Wireless CAN without WLAN or Bluetooth

In two developed concepts, dual-mode radio enables CAN nodes to be integrated wirelessly into a CAN network. Constructed from a few components, a protocol-free, real-time transmission is provided.

Eye-diagram at 1 MHz (Photo: FH Aachen)

Felix Huening, Holger Heuermann, and Franz-Josef Wache have developed two concepts to integrate CAN nodes wireless into a CAN network. They describe these concept in an article published in the December 2018 issue of the CAN Newsletter. The authors concludes: “The wireless CAN described here is based on dual-mode radio and enables CAN participants to be integrated wirelessly into a CAN network. Both presented and developed concepts function correctly and enable the construction of wireless CAN interfaces. For the CAN nodes involved, it is irrelevant whether the data transmission is wired or via the radio link. With this concept, the cable can be replaced 1:1 and the other advantages listed above can be realized. Due to the simple design with only a few components, a transfer of the discrete design into a simple and small IC for use in embedded systems is possible and in planning. The development of suitable ICs up to component size would enable even better integration into embedded systems.”

The researchers from the University of Applied Science in Aachen adds: “The dual-mode system works independently of the antennas used, so that an optimized antenna geometry can be used for embedded applications with the IC. The antennas used in this study do not yet provide optimal characteristics. The use of directional antennas, such as patch arrays or printed Yagi antennas, would be advantageous as it reduces crosstalk between two dual- mode systems and allows the transmitter and receiver to be integrated into one housing.

Compared to classic radio systems, dual-mode radio offers two security aspects. Since dual-mode radio uses two antennas with different polarizations, a potential attacker must insert two receiving antennas with exactly the same polarization into the radio path in order to be able to monitor the signal. Furthermore, by using a voltage- controlled oscillator, it is possible to make the baseband signal noisy and distribute the high-frequency energy over a wider frequency range. This ensures that the dual-mode signal almost disappears in the noise. Demodulation of the signal by the receiver is still possible, but finding the dual-mode signal is more difficult for an attacker without a more-detailed knowledge of the system.”

Download the complete article in PDF format here or the full magazine.

hz