The CANopen stack ISIT range, an ideal solution for the communication needs of embedded/industrial systems.

Reading time: 5 minutes

Many embedded systems require means of communication, either between modules or externally. Unless integration into an environment requires a particular protocol, it may make sense to use an efficient, standardized, simple to implement protocol such as CANopen offers. ISIT has developed a range of protocol stacks allowing a quick implementation of CANopen in an embedded system, even critical.

CANopen, derived from CAN

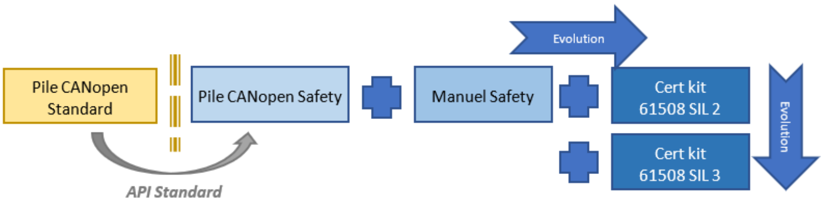
Initiated by Bosch in 1991 and standardized in 1993 (ISO 11898), the CAN bus has experienced uninterrupted growth since its beginnings, extending far beyond the automotive sector. Its robustness, reliability, simplicity and the low cost associated with its implementation have made it the ideal protocol for controlling real-time networks, especially when the amount of data to be processed is limited. The family of standardized protocols around CAN is regulated and promoted by the CiA (CAN in Automation), an independent non-profit organization. Corresponding to layer 7 of the OSI model, CANopen is a communication system based on the CAN network, providing flexible and high-performance services for configuration, diagnosis, network supervision and process data exchange. The definition of profiles for application categories simplifies the design of interoperable products and makes it much easier to design a complex system. Today it is used in a wide range of application areas, such as medical equipment, off-road vehicles, marine electronics, railway applications, building automation as elevator control for example.

CANopen in your system

If the system you are developing is based on a modular architecture with a need for communication between modules, CANopen can be an elegant and simple to implement solution, rather than inventing a specific mode of communication. Indeed, CANopen offers a standardized, fast and efficient protocol. The standard aspect allows a clear architecture, for a scalable and modular system, with a well-defined and reliable communication mode. Many microcontroller manufacturers (ST, TI, Renesas, Infineon, Microchip...) integrate CAN controllers into their processors, which again facilitates hardware design.

CANopen and operational safety

For applications with operational safety requirements, the CiA has defined a safety extension to the CANopen protocol (CiA 304 standard transferred to EN50325-5) based on the concept of SRDOs (Safety Relevant Data Objects). By defining SRDOs, it is possible to transmit safe and unsafe information via the same CAN medium in a functionally safe manner. An SRDO consists of two CAN messages (redundancy), which are transmitted cyclically with inverted data content, a different CAN identifier and a strict transmission timing. As a result, the security functions can be integrated into existing systems or for a new design.



The ISIT approach, an à la carte offer

Depending on the context of the project, the need to use the protocol may vary, as well as the need on the product. ISIT has therefore built an à la carte offer, which "plays" on several parameters to best adapt to the development framework.

On the one hand, there are 3 main variants of the CANopen stack
- “Standard" CANopen stack, supporting the entire CANopen protocol, compliant with CiA-301 V4.2 and CiA-302 standards
- CANopen Safety stack, with safety extension in accordance with CiA 304
- Certified CANopen Safety stack, the only "off-the-shelf" solution on the market available with the entire certification package.

To add to the versatility of the certified solution, the ISIT stack has been developed to meet several safety standards (IEC 61508, DO-178, ISO 26262...) and the certification package is available for the desired level of safety.

In addition, it is also possible to determine the following choices:
- Binary, pre-ported by ISIT on a specific environment (CPU/OS) or source which will give more flexibility for use (depending on the version)
- Master/Slave or simply Slave, depending on the nature of the equipment to be developed
- Project or site depending on whether it is a single project or several projects

Robust code

ISIT's approach in this development consisted in first developing the certified CANopen Safety stack, in order to meet a specific market demand, at the crossroads of its skills: industrial protocols, embedded software and software quality. This approach was also linked to the absence of such a product on the market. It was only after having finalized the 1st version of this product that ISIT decided to expand its range, also offering a non-certified version, and then to offer the "standard" CANopen stack. But as the entire range is based on a rigorous approach with the objective of certification at the highest level of safety, all versions benefit from this intrinsic robustness.

In conclusion, the choice of the CANopen protocol offers a simple, reliable and high-performance solution for the communication needs of a real-time embedded system, and the ISIT range, with its versatility and scalability, is a wise choice to adapt to different working contexts and safety requirements.

Solution Contact: Gilles FAUGÈRE – mailto:gfaugere@isit.fr