MilCAN Fault Tolerance Layer

Panagiotis Ioannis Oikonomidis (UoS), Elias Stipidis (UoS), Periklis Charchalakis (UoS),
Falah Ali (UoS)
- Vetronics Research Centre -

The operational environment and physical conditions can affect significant embedded control networks to the point of failure. Fault tolerant systems usually require customized platforms which makes them not as flexible to use when only determinism is required rather than safety critical operation. In this paper, a Fault Tolerance layer is introduced that is designed as an add-on to the MilCAN standard, which offers an option to use off-the-self equipment achieving determinism and redundancy.

Network Electronic Architectures (EA) are dependent largely by their operational environment and physical condition of the network at any given time. In an ideal world everything should work flawlessly according to the theoretical specification, but in practice, under stressful and demanding conditions this is not the case.

Fault tolerant applications require EA that provide continuity of service and determinism which require redundant network architectures. To provide high level deployability with off-the-shelf CAN equipment is a hard task. MilCAN [1, 2, 3] is a deterministic high layer protocol used primarily in military vehicle EA located between the application and the CAN hardware. To enhance the MilCAN capabilities and application suitability a Fault Tolerance (FT) layer is being introduced that is located between the application and MilCAN layers. The FT layer is responsible to manage the physical connections of the node with multiple buses.

FT layer characteristics

The FT layer is transparent to the application and is operating on two or more MilCAN buses in order to achieve continuous operation and manage the physical connections of devices. It doesn't require any modification of the key MilCAN operational characteristics as it is based on existing MilCAN capabilities and methodologies to reduce complexity. FT and non-FT devices can co-exist within a single network (inter and intra segment) as the FT layer is a non invasive software component keeping the hardware requirements to a minimum. Furthermore the FT layer is transparent to the application layer abstracting its operation from the number of physical CAN network interfaces available as can be seen at figure 1. In this way the development of the application becomes much easier and can be ported to a number of COTS devices and still keep high level of determinism.

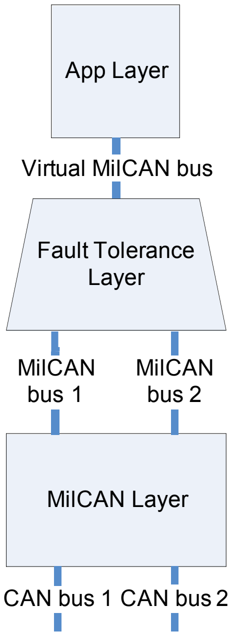

Figure 1: FT layer

During normal network operation the FT layer is responsible to collecting information on the buses status and manages them according to the instantaneous requirements. As being responsible for the continuity of service it is dependable to moving the traffic on the healthiest bus and tries to recover any potential faulty ones.

It is using an elected master device which is responsible to manage the operation of the network by using a synchronization protocol. Also the use of the FT layer on a device connected on one bus is still beneficial because it allows the device to recover the bus back to operational.

MilCAN

MilCAN [1] is an open-standard interface to the CANbus technology aiming to provide the capabilities required by military applications. MilCAN defines compulsory features that are required to accomplish a deterministic network operation. To be able to achieve deterministic operation MilCAN is using a prioritized bus access and bounded throughput to support deterministic data transmission on the network, based on the criticality of each nodes function. There is guaranteed maximum transmission latency for the different priorities. The message generation can be limited within their allocated period; the network traffic can be pre-scheduled to provide this deterministic operation.

CAN error detection

The CAN [2] controllers have 5 measures to detect errors: bit monitoring, 16-bit cyclic redundancy check, acknowledgement check, variable bit stuffing and frame check. These errors are being reported to the Bit Stream Processor (BSP) which is responsible for incrementing and decrementing the Error Management Logic’s (EML) Receive Error Counter (REC) and the Transmit Error Counter (TEC). When at least one of these counters exceeds the error warning limit of 96, the Error Warning (EWRN) flag is set; and when both of the error counters are less than the error warning limit, the flag is reset. For the CAN nodes to distinguish short disturbances from permanent failures and to act accordingly the nodes can have three different states. The three states are error-active when the REC or TEC is smaller than 128, the error-passive when the REC or TEC is bigger than 127 and the bus-off when the TEC is bigger than 255. At the error-active state the node takes part in bus communication and when an error is been detected an active error flag is sent. Also at the error-passive state the node is able to take part in bus communication, but when an error has been detected a passive error flag is sent. The third state is the bus-off where the node is switched off the bus due to a request of fault confinement entity. During this state the node is unable to send or receive any frames. The device remains in this state, until the bus-off recovery sequence is finished.

MilCAN system modes

MilCAN has three system modes, these modes are: Pre-operational (Pre-op), Operational (Op) and System Configuration. When a node powers on, it goes first to pre-op mode and when it receives a valid sync frame message then it goes to operational mode. Then from the operational mode if the node receives the enter configuration mode sequence it goes to system configuration mode and if it doesn’t receive a sync frame for 8 PTUs then it goes back to pre-operational.

FT layer design

The FT layer is completely independent of the App layer; however the FT layer is controlled by the application. In case that the application is not responding, the FT would still be operational due to a higher priority interrupt which becomes active in case of application inactivity after a predefined time interval.

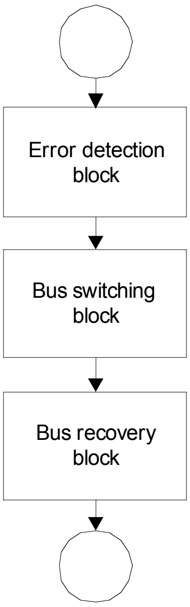

Figure 2: FT layer design

To achieve a synchronized MilCAN configuration and switching between the nodes during operation time there is communication between them. Control messages are transmitted at all times to indicate which bus is active and its current speed. These messages are periodically transmitted every 512 slots in order to reassure that nodes which just became alive are informed and operate correctly. These messages are being transmitted by the FT master which at the moment has been designed to be the same as the MilCAN master. In case of bus problems every node is responsible to inform the rest by transmitting an asynchronous message.

The FT layer design is based on three blocks each with different task as can be seen at figure 2. These blocks are error detection and handling, bus switching and last bus recovery. These blocks are independent but combined provide the FT layer operation.

Error detection and handling

The FT layer is responsible for the communication of the App layer with the rest of the network. Whilst operating, various faults can cause errors on the communication or even preventing it from happening completely. The reasons for this can be either the physical damage of the bus or interference caused from other systems on the vehicle.

The block that is responsible for the error detection is gathering information for the bus status to act accordingly in order to achieve continuous communication. The bus-off from CAN and Pre-op from MilCAN is used for the health detection of the bus as can been seen in figure 3. As described above when the status is at bus-off that means that many errors have occurred on the bus and the bus is switched off. Also when the node cease to receive Sync Frames for 8 PTUs goes from operational mode to pre-operational, this can happen due an isolation of the node from the rest of the network or errors on the MilCAN layer. With these two sources for error detection all possible faults are being covered with good respond times. Good respond times because in case the node is disconnected from the bus the FT layer does not have to wait until the TEC reaches the bus-off limit and with the help of pre-op manages to detect it quicker. When the error detection block detects errors on the bus the switching block is responsible to switch the traffic to a healthy bus and the recovery block to try to recover the bus that the errors were detected.

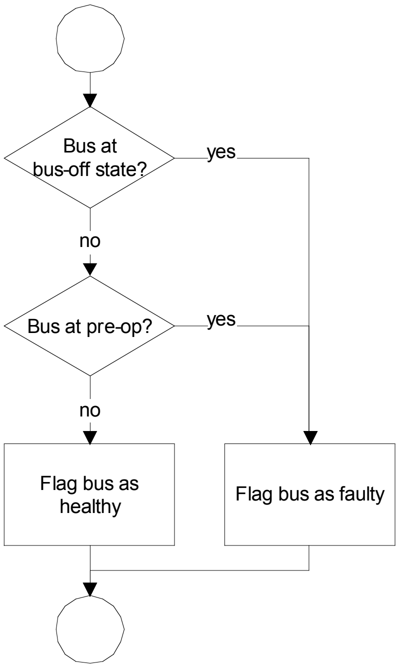

Figure 3: Error detection

Bus switching

The switching block is responsible of ensuring continuous communication between the nodes when errors are being detected. The switching procedure triggers by two different ways, when the node detects error on the bus or when the node receives message from another node that has errors on the active bus. Then the switching block is trying to move the traffic to the next healthy bus with the best possible characteristics as seen in figure 4. In the case that the traffic has been moved to a bus that operates error free at maximum bus speed then the traffic remains to that bus until errors are being introduced and needs to switch the traffic again. In the case that the traffic has moved to a bus that operates at lower bus speed, the traffic switches to another bus the moment it detects a bus with higher operating bus speed. That can happen because the recovery block managed to recover a faulty bus back to maximum operating bus speed.

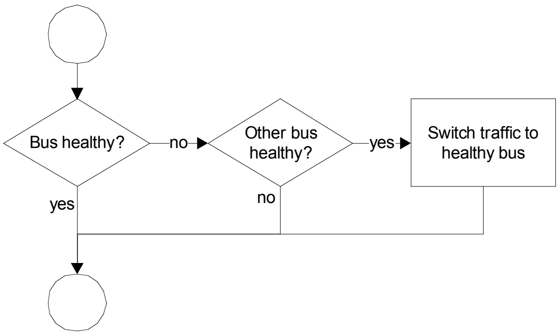

Figure 4: Bus switching

Bus recovery

Due to the nature of the FT layer, which resides above the MilCAN layer, the actions that it can use for bus recovery are limited. The options are a combination of bus switching and various bus operational speeds. When a bus was detected to have errors by the error detection block and the traffic is no longer on that bus, the recovery block tries to bring that bus back to an error free state as soon as possible. To achieve this, the faulty bus is deactivated and activated periodically every second until it becomes functional again, additionally the speed of the bus is changed every three attempts. The three attempts are a suggested number, and can be up to the system designer and operational system requirements.

When the errors on the bus continue to exist then the bus speed is dropped until the bus reaches the minimum possible speed and if this fails too restarts from the highest speed. The reason the bus speed is reduced is that the bus becomes less sensitive to external interferences at lower bus speeds due to longer bit timings. In the case that the source of the bus errors was external interference, the bus can become operational again by working at lower bus speeds. The operation can be seen in figure 5.

In order to recover the bus back to operational mode the CAN speed may change, so the bus becomes less sensitive. However, this could affect the scheduling of the application, because at lower speeds the MilCAN cycle becomes longer and the synchronous messages assigned to specific slots would be transmitted with delays. To overcome this problem there are various options and this is up to the developer to select a suitable one. The developer can use different schedules for every given CAN speed hardcoded or adjust the frequencies of the messages dynamically. The frequency of transmission can be divided or multiplied depending on the priority of the message. For example, the frequency on the HRT messages can be multiplied and the frequency on the SRT messages can be divided or even the message can be dropped. This way there would be enough available bandwidth for the higher priority messages. If the operation of a node is not so important, it can stop transmitting messages completely. Any kind of solution adopted has to make sure that the limit of the bandwidth of the bus is not exceeded.

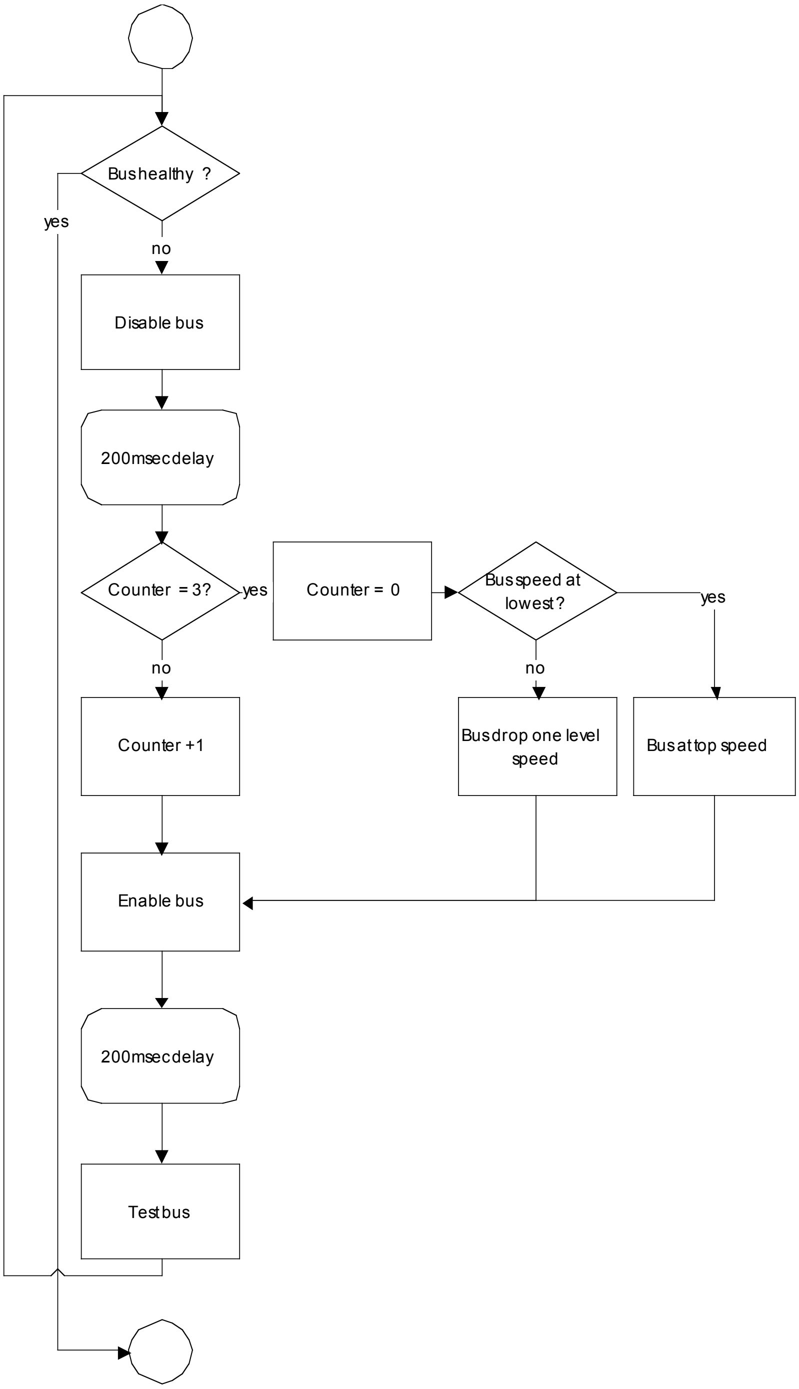

Figure 5: Bus recovery

Testing

For initial verification testing the FT layer has been implemented on the Infineon C167CS microcontroller using two CAN buses in a test rig segment composed of four nodes to realize a dual redundancy MilCAN bus system. To ensure the responsiveness of the FT layer different faults are injected to the buses using of-the-shelf test equipment such as CANstress from vector to introduce short-circuit between the CAN-high and CAN-low, increasing bus length, and corrupt CAN messages.

Timing is very important for the operation of the FT layer. The switch over of the microcontroller to an operational bus from a non operational has to happen very quickly in order to lose the least transmitted messages. Very important is also the time it takes to detect an unhealthy bus and the time to repair it from the moment that there are no errors introduced to it. Throughout the testing of the FT layer on the testbed the time durations for the above mentioned periods were recorded. The average time for the bus switch from a faulty bus to a fully functional one is 532µs with a minimum of 307µs and a maximum of 819µs as seen in figure 6. For the bus recovery when there are no errors being introduced any more there is a constant time of 198ms to recover it back to a fully operational.

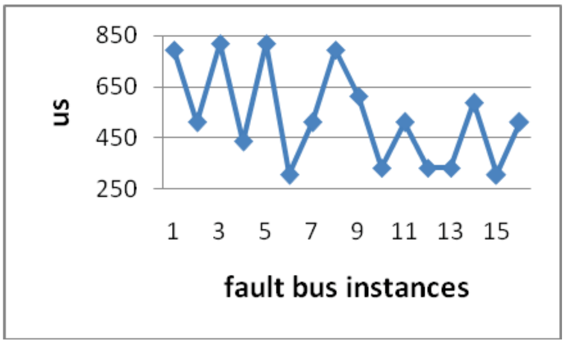

Figure 6: Bus switch times

Conclusion and Discussion

The use of the FT layer provides the benefit of converting off-the-self CAN equipment to redundant network architecture. It can operate successfully with FT and non FT devices on the same network and can benefit even when devices are connected to only one bus by being able to recover it. The implementation of the FT layer in an existing system is easy and straight forward with no extra costs. The recorded performance of the layer is rapid enough and doesn't overload the device; as a result the application is unaffected and continues operating smoothly.

By having a successful operation of the FT layer on the above mentioned testbed which is four nodes connected with two buses, the next step is to test it on a multi-segment testbed which consists of at least five nodes on each three segments that are again connected on two buses.

Furthermore an important feature of the FT layer is the ability to change the bus speed in case the bus is not recoverable. The reason is when the bus operates at high speed tends to be more sensitive to external interferences than lower speeds. Another operation has to be implemented in the FT layer, a weight selection mechanisms that is able to choose with a weighting process the most appropriate bus for the traffic to be forwarded; according to which devices are connected on every bus and what the operational speed of the bus is.

Acknowledgements

This work is sponsored by the UK Ministry of Defence (Research Acquisition Organisation and Directory of Equipment Capability Ground Manoeuvre) and supported by the MilCAN Working Group.

.

Panagiotis Ioannis Oikonomidis
Vetronics Research Centre
University of Sussex
Brighton
East Sussex
United Kingdom
BN1 9QT
Tel: +44 (0) 1273 872622
Fax: +44 (0) 1273 678766
p.i.oikonomidis@sussex.ac.uk
www.vetronics.org

Dr Elias Stipidis
Vetronics Research Centre
University of Sussex
Brighton
East Sussex
United Kingdom
BN1 9QT
Tel: +44 (0) 1273 678957
Fax: +44 (0) 1273 678766
E.Stipidis@sussex.ac.uk
www.vetronics.org

Dr Periklis Charchalakis
Vetronics Research Centre
University of Sussex
Brighton
East Sussex
United Kingdom
BN1 9QT
Tel: +44 (0) 1273 872622
Fax: +44 (0) 1273 678766
P.Charchalakis@sussex.ac.uk
www.vetronics.org

Bob Connor
Technical Leader Systems Integration, Platform Systems & Engineering
QinetiQ
Bldg A5 Rm G072
Cody Technology Park
Ively Road, Farnborough
Hants, GU14 0LX
Tel: +44 (0) 1252 397011
Fax: +44 (0) 1252 392437
rmconnor@QinetiQ.com
Web: www.QinetiQ.com

Dr Falah H. Ali
Vetronics Research Centre
University of Sussex
Brighton
East Sussex
United Kingdom
BN1 9QT
Tel: +44 (0) 1273 678445
Fax: +44 (0) 1273 678766
f.h.ali@sussex.ac.uk
www.vetronics.org

References

[1] MilCAN Working Group, MilCAN A Specification Rev. 1, March 2006
[2] Controller area network (CAN), ISO 11898
[3] MilCAN - Adapting COTS CANBus to Military Vetronics, CIA/COTS February 2002