Protecting One’s Investments by Adhering to the CANopen Standard

Monika Mack
CAN in Automation, am Weichselgarten 24, DE-91058 Erlangen, Germany
Tel.: +49-9131-690-86-0, fax: +49-9131-690-86-79
E-mail: headquarters@can-cia.org

Received: 24 May 2006 /Accepted: 20 September 2006 /Published: 25 September 2006

Abstract: CAN in Automation (CiA) offers a software tool to test devices for conformance to the higher-layer protocol CANopen. Also, the CiA international users’ and manufacturers’ group certifies CANopen devices with the help of this tool. The CAN-based higher-layer protocol CANopen is used in many different application areas, e.g. in machine building, in medical technology, in rail vehicles, in building automation and in commercial vehicles. Error-free communication, the base for liability exclusion and customer retention, is only possible if the interfaces have been implemented correctly.

Keywords: CANopen conformance, Conformance test tool

The CANopen protocol (EN 50325-4) networks sensors, actuators and controllers in many different application areas, e.g. in industrial automation, machine building, medical technology, rail vehicles, building automation and in commercial vehicles. The increasing significance of CANopen results in more and more devices being equipped with a CANopen interface. System designers and network integrators are thus able to choose products from a variety of manufacturers and to integrate them with little configuration in their networks.
A major requirement for simple system integration of the devices, however, is the correct and complete implementation of the CANopen protocol. Open communication interfaces are defined in specifications, but reality shows that every developer interprets these slightly different. This may lead to problems in the system integration. To avoid these problems, there must be a single valid interpretation of the specification, or rather a conformance testing tool, to test if the implementation of the specification is correct. For the CANopen protocol this testing tool exists; it is the CANopen Conformance Test Tool developed and produced by CAN in Automation (CiA).

Manufacturers of CANopen devices may purchase this software tool from CiA and test their devices for conformity with CANopen. Should the device tested successfully complete all test steps, it adheres to the CANopen specification and is operable with other CANopen devices in the same network. Every manufacturer may test their devices for themselves. However, the credibility of such a test will rise significantly, if the testing is done by a manufacturer-independent entity. Also, such an external entity may be able to look at the device’s functionality with an open mind, and e.g. find errors by creating a different set-up. It may, for instance, happen that a device manufacturer has tested their device with the default settings and it works just fine. If, however, node-ID and bit-rate are changed, the device’s communication may be faulty and not pass the test.

CiA offers manufacturer-independent certification of CANopen devices. This means manufacturers may have their products certified for CANopen conformance in the CiA lab. With the CANopen certificate, they may then prove to customers that the device adheres to the CANopen specification. “The successful testing of CANopen conformity is an important mark of quality for purchasers of CANopen devices,” says Holger Zeltwanger, CEO of CiA.
“CANopen devices that pass the test, pose less problems than those that have not been tested. As a matter of fact, the tested ones are usually integrated without any problem at all.”

Having a CANopen device certified is a quality-proof. Still many manufacturers prefer not to submit to the certification. They may be simply convinced that their products are just fine or they may shy from the cost of having it certified. A third reason may be that it is obvious the product will not comply to the specification. The most important argument to convince these manufacturers may be that of product liability. Loss or damage incurred by a non-CANopen conform device that claims to be a CANopen device will fall back on the manufacturer and can cause substantial regress claims. Even slight differences to the specification may cause complete facilities to come to a standstill. Down times, costs, loss of customer, even liability law suits may be the result. However, also device manufacturers that are confident of their device’s correct implementation of the protocol may want to consider that about half of all devices tested by CiA so far, have not passed the test in the first instance. Often the reasons are errors that the manufacturer is not aware of. Mostly the error source is simple mix-ups or wrong interpretations of the CANopen specification. In the past, especially the “SDO abort codes” have been interpreted incorrectly and the default values have not been implemented as defined. In other cases the quality of the electronic data sheets (EDS) is not sufficient. The device under test may function correctly but its electronic description is faulty. Taking into consideration that most configuration tools use the EDS as base, this may keep a device from being correctly configured or render it non-configurable altogether.
Again, conformity to the standard is not optional; it is a major quality aspect, if not the deciding one. What matters more to a customer than a product that is worth its money? Having to experiment around with a cheap device and putting a lot of time into figuring out how to work around a problem is not what keeps most customers happy. It certainly is not a good way of protecting one’s own backside.

Details about the CANopen Conformance Test and the CANopen Certification are available at http://www.can-cia.org/canopen/conformance, or by writing to CiA at headquarters@can-cia.org.