Hybridization of CAN and CAN FD networks

Tony Adamson, NXP

Many automotive manufacturers are now in full evaluation of a CAN FD introduction and over the next five years, we can expect to see these new platforms in production. This is predominantly driven by the need for bandwidth to handle more complex operations, introduce security on the CAN network and for ECU (electronic control unit) fast flashing, when software is downloaded via the CAN network onto ECUs in the production line. In fast flashing, CAN FD can increase the net-bit-rate dramatically, with a resultant reduction in flashing time. In general operation, bit-rates can also be accelerated, but are limited by EMC and network topology constraints.

Implications of CAN FD adoption

When introducing CAN FD, there are several challenges that need to be overcome, affecting both the physical layer and controllers. Firstly, new physical layer parameters need to be guaranteed supporting higher data rates of operation. These are defined in ISO 11898-2:2015, which (at the time of writing) is submitted for DIS (Draft International Standard) balloting. Many physical layer providers have already released updates to their datasheets supporting the “loop delay symmetry” parameter and subsequent updates will follow to finalize the additional parameters.

Secondly, when moving to higher data rates, the network topology needs to be verified to check all delays and ringing. To cope with this, accurate physical layer simulation models supporting data rates >1 Mbit/s are required to ensure topologies are validated at accelerated speeds.

Lastly, and most relevant for this topic, since CAN FD is a protocol change, new CAN FD controllers are required. While CAN FD controllers can interpret and transmit both CAN FD and Classical CAN messages, Classical CAN controllers will report CAN FD messages as an error. This mandates a strict separation of CAN FD and Classical CAN networks, with every node on a CAN FD network required to support CAN FD.

The availability of CAN FD controllers is a challenge for the industry, and one currently being addressed by the industry. But even in the longer term, the necessity to make a change to bring a Classical CAN ECU into a CAN FD network remains. This will require engineering investment, a potential change in component cost (especially short term, as CAN FD controllers still emerge), and a potential module requalification, each with their own effort and cost, not to mention risk, for a network owner when transitioning from Classical CAN to CAN FD.

To minimize this impact, the most efficient approach to introduce CAN FD is to apply it only where bandwidth improvement is most valuable. Taking into account the required separation of Classical CAN and CAN FD, this essentially leaves two options: create a fast CAN FD branch through a gateway function, or upgrade all ECUs on those affected branches to CAN FD. Assuming that upgrading a complete branch presents the same challenges as a full network branch, but with fewer nodes, the discussion will be focused on the first of these options.

First approach: Creating a “fast branch”

To create a fast branch is to co-locate all CAN FD nodes on a dedicated CAN FD branch, connected to other nodes via an already existing central gateway. Communication between CAN FD nodes runs at faster bit-rates and the gateway manages routing to Classical CAN nodes. This strategy is definitely preferred in networks where the number of branches is high and the number of nodes per branch is low. In this case, the transition can be quite easy and preferred in terms of operation.

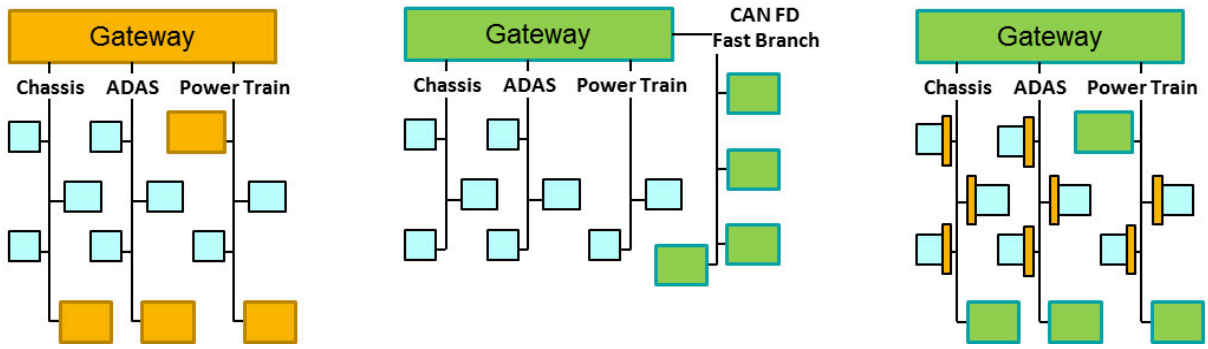

Figure 1: Options for partial CAN FD migration of a vehicle network.

For networks with fewer branches, or where the number of nodes per branch is higher, this approach can be more problematic. It implies that branches are no longer organized by function, but by technology. This creates additional routing via the gateway and prevents a domain-based security approach with rigid access control being implemented. It also has a fundamental scalability problem (if an extra ECU is upgraded, it must be moved to the physically different fast branch, on which the wiring will be non-optimized for ringing).

A different solution: hybrid networks

Having already seen that a complete upgrade of either a branch or network comes with its own costs, an alternative remains to be considered: a hybrid network of Classical CAN and CAN FD nodes, where only data intensive functions and messages are upgraded and the rest remain on Classical CAN. This minimizes upgrade costs by restricting them to only those ECUs that are required to be upgraded and maximizes the re-use of existing Classical CAN ECUs.

A solution to do this for the ECU fast-flashing usecase has already been realized with the introduction of the “FD Passive” extension to partial networking, available in NXP’s TJA1145/FD and UJA1168/FD. Prior to a CAN FD transmission, all Classical CAN nodes are put into selective wake-up mode with the FD Passive function in the transceiver active. Once completed, the CAN FD communication begins to flash the ECUs. The CAN FD Frame Identifier in the frame – the “FDF” bit – is detected in the FD passive transceiver and the frame is dropped, avoiding any CAN FD frames being seen by the Classical CAN controllers, thus avoiding any errors. Once CAN FD communication has completed, the network wakes all Classical CAN nodes and the network begins communicating with Classical CAN again. FD Passive is an elegant solution to resolve the ECU fast-flashing use-case, but it is not applicable for general operation, due to its additional network management operations.

In the ideal case, a true hybrid solution for general operation must fulfill strict requirements, in order to function correctly and deliver the true benefits of a hybrid approach:

- It must be a drop-in replacement to existing HS-CAN transceivers,
- It must not imply any software changes and must work seamlessly with Autosar,
- It must fully comply with the rules of ISO11898-1 and -2,
- It must allow CAN FD and Classical CAN messages to arbitrate against each other,
- It must support all low-powers of HS-CAN transceivers (both 8- and 14-pin devices),
- It must ensure no messages are lost and all ECUs stay synchronized to the bus at all times,
- It must handle all error scenarios on the bus.

To fulfill these requirements, NXP defined the FD Shield technology – a smart transceiver able to dynamically filter CAN FD messages on the network, while being a drop-in replacement for conventional HS-CAN transceivers. No additional software changes are required, nor are any additional components; this ensures migration costs for an existing ECU are limited to changing the HS-CAN transceiver to FD Shield as a drop-in replacement.

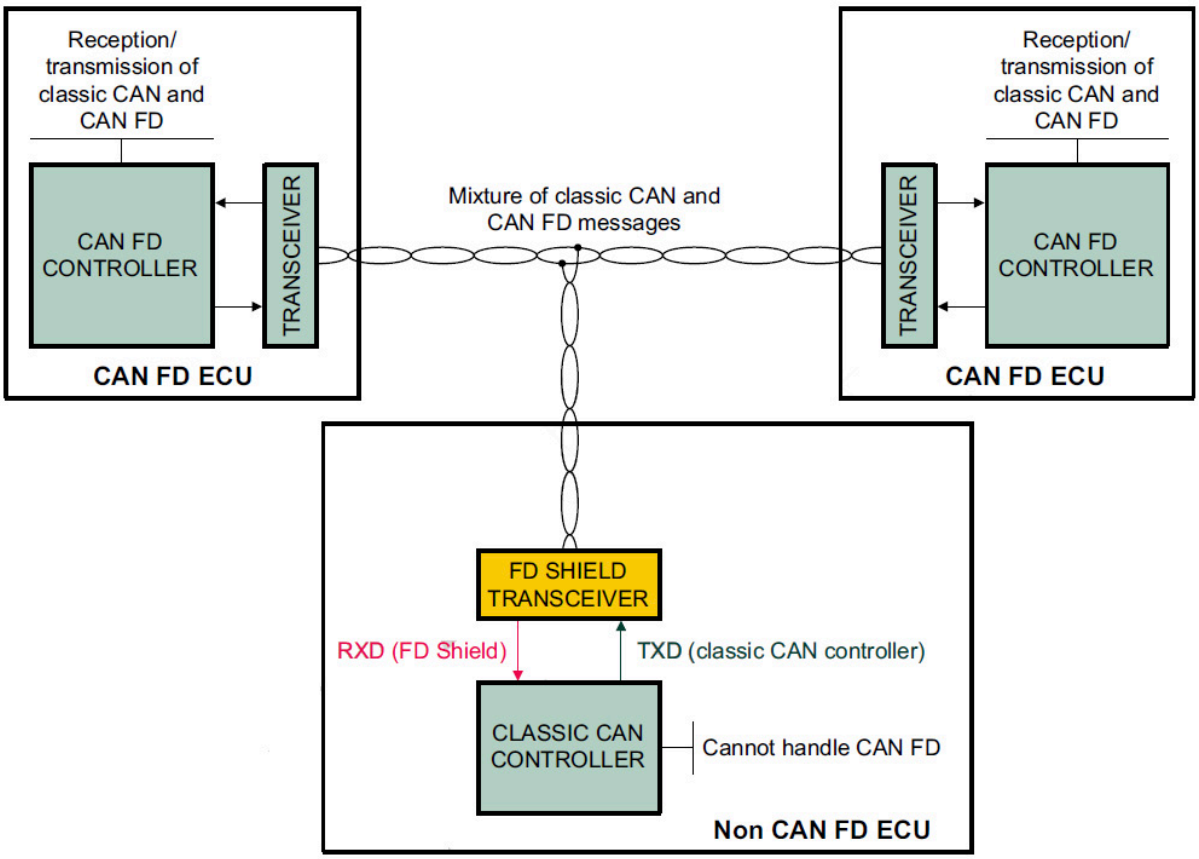

Figure 2: FD Shield set up within a Hybrid CAN FD and Classic CAN Network

Technical implementation of FD Shield

In its simplest terms, FD Shield essentially manipulates the TXD and RXD lines of a Classical CAN controller, based on what is received on the network. FD Shield works by having an integrated CAN FD controller and a highly accurate oscillator in the transceiver itself. As a frame arrives, the SOF and ID of the frame are passed to the CAN controller as usual. On receiving an “FDF” bit, indicating a CAN FD frame, which would cause a Classical CAN controller to generate an error, the FD Shield sets and holds its RXD output to dominant. After 6 bits, the shielded Classical CAN controller generates a stuff error, but the error frame’s TXD signal is blocked by the FD Shield towards the CAN lines, so it does not disturb the bus. The Classical CAN controller then waits for RXD to return to recessive (ISO 11898-1: “10.4.4.3 Error delimiter [...] After sending an error flag, each node shall send recessive bits and monitors the bus until it detects a recessive bit.”).

FD Shield continues to listen to the bus and at the end of the CAN FD frame (during the acknowledge field) it releases RXD to reflect the status of the bus again. This triggers the shielded CAN controller to send the (recessive) error delimiter, which concurrently occurs with the CAN FD controllers processing the end of frame field (EOF). The error delimiter and the EOF end at the same point in time, thus bringing the shielded Classical CAN and CAN FD controllers immediately back in synch; both types of controllers are now ready to start the next SOF and can arbitrate their frames against each other.

The consequence of this approach is that the Classical CAN controller increments its receive error counter by at least 9 (but possibly more) for each CAN FD frame and decrements it by 1 for each Classical CAN frame received. The Classical CAN controller will therefore likely become ‘error passive’ unless there is a high ratio of Classical CAN vs. CAN FD frames. Being ‘error passive’ means the CAN controller has to wait an additional 8 bit times after a successful transmission before starting the next (see ISO 11898: section ‘suspend transmission’). But, since the time penalty only applies to consecutive transmissions and the

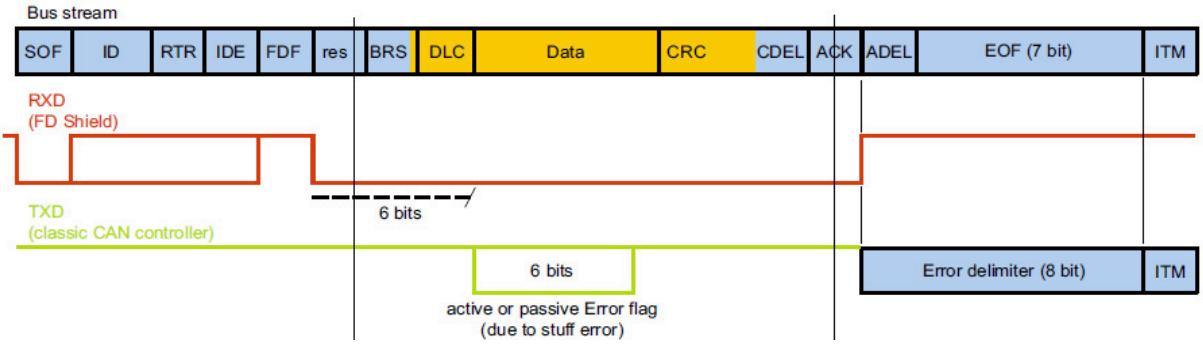

Figure 3: Time-axis view of FD Shield's behavior when receiving a CAN FD frame. The top row shows the data on the bus; the second row shows the RXD pin of the FD Shield; the bottom row shows TXD output of the Classic CAN controller, where the error is blocked towards the bus.

Classical CAN node has just lost the arbitration to the CAN FD frame, there is no additional waiting time after receiving a frame and being error passive.

As the receive and the transmit error counters are independent, there is also no risk of the shielded CAN controller entering 'bus off' state. A full elaboration of FD Shield's behavior extends beyond the scope of this article, but is described in NXP's TR1406 Technical Report and covers all corner cases and implications of the error passive state.

Industry acceptance

NXP has been actively working with partners in the industry to validate this concept. The aforementioned technical report has been assessed by a leading industry CAN conformance test house and confirmed as having no blocking criteria that would prohibit its use within the vehicle. A full conformance test of the FD Shield function is also in progress at the time of writing, where the assessment is made against the official ISO "CAN FD Tolerant" test specification.

Additionally, an assessment of FD Shield together with Autosar has been completed by a leading Autosar software provider, confirming that an Autosar node can handle both Classical CAN and CAN FD messages and that as the receive error counter is not passed beyond the CAN Driver interface, there is no issue with the node being error passive.

Finally, NXP is working with toolchain providers to enable automotive manufacturers to assess their existing CAN networks and understand which nodes are generating the most bandwidth, and what the effect of upgrading just these specific nodes can be on the overall network performance, to keep upgrade costs to a minimum and increase the adoption of CAN FD. Status and plans for the future NXP is currently developing a first silicon concept, which will have a first implementation of the FD Shield function ready for sampling in October 2015. A full product development will continue thereafter.

In conclusion, FD Shield is positioned both as an interim solution for fast CAN FD adoption while CAN FD controllers become available allowing a mix of Classical CAN and CAN FD controllers on the same bus, and as a longer term solution to avoid legacy ECU upgrade costs and maximize re-use. Unlike other strategies for the gradual introduction of CAN FD, it is fully scalable overtime, allowing additional CAN FD nodes to be ported easily without future changes to the architecture, and allows the network architecture to be function driven, rather than technology driven, with benefits for routing and easier security management.

Tony Adamson
NXP Semiconductors
Gerstweg 2
NL-6534 AE Nijmegen

Tel. +31-24-353-0
tony.adamson@nxp.com
www.nxp.com