Implementing a CANopen injector FSA

An injector compliant with the CiA 425-2 implements a CANopen NMT (network management) slave FSA (finite state automaton) and an injector FSA. The coupling possibilities of the both FSA are analyzed in this article.

The CiA 425 specification available from CAN in Automation (CiA) is a CANopen application profile for medical diagnostic add-on modules. The part 2 (CiA 425-2 [3]) specifies the CANopen interface of an injector. The document does not explicitly specify the relationship between the injector's CANopen NMT slave FSA and the injector FSA. It states that the both automata are only loosely coupled, as an injector provides local control functions (local safety requirements) even if communication between the injector and its communication partner (scanner) breaks down. The latter is commonly known as a communication loss. CiA 425-2, nevertheless, specifies for the injector FSA selectable safety-behavior options in case of a communication loss. Similarly, the CiA 301 ([1], base CANopen specification) specifies options for the CANopen NMT slave FSA.

This article tries to establish a relationship between the two state machines, if a communication loss occurs. Achievable and realistic relationship with currently available options (see CiA 425-2 and CiA 301) is analyzed regardless of injector's local safety requirements.

CANopen NMT slave FSA and injector FSA

The CANopen NMT slave FSA (see CiA 301) models the behavior of the communication function unit on a CANopen device. The injector FSA (see CiA 425-2) models the application behavior of the injector device. The latter utilizes its underlying CANopen communication function unit to communicate with its counterpart CANopen communication function unit on a scanner device. In a CANopen network consisting of an injector and a scanner, the injector is the NMT slave, and the scanner is the NMT master (specified in CiA 425-1 [2]). Thus, the injector implements an NMT slave FSA, which is controlled by the scanner. This is valid regardless of the injector's operation mode.

Which injector functions can be controlled by the scanner depends on the currently active operation mode (see CiA 425-2), namely monitor, tracking, or control mode. The scanner can choose in which operation mode the injector shall operate. In other words, the scanner decides how much control it has over the injector FSA.

In the monitor mode, the scanner has no control over the injector FSA. The injector and the scanner start and operate independently. But the injector notifies the scanner about its current state (therefore the monitoring).

Compared with the monitor mode, the tracking mode is different in the following two points:

- The injector cannot enter the system ready state until the scanner informs the injector that it is also ready.
- If the injector starts locally, the scanner is triggered to start itself (therefore the tracking).

Consequently, the only difference between the monitor mode and the tracking mode is the way in which the injector and scanner start. In the monitor mode, the injector and scanner start separately. In the tracking mode, the injector starts locally, which then triggers the scanner to start automatically. But, the scanner prevents the injector from entering the system ready state when it is not ready itself. This guarantees that the scanner and the injector can start at the same time. This is the only control function, which the scanner has over the injector FSA in the tracking mode.

In the control mode, the scanner takes full control over the injector FSA. For example, when the scanner starts, it sends a command to start the injector as well. However, due to the different safety control requirements in the injectors implemented by the OEMs, the scanner's control over the injector FSA is more restricted than it is allowed in the CiA 425-2. For example, scanner's request to arm the injector (i.e. remote arming by transitioning state from idle to injector ready) may be denied by the injector, even though the state transition is remotely allowed per CiA 425-2.

As described above, in the tracking mode, the scanner is triggered by the injector to start. In the control mode (in addition to being triggered by the injector) the scanner started by the operator, can also command the injector to start at the same time. As far as the starting (entering into the procedure-executing state) is concerned, it is a one-way issue in the tracking mode, but a both-way issue in the control mode.

The scanner command (i.e. the control word, including selection of injector's operation mode and controlling the injector FSA) is received by the injector through RPDO 1 (receive process data object). The injector state

Table 1: Value definition for object 1029_h (Source: CiA 301)

Value	Meaning
0x00	Change state to NMT pre-operational if the current state is NMT operational
0x01	Stay in the current NMT state.
0x02	Change state to NMT stopped regardless of the current NMT state

Table 2: Injector FSA reaction to a communication loss (Source: Bayer)

Case	Injector State	Mode		
		Monitor	Tracking	Control
1	Idle configuration Ready configuration Injector ready System ready	No effect	• Transition automatically to idle state, • Change mode immediately to monitor, and • Set global bit-10 to 1 (scanner not ready)	
2	Procedure executing Hold Hold configuration Injection completed	No effect	• Remain in current state or transition to procedure interrupted state (see Table 3), • Change mode immediately to monitor, and • Set global bit-10 to 1 (scanner not ready)	

notification (i.e. the status word, sent either as a response to the scanner control word, or due to a state transition on the injector) is sent to the scanner through TPDO 1 (transmit PDO). This implies that the injector NMT state must be NMT operational, as it is the only NMT state in which a PDO communication is possible. In other words, the injector FSA "lives" in the NMT operational state, regardless of its operation mode. This is the case until the communication breaks down between the injector and the scanner (commonly known as a communication loss).

Communication breakdown

Communication loss happens in two situations: loss of the heartbeat from either side (or both sides), and CAN bus-off on either side, which is eventually detected from the other side as a loss of the heartbeat. So, in the context of the injector FSA, communication loss comes down to two scenarios: loss of the scanner heartbeat and CAN bus-off on the injector.

According to ISO 11898-1 [4], a CAN node is always in one of the three bus error states, namely error-active, error-passive, or bus-off. The error state transitions are controlled by the FCE (fault confinement entity) within the node. A node is said to be in the bus-off state when it is switched off from the CAN bus by the physical layer upon request from the node's FCE. In the bus-off state, the node can neither send nor receive any frames (messages), and can only recover from the bus-off state upon request from the user. The user request here usually means hard- or soft-reboot of the node.

According to CiA 301, loss of the heartbeat is a heartbeat event. Here the heartbeat consumer declares a heartbeat error if no heartbeat messages are received from the heartbeat producer within the pre-determined consumer time (defined in object 1016_h). What has happened to the heartbeat producer is unknown to the heartbeat consumer. The heartbeat producer could have simply failed to send heartbeats in time (but otherwise have been functioning properly) or it could have gone bus-off.

In the injector's object dictionary, object 1029_h (error behavior) informs the scanner what happens with the injector's NMT slave FSA when communication loss occurs. CiA 301 defines three possible options for this object (see Table 1).

If the communication loss is caused by the loss of heartbeat, all three options are possible. But if the communication loss is caused by the injector going bus-off, the first option (0x00) seems to be the only achievable one. The reason is that the NMT pre-operational will be the resulting state after injector's recovery from the bus-off state. It is the only NMT state to which an NMT slave (injector) can be rebooted to.

When the communication loss occurs, CiA 425-2 specifies for the injector FSA the transitions as shown in Table 2. These depend on the current operation mode and the injector state.

The object 6006_h (communication lost) is defined in CiA 425-2 with four possible options (see Table 3).

In the monitor mode, the injector FSA will not be affected by a communication loss regardless of what state it is in. In the tracking or control mode, the injector (regardless of its current state) can choose to change to the monitor mode immediately or to remain in the current mode. But the injector FSA will be impacted by its current state. If the current state is one of the pre-procedure-active states

Table 3: Value definition for object 6006_h (Source: CiA 425-2)

Value	Meaning
0x00	Current injection shall abort immediately, but the injector shall remain in current mode
0x01	Current injection shall complete, and the injector shall remain in current mode
0x02	Current injection shall abort immediately, and the injector shall change to monitor mode immediately
0x03	Current injection shall complete, but the injector shall change to monitor mode immediately

Table 4: NMT slave FSA and injector FSA relationship while normal operation (reliable communication) (Source: Bayer)

Scanner Control Over FSA		
Injector FSA		NMT FSA
Monitor	No control	Full control
Tracking	No control other than: • Able to prevent injector from entering system ready state • Scanner's start triggered by injector's local start	
Control	Full control including: • Able to prevent injector from entering system ready state • Scanner's start triggered by injector's local start • Able to start injector at same time as scanner starts	
Relationship between Injector FSA and NMT FSA		
Injector FSA exists and lives in NMT operational state		

Table 5: NMT slave FSA and injector FSA relationship during a communication loss (Source: Bayer)

Injector FSA			NMT FSA
Monitor	No effect		Injector moves to NMT pre-operational state
Tracking Control	If current state is:	Injector reacts by:	
	Idle configuration, Ready configuration, Injector ready, or System ready	• Changing mode to monitor, and • Moving state to idle	
	Procedure executing, Hold, Hold configuration, or Injection completed	• Changing mode to monitor, and • Aborting or completing injection	
Relationship between Injector FSA and NMT FSA			
Injector FSA exists and lives in NMT pre-operational state			

(case 1 in Table 2), the injector will disarm (by transitioning to the idle state). But if the injector is in one of the procedure-active states (case 2 in Table 2), the injector will either stay in the procedure-executing state to complete the injection, or transit to the procedure interrupted state to abort the injection.

The objects 1029_h and 6006_h make it clear to the scanner that, during a communication loss, the injector FSA may live in the NMT pre-operational, NMT stopped state or in the NMT operational state. However, injector's staying in the NMT operational state (if communication loss occurs) means that TPDO 2 and TPDO 3 will still be transmitted by the injector at the rate set by the scanner. But, these TPDOs are most likely to fail, eventually resulting in the error of CAN Tx buffer overrun on the injector. This will force the injector to change its NMT state anyway (i.e. to stop the TPDOs), in violation of the 0x01 option (stay in the current NMT state) set in the object 1029_h sub-index 01_h. Therefore, remaining in the NMT operational state in case of a communication loss is not a realistic option.

The state and mode transitions make more sense if the communication loss is caused by the heartbeat loss. If the injector goes bus-off, it will go to the idle state and the monitor mode after a reboot (recovering from the bus-off). But the CiA 425-2 does not differentiate between the heartbeat loss and the bus-off as far as the objects 1029_h and 6006_h are concerned.

Therefore, in order to satisfy both cases (heartbeat loss and bus-off), the most realistic options for object 1029_h sub-index 01_h seems to be 0x00 or 0x02. For the object 6006_h it seems to be 0x02 or 0x03 (if the injector has a separate sub-system that can go bus-off without interrupting the injector). This means that during a communication loss, the injector FSA, with the mode changing to monitor, most likely lives in the NMT pre-operational state.

When the communication loss recovers, the scanner reconnects with the injector, and switches the injector back to the NMT operational state, so that the injector FSA will be living in the NMT operational state again. But the injector may deny the connection until the current injection has completed (if 6006_h has the option 0x01 or 0x03) and the injector state has moved to idle (either automatically or by a user interaction).

Summary

The relationship between the injector's NMT slave FSA and the injector FSA is summarized in the Table 4 (normal operation) and Table 5 (communication loss). ◀

References

[1] CiA 301: CANopen application layer and communication profile, v. 4.02

[2] CiA 425-1: CANopen application profile for medical diagnostic add-on modules, Part 1: General definitions, v. 2.1

[3] CiA 425-2: CANopen application profile for medical diagnostic add-on modules, Part 2: Injector, v. 2.3

[4] ISO 11898-1: Road vehicles – Controller area network (CAN) – Part 1: Data link layer and physical signaling, 2015

Author

Ron Kong
Bayer US LLC
ron.kong@bayer.com
www.bayer.us