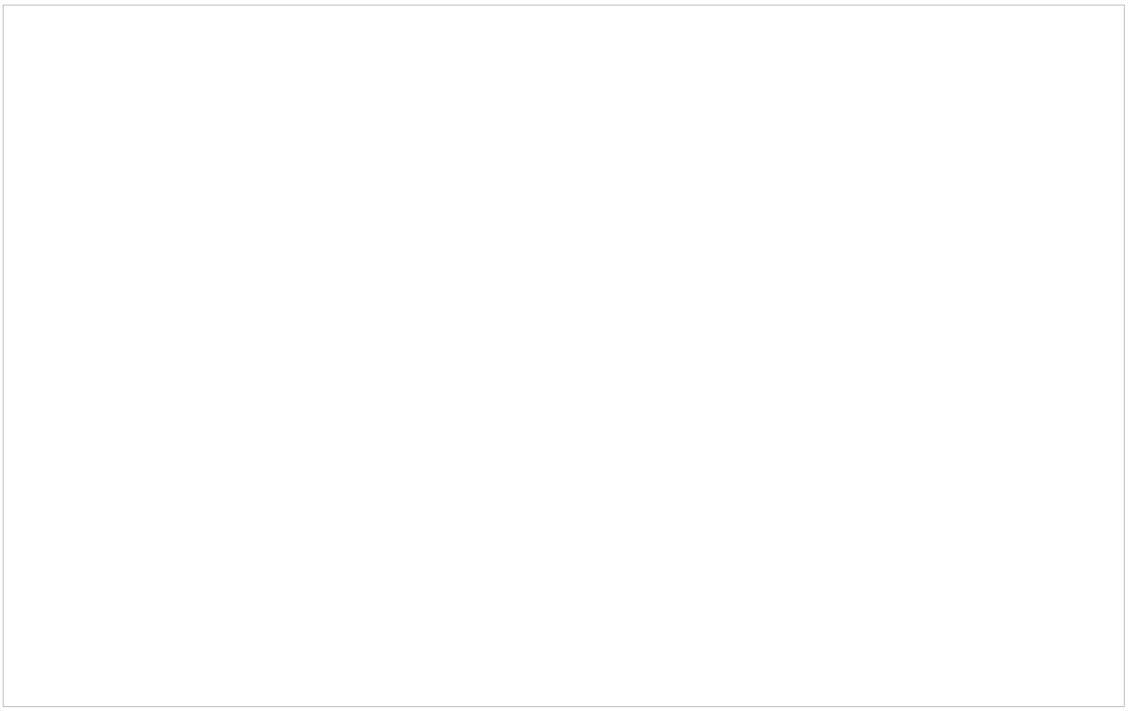
Securing the CAN network with hardware

The partnership of Ultrasoc and Canis Automotive Labs addresses the lack of security features within CAN. CAN is commonly used to interconnect in-vehicle systems such as brakes, steering, engine, airbags, door locks, and headlights.



The partnership addresses a cybersecurity vulnerability in the automotive industry (Source: Adobe Stock)

The partnership between the two companies will yield hardware-based intrusion detection and mitigation techniques for common exploits on the CAN networks. These include automatic hardware anti-spoofing; defense against bit-level attacks such as the Bus-Off attack and bit-glitching; and resistance to denial of service (DOS) style attacks. The collaboration centers on the deployment of Canis Labs' CAN-HG technology, a fully-compatible augmentation of the CAN protocol that includes bus guardian security features, and has the added benefit of being able to carry payloads twelve times larger than standard CAN frames.

When combined with Ultrasoc's semiconductor IP for detection and mitigation of cyber threats, CAN-HG allows designers to secure their CAN network designs at the hardware level. The cybersecurity capabilities enabled by the collaboration employ fast bits within the CAN-HG augmented part of a CAN frame to add security information to CAN frames. This can be used by Ultrasoc's protocol-aware monitoring hardware to identify and block suspicious or unauthorized traffic traveling over CAN. These capabilities will be refined and proved for deployment as part of Secure-CAV: a project that seeks to improve the safety and security of tomorrow's connected and autonomous vehicles (CAVs).

Aileen Ryan, Ultrasoc CSO, commented: "Automotive cybersecurity requires an ecosystem approach. We're delighted to add Canis Labs to our list of partners working in this area, which already includes Nsitexe-Denso and Agile Analog; as well as our partners in the Secure-CAV project, Copper Horse, and the Universities of Coventry and Southampton. Up to now the industry has been forced to use sticking plaster solutions to defend CAN interconnect, relying on software techniques or perimeter security. Incorporating Canis Labs' CAN-HG technology into Ultrasoc's products allows us to secure the vehicle 'from the inside out': within the underlying electronic hardware."

Ken Tindell, Canis Labs' CTO, added: "The most effective way to protect a CAN bus from attacks is to deploy a hardware security device – or better still, use semiconductor IP to incorporate hardware protections into the underlying system. We believe that the combination of Ultrasoc and Canis Labs IP provides a robust solution to CAN security, which is one of the most pressing problems for any CAN bus user – whether they are in automotive, aerospace, or any other industry sector."

The CAN interconnect protocol emerged in the 1980s in response to the need for an efficient, lightweight interconnection method that could cope with the harsh environments found in vehicles. Today it remains a choice not only in the automotive industry but also in industrial, cyberphysical, and robotics applications, where safety is paramount. But while it is physically robust, CAN is almost entirely lacking in cybersecurity features.

Most existing approaches to CAN security are software-based, meaning that they are often unable to react quickly enough to prevent protocol-level attacks. Because it is hardware based, a joint Canis Labs / Ultrasoc solution can react quickly enough to prevent an attack from completing, explained the companies. This has two implications. First, many exploits rely on creating a "window of opportunity" during which the system is in a vulnerable or unknown state. A fast reaction time can eliminate this window and improve the overall robustness of cybersecurity defenses. Second, CAN is used in many cyberphysical systems, in which elapsed time equates to distance traveled. According to the companies, faster response time therefore has benefits in terms of mitigating the physical consequences of an attempted intrusion, better protecting the safety of citizens and infrastructure.

CW