CANopen FD

The art of embedded networking

Front-end control: Based on well-established CANopen functions

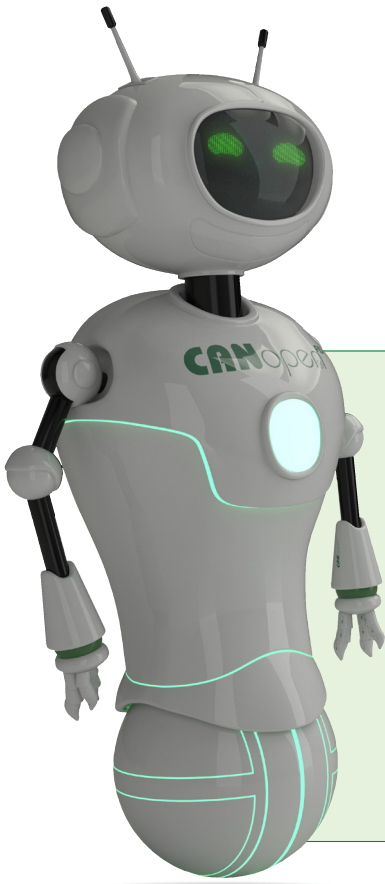Low-cost: Hardware, software, and tools

State-of-the-art: Real-time capable, robust, and reliable

Future-proof: Ready for advanced safety and security

Independent: Second sources and interoperable devices

Five facts

www.can-cia.org

Front-end control: Based on well-established CANopen functions

CANopen FD is designed for front-end control applications. It is based on the classic CANopen protocols and provides a new protocol for cross-communication. This Universal Service Data Object (USDO) enables a default access from any device to any other one. The higher data throughput and the longer frames, provided by the CAN FD hardware, supports comprehensive condition monitoring and big data applications as required by "Industry 4.0" applications. The user can easily migrate from classic CANopen to CANopen FD.

▶ Network-wide default cross communication between devices

▶ Simplified embedding of devices into IIoT environments

▶ Ready for integration into "Industry 4.0" architecture

▶ Suitable for condition monitoring

▶ Much faster download and upload

## *Low-cost: Hardware, software, and tools*
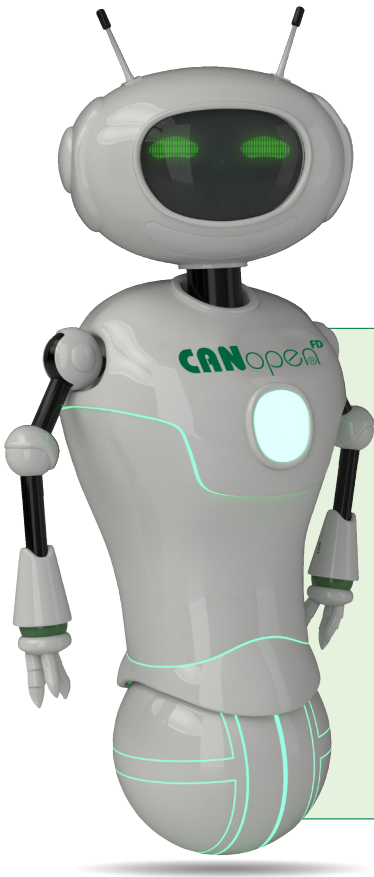
CANopen FD software and hardware products as well as tools are available at reasonable prices. CAN FD and CANopen FD implementations are very scalable. Taking this into account, CANopen FD users are in a comfortable position. They are enabled to select the best-suited units with regard to implemented functionality and price. Reusing knowledge and experiences in system design simplify migration from classic CANopen to CANopen FD solutions.

▶ CANopen FD stacks scalable to hardware resources

▶ Devices adaptable to application or system requirements

▶ Reasonable prices due to real second sources

▶ No dependence on a single source

▶ Low hardware costs because of high volumes

State-of-the-art: Real-time capable, robust, and reliable

CANopen FD is based on CAN FD providing more throughput and larger payloads per frame. Because CAN FD is designed for automotive applications, it meets the very strict requirements on reliability, robustness, and power consumption. CANopen FD keeps the advantages of the well-proven CANopen. In addition, CANopen FD was designed with simplicity in mind. The event-driven CAN FD protocols, combined with efficient implementations, allow very short latency times including recovering from a fault state.

▶ Short latency times by using event-driven short frames

▶ Much faster than Classical CAN

▶ Residual error probability even better than in Classical CAN

▶ Designed for harsh environmental conditions

▶ Low-energy consumption including optional low-power mode
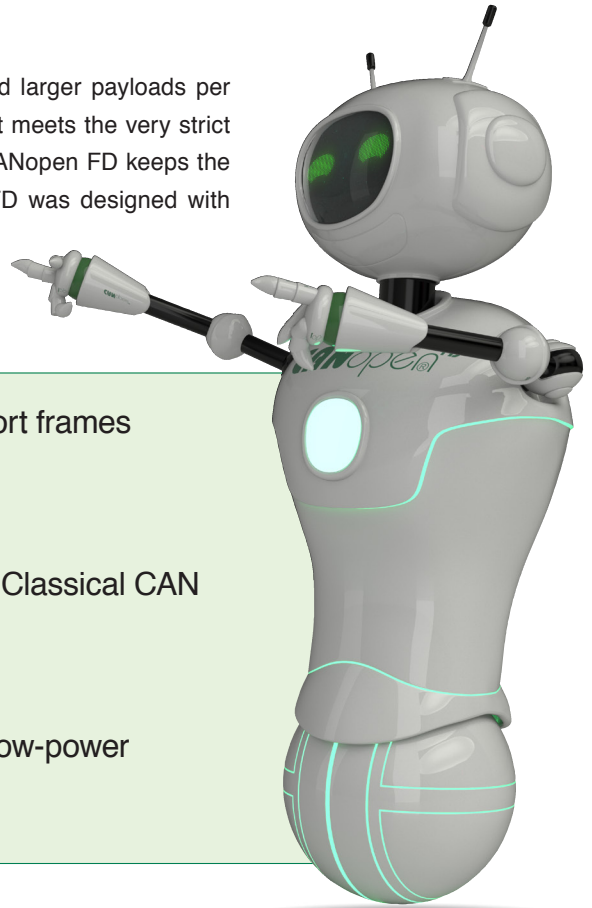
Future-proof: Ready for advanced safety and security

Embedded networks are faced with increasing safety and security requirements. Authentication of the correct network players is one typical aspect. In other applications even encryption of data or data frames is considered. The lengthened data field, provided by CAN FD hardware, enables to support CANopen FD protocols meeting safety and security requirements. These protocols allow the transfer of keys, signatures, and results of data integrity checks.

▶ Transfer of signatures authenticating the source of the data together with the data

▶ Transmission of encryption keys in not segmented CANopen FD messages

▶ Enabler for mission-critical and high-available systems

▶ Adaptation of system-wide functional safety concepts

▶ Compound data sets in single 64-byte CANopen FD messages

CANopen FD

Independent: Second sources and interoperable devices

Scalable CAN FD hardware is available from several chipmakers. Moreover, several companies have implemented the CANopen FD protocols. First CANopen FD prototypes demonstrated interoperability in a multi-vendor system during CANopen FD plugfests. Various suppliers provide CANopen FD interface-boards and tools. The mandatory CANopen FD assessment by CiA validates the conformity. In addition, CANopen FD profile specifications enable device interoperability.

▶ CAN FD hardware long-term availability by various suppliers

▶ Scalable CANopen FD protocol stacks by several suppliers

▶ Configuration and diagnostic tools from different sources

▶ Improved conformity by means of mandatory CiA testing

▶ Verification of interoperability by means of CANopen FD plugfest