China roadshow 2025

Title: Enhancing functional safety & security aspects of CAN XL in automotive systems

Speaker: Dr. Nikos Zervas (CAST)

Abstract: In the rapidly evolving automotive landscape, advanced communication protocols like CAN XL present both opportunities and challenges, particularly in functional safety and data security. Our presentation will explore the functional safety aspects of CAN XL, emphasizing the importance of higher-layer protocols such as CANopen Safety. These protocols ensure that safety-critical applications operate reliably, even amid faults.

A key component of data integrity in CAN XL links is its inherent capability for error detection, primarily through its Cyclic Redundancy Check (CRC) mechanism. However, functional safety extends beyond just error detection on the channel; it also encompasses strategies to mitigate the effects of permanent and transient faults in the complete communication chain including controllers but also improves the overall availability of the system. ISO 26262 standardizes functional safety in the automotive context. We will explain how techniques such as Error Correction Code (ECC) and Triple Mode Redundancy (TMR) further improve functional safety and reliability of systems by ensuring that even in the event of a fault, the system can continue to function correctly.

In addition to functional safety, our presentation will highlight the critical need for cyber security in automotive systems due to increasing vehicle connectivity. The CANsec extension, currently being standardized at CAN-in-Automation, represents a significant advancement in this area. As vehicles become more interconnected, the risks of data breaches and cyber threats escalate. CANsec provides a robust encryption data layer specifically designed for CAN XL, ensuring secure and resilient encrypted data communication.

Kontumazgarten 3
DE-90429 Nuremberg
Tel. +49-911-928819-0
Fax +49-911-928819-79
headquarters@can-cia.org
www.can-cia.org

From the experience of the CANsec IP core, „CAN-SEC,“ developed by the Fraunhofer Institute for Photonic Microsystems (IPMS), we will show how seamlessly it integrates with existing CAN XL communication controllers, offloading security tasks without straining host resources. Utilizing the Advanced Encryption Standard (AES) in Galois/Counter Mode (GCM) with 128-Bit or 256-Bit keys, CANsec delivers essential cryptographic security for protecting sensitive in-car communication streams. We will discuss the technical aspects of CANsec, including its encryption methods, authentication processes, and real-time monitoring capabilities. By implementing these advanced security measures, automotive manufacturers can mitigate data-sharing risks, safeguarding their products and customer trust.

Attendees will gain valuable insights into the future of safe and secure communication in connected vehicles and understand the significance of implementing CAN XL and CANsec in the development of automotive systems.

Kontumazgarten 3
DE-90429 Nuremberg
Tel. +49-911-928819-0
Fax +49-911-928819-79
headquarters@can-cia.org
www.can-cia.org