Smart-bridging CANopen and CANopen FD

This article gives an description on how to smart-bridge classic CANopen and CANopen FD networks.

The CANopen FD protocol has several advantages over classic CANopen: A much more flexible communication model that includes fully-meshed and broadcast communication with Universal Service Data Objects (USDOs), a higher potential bandwidth and larger messages that through the use of CAN FD also offer the extra space needed for authentication, for example with CANcrypt.

However, existing classic CANopen devices cannot be mixed with CANopen FD devices on the same network cable since classic CANopen devices will destroy and generate errors for any CANopen FD communication they detect. So today, when designing new CANopen based networks or adding new functions, features, nodes, or security to an existing CANopen system, you have the following options:

1. Stay entirely in classic CANopen
2. Do a complete transition to CANopen FD
3. Mix classic CANopen and CANopen FD using a smart bridge

Let's evaluate these options

Stay entirely in classic CANopen: For any development you initiate today, no matter if it is something new from scratch or a complete or a partial redesign of an existing system, ask yourself how long the system needs to last and which future enhancements or requirements may come up. Take firmware updates over classic CANopen for example, which are possible but not particularly fast or secure. Security through authentication and encryption during normal operation also could become a requirement, if not today then a few years from now. Would this be possible with only a firmware update?

Our recommendation is to not lock yourself into classic CANopen for new developments. Any new CANopen device you build today should be at least CANopen FD "ready" so that you can easily add enhanced features, faster updates, and security "at any time".

Do a complete transition to CANopen FD: This option requires that all devices connected are CAN FD capable. This typically requires new hardware designs or replacement of off-the-shelf CANopen with CANopen FD components and is only an option if a new system design or a complete redesign of an existing system is started.

You may think that your system will then be "future proof" as all existing and future CANopen FD functions and services are available. However, most devices that currently exist still only speak classic CANopen and you'd be locking yourself out of using any of these for a considerable period of time.

Chances are, you still need an easy migration path from classic CANopen to CANopen FD or vice versa no matter which route you take.

Mix classic CANopen and CANopen FD using a smart bridge: This third option allows you do both: a step-by-step transition from classic CANopen to CANopen FD or to add legacy devices and networks to a new CANopen FD design. The idea is that you use two network branches in your system: a classic CANopen branch with those devices without CANopen FD support and a CANopen FD branch with the newer devices that already have it. Making sure that all node IDs are unique, the two are connected as segments of a single virtual network, using a smart bridge as illustrated in Figure 1.

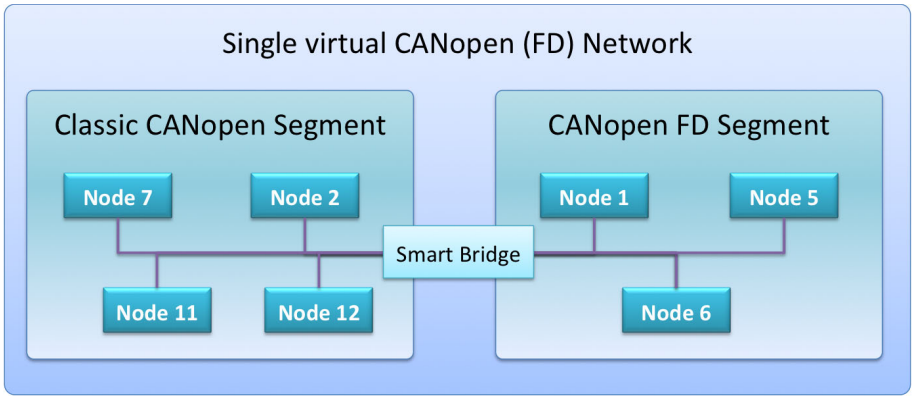

Figure 1: Connecting classic CANopen to CANopen FD using a smart bridge (Source: Emsa)

How does a smart bridge for classic CANopen and CANopen FD work?

Note that while there is no official standard for this type of bridge yet, we at Embedded Systems Academy saw the need for such a device to ease the transition to the emerging CANopen FD protocol and so came up with its concept.

By monitoring the CANopen (FD) traffic on both sides of the bridge, the bridge learns which node IDs are on which side and where the NMT Master is located. Once the bridge has the complete picture of the network segments, USDO and SDO requests and responses involving a node ID are forwarded if required, based on the position of the sender and receiver.

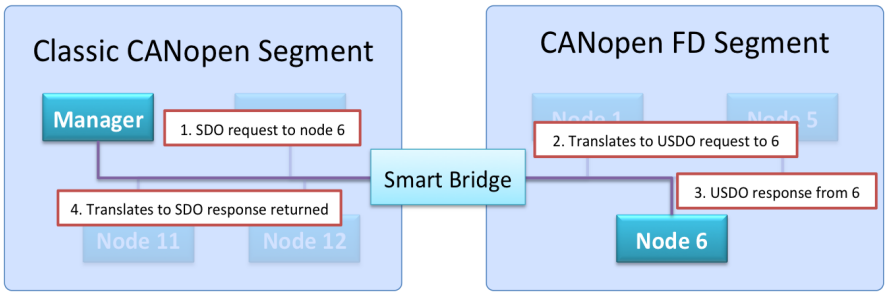

Figure 2: Handling SDO / USDO forwarding (Source: Emsa)

Some messages such as NMT Master messages, bootup messages, Sync messages, and heartbeats are always forwarded to the other segment, as their content is the same in CANopen and CANopen FD. The Emcy (Emergency) messages are forwarded and converted into the respective format.

All default PDOs with a length of eight bytes or less are forwarded as well. An advanced configuration mode allows filtering as well as merging and splitting of PDOs. The “smart” part of the bridge refers to the handling of the (Universal) Service Data Objects - (U)SDO. These are completely transparent for all nodes connected on either side.

If the default SDO client on the classic CANopen side sends an SDO request to a node on the CANopen FD side, the bridge translates it to a USDO request from the bridge itself to the node on the CANopen FD side. The USDO response is received and converted back to an SDO response on the classic CANopen side. These steps are shown in Figure 2.

If any CANopen FD device sends a USDO request to a node located on the classic CANopen side, the bridge translates this USDO request to a default SDO client request on the classic CANopen side. It waits for the SDO response and translates that back to an USDO response on the CANopen FD side.

Those of you with CANopen (FD) experience will immediately see some challenges and limitations:

1. Potential default SDO client collision on classic CANopen side
2. Segmentation handling of SDO and USDO

In classic CANopen there is only “one set” of SDO client channels available. By default, these belong to the CANopen Manager, so only this device may actively produce SDO requests. Note that there are mechanisms to support additional client channels organized by an SDO ▷

Manager, but due to the complexity involved, this is rarely used.

With the smart bridge, the preferred method is that the classic CANopen side has no device producing SDO client requests. This ensures that the bridge itself can use all default SDO client channels on this side. If another device actively uses the default SDO client channels like a CANopen Manager is present on the classic CANopen side, then CANopen FD devices connected to the bridge must not send USDO client requests to devices on the classic CANopen side of the smart bridge. Future versions of the smart bridge will support SDO Manager-style handling of SDO channels on the classic CANopen side to support more SDO flexibility.

Segmentation handling of SDO and USDO

If SDO / USDO requests and responses only deal with data transferred that is four bytes or less, the bridging process is relatively simple. One pair of USDO request and response is translated into a single SDO request and response and vice versa.

The handling becomes more challenging with segmentation. On the CANopen FD side, a USDO expedited transfer involving a single USDO request and response message can transfer up to 56 bytes of data.

To convert such a transfer to classic CANopen, we need to use segmented or block SDO transfer. On the CANopen FD side, this also means that USDO requests send to devices in the CANopen segment will be slower, as they translate to multiple messages being exchanged on the classic CANopen side of the bridge. To cope with this situation, the USDO timeout might need to be increased. Figure 3 illustrates the scenario.

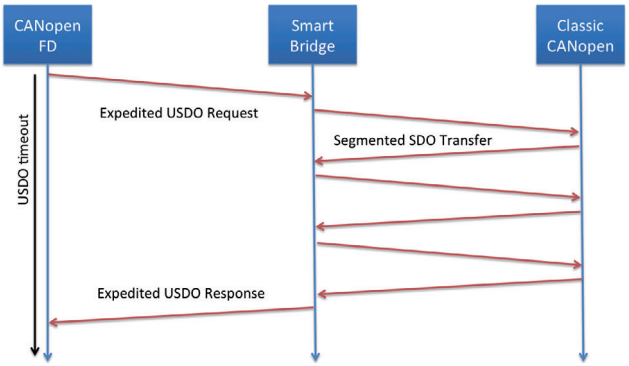

Figure 3: Expedited USDO transfer > 4 bytes translates to segmented SDO transfer (Source: Emsa)

As with all bridging applications involving different performance parameters on each side of the bridge, there will be some limitations with transfers of large data packages like firmware code or configuration tables but we are working on concepts to support these as well.

Availability of the smart bridge CANopen FD

Our first implementation of the smart bridge is for the PCAN-Router FD from Peak-System Technik and will be available in the upcoming weeks. These devices are based on an ARM Cortex M4F micro-controller from NXP and offer two CAN (FD) ports. A configuration utility provided will support loading, registration, and configuration of the smart bridge firmware. Versions for other hardware platforms with multiple CAN (FD) ports are available on request. The smart bridge CANopen FD makes a smooth transition from CANopen to CANopen FD technology possible today. ◀

Figure 4: Peak's PCAN-Router FD as initial hardware for the smart bridge (Source: Emsa)

Authors

Olaf Pfeiffer, Christian Keydel
Emsa (Embedded Systems Academy)
info@esacademy.com
www.esacademy.de

COMPLETE MINING TRUCK CONTROL SOLUTIONS.

DSE®

DSEM240
CAN Slave Module (44 I/O)

DSEM640
Programmable Controller (68 I/O)

DSEM643
Programmable Controller (34 I/O)

DSEM840
4.3" Programmable Display

DSEM870
7" Programmable Display

DSEControl® M-Series

DSE has been delivering world-class control solutions to its customers for over 40-years. During this time the company has developed a reputation across the globe for its UK engineering and manufacturing excellence.

The **DSE M-Series** builds on this reputation. The innovative collection of programmable controllers & displays and CAN slave modules provide customers with complete mining truck control solutions.

To learn more about **DSE M-Series** products, visit **www.deepseaelectronics.com**

DEEP SEA ELECTRONICS LTD
Highfield House, Hunmanby Industrial Estate Hunmanby, North Yorkshire, YO14 0PH, UK
TELEPHONE: +44 (0) 1723 890099

UKMADE