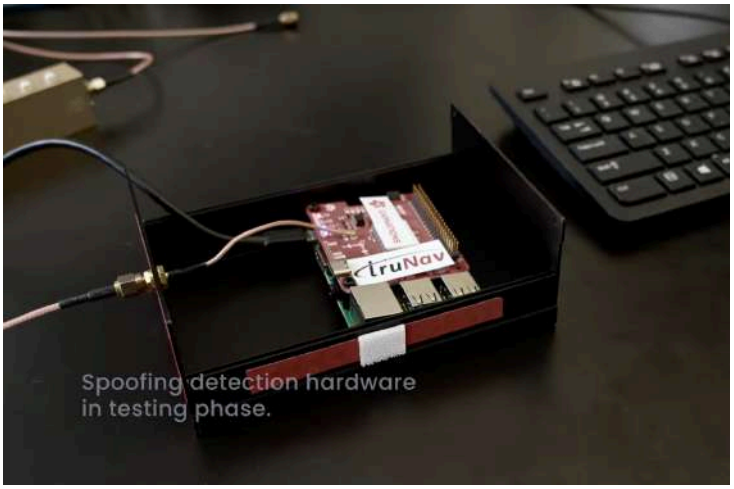
This research aims at advancing resilient PNT technology by developing more effective interference detection and integrity monitoring algorithms. Achieving high navigation integrity with high availability and without unexpected interruption is essential in safety-critical applications, especially in our transportation system's user equipment and infrastructure.

06 News & Recognition

Awards, arrivals, and a new podcast — a year of momentum across the Center.

NEWS & RECOGNITION

A year of awards and arrivals



Spoofing detection hardware in testing phase.

Patent: IMU-Based GNSS Spoofing Detection

CARNATIONS' provisional patent for detecting GNSS spoofing using Inertial Measurement Unit (IMU) technology is on track for approval by Summer 2025. The innovation offers a low-cost, high-reliability approach to spoofing detection that can be integrated into existing receiver hardware.

A commercialization and marketing strategy has been developed in collaboration with the Kaplan Institute at Illinois Tech, positioning this technology for rapid industry uptake.

IN BRIEF

STUDENTS

Two CARNATIONS papers win Best Presentation at ION GNSS+ 2025

TECH TRANSFER

TruNav reaches ARPA-I Ideas Challenge Finals

STUDENTS

Liam Carey receives DOT Outstanding Student Award 2025

PUBLICATION

New research advances Starlink-based backup PNT

UPDATES

Mapping the Invisible Threat: Inside the CARNATIONS Navigator AI Platform

LAUNCHED IN SUMMER 2026 · PODCAST

CARNATIONS Waypoint

A thought-leadership series on the future of transportation.
www.youtube.com/@illinoistechcarnations
Ep. 1 — Dr. Todd Walter (Stanford). Ep. 2 — Dr. Sherman Lo (Stanford).

NEWS & RECOGNITION

Two CARNATIONS papers win Best Presentation at ION GNSS+ 2025

Two CARNATIONS-affiliated papers authored by Ph.D. students Hasan Kinatas and Liam Carey received Best Presentation Awards at the Institute of Navigation's GNSS+ Conference — one of the most prestigious events in the navigation research community.

Liam Carey & Dr. Mathieu Joerger
"CUSUM-Based Innovations Monitoring Against Spoofing Threats"
Advanced techniques for detecting and mitigating GNSS spoofing attacks using continuous monitoring methods.

Hasan Kinatas & Dr. Mathieu Joerger
"Experimental Evaluation of Collaborative Navigation Through Shared Motion Constraints During GNSS Interference"
Demonstrates how collaborative navigation enhances resilience during GNSS interference events through shared motion data.

TruNav Wins ARPA-I Semifinals

TruNav-CARNATIONS Tech-transfer partner advanced through the final 4 out of 448 submissions of the DOT ARPA-I Ideas Challenge; patent application filed.

NEWS & RECOGNITION

Liam Carey receives DOT Outstanding Student Award 2025

CARNATIONS is proud to recognize Liam Carey, a student of the CARNATIONS program at Virginia Tech, for receiving a distinguished national award that highlights his excellence in navigation research. Liam Carey won the UTC Outstanding Student of the Year Award from the U.S. Department of Transportation (DOT). This award recognizes students who demonstrate exceptional academic achievement, and meaningful contributions to transportation research.

New research advances Starlink-based backup PNT

CARNATIONS researchers Dr. Mark Psiaki and John Bowman (Virginia Tech) have co-authored a new paper that advances the understanding and use of Starlink Ku-band downlink signals for opportunistic Positioning, Navigation, and Timing (PNT). The paper, led by student first author Wenkai Qin, is titled “Pilots and Other Predictable Elements of the Starlink Ku-Band Downlink” and is now available on arXiv while under peer review.

NEWS & RECOGNITION

CARNATIONS Waypoint

CARNATIONS launched Waypoint, a thought-leadership podcast series dedicated to navigating transportation research and innovation. The name reflects our dual mission: CARNATIONS represents research excellence and academic collaboration, while Waypoint signifies a guiding landmark in navigation — a platform where leading voices share ideas, insights, and innovations in transportation, GPS, and navigation research.

Episode 1 — Dr. Todd Walter, Stanford

In the first episode of the CARNATIONS Waypoint Podcast, Dr. Todd Walter of Stanford University's GPS Laboratory breaks down how modern navigation systems stay accurate — and what it takes to keep them resilient when the signals we depend on come under threat.

Episode 2 — Dr. Sherman Lo, Stanford

What happens when GPS cannot be trusted?
Dr. Lo examines real-world spoofing events, the threat landscape facing transportation systems, and the strategies researchers are developing to detect and defeat manipulation.

LAUNCHED IN SUMMER 2026 · PODCAST

New episodes feature leading researchers, industry practitioners, and policy experts discussing the future of transportation navigation. Find CARNATIONS Waypoint on all major podcast platforms.
iitcarnations.org/podcast

NEWS & RECOGNITION

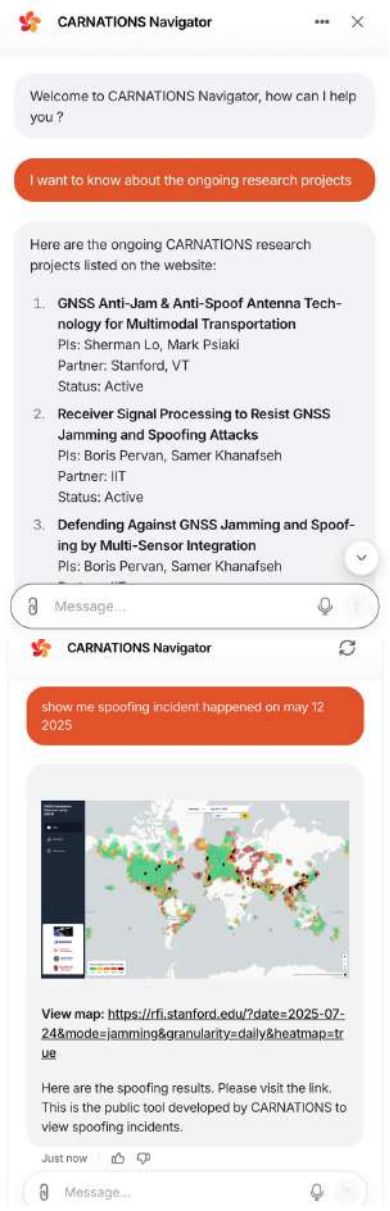
Mapping the Invisible Threat: Inside the CARNATIONS Navigator AI Platform

When GPS signals disappear — jammed by a hostile actor or spoofed by a counterfeit broadcast — the consequences can ripple across aviation, maritime shipping, road freight, and emergency response in seconds. Making sense of the global landscape of such incidents has long required piecing together disconnected tools, datasets, and research scattered across institutions and disciplines. That fragmentation is exactly what the CARNATIONS Navigator was built to solve.

Developed by Aashish Narang, the Navigator is an AI-powered platform that acts as an intelligent front door to everything CARNATIONS — and it does far more than track threats.

At its core, Navigator serves as a comprehensive knowledge companion for everything the Center does and everyone it works with. Ask it about ongoing research projects, and it draws from the full depth of CARNATIONS' three-pillar mission — toughening, augmenting, and protecting Positioning, Navigation, and Timing (PNT) systems across multimodal transportation. Ask about industry partnerships, and it surfaces connections spanning the FAA, Caltrans, DOT, Collins Aerospace, and more than two dozen other partners embedded in the Center's consortium. Ask about education opportunities, workforce development programs, publications, events, or USDOT reports — Navigator knows, and it answers.

Two of its most powerful features come directly from tools built by CARNATION's partner institutions. Stanford University's Spoofing Incident Tracker maps spoofing events worldwide using its WAAS-NAS Heatmap, while Virginia Tech's Jamming Detection App delivers real-time and historical views of jamming activity globally. Navigator layers AI intelligence on top of both, making their outputs queryable and contextualized within the broader landscape of CARNATIONS research — something neither tool could achieve in isolation.



> The result is a platform that meets its users wherever they are. A graduate student getting oriented in the field, a policymaker trying to understand the threat environment, an industry partner exploring collaboration opportunities, or a seasoned researcher looking for the latest project updates — all find what they need through a single, conversational interface. In a Center dedicated to protecting the Nation's most critical navigation infrastructure, the Navigator represents something fitting: a tool that makes the sum of CARNATIONS' work greater than its parts.

07 Community & Events

Five universities and dozens of partners – one shared mission to secure navigation.

COMMUNITY & EVENTS

Connecting the CARNATIONS network

CARNATIONS DAYS 2025

RECAP · 2025 · VIRGINIA TECH

Two days of consortium collaboration

CARNATIONS Days 2025 brought researchers, PIs, students and industry partners together at Virginia Tech for an intensive two-day convening — sharing project updates, reviewing progress, running cross-team collaboration sessions and connecting with the industry advisory board. It underscored the strength of the consortium model and generated new collaborative research directions.

JULY 15–16, 2026 · UC RIVERSIDE

CARNATIONS DAYS at Riverside

CARNATIONS Days 2026 on July 15–16, 2026, hosted by the University of California, Riverside in collaboration with Illinois Institute of Technology. Join us for two days of collaboration, research updates and discussion at the Riverside Innovation Corridor.

CENTER ACTIVITY

The year across the consortium

50

RESEARCH DISCUSSION CALLS

Bi-weekly sessions keeping the full consortium connected and informed on project progress.

7

WEBINARS HOSTED

Expert-led sessions covering key topics in navigation, cybersecurity and transportation.

7

CROSS-CUTTING COURSES

Specialized courses in navigation, GPS design and autonomous systems across partner universities.

2

INTERNATIONAL TESTS

Real-world data-collection campaigns in Norway and the Eastern Mediterranean.

08 Publications

Eighty-three peer-reviewed papers — the full record behind the year's research.

83
PAPERS & PRESENTATIONS

5
PARTNER UNIVERSITIES

4
YEARS · 2023–2026

SELECTED PUBLICATIONS · 2023–2026

The published record

Eighty-three peer-reviewed papers, conference presentations and submissions from the CARNATIONS consortium — journals, ION and IEEE proceedings, and field campaigns, listed by year.

2023 2 PAPERS

01 GNSS spoofing detection and exclusion by decomposition of the complex cross-ambiguity function with INS aiding

Ahmed, S. · Khanafseh, S. · Pervan, B.

PROC. ION GNSS+ · DENVER, CO · SEP 2023

02 Resilient PNT for safe transportation

Joerger, M. · Jada, S. · Yan, C. · Psiaki, M. · Bowman, J.

AUVSI SYMPOSIUM · BLACKSBURG, VA · OCT 2023

2024 28 PAPERS

03 Outlier accommodation for multi-GNSS precise point positioning using a risk-averse performance-specified approach

Hu, W. · Uwineza, J.-B. · Farrell, J. A.

AMERICAN CONTROL CONFERENCE (ACC) · JAN 2024

04 Integrity with LiDAR incorrect-extraction faults in adverse weather conditions

Nagai, K. · Ahmed, S. · Pervan, B.

PROC. ION ITM · LONG BEACH, CA · JAN 2024

05 Infrastructure-assisted cooperative state estimation via augmentation of asynchronous kinematic measurements

P. Saswat

ION ITM · LONG BEACH, CA · JAN 2024

06 Feasibility studies on CAV applications with state uncertainties: a survey

P. Saswat

IEEE FISTS · FEB 2024

07 Fault-free integrity and continuity for driverless urban vehicle navigation with multi-sensor integration: a case study in downtown Chicago

Nagai, K. · Spenko, M. · Henderson, R. · Pervan, B.

NAVIGATION 71(1) · MAR 2024

08 Optimal INS monitor for GNSS spoofer tracking-error detection

Kujur, B. · Khanafseh, S. · Pervan, B.

NAVIGATION 71(1) · MAR 2024

09 Jamming-resilient mirror-element allocation scheme for OIRS-aided UAV-based FSO networks

M. Ayyash

IEEE TRANS. INTELLIGENT VEHICLES · MAR 2024

10 Impacts of GNSS interference on CAVs

Joerger, M. · Jada, S.

ERASMO, UTC FRANCE · MAR 2024

11 Optimization-based outlier accommodation for CAV state estimation

Hu, W. · Mohsenian-Rad, H. · Farrell, J. A.

SUBMITTED · IEEE TRANS. VEHICULAR TECHNOLOGY · MAR 2024

12 Convex reformulation of risk-averse state estimation with binary variables

Hu, W. · Jiang, Z. · Mohsenian-Rad, H. · Farrell, J. A.

SUBMITTED · CDC · MAR 2024

13 Resilient, federated large language models over wireless networks: why the PHY matters

Andrei, V. · Djuhera, A. · Li, X. · Monich, U. · Boche, H. · Saad, W.

SUBMITTED · IEEE GLOBECOM · APR 2024

14 Fault-free integrity of urban driverless vehicle navigation with multi-sensor integration: a case study in downtown Chicago

K. Nagai

ION WEBINAR · APR 2024

15 An automated pipeline for detection and localization of GNSS interference sources

Z. Liu

AEROSPACE UPP CONFERENCE · APR 2024

16 Low-cost GNSS monitors for RFI detection

A. Kriezis

AEROSPACE UPP CONFERENCE · APR 2024

17 Jamming attacks on FSO networks: challenges, opportunities, and a public-safety use case

M. Ayyash

IEEE WF-PST · MAY 2024

18 Resilient, federated large language models over wireless networks: why the PHY matters

Andrei, V. C. · Djuhera, A. · Li, X. · Monich, U. J. · Boche, H. · Saad, W.

PROC. IEEE ICC WORKSHOP · DENVER, CO · JUN 2024

2024 28 PAPERS · CONT.

19 Fundamental architectures for high-integrity georeferenced LiDAR positioning
Rife, J. · Wassaf, H. · Khanafseh, S. · Pervan, B.
PROC. ION GNSS+ · BALTIMORE, MD · SEP 2024

20 Optimization-based outlier accommodation for tightly-coupled RTK-aided inertial navigation in urban environments
M. Stas
IEEE ITSC · EDMONTON · SEP 2024

21 Uncertainty quantification for radar/inertial pose estimation in GNSS-denied areas
Becker, J. · Joerger, M.
ION GNSS+ · BALTIMORE, MD · SEP 2024

22 Wrong-association risk bounding using innovation-projections for landmark-based LiDAR localization
Joerger, M. · Hassani, A.
ION GNSS+ · BALTIMORE, MD · SEP 2024

23 Integrity with LiDAR positioning: case studies in automatic feature extraction
Nagai, K. · Pervan, B.
ION GNSS+ · BALTIMORE, MD · SEP 2024

24 Enhanced integrity of LiDAR localization: a study on feature-extraction techniques
Nagai, K. · Pervan, B.
ION GNSS+ · BALTIMORE, MD · SEP 2024

25 Time-diverse Doppler-only LEO PNT: initial solution
Moore, M. O. · Psiaki, M. L. · Buehrer, R. M.
ION GNSS+ · BALTIMORE, MD · SEP 2024

26 Design and analysis of resilient vehicular platoon systems over wireless networks
Shui, T. · Saad, W.
PROC. IEEE GLOBECOM · DEC 2024

27 Fast geometric learning of MIMO signal detection over Grassmannian manifolds
Shelim, R. · Saad, W. · Ramakrishnan, N.
PROC. IEEE GLOBECOM · DEC 2024

28 Resilient, federated large language models over wireless networks: why the PHY matters
Andrei, V. C. · Djuhera, A. · Li, X. · Monich, U. J. · Saad, W. · Boche, H.
PROC. IEEE GLOBECOM · DEC 2024

29 Uncovering subtle GNSS spoofing via cross-ambiguity decomposition
Ahmed, S. · Khanafseh, S. · Pervan, B.
IEEE TRANS. AES · DEC 2024

30 GNSS spoofing observed in Israel using wideband RF data and software radio
Psiaki, M. · Frid, A.
ISRAEL ANNUAL CONF. ON AEROSPACE SCIENCES · HAIFA · MAY 2024

2025 46 PAPERS

31 Combining ADS-B, LCM and DPA for GNSS jammer detection
Chen, Y.-H. · Liu, Z. · Kriezis, A. · Lo, S. · Walter, T.
ION ITM · LONG BEACH, CA · JAN 2025

32 Performance of an optimal INS monitor against live spoofing
Kujur, B. · Khanafseh, S. · Pervan, B.
ION ITM · LONG BEACH, CA · JAN 2025

33 Interference detection in a massive GNSS jammer test
Chen, Y.-H. · Liu, Z. · Kriezis, A. · Lo, S. · Walter, T.
ION ITM · LONG BEACH, CA · JAN 2025

34 Observations of GNSS spoofing in Russia, 2023–2024
Lo, S. · Liu, Z. · Ibrahim, L. · Chen, Y.-H. · Walter, T.
ION ITM · LONG BEACH, CA · JAN 2025

35 Real-world spoofing detection with low-cost receivers
Kriezis, A. · Chen, Y.-H. · Akos, D. · Lo, S. · Walter, T.
ION ITM · LONG BEACH, CA · JAN 2025

36 Low-cost receiver RF-interference analysis
Kriezis, A. · Chen, Y.-H. · Lo, S. · Walter, T. · Pullen, S. · Akos, D.
INSIDE GNSS · MAR 2025

37 Jammertest 2024 results & lessons learned
S. Lo
NORDIC NAVIGATION FORUM GENERAL ASSEMBLY · APR 2025

38 Experimental validation for GNSS spoofing detection by decomposition of the complex cross-ambiguity function
Ahmed, S. · Khanafseh, S. · Pervan, B.
PROC. IEEE/ION PLANS 2025 · SALT LAKE CITY, UT · APR 2025

39 Exploring LiDAR resilience: a review of spoofing threats in autonomous driving
Nemana, M. · Nagai, K. · Khanafseh, S. · Pervan, B.
PROC. IEEE/ION PLANS 2025 · SALT LAKE CITY, UT · APR 2025

40 Analysis of time-diverse Doppler-only LEO PNT
Moore, M. O. · Psiaki, M. L. · Buehrer, R.
IEEE/ION PLANS 2025 · SALT LAKE CITY, UT · APR 2025

2025 46 PAPERS · CONT.

41 Fault-detector sensitivity in centralized collaborative localization
Kuwada, S. · Joerger, M. · Spenko, M.
IEEE/ION PLANS 2025 · SALT LAKE CITY, UT · APR 2025

42 GNSS spoofing detection and exclusion using decomposition of the complex cross-ambiguity function (CCAF)
S. Ahmed
PH.D. ORAL DEFENSE · MAY 2025

43 SEE-V2X: a C-V2X direct-communication dataset – an application-centric approach
Mo, R. · Wu, B. · Qiu, H.
ACM SENSYS · MAY 2025

44 Integrity monitoring for centralized connected-autonomous-vehicle localization
Kuwada, S. · Joerger, M. · Spenko, M.
ICRA 2025 · ATLANTA, GA

45 Uncovering subtle GNSS spoofing by decomposing the complex cross-ambiguity function
Ahmed, S. · Khanafseh, S. · Pervan, B.
IEEE TRANS. AES · ACCEPTED JUN 2025

46 Data association using innovation-projections for landmark-based LiDAR localization
Joerger, M. · Hassani, A. · Spenko, M. · Becker, J.
NAVIGATION · 2025

47 Spherical grid-based IMU/LiDAR localization and uncertainty evaluation using signal quantization
Hassani, A. · Joerger, M.
NAVIGATION · 2025

48 Advanced receiver autonomous integrity monitoring for multi-constellation and LEO-augmented GNSS
D. Racelis
PH.D. DISSERTATION · VIRGINIA TECH · JUL 2025

49 QoS-enabled wireless split federated learning: a reinforcement-learning and optimization approach
CARNATIONS consortium
IEEE TRANS. CONSUMER ELECTRONICS · JUL 2025

50 Multi-stage enhanced zero-trust intrusion-detection system for unknown-attack detection in IoT and traditional networks
CARNATIONS consortium
ACM TRANS. PRIVACY & SECURITY · AUG 2025

51 TDOA-based spoofing-source localization using multi-constellation unsynchronized receivers
Babcock-Chi, J. · Lo, S. · Chen, Y.-H. · Blanch, J. · Walter, T.
PROC. ION GNSS+ 2025 · BALTIMORE, MD · SEP 2025

52 Blind multi-vehicle GNSS spoofing detection with extended baselines
Beatty, D. · Psiaki, M. L.
PROC. ION GNSS+ 2025 · BALTIMORE, MD · SEP 2025

53 Performance of an optimal INS monitor against jamming-then-spoofing scenarios
Kujur, B. · Khanafseh, S. · Pervan, B.
PROC. ION GNSS+ 2025 · BALTIMORE, MD · SEP 2025

54 Integrity analysis of GNSS/LEO positioning using range and Doppler measurements
Wang, S. · Racelis, D. · Joerger, M.
PROC. ION GNSS+ 2025 · BALTIMORE, MD

55 The why & the how of research into LEO-based signals of opportunity
M. L. Psiaki
PROC. ION GNSS+ 2025 · BALTIMORE, MD

56 A generalized GDOP analysis for PNT that requires sequential filtering
M. L. Psiaki
PROC. ION GNSS+ 2025 · BALTIMORE, MD

57 CUSUM-based innovations monitoring against spoofing threats
Carey, L. · Langel, S. · Joerger, M.
PROC. ION GNSS+ 2025 · BALTIMORE, MD

58 Experimental evaluation of collaborative navigation through shared motion constraints during GNSS interference
Kinatas, H. · Joerger, M.
PROC. ION GNSS+ 2025 · BALTIMORE, MD

59 Kalman-filter integrity monitoring over finite time intervals
Marti, M. · Joerger, M.
PROC. ION GNSS+ 2025 · BALTIMORE, MD

60 Enhancing GNSS resiliency against spoofing and jamming employing deep neural networks
CARNATIONS consortium
IEEE WF-PST 2025 · SEP 2025

61 The role of integrity monitoring in connected and automated vehicles: current state of practice and future directions
Nayak, S. P. · Barth, M.
IEEE ITS MAGAZINE · 2025

62 Artificial-intelligence-based semantic communications with multimodal data: framework and implementation
J.-L. DeRieux
M.S. THESIS · VIRGINIA TECH · 2025

2025 46 PAPERS · CONT.

63 Sensing-safety analysis for vehicular networks with integrated sensing and communication (ISAC)
Shui, T. · Saad, W. · Chen, M.
IEEE GLOBECOM · 2025

64 BEVCALIB: LiDAR-camera calibration via geometry-guided bird's-eye-view representations
Yuan, W. · Li, J. · Yue, J. · Shah, D. · Qiu, H.
CONF. ON ROBOT LEARNING (CORL) · SEP 2025

65 Determining protection levels using multiple antennas under spoofing conditions
Blanch, J. · Lo, S. · Chen, Y.-H. · Kriezis, A. · Walter, T.
PROC. IEEE/ION PLANS · SALT LAKE CITY, UT · APR 2025

66 A GNSS radio-frequency interference tour of Israel
Psiaki, M. · Frid, A. · Caravaca, C.
PROC. ION JOINT NAVIGATION CONF. · COVINGTON, KY · JUN 2025

67 Uncovering subtle GNSS spoofing by decomposing the complex cross-ambiguity function
Ahmed, S. · Khanafseh, S. · Pervan, B.
IEEE TRANS. AEROSPACE & ELECTRONIC SYSTEMS · VOL 61 NO 5 · OCT 2025

68 Fundamental architectures for high-integrity georeferenced LiDAR positioning: a review
Rife, J. · Khanafseh, S. · Pervan, B. · Wassaf, H.
NAVIGATION · VOL 72 · WINTER 2025

69 Integrated DME/INS alternative-PNT system for RNP 1.0
Kujur, B. · Khanafseh, S. · Pervan, B. · Vitan, V. · Berz, G. · Osechas, O.
PROC. ION GNSS+ 2025 · BALTIMORE, MD · SEP 2025

70 Performance of an optimal INS monitor against jamming-then-spoofing scenarios
Kujur, B. · Khanafseh, S. · Pervan, B.
PROC. ION GNSS+ 2025 · BALTIMORE, MD · SEP 2025

71 Exploring LiDAR resilience: a review of spoofing threats in autonomous driving
Nemana, M. · Nagai, K. · Khanafseh, S. · Pervan, B.
PROC. IEEE/ION PLANS 2025 · SALT LAKE CITY, UT · APR 2025

72 Performance of an optimal INS monitor against live spoofing
Kujur, B. · Khanafseh, S. · Pervan, B.
PROC. ION ITM · LONG BEACH, CA · JAN 2025

73 Sensing-safety analysis for vehicular networks with ISAC
Shui, T. · Saad, W. · Chen, M.
PROC. IEEE GLOBECOM (COMM. & INFO. SYSTEMS SECURITY) · TAIPEI · DEC 2025

74 Resilient vehicular communications with minimal jitter
Paul, P. · Saad, W. · Burger, E. W.
59TH ASILOMAR CONF. ON SIGNALS, SYSTEMS & COMPUTERS · PACIFIC GROVE, CA · NOV 2025

75 Enhancing GNSS resiliency against spoofing and jamming employing deep neural networks
Gandhi, D. · Shah, M. · Singh, A. · Ayyash, M.
IEEE WF-PST · ORLANDO, FL · 2025 · PP. 212–218

76 The role of integrity monitoring in connected and automated vehicles: current state of practice and future directions
Nayak, S. P. · Barth, M.
IEEE ITS MAGAZINE · VOL 17 NO 6 · NOV–DEC 2025

2026 7 PAPERS

77 GNSS jamming mitigation with a pilot-signal-aided deep-integration framework
Nagai, K. · Khanafseh, S. · Pervan, B.
PROC. ION ITM · ANAHEIM, CA · JAN 2026

78 Pilots and other predictable elements of the Starlink Ku-band downlink
Qin, W. · Psiaki, M. L. · Bowman, J. R. · Humphreys, T. E.
SUBMITTED · NPJ WIRELESS TECHNOLOGY · FEB 2026 · IN REVIEW

79 Global incidents of aviation spoofing in 2024–2025 detected with ADS-B
Lo, S. · Liu, Z. · Ibrahim, L. · Chen, Y.-H. · Akos, D. · Walter, T.
PROC. ION ITM · ANAHEIM, CA · JAN 2026

80 Fault-mode-aware integrity monitoring for collaborative CAV localization
Kuwada, S. · Joerger, M. · Spenko, M.
PROC. ION ITM · ANAHEIM, CA · 2026 · PP. 288–301

81 An augmented GNSS-DAS architecture for continuous and robust positioning
Wang, K. · Zhong, R. · Singh, A. · Jaber, M. · Ayyash, M.
IEEE ICC 2026 · GLASGOW, UK · ACCEPTED

82 Sensor- and communication-based GNSS spoofing and jamming detection framework for CAV applications
Stas, M. · Nguyen, J. · Snyder, R. W. · Mo, R. · Barth, M. J.
PROC. ION PACIFIC PNT 2026

83 R'CV2X: RSU-coordinated cooperative perception via C-V2X direct communication
Mo, R. · Tan, Z. · Qiu, H.
ACM MOBICOM 2026 · AUSTIN, TX · IN SUBMISSION

09
In closing

The road forward — and a reference to the terms behind the work.

LOOKING AHEAD

The Road Forward

With 14 active projects, a first patent on the horizon, a growing podcast platform and a technology-transfer partner advancing to national-competition semifinalist status, CARNATIONS is demonstrating what a Tier-1 University Transportation Center can achieve in just two years of operation.

The threats to GPS-dependent transportation are not hypothetical.

Jamming and spoofing incidents are increasing in frequency and sophistication worldwide. As autonomous vehicles, connected aircraft and smart infrastructure become more prevalent, the stakes grow higher. CARNATIONS is building the research foundation — and the next generation of scientists and engineers — that will keep America's transportation systems secure and resilient.

> *"As CARNATIONS enters its next phase, our focus is on translating research into real-world impact. The advances developed through our collaborative research will continue moving beyond the laboratory and into practical applications that strengthen the resilience of aircraft, highways, ports, and rail corridors that support our nation's transportation system."*
> *– Aashish Narang, Program Manager, CARNATIONS, Illinois Tech*

CONNECT WITH CARNATIONS

We invite industry partners, policymakers, students and fellow researchers to connect with us — through collaboration on a research project, participation in CARNATIONS Days, enrollment in a course, or a conversation about technology transfer.

WEBSITE	PODCAST	LINKEDIN	INSTAGRAM	YOUTUBE
iitcarnations.org	iitcarnations.org/podcast	IIT CARNATIONS	@iitcarnations	@IllinoistechCARNATIONS

To submit a research project, explore partnership opportunities, or subscribe to the CARNATIONS newsletter, visit iitcarnations.org.

REFERENCE

Glossary

A quick reference to the navigation, signal and transportation terms used throughout this issue.

GNSS

Global Navigation Satellite System — the satellite constellations (GPS, Galileo, GLONASS, BeiDou) that broadcast positioning signals.

PNT

Positioning, Navigation & Timing — the three services derived from GNSS that underpin modern transportation.

R-PNT

Resilient PNT — positioning that keeps working accurately when signals are degraded, denied or attacked.

Jamming

Overpowering a receiver with radio-frequency noise to deny access to the true navigation signal.

Spoofing

Transmitting counterfeit signals to deceive a receiver into computing a false position or time.

Integrity monitoring

Techniques that quantify how much a position solution can be trusted and flag faults in real time.

CUSUM

Cumulative sum — a statistical method that detects the onset of an attack from small changes in receiver innovations.

Inertial sensing

Accelerometers and gyroscopes (an IMU) that estimate motion independently of GNSS to bridge signal outages.

CAV

Connected & Automated Vehicle — a vehicle that both communicates with its surroundings and drives itself.

V2X

Vehicle-to-Everything — wireless links between a vehicle and other vehicles, infrastructure and networks.

Cooperative perception

Vehicles sharing sensor data so each sees beyond its own line of sight.

LEO

Low Earth Orbit — the altitude band of constellations such as Starlink, explored as a backup PNT source.

Edge AI

Machine-learning models running on local devices to detect signal degradation and improve positioning.

Multimodal transportation

The full network of surface, air and maritime modes — road, rail, ports and aviation.

UTC

University Transportation Center — a U.S. DOT-funded research consortium; CARNATIONS is a Tier-1 UTC.

U.S. DOT

United States Department of Transportation — the federal agency funding the CARNATIONS Center.

ION GNSS+

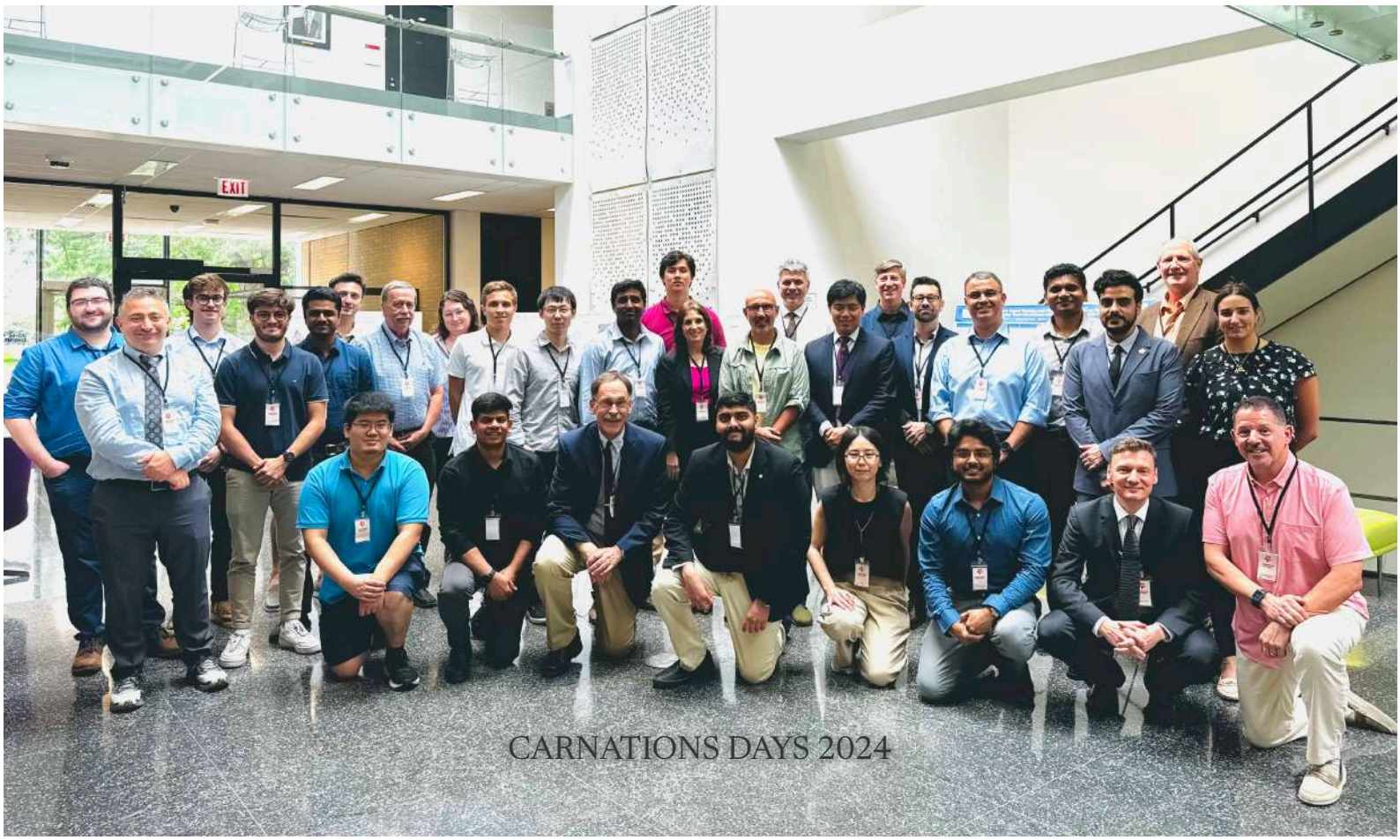
The Institute of Navigation's flagship annual conference on satellite navigation research.

Federated learning

Training a shared model across many devices without pooling their raw data centrally.

Notes

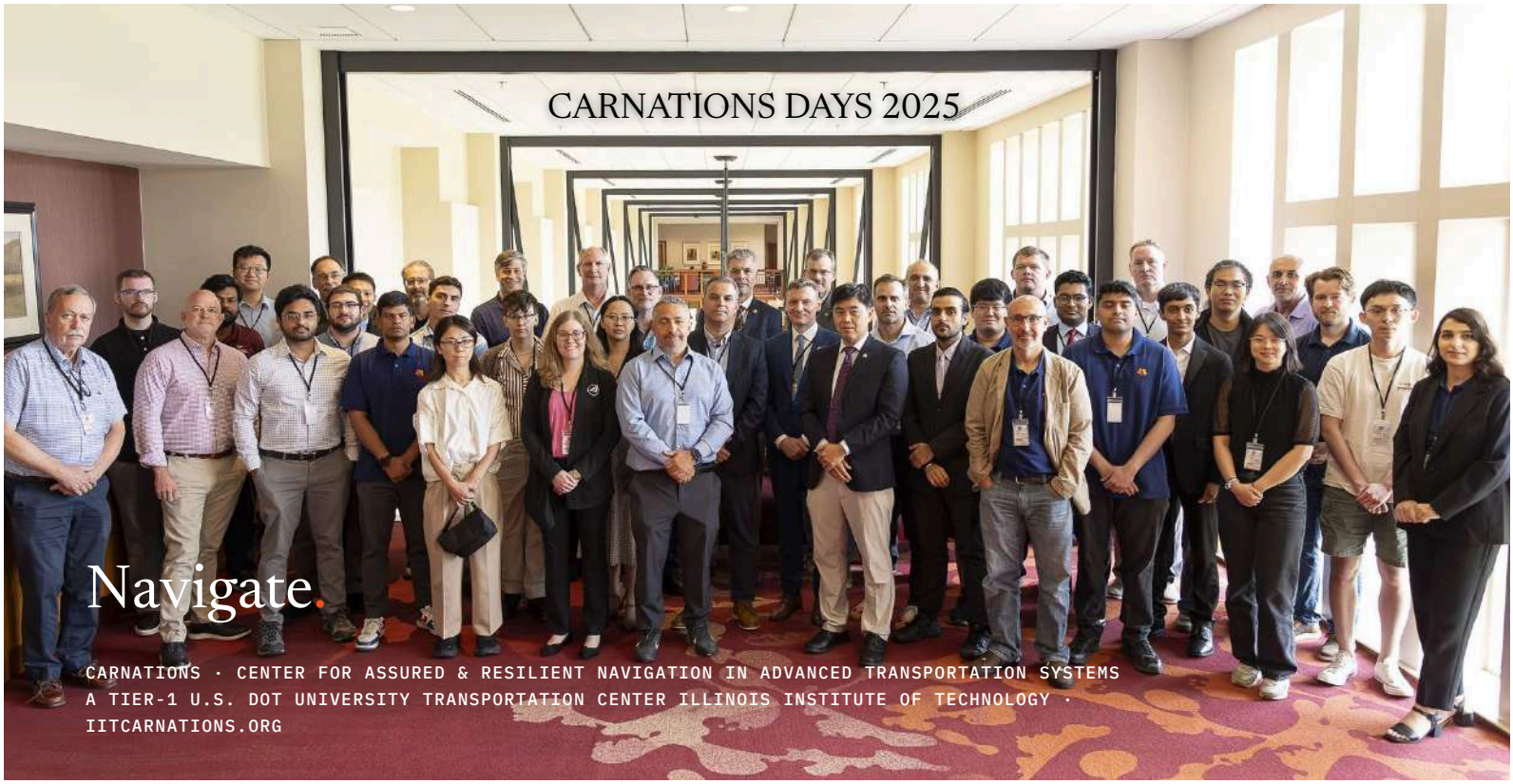
Notes



CARNATIONS DAYS 2024

DEPARTMENT OF TRANSPORTATION · UNITED STATES OF AMERICA

ILLINOIS TECH · CHICAGO STATE UNIVERSITY · UC RIVERSIDE · Stanford · VIRGINIA TECH



CARNATIONS DAYS 2025

Navigate.

CARNATIONS · CENTER FOR ASSURED & RESILIENT NAVIGATION IN ADVANCED TRANSPORTATION SYSTEMS
A TIER-1 U.S. DOT UNIVERSITY TRANSPORTATION CENTER ILLINOIS INSTITUTE OF TECHNOLOGY ·
IITCARNATIONS.ORG