



Vehicle-to-vehicle (V2V) communication's ability to wirelessly exchange information about the speed and position of surrounding vehicles shows great promise in helping to avoid crashes, ease traffic congestion, and improve the environment. But the greatest benefits can only be achieved when all vehicles can communicate with each other. That's why NHTSA has been working with the automotive industry and academic institutions for more than a decade to advance V2V communication's lifesaving potential into reality.

### **What is V2V communication?**

Vehicle-to-vehicle (V2V) communication enables vehicles to wirelessly exchange information about their speed, location, and heading. The technology behind V2V communication allows vehicles to broadcast and receive omni-directional messages (up to 10 times per second), creating a 360-degree "awareness" of other vehicles in proximity. Vehicles equipped with appropriate software (or safety applications) can use the messages from surrounding vehicles to determine potential crash threats as they develop. The technology can then employ visual, tactile, and audible alerts—or, a combination of these alerts—to warn drivers. These alerts allow drivers the ability to take action to avoid crashes.

These V2V communication messages have a range of more than 300 meters and can detect dangers obscured by traffic, terrain, or weather. V2V communication extends and enhances currently available crash avoidance systems that use radars and cameras to detect collision threats. This new technology doesn't just help drivers survive a crash—it helps them avoid the crash altogether.

Vehicles that could use V2V communication technology range from cars and trucks to buses and motorcycles. Even bicycles and pedestrians may one day leverage V2V communication technology to enhance their visibility to motorists. Additionally, vehicle information communicated does not identify the driver or vehicle, and technical controls are available to deter vehicle tracking and tampering with the system.

V2V communication technology can increase the performance of vehicle safety systems and help save lives. There were an estimated 6.8 million police-reported crashes in 2019, resulting in 36,096 fatalities and an estimated 2.7 million people injured. Connected vehicle technologies will provide drivers with the tools they need to anticipate potential crashes and significantly reduce the number of lives lost each year.

As cars advance toward self-driving capability and roadside entities on public networks start to communicate with a vehicle's On Board Units (OBU) to influence vehicle actions, security solutions can be expected to pop up like packs of ramen noodles at a dormitory. Last month

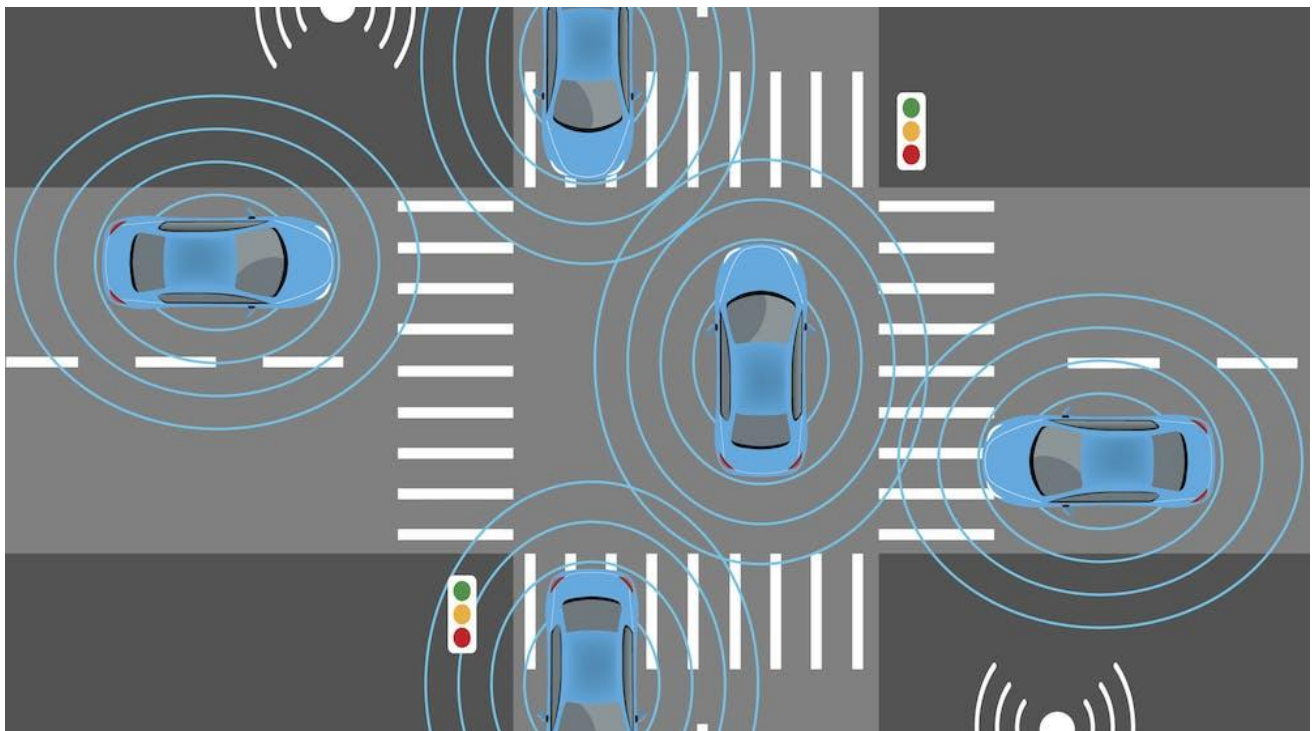


Topic Secure platforms, and Secure vehicle-to-vehicle safety application communication

the first platforms—the tip of a metaphorical iceberg—to address automotive cybersecurity challenges was demonstrated at the TU-Automotive Detroit conference in Novi, Mich.

There, Green Hills Software together with its Integrity Security Services (ISS) unit and partners Autotalks and Commsignia introduced a connected-car platform to enable OEMs and Tier-1s to design, develop, and deploy secure vehicle-to-anything (V2X) systems. Called the “Platform for Secure Connected Car,” it is said by Green Hills to enable automotive and smart-city product manufacturers and operators to obtain both V2X and European car-to-anything (C2X) certification.

The platform features the Integrity RTOS, which offers Common Criteria EAL 6+ security credentials and ISO 26262 ASIL D safety certification. Common Criteria is an internationally approved set of security standards that ensures a clear and reliable evaluation of the security capabilities of IT products for government customers. The Evaluation Assurance Level (EAL1 through EAL7) of a product or system is a numerical grade assigned following the completion of a Common Criteria security evaluation.



Connected vehicle signals