CARNATIONS

Center for Assured & Resilient Navigation in Advanced Transportation Systems

2025 ANNUAL MAGAZINE

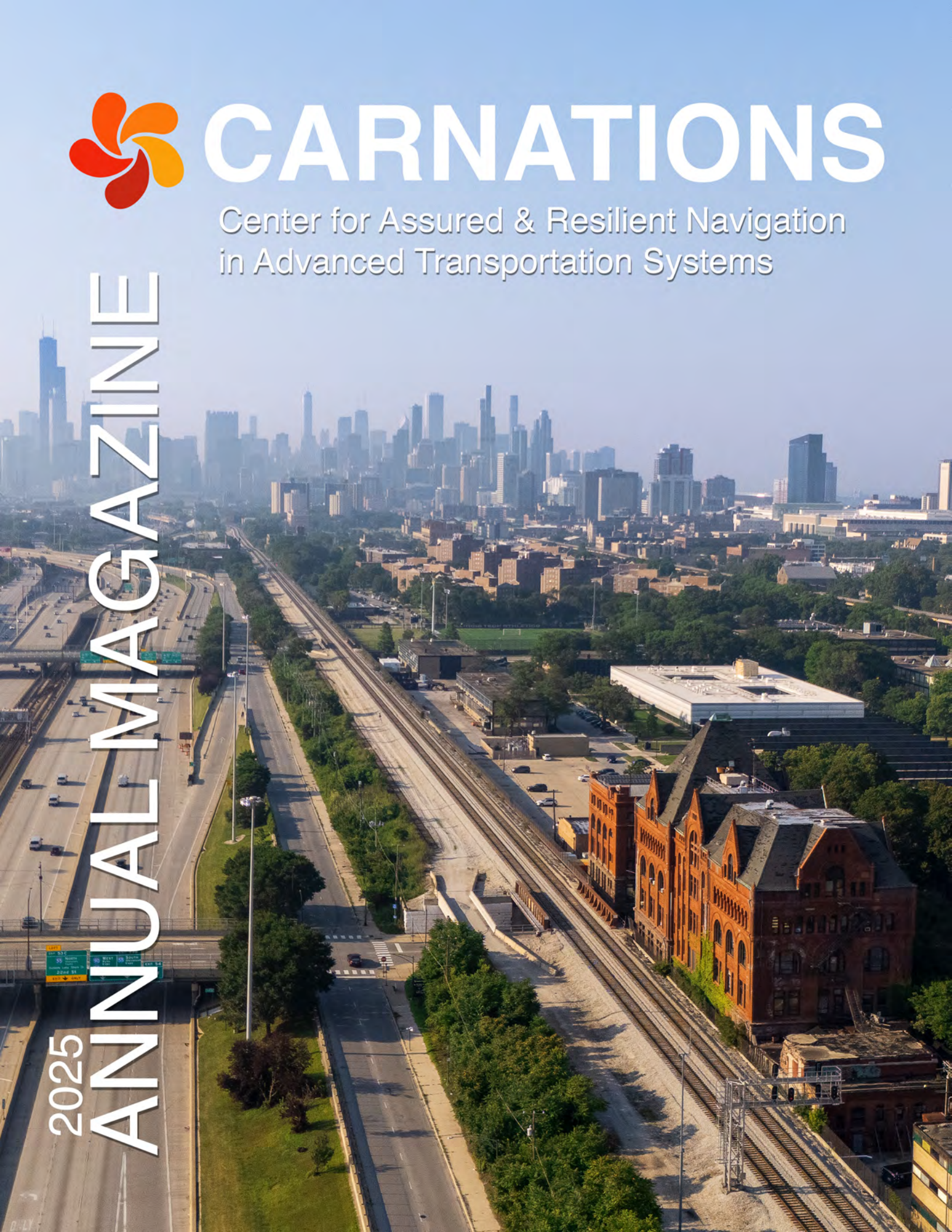
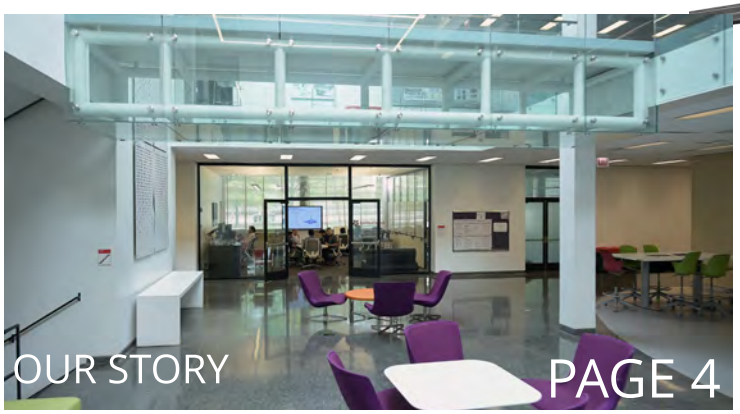


Table of Contents



Letter from the Director

Dr. Boris Pervan

"This year, CARNATIONS has advanced resilient PNT research like never before. Our work strengthens infrastructure against spoofing and jamming to protect U.S. transportation security."

As Director of CARNATIONS, I am proud to present this annual publication, which captures the remarkable progress made by our researchers, students, and partner institutions in advancing the field of Resilient Positioning, Navigation, and Timing (R-PNT).

At a time when transportation systems are increasingly reliant on precise and trustworthy navigation technologies, our work has grown in national relevance. From protecting against GPS spoofing and jamming threats to supporting emerging modes of mobility, such as autonomous vehicles and urban air mobility, CARNATIONS plays a central role in delivering dependable, secure, and innovative solutions for the U.S. transportation ecosystem.

Our accomplishments this year include a fivefold increase in scholarly output, expansion of inter-university collaborations, and enhanced partnerships with government and industry stakeholders. These successes reflect the strength of our mission—to drive research that not only informs but also transforms.

OUR STORY

CARNATIONS — Advancing Resilient Navigation for Safer Transportation

The Center for Assured and Resilient Navigation in Advanced TransportatION Systems (CARNATIONS) is a newly established Tier-1 University Transportation Center (UTC) focused on ensuring the security and reliability of Positioning, Navigation, and Timing (PNT) in multimodal transportation. Led by Illinois Tech with partner institutions Chicago State University, Stanford University, University of California Riverside, and Virginia Tech, CARNATIONS addresses the increasing vulnerabilities that threaten modern transportation systems, including radio frequency jamming and spoofing.

With transportation infrastructure heavily reliant on accurate navigation and communication, incidents like the severe 2022 jamming disruption at Denver International Airport underscore the critical need for resilient solutions.

CARNATIONS focuses on three core pillars to meet this challenge:

- **Toughen**: Strengthening existing PNT infrastructure to resist interference and cyber- physical

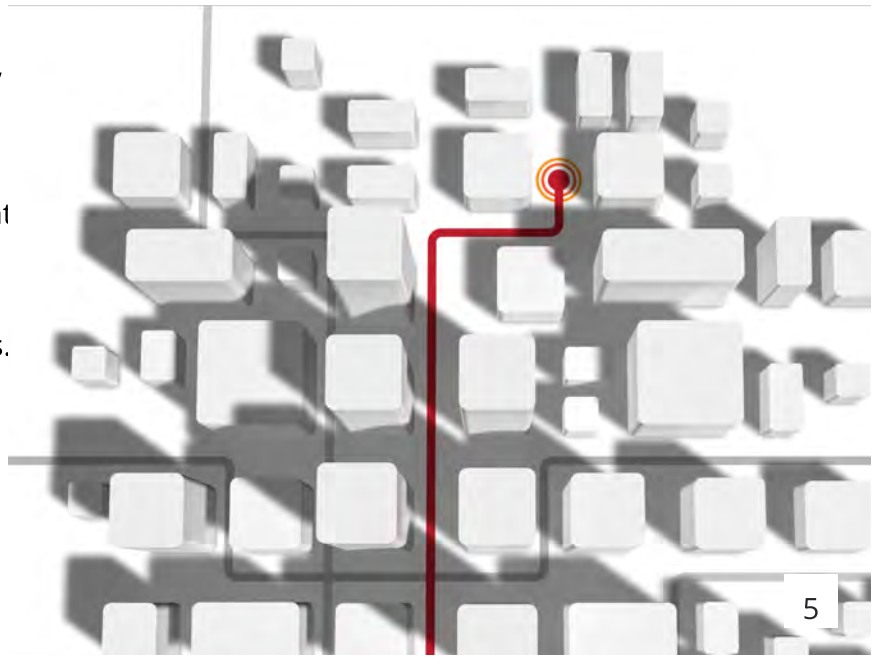
4

disruptions, including improvements in GNSS antennas and signal processing.

- **Augment**: Enhancing navigation capabilities by integrating multiple sensors and alternative signals, ensuring reliable positioning even when traditional signals are compromised.
- **Protect**: Developing advanced methods, including machine learning and collaborative vehicle communication, to detect and mitigate threats to PNT and detect, locate and mitigate related systems.

These efforts support the U.S. Department of Transportation's goals of reducing cybersecurity risks and promoting safety and mobility across transportation modes. CARNATIONS research from theoretical foundations to practical deployment, ensuring transportation networks remain secure and dependable.

Beyond research, the Center is dedicated to education and workforce development. Through new academic programs, CARNATIONS prepares the next generation of transportation professionals to address resilient navigation challenges.



The Meaning Behind the CARNATIONS Logo

From Petal to Partnership

The CARNATIONS logo, designed by Ana Pervan, symbolizes the consortium's collaborative spirit. It takes the natural form of five interwoven petals and stylizes them into a dynamic, circular arrangement. This evolution from a simple petal concept to a more abstract design signifies how individual entities (the institutions) come together to form a unified, forward-moving whole. The generated image showing a more realistic, detailed flower with distinct petals can be seen as the inspiration for the abstract form, where the organic shape is streamlined into a symbolic representation of partnership.

Institutions as Petals

Each of the five distinct, colored petals in the CARNATIONS logo embodies one of the core academic institutions contributing to the consortium. This design powerfully illustrates the strength of partnership and shared purpose across these diverse communities. The interlocking nature of the petals emphasizes how these individual institutions are not separate but are deeply connected and reliant on each other for collective advancement in transportation resilience.

The five academic partners that each petal describes are:

- **Illinois Tech**
- **Chicago State University**
- **UC Riverside**
- **Stanford University**
- **Virginia Tech**

CARNATIONS
Center for Assured & Resilient Navigation In Advanced Transportation Systems

UC RIVERSIDE
CHICAGO STATE UNIVERSITY
Stanford
ILLINOIS TECH
VIRGINIA TECH

RESEARCH PORTFOLIO: DRIVING INNOVATION ACROSS PROJECTS

Hardening the Core: CARNATIONS' Mission to Secure Positioning, Navigation, and Timing (PNT)
In today's transportation landscape, Positioning, Navigation, and Timing (PNT) is the invisible infrastructure powering everything from connected vehicles to air traffic control and port logistics. As these systems become increasingly embedded in the flow of everyday life, they also become high-value targets for malicious interference. From jamming and spoofing to broader cyber-physical disruptions, these threats not only risk individual safety but undermine confidence in the very systems designed to improve mobility.

CARNATIONS, the U.S. Department of Transportation's Tier-1 University Transportation Center, has identified the protection and enhancement of PNT systems as a strategic imperative. Through three synergistic research thrusts—Toughening, Augmenting, and Protecting PNT—the center is working to secure the transportation sector's digital nervous system.

I - TOUGHENING PNT: REINFORCING GNSS AT THE CORE

The “Toughening PNT” initiative targets the physical and algorithmic foundation of navigation systems. This effort involves enhancing hardware such as antennas and advancing embedded receiver to resist interference at its earliest point of entry.

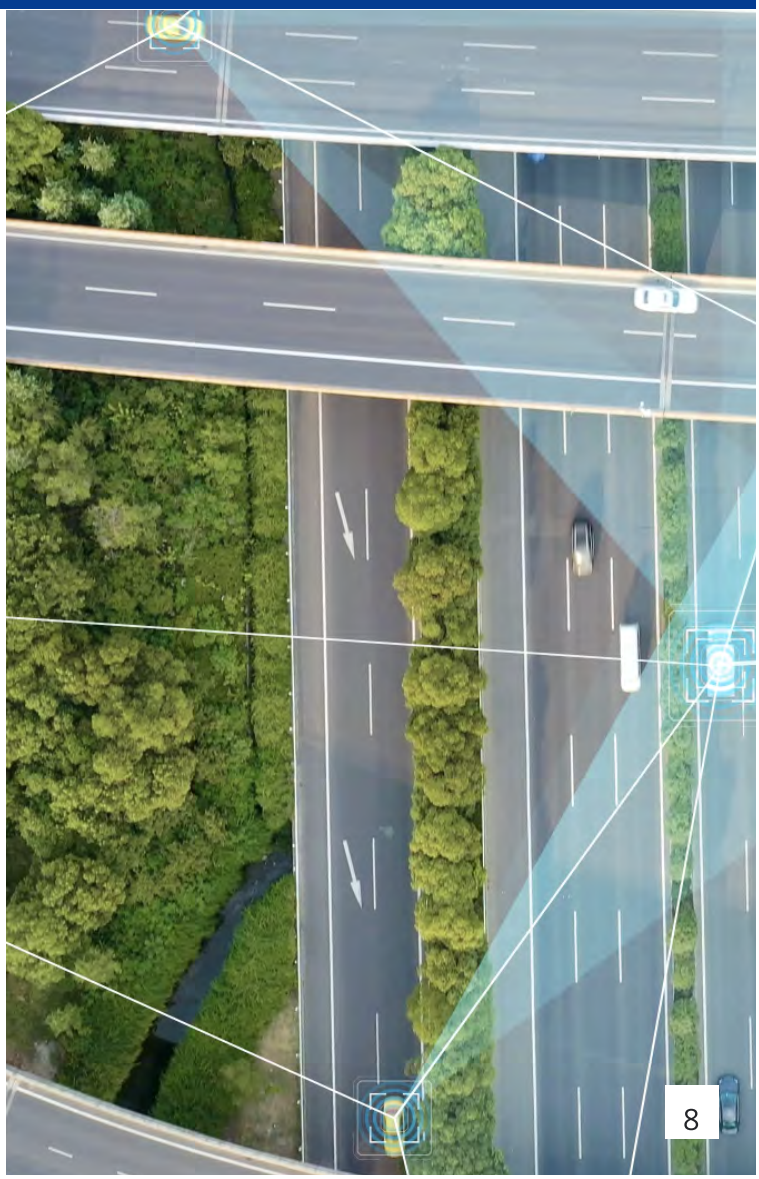
GNSS Anti-Jam & Anti-Spoof Antenna Technology

Principal Investigators:
Sherman Lo (Stanford), Mark Psiaki (Virginia Tech)

Antennas are the gateway to navigation signals. To make that gateway more secure, this project has developed advanced multi-element antenna systems, including Controlled Reception Pattern Antennas (CRPAs), Dual Polarization Antennas (DPAs), and distributed patch arrays. These antennas are engineered to identify and reject unwanted interference by analyzing and exploiting the signal’s direction and polarization.

In a major milestone, these systems were successfully tested in high-threat environments during the JammerTest 2024 event in Norway. The antennas, integrated with direction-of-arrival (DOA) estimation and paired with advanced GNSS receivers like the NovAtel PwrPak7D and Trimble BX992, were able to detect and mitigate spoofing and jamming events in real-time.

The project is not only pushing the performance envelope for resilient GNSS antennas but also focusing on scalability. Practical toolkits are being developed for deployment in diverse environments—from ports to smart road corridors—ensuring broad applicability across transportation modes.



Signal Processing Innovations for Receiver-Level Defense

Principal Investigators:
Boris Pervan, Samer Khanafseh (Illinois Tech)

While antennas shield systems from intrusion, receivers must interpret and validate the information they ingest. This project embeds advanced algorithms within the receiver's processing pipeline, enabling it to autonomously detect anomalies and defend against spoofed or jammed signals.

One of the key innovations is an autocorrelation-based spoofing detection method using the Complex Cross Ambiguity Function (CCAF). This technique dissects overlapping signals by their phase and timing signatures, allowing the system to isolate legitimate transmissions even when spoofers attempt to match frequency and delay parameters.

In parallel, the team developed a Kalman filter-based alternative to the conventional Phase Lock Loop (PLL) approach for carrier signal tracking. Designed to resist broadband jamming, this adaptive algorithm integrates seamlessly with inertial systems to maintain accurate tracking even under severe signal degradation.

The next stage will involve extensive field validation and integration into commercial-grade receivers used in both automotive and aviation sectors.

II - AUGMENTING PNT: DIVERSIFYING DATA SOURCES TO MAINTAIN ACCURACY AND INTEGRITY

Recognizing that no single signal source can guarantee integrity under all conditions, the "Augmenting PNT" research thrust focuses on redundancy. By combining traditional GNSS with inertial systems, perception sensors, and emerging signals from space, CARNATIONS aims to ensure that vehicles can navigate confidently—even when GNSS alone becomes unreliable.

Multi-Sensor Integration for Spoofing and Jamming Resilience

Principal Investigators:
Boris Pervan, Samer Khanafseh (Illinois Tech)

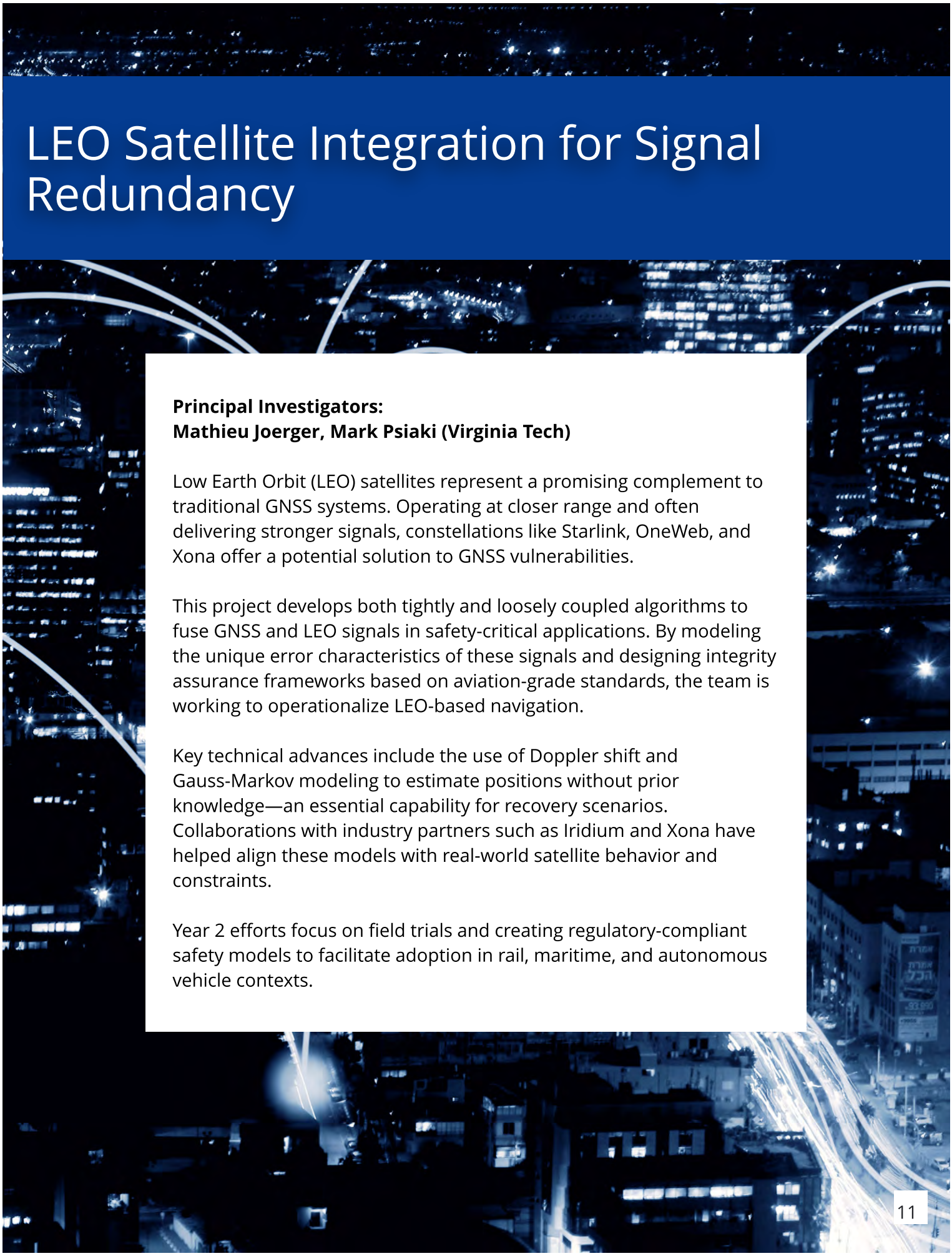
This project takes a layered approach to navigation resilience by integrating inertial measurement units (IMUs), vision systems, LiDAR, radar, and kinematic constraints. The goal is to detect inconsistencies in GNSS signals through comparison with independent sources of motion and positioning data.

For instance, the integration of IMU data with GNSS allows the system to identify spoofing attempts through temporal discrepancies in expected movement. Doctoral work by Birendra Kujur introduced a novel monitoring method that flags suspicious deviations in trajectory kinematics—technology that has since led to a patent filing and presentations at leading conferences.

The team also introduced "virtual augmentation" techniques that use vehicle-specific motion constraints to maintain accurate positioning in structured environments like urban corridors.

Meanwhile, fusion with lidar and radar data enables fallback localization methods in GNSS- denied areas such as tunnels and dense city centers. These systems are now being tested in a hybrid simulation platform that mimics both spoofed and authentic environments.

LEO Satellite Integration for Signal Redundancy



Principal Investigators:
Mathieu Joerger, Mark Psiaki (Virginia Tech)

Low Earth Orbit (LEO) satellites represent a promising complement to traditional GNSS systems. Operating at closer range and often delivering stronger signals, constellations like Starlink, OneWeb, and Xona offer a potential solution to GNSS vulnerabilities.

This project develops both tightly and loosely coupled algorithms to fuse GNSS and LEO signals in safety-critical applications. By modeling the unique error characteristics of these signals and designing integrity assurance frameworks based on aviation-grade standards, the team is working to operationalize LEO-based navigation.

Key technical advances include the use of Doppler shift and Gauss-Markov modeling to estimate positions without prior knowledge—an essential capability for recovery scenarios. Collaborations with industry partners such as Iridium and Xona have helped align these models with real-world satellite behavior and constraints.

Year 2 efforts focus on field trials and creating regulatory-compliant safety models to facilitate adoption in rail, maritime, and autonomous vehicle contexts.

III - PROTECTING PNT: GUARDING THE ECOSYSTEM WITH SMART, DISTRIBUTED DEFENSES

As attacks grow more sophisticated and coordinated, traditional point defenses may not suffice. The “Protecting PNT” pillar introduces intelligent, distributed systems that protect not just the signal—but the entire mobility ecosystem.

Resilient V2X Communications Over 5G/6G Networks

Principal Investigators:
Walid Saad (Virginia Tech)

This project focuses on safeguarding the communications that connected and automated vehicles (CAVs) rely on. Through ultra-reliable low-latency communication (URLLC) systems researchers are mitigating threats like jamming, synchronization attacks, and malicious reconfigurable intelligent surfaces (mRIS).

The team developed several innovative tools:

- A Time-Critical Message Error (TCME) metric to evaluate the timing integrity of vehicle-to-everything (V2X) messages.
- Game-theoretic models that anticipate and neutralize network-level attacks.
- Integrated sensing and communication (ISAC) systems that account for dual-use sensing and communication pathways.

These systems are being prepared for field validation in collaboration with UC Riverside.

Improving GNSS Resiliency using Edge AI Solutions

Principal Investigators:
Moussa Ayyash (Chicago State University)

In environments where connectivity is poor and centralized systems are too slow, local intelligence is vital. This project decentralizes GNSS resilience using TinyML models deployed on edge devices within vehicles. The system combines GNSS with sensor data (e.g., LiDAR, Wi-Fi, 5G) to analyze spoofing and jamming threats directly onboard. Key deliverables include:

- An OIRS-aided V2V model for blind spot and collision detection.
- A Free Space Optical (FSO) network design to maintain UAV connectivity under interference.
- Deep learning spoofing classifiers trained on high-noise urban datasets.

Development of Generalized Integrity Monitoring Framework for CAV Application

Principal Investigators:
Matthew Barth (UC Riverside)

Positioning systems must not only detect errors—they must assess risk. This project develops a unified generalized Integrity Monitoring (IM) Framework tailored for CAVs.
Key advancements include:

- A co-simulation testbed built from CARLA (Car Learning to Act)and SUMO (Simulation of Urban Mobility) creating a realistic digital twin of a smart intersection.
- An integrity usability metric that classifies positioning data based on operational risk.
- On-road validation using AVL's Drive Generation Toolkit (DGT), exploring how V2X and perception sensors work together to maintain navigation accuracy.

The research is gaining traction in standards bodies like SAE and IEEE, marking progress toward consistent, nationwide metrics for vehicle integrity monitoring.

Enhancing Spoofing Detection with BSM Intelligence

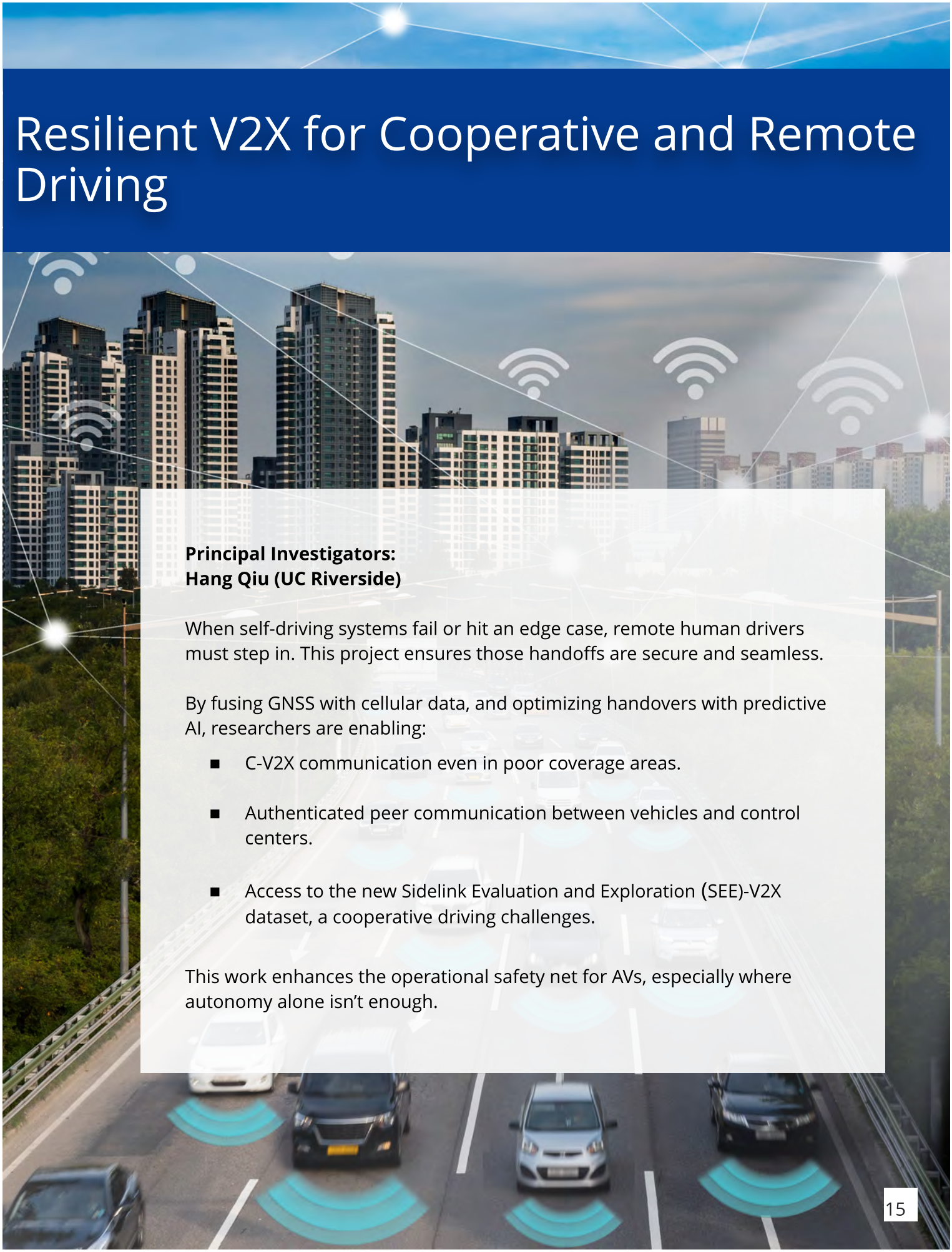
Principal Investigators:
Matthew Barth & Hang Qiu (UC Riverside)

This project adds a cooperative layer to spoofing defense using Basic Safety Message (BSM) data from nearby vehicles. When one car's GNSS data is suspicious, others can help confirm or refute it. Key results:

- Design of a Level 2 BSM message format capable of broadcasting spoofing alerts.
- Use of PNTAX24 field data to validate spoofing detection performance across L1/L2/L5 GNSS bands.
- Identification of clock drift behavior and its role in detecting spoofed receivers.

The Department of Defense has taken note of this project's potential for national infrastructure protection, emphasizing its broad applicability.

Resilient V2X for Cooperative and Remote Driving



Principal Investigators:
Hang Qiu (UC Riverside)

When self-driving systems fail or hit an edge case, remote human drivers must step in. This project ensures those handoffs are secure and seamless.

By fusing GNSS with cellular data, and optimizing handovers with predictive AI, researchers are enabling:

- C-V2X communication even in poor coverage areas.
- Authenticated peer communication between vehicles and control centers.
- Access to the new Sidelink Evaluation and Exploration (SEE)-V2X dataset, a cooperative driving challenges.

This work enhances the operational safety net for AVs, especially where autonomy alone isn't enough.

IV - ACTIVE CROSS-CUTTING PROJECTS: INTEGRATING AND EVALUATING RESILIENT PNT SOLUTIONS

Complementing the core pillars, CARNATIONS leads projects that integrate and evaluate resilient PNT technologies holistically. These initiatives develop comprehensive threat models simulating cyber-physical attacks and assess vulnerabilities across transportation networks. Advanced virtual simulation platforms allow testing of combined solutions in controlled environments, promoting iterative refinement and system optimization. Prototyping and live testing ensure technologies perform effectively in real-world conditions, bridging research and deployment. Together, these efforts establish standardized performance metrics and transparent evaluation methods, fostering trust and accelerating adoption among public agencies and industry partners.

Threat Models and Use Cases for Multimodal Transportation

Principal Investigators:
Todd Walter, Sherman Lo, Sam Pullen (Stanford University)

This project adapts the rigorous interference assessment methods used in aviation and applies them to ground-based and maritime transportation systems. Unlike aviation, where interference protection standards are mature, surface transportation systems face a broader spectrum of threat vectors in more varied environments.

By simulating vehicle trajectories and overlaying them with jamming and spoofing signals, researchers are creating threat models that span suburban intersections, rail corridors, and maritime ports. The research team has also deployed low-cost GNSS monitoring kits in regions known for interference activity—including Israel and Norway—to gather large-scale field data. One striking finding occurred in an Israeli port, where spoofing signals were combined with targeted jamming designed to force receivers into a reacquisition state, increasing susceptibility.

In contrast, some low-cost receivers demonstrated surprising resilience in Norway's jamming zones, rejecting partial spoof attempts and maintaining positional accuracy. The project has emphasized the importance of independent time sources—particularly in ground transport where two-way communication makes implementation feasible. Contributions to RTCA's Special Committee 159 Working Group 2 are helping standardize spoofing scenarios for broader system testing.

R-PNT Virtual Conflict Simulation

Principal Investigators:
Hesham Rakha, Mark Psiaki (Virginia Tech)

This simulation-based project examines how cyber-physical attacks affect overall transportation system efficiency. By embedding attack models into the INTEGRATION traffic software, the research team simulates scenarios where vehicles submit falsified travel times or positions to central routing algorithms.

Dynamic red-team/blue-team exercises help identify tipping points at which false data degrades route optimization. Even with only 10% of vehicles broadcasting inaccurate data, simulations revealed widespread congestion and degraded system throughput—particularly during periods of high demand.

Next-phase goals include expanding the simulated environments and developing mitigation strategies, such as anomaly-detection algorithms that flag inconsistent vehicle behavior in real time. This research supports the design of more secure traffic management applications that resist adversarial inputs.

Comprehensive Testing and Evaluation of Resilient PNT Systems

Principal Investigators:
Mathieu Joerger (Virginia Tech), Matthew Spenko (Illinois Tech)

This project tackles a major testing gap: evaluating GNSS resilience and high- fidelity simulated conditions. Due to regulatory restrictions on live signal spoofing, the team developed a hybrid test strategy combining crowd sourced signal monitoring, virtual testbeds, and collaborative field exercises.

A key outcome is a national RFI monitoring network using over 900 GNSS sensors, which feeds into jamming prediction tools accessible to transportation operators and researchers. Meanwhile, partnerships with Spirent have enabled the creation of a remote spoofing testbed, allowing legal, repeatable tests that mirror interference.

Field campaigns at U.S. military exercises like PNTAX, combined with international deployments in Norway and Israel, round out a comprehensive approach to PNT validation. Future milestones include the construction of an anti-RFI test facility at Virginia Tech's Smart Roads and broader collaboration with UC Riverside for the APEX25 field trial.

These projects embody CARNATIONS' commitment to protecting the integrity of modern navigation, not only through innovation—but through transparency, testing, and global collaboration.

QUICK FACTS FROM THE PROGRAM MANAGER

Aashish Narang

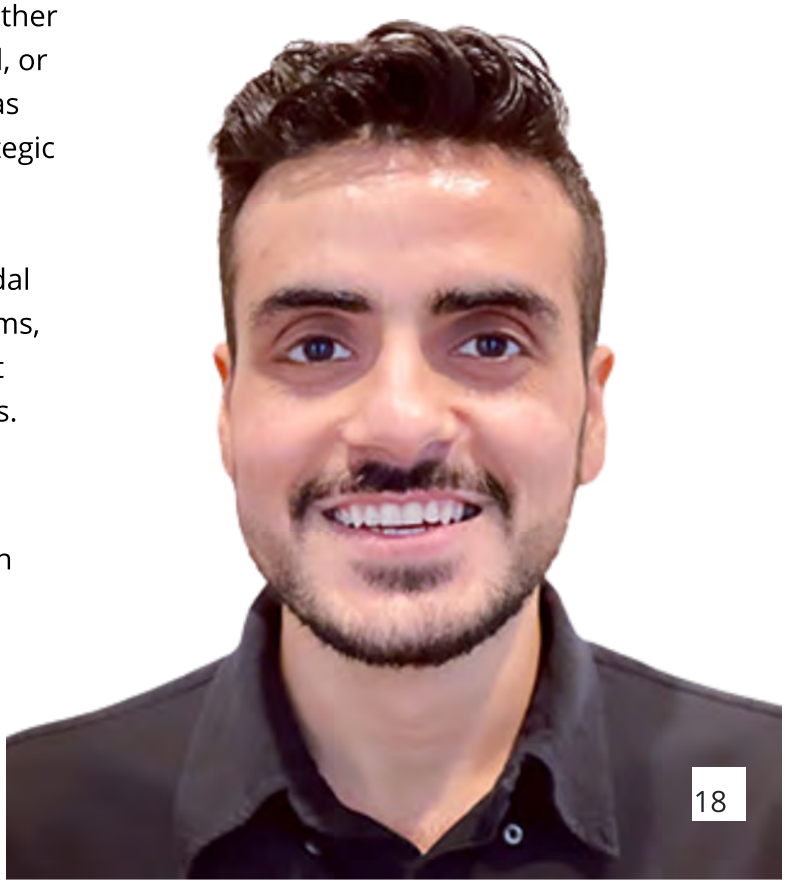
"Coordinating our projects and student teams across five institutions has been vital in keeping pace with federal research goals and delivering practical, deployable tools."

Serving as the Program Manager for CARNATIONS has been both a challenging and rewarding experience. With researchers, students, and stakeholders spanning five premier institutions, managing a growing portfolio of nationally significant projects has required unwavering focus, coordination, and collaboration.

This past year, our work has been grounded in the Center's three foundational pillars: ***Toughen, Augment, and Protect*** the nation's Positioning, Navigation, and Timing (PNT) infrastructure.

Every initiative—whether in the lab, in the field, or in the classroom—has advanced these strategic goals to address vulnerabilities, strengthen multimodal transportation systems, and prepare the next generation of experts.

Our progress can be clearly measured through the impact in numbers:



CARNATIONS Impact In Numbers (March 2024- March 2025)

Principal investigators	Partner institutions	Students supported	Active projects
13	5	30+	13+

7+	Cross-cutting courses
1	Patent filed
2	International field tests
5	Webinars hosted
35+	Peer reviewed papers

Industry and Government partners
41+

OUTREACH, EVENTS & PARTNERSHIPS

CARNATIONS continues to strengthen its national presence through outreach activities, events, and strategic partnerships with industry and government stakeholders.

CARNATIONS Days, our signature annual gathering, brings together researchers, federal partners, and industry leaders to exchange insights, showcase progress, and foster collaboration. In 2024, the event was hosted at Illinois Institute of Technology and featured Karen Van Dyke from the U.S. Department of Transportation as the keynote speaker. The event drew 52 participants, including 32 in-person attendees representing our partner institutions and 20 remote participants. The program included research presentations, panel discussions, and strategy workshops that aligned with CARNATIONS' mission to enhance resilient PNT systems.

Looking ahead, CARNATIONS Days 2025 will be hosted by Virginia Tech from July 28–30 and will feature exclusive tours of the CARNATIONS testbeds. These testbeds serve as environments where researchers are deploying and evaluating resilient navigation and communication technologies, offering attendees exposure to our most advanced research efforts.

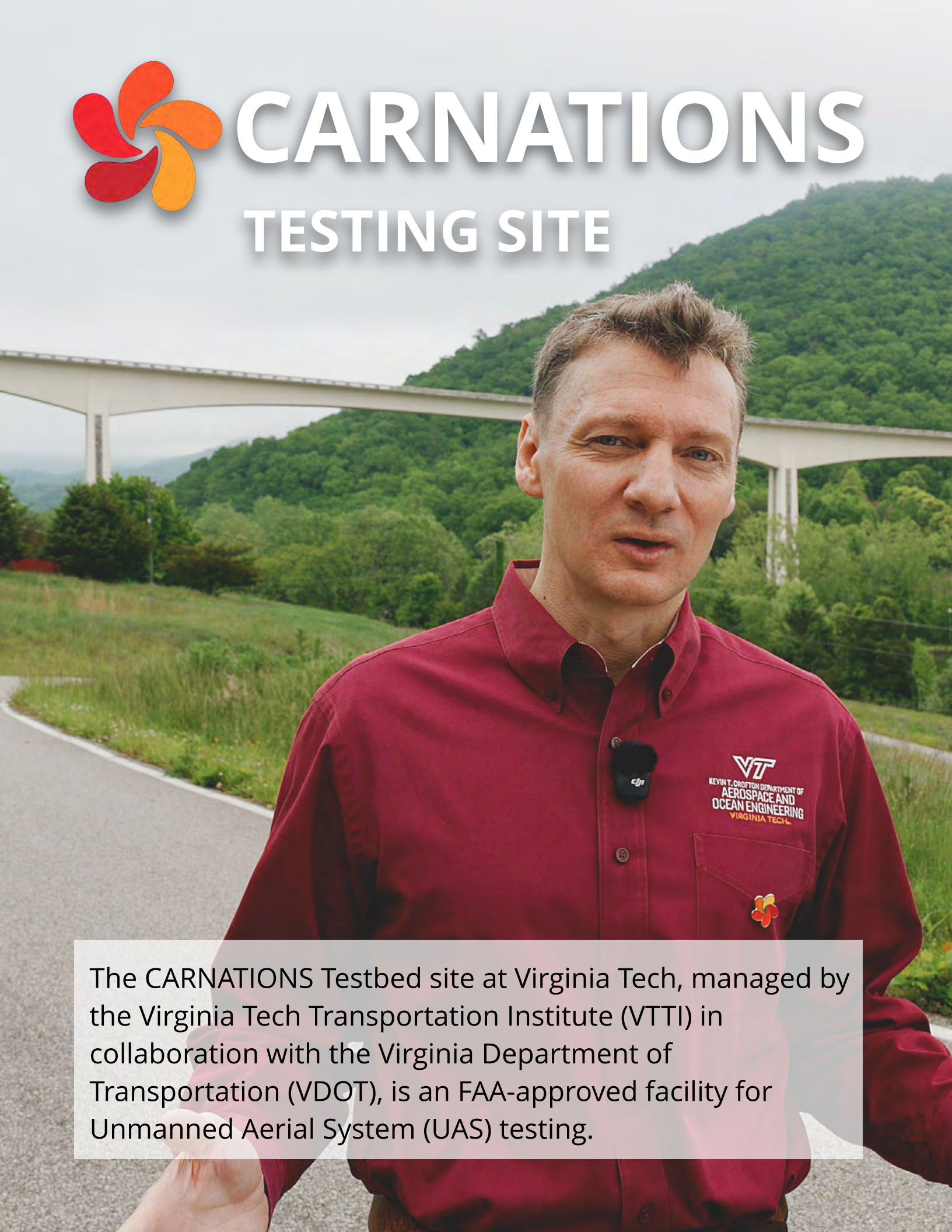
In addition to the annual summit, CARNATIONS hosts team meetings during national conferences, including ION ITM and ION GNSS+, enabling further alignment of research goals and expanding the visibility of our initiatives.

LOOKING AHEAD: 2025 - 2026

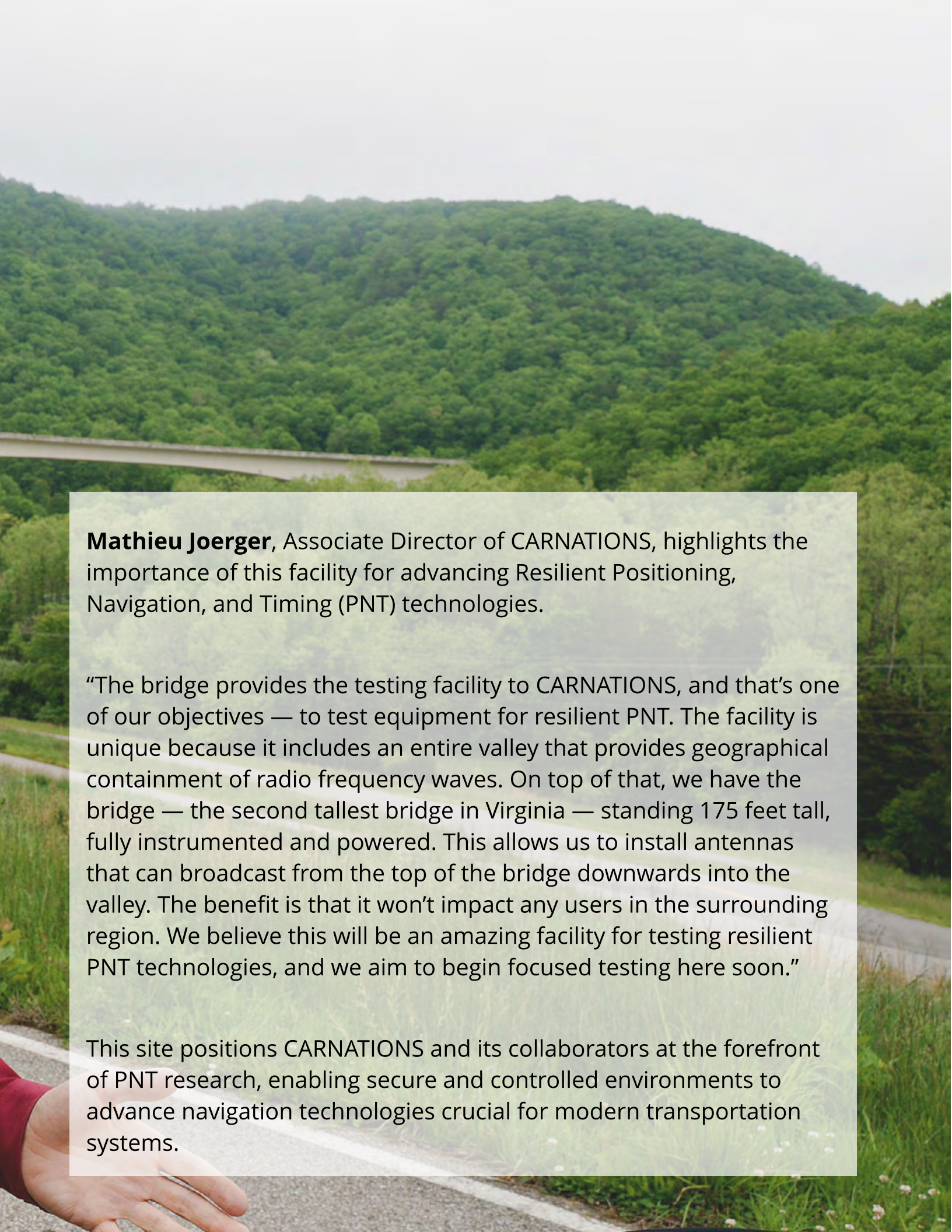
- Finalize patent and commercialization strategies for sensor-aided GNSS systems.
- Upgrade testing platforms with deployments.
- Continue expansion into AI-enabled, edge-based navigation solutions.
- Start testing at testing site in Virginia-tech.
- Enhance student mentorship and internships.

CARNATIONS

TESTING SITE



The CARNATIONS Testbed site at Virginia Tech, managed by the Virginia Tech Transportation Institute (VTTI) in collaboration with the Virginia Department of Transportation (VDOT), is an FAA-approved facility for Unmanned Aerial System (UAS) testing.



Mathieu Joerger, Associate Director of CARNATIONS, highlights the importance of this facility for advancing Resilient Positioning, Navigation, and Timing (PNT) technologies.

“The bridge provides the testing facility to CARNATIONS, and that’s one of our objectives — to test equipment for resilient PNT. The facility is unique because it includes an entire valley that provides geographical containment of radio frequency waves. On top of that, we have the bridge — the second tallest bridge in Virginia — standing 175 feet tall, fully instrumented and powered. This allows us to install antennas that can broadcast from the top of the bridge downwards into the valley. The benefit is that it won’t impact any users in the surrounding region. We believe this will be an amazing facility for testing resilient PNT technologies, and we aim to begin focused testing here soon.”

This site positions CARNATIONS and its collaborators at the forefront of PNT research, enabling secure and controlled environments to advance navigation technologies crucial for modern transportation systems.

ILLINOIS TECH

Contact us:

www.iitcarnations.org

carnations@iit.edu

10 W 32nd St, Chicago, IL 60616

DEPARTMENT OF TRANSPORTATION · UNITED STATES OF AMERICA

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