

CAN is not the hot topic

The consumer electronic innovation show sets the technical trends for this year. Embedded and deeply embedded technologies are not in the main focus.

□

The CES 2019 opens its doors on January 8 (Photo: CES)

The organizer of the CES 2019 tradeshow expects more than 150 000. Every January, technology enthusiasts and nerds make a pilgrimage to Las Vegas in Nevada to see the innovations and products of more than 4500 exhibitors. This year, the government shutdown causes eventually some travel cancellations of government speakers.

Not everything what is exhibited at CES, will be successfully on the market. On the other hand, some of the not so fancy products, not standing in the spotlight, will generate a huge business. The hot topics of this year's CES include any kind of artificial intelligence (AI), 5G devices, autonomous driving vehicles, new display technologies, and voice assistance devices such as Alexa. Embedded networks such as CAN are not in the main focus of the exhibitors. They do their jobs invisible in the backyard. Nevertheless, some exhibitors show CAN-related products and solutions.

Cyber security is an issue

Karamba Security (Israel) demonstrates in Las Vegas its solutions for securing vehicles. "The industry has been investing heavily in transforming to smart mobility and a self-driving future. However, this future relies on assuring consumer safety," said Ami Dotan, Karamba's CEO. "We will use CES 2019 as an opportunity to share our customers' experiences in securing their next-generation vehicles, while maintaining safety and minimizing legal exposure. We are excited to demonstrate live attacks on connected vehicles and showcase how they are deterministically prevented, without running into risks of false alerts, and without the associate cost and legal exposure of heuristic detection solutions. We are proud to showcase six different partners from across the vehicle industry." Teaming up with Karamba Security at CES 2019 are leading automotive platform providers Micron, STMicroelectronics, Arm, Wind River, and innovative top-tier global providers Ficosa and Alpine - all companies that are investing to increase cybersecurity protection in today's vehicles.

Karamba's SafeCAN, running on ARM processors, is offering authentication encryption technology for CAN that is providing source authentication for each message, with zero bandwidth overhead. The SafeCAN key management does not require any key exchange over the CAN network. In the future, basing Karamba SafeCAN's root of trust on ARM's Trustzone technology will allow the encryption key to be deployed once in a trusted secure element, thus increasing the overall security level of the solution.

Audio amplifiers with CAN connectivity

Fiberdyne Research (Australia) has announced that it has been named a CES 2019 Innovation Awards Honoree for its range of integrated audio amplifiers. Building on the company's expertise in DSP algorithms, vehicle bus networks, and their high fidelity amplification system.

□

The M-bridge audio amplifier provides CAN connectivity (Photo: Fiberdyne)

"This is the world's first aftermarket amplifier compatible with MOST25, MOST50, MOST150, CAN bus, and the new Analog Devices A2B bus system," said Julian Merritt, Director of Fiberdyne Research. "This will finally allow non-intrusive additions of amplifiers directly into the digital bus networks of modern vehicles without the need to start tapping into speaker wires. We also now have the pre-amp versions for all vehicle bus networks for those people who wish to use other amplifiers in the car." Merritt went on to say: "Fiberdyne specializes in these vehicle bus systems and our amplifiers are now being used in a number of OEM vehicles on these networks."

Reference board with galvanic-isolated CAN transceiver

At CES 2019, Recom (Austria) shows its R-REF03-CAN1 reference board featuring Texas Instruments (USA) isolated ISO1042 CAN transceiver, which is supplied by the thumbnail-sized R15X DC/DC converter. The reference board has been developed in partnership with the US-chipmaker. It allows design engineers to develop and analyze isolated CAN systems. The CAN transceiver supports bit-rates of up to 5 Mbit/s. The galvanic isolation prevents noise currents on the CAN bus-lines or other circuits from entering the local ground and interfering with or damaging sensitive circuitry.

□

The reference board comprises the galvanic-isolated ISO1042 CAN transceiver (Photo: Recom)

To supply the reference board, only one 3,3-V external supply is required. It is pre-configured with a "split" termination network with a common-mode capacitance and additional capacitors on the CAN network for protection. Protection components like TVS diodes and common mode choke are populated as well. Bypass paths for these components and a place for the termination resistors are given.

The output of the DC/DC converter is used to supply the secondary side of the digital isolator and the green LED, which indicates the presence of the supply voltage. Since the reference board internally consumes about 80 mA from the output, 120 mA are available to supply circuits outside of this reference board through a connector pin or test point.

[hz](#)