
# Securing PNT for Highly Automated Transportation Systems

Zak M. Kassas

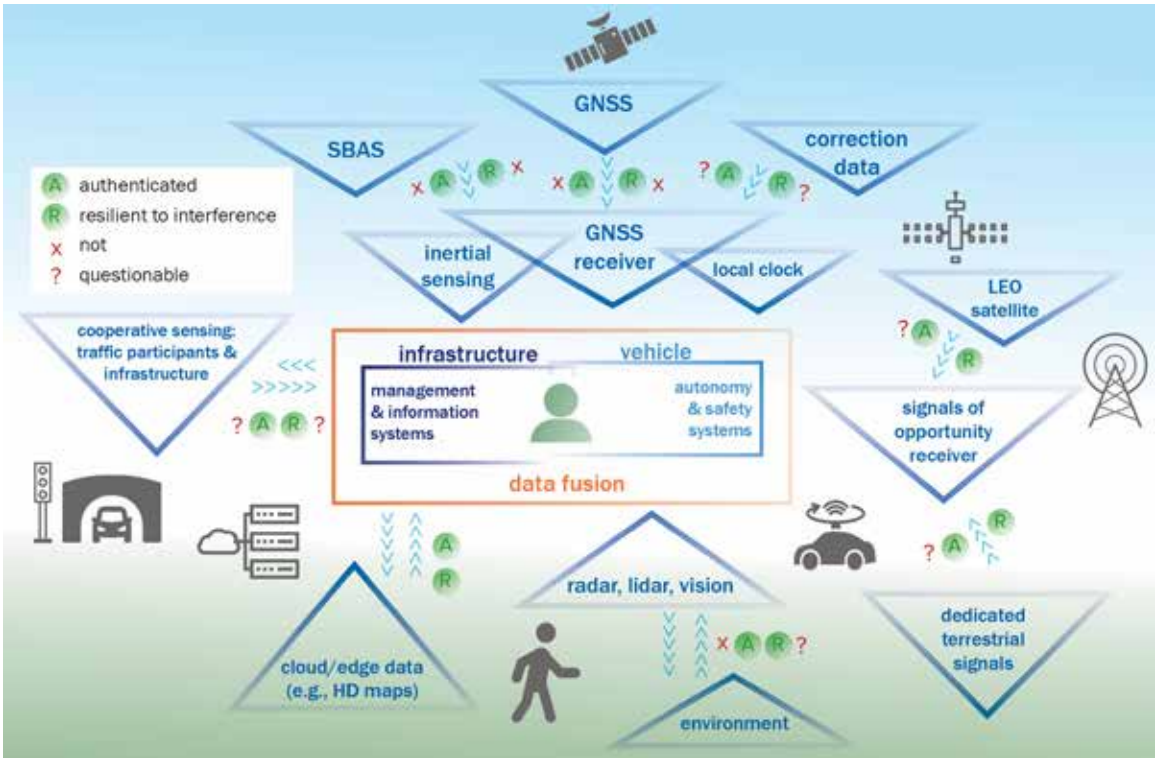
Transportation systems are undergoing the automation revolution. From urban air mobility to self-driving cars, integrating these highly automated vehicles into our daily lives will have astounding societal and economic impacts.

Highly automated transportation systems (HATS)–whether ground, air, or maritime; rely on a steady stream of signals and information from external sources for localization, route planning, perception, and general situational awareness. This includes reliance on positioning, navigation, and timing (PNT) information: Location is essential both for short-range driving control and long-range navigation and planning; and accurate timing is a precondition for on-board sensor fusion, cooperative planning and control, and management based on information from other vehicles or the infrastructure.

Current HATS are too trusting of such external information, and too fragile in the face of loss or attenuation of vital PNT and communications links.

There is a global trend of increasing interference, whether accidental or deliberate, in radio bands crucial for HATS. GNSS jamming and spoofing have evolved from a hypothetical threat, to an experimentally-verified vulnerability, to an emerging public safety hazard. The obvious risk for highly automated vehicles is loss of ability to produce an accurate, sustainable position, velocity, and time solution in a global map with sufficiently high integrity. The risks for vehicle networks and transportation management systems are increased traffic congestion and collisions due to inadequate or misleading situational information.

Despite encouraging progress over the past decade, the vulnerability of externally-sourced information vital to PNT




*CARMEN UTC Vision: Human transportation participants (center) depend on vehicles and infrastructure that fuse data from a host of external sources. Many of the vital links to these sources lack authentication (A) or resilience (R). The CARMEN UTC identifies, develops, and validates PNT sensing techniques for HATS that are both resilient to unusual natural or accidental events and secure against deliberate attack.*


*CARMEN UTC proving grounds at OSU: (a) Skyview of the Transportation Research Center; (b) an autonomous vehicle at the Center for Automotive Research, (c) anechoic chamber at the ElectroScience Laboratory, and (d) OSU Airport*

and to situational awareness remains an open problem for HATS. Yet a solution must soon be found: interference cannot be allowed to paralyze a city's transportation network. Vehicle manufacturers, suppliers, fleet operators, and human drivers/pilots have some knowledge of the threats to HATS PNT, but they do not fully appreciate the threats' scope and seriousness. They tend to rely on security and resiliency schemes that address bare minimum requirements, leaving serious weaknesses exposed.

## US DOT CARMEN

In March 2020, the US Department of Transportation (DOT) announced a competition to establish Tier 1 University Transportation Centers (UTCs) in four topic areas. The competition was fierce, with 67 consortia applications. The Ohio State University (OSU) led a consortium comprising The University of Texas at Austin (UT); University of California, Irvine (UCI); and University of Cincinnati, that was awarded a UTC in the area of HATS.

This UTC, named CARMEN: Center for Automated Vehicles Research with Multimodal AssurEd Navigation, is squarely focused on four main objectives:

1. Gather and systematize existing knowledge and identify gaps in knowledge/practice related to GNSS/PNT threats to HATS
2. Carryout risk identification studies to understand the impact of PNT threats on HAVs
3. Develop new PNT lapse mitigation strategies for HATS, which are (i) robust in the face of unusual natural or accidental events and (ii) secure against deliberate attacks
4. Complement existing methods for cyber resilient PNT receiver testing, develop new mitigation methods, and propose standards and create "best practices" documents and guidelines

Led by Prof. Zak Kassas, the CARMEN UTC comprises a blue- ribbon team with complementary expertise in (i) PNT: Zak Kassas, Dorota Grejner-Brzezinska, Todd Humphreys, Charles Toth, and Teh-Hong Lee; (ii) Automotive: Keith Redmill, Qadeer Ahmed, Alfred Chen, Giorgio Rizzoni, and Kelly Cohen; and (iii) Transportation: Chandra Bhat, Umit Ozguner, Stephen Ritchie, and Craig Rindt.

OSU, the CARMEN UTC lead institution, possesses unparalleled facilities being utilized to validate the UTC's research outcomes: (i) Transportation Research Center (TRC, Inc.): North America's largest multi-user automotive proving ground; (ii) Center for Automotive Research (CAR): 30-plus years of experience in the research and development of intelligent transportation systems and highly automated vehicles (sensing, control, communication systems, embedded systems, cybersecurity, testing, and deployment); (iii) Electroscience laboratory (ESL): world-class research center in electromagnetic scattering, antennas, propagation, remote sensing, signal processing, and photonics, housing the largest active academic anechoic chamber in the world; and (iv) OSU airport: one of three airports owned by top-tier research universities nationwide with three runways and a control tower supporting over 80,000 aircraft operations annually.

## Future Outlook

In February 20223, DOT announced the selection of the CARMEN+ UTC, from among 169 UTC proposal applications, as one of its 20 new Tier 1 UTCs. Building on CARMEN's success and expanding its scope, CARMEN+ will receive $15M over the next five-years to address DOT's research priority of cybersecurity. Led by Kassas, CARMEN+ will involve 20 PIs from OSU (lead institution), UT, UCI, and NC A&T.

*Zak M. Kassas is a Professor of Electrical and Computer Engineering at The Ohio State University and Director of the US DOT CARMEN UTC. His emails is: kassas.2@osu.edu*