Detecting CAN nodes with different or drifting bit-rates

Thomas Waggershauser, Tobias Frey

Authors
Thomas Waggershauser
Tobias Frey

Ixxat Automation GmbH
Leibnizstr. 15
DE-88250 Weingarten
Tel.: +49-751-56146-0
Fax: +49-751-56146-29

Link
www.ixxat.com

Introduction
If one or more devices in a CAN network use different bit-rates as the others, it is hard to find them. The same problem occurs, if the bit-rates are drifting in one or more devices. In order to detect such "bad boys" and other error-causing nodes , the authors present a method based on evaluating the signal characteristics like a fingerprint.

Reference
This article is based on the paper "New methods for the analysis of the physical layer of CAN networks and possibilities for robustness improvement" by the same authors held on the 13th iCC in Hambach Castle (Germany) in March 2012. It can be downloaded from the CiA website (www.can-cia-org).

CAN network systems in which one or more devices use another bit-rate as the rest of the system, are often caused by new installed or replaced devices. Sometimes the bit-rate setting was misconfigured or has been simply forgotten. It may also be due to faulty configurations on devices using soft-configuration, e.g. using LMT or LSS services as specified by CiA. Detecting a globally misconfigured bit-rate can easily be done using most CAN-monitoring tools with included bit-rate auto-detection or an oscilloscope.

However, common CAN monitoring tools fail, when several bit-rates are used in a single network, as these only check for a valid bit-rate. As soon as one valid bit-rate is detected, the tools normally stop auto-detection and provide the first found bit-rate as the correct one.

When a single device is set to another bit-rate, whilst all other devices are using the defined bit-rate, the failure scenario depends on the used higher-layer protocol respectively the application software. In CANopen for example, all device start sending after initialization their Boot-up messages. Depending on several factors, including bus-load, location of nodes on the bus media and difference of the bit-rates used, the CAN network might work or may also fail immediately or after specific operation duration. At least the node with the faulty bit-rate will not be able to communicate with other nodes. Correspondingly, it will not be visible to the other nodes. Therefore, this node is effectively missing even though it is attached to the network.

As an example: In a network with a limited number of nodes, low busload (less than 20%) and significantly different bitrates, the main system (the nodes operating at the correct bit rate) will work. Assuming an existing system controller does not stop the system as one device is missing or the application software stops node due to missing data. All devices operating at the same bit-rate will work. But the single device with a faulty bit-rate will either:

- Enter error passive state due to the absence of an acknowledgement – it continuously repeats this message until it either gets an acknowledgement or until it goes into bus-off due to other errors.
- Enter bus-off state as its and other CAN-frames are destroyed due to the different bitrates.

For networks with high busloads, significantly more CAN-frames will be destroyed; therefore the probability of restarting CAN-nodes is high.

If multiple devices are configured with a differ- ▷

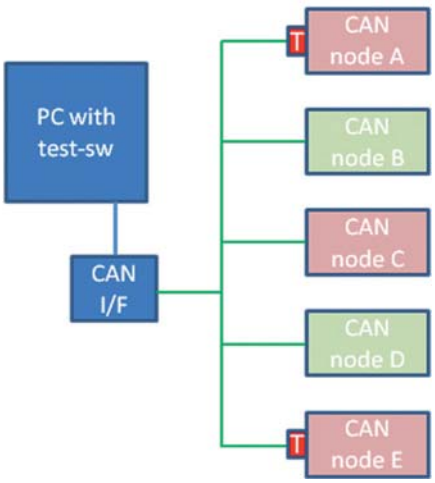

Figure 1: Multiple devices with different bit-rates

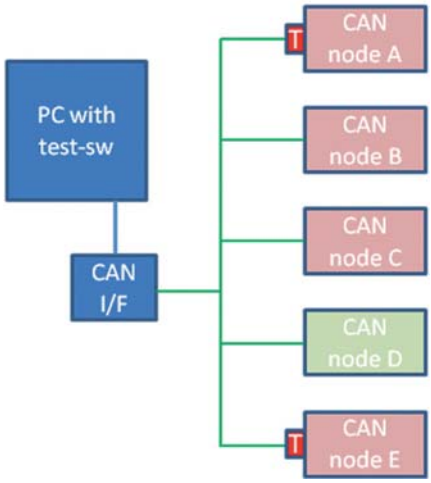

Figure 2: Singe device with a different bit-rate

CANlink® GSM / UMTS

PROEMION
Telematics Systems

Global CAN communication

Monitoring and maintaining machines

CANlink® GSM

Cost-efficient remote diagnostics via GSM/GPRS

Use the sophisticated Proemion Telematics Solutions and the reliable CANlink GSM hardware for remote diagnostics of CAN-based systems. CANlink GSM transmits CAN data via GSM/GPRS from your machine or vehicle to the Proemion Server and vice versa.

You can choose from three available CANlink GSM models. They each offer different features such as a GPS module for positioning and tracking or I/Os, which can be used for overheat and theft protection as well as for many other applications.

Optimally suitable for

- All kinds of mobile and stationary CAN bus systems
- Reliable and economic diagnostics and monitoring

Mechanical Data	5001	5101	5102
Dimensions width / height / depth [mm]	126 / 120.5 / 42		126 / 128 / 42
Degree of protection	IP 65		
Temperature range	-30 °C … +75 °C / -22 °F … +167 °F		
Weight	650 g		
Electrical Data			
DC power supply	6 V – 32 V		
Power input (@ 24 V - Model 5102)	ø 140 mA / max. 500 mA		
Memory: Program / Configuration / Data	384 kB / 4 MB / 512 kB		
Real-time clock with backup capacitor	Backup time 24 h (typical @ 25 °C)		
Status LEDs (2 colors)	3	4	
Interfaces/Protocols			
CAN	1 (ISO 11898-2 high speed, 2.0 A/B)		
GSM / GPRS (class 10) quad band	850 / 900 / 1800 / 1900 MHz		
GPS tracking capability / accuracy	-	22 channels / 3 m	
CANopen®, Layer 2	✓		
Input / Output	-		2x analog / 2x digital
Software			
RM System Tools	157 002 059		
Configuration license	259 000 101	259 000 100	259 000 116
Product Number			
CANlink® GSM	253 004 028	253 004 027	253 004 032
Certifications			
CANlink® GSM	CE, FCC, E1		

For more details please visit proemion.com

Construction Industry

Transport & Logistics

Agriculture & Forestry

Rail Traffic

CANlink® UMTS

High-speed data transmission via 3G/HSDPA

Transmitting CAN data via 3G/HSDPA has one major advantage: The high transmission speed. If you combine CANlink UMTS with Proemion solutions you can manage and monitor your machines regardless of the distance between you – fast and easily.

Choose your hardware from two CANlink UMTS models, available with GPS functionality and I/Os. No matter which one you decide on: You can always be sure to have the best and fastest connection to your machine or vehicle.

Optimally suitable for

- All kinds of mobile and stationary CAN bus systems
- Applications which require fast data transfer rates and reduced latency

Mechanical Data	5201 A1 · A2	5302 A1 · A2
Dimensions width / height / depth [mm]	126 / 120.5 / 42	126 / 128 / 42
Degree of protection	IP 65	
Temperature range	-30 °C … +75 °C / -22 °F … +167 °F	
Weight	650 g	
Electrical Data		
DC power supply	6 V – 32 V	
Power input (@ 24 V - Model 5302)	ø 80 mA / max. 140 mA (UMTS mode)	
Memory: Program / Configuration / Data	384 kB / 4 MB / 512 kB	
Real-time clock with backup capacitor	Backup time 24 h (typical @ 25 °C)	
Status LEDs (2 colors)	3	4
Interfaces/Protocols		
CAN	1 (ISO 11898-2 high speed, 2.0 A/B)	
GSM / GPRS / EDGE (class 12)	A1: 850 / 900 / 1800 MHz · A2: 850 / 900 / 1800 / 1900 MHz	
UMTS / HSDPA dual band	A1: 900 / 2100 MHz · A2: 850 / 1900 MHz	
GPS tracking capability / accuracy	-	22 channels / 3 m
CANopen®, Layer 2	✓	
Input / Output	-	2x analog / 2x digital
Software		
RM System Tools	157 002 059	
Configuration license	259 000 102	259 000 118
Product Number		
CANlink® UMTS	A1: 253 004 029 · A2: 253 004 040	A1: 253 004 037 · A2: 253 004 038
Certifications		
CANlink® UMTS	A1: CE, E1 · A2: FCC	

* Area 1 (Europe,…) / Area 2 (USA,…): frequency depending on country

Shipping · Mining · Automation · Equipment Leasing · Material Handling

ALL FROM ONE SOURCE

Hardware and Software

The hardware is installed in your machine or vehicle and will reliably transmit data via GSM/GPRS/EDGE/3G/HSDPA. On the software side, Proemion offers the possibility to either display and monitor CAN data with Proemion Web Portal or to access them with Proemion Real-Time.

Proemion offers

- A complete package for telematics
- Easy integration
- Outstanding usability
- Highest system availability

The interaction between hardware and software is a decisive factor for a successful telematics solution. Therefore, Proemion trusts in hardware products which are optimally suitable for all its solutions: CANlink GSM / UMTS.

Many international clients already use the powerful combination of CANlink GSM / UMTS devices and Proemion successfully. They also benefit from the expert support and comprehensive web hosting which Proemion offers.
Just let us know your needs and try the numerous possibilities of Proemion today!

Add-Ons

Proemion Web Portal already offers a sophisticated range of functions in the standard version. However, you can extend the functionality with different add-ons at any time.

Theft protection via geofencing, administration of users, groups and rights, remote diagnostics or notifications on specified events – add all these extra functions according to your needs.
That way, you can create your own, customized Proemion Web Portal.

Proemion Real-Time not only allows for real-time access to diagnostic data, but can also be extended with the Proemion Web Portal functionality.

Proemion can offer you the following versatile add-ons:

- Geofencing
- Administration
- Events (SMS/e-mail)
- Display Values
- Additional Values
- Real-Time

SIM Card Handling

Apart from the hardware and software, Proemion can also provide you with SIM cards for the CANlink GSM / UMTS devices and thus deliver the hardware preconfigured and ready-to-start.

The use of this "all-in-one package" ensures that the software, hardware and SIM card are perfectly adjusted and allow for an optimal use in your machine or vehicle.

Best of 2012 Award

Proemion Real-Time has been honored with the "Best of 2012" award by an expert jury of "Initiative Mittelstand". This initiative is in charge of a well-known German innovation award for medium-sized businesses and states with the "Best of 2012" award that Proemion Real-Time is one of the top products in the category "Mobile".

Superior Quality MADE IN GERMANY

PROEMION GMBH

Headquarters
Donaustr. 14, 36043 Fulda, Germany

Phone: +49 661 9490-600, Fax: -666
info@proemion.com, proemion.com

PROEMION CORP.

US Subsidiary
711 E. Monument Ave., Suite 310
Dayton, Ohio 45402-1490, USA

Toll-Free US: +1 877 RMCAN-US
Phone: +1 937 558 2211
Fax: +1 937 641 8787
info@proemion.com, proemion.com

ent bit-rate, this leads to several different bit-rates in the network. If we use the same assumptions as above (low bus-load, significantly different bit-rates, limited amount of nodes and no main system controller stopping the system) the system might work – at least the nodes with same bit-rate will be able to communicate with each other. Nevertheless, there will be a significantly high number of error-frames.

Even if devices are correctly configured, it might happen that devices show a wide-drifting range of their bit-rate. This also leads to temporary different bit-rates and may show similar behavior as described in the case of a single device or several devices using faulty set bit-rates.

Detection of different bit-rates

To detect the different bit-rates, several tools may be used:

- Oscilloscope
- CAN service, diagnostic and monitoring tools
- CAN-based host controllers

When using an oscilloscope, a very detailed analysis is possible and also very small bit-rate variations can be measured. This is often the only way of identifying the CAN node with a faulty set bit-rate. However, an oscilloscope is more expensive than the other tools and analysis requires significantly more CAN know-how and effort if a basic oscilloscope without CAN trigger and CAN decode functionality is used.

CAN service tools, whether hand-held stand-alone tools or PC-based solutions, e.g., PC-CAN interface with CAN monitoring software, are commonly used to check the basic operation parameters of CAN networks such as bus-load, active CAN nodes and CAN identifiers. But these tools may also allow a very detailed analysis of the data communication.

Some of these CAN monitoring and test tools provide automatic bit-rate detection, which sets the CAN controller to different bit-rates and selects the bit-rate, which provided valid CAN data frames. This allows to detect different bit-rates.

CAN-based host controllers can also be equipped with this bit-rate scan mechanism.

As we will focus on the user-view, we will only explain the possibilities, when using CAN test tools and will omit the usage of oscilloscopes. We will also omit the host-controller, as the results are identical to the results when using CAN test tools.

With some modifications by the tool providers, it is possible to enable checking for several simultaneously used bit-rates in a CAN network. To verify the operation and reliability of this idea, we generated a prototype test software. The automatic bit-rate detection of our CANopen Device Manager was used as a basis for this test software. The test software interacts with a CAN controller scanning for common bit-rates, including the bit-rates as specified for CANopen networks. Scanning is done by setting the CAN controller to a bit-rate and checking, if valid CAN frames are received within a pre-defined check time. If valid CAN frames are received, the selected bit-rate is included in the list of active bit-rates. After expiration of the check time, the CAN controller is set to the next bit-rate to be tested. To make sure that the check time does not fall into the restart time of a CAN-node going into bus-off, the complete scan procedure was repeated.

A PC-CAN interface using a standard SJA1000 CAN stand-alone controller by NXP was used. In addition, the test setup included the modified monitoring tool with bit-rate-detection and a CAN network consisting of five CAN nodes as shown in Figure 1. The termination resistors are attached to nodes A and E.

Nodes A, C and E use bit-rate 125 kbit/s, the nodes B and D are configured to communicate with 250 kbit/s.

After running the automatic bit-rate detection, the test software shows both used bit-rates. Several CAN test tools used for comparison show only the first found bit-rate depending on the implementation of the bit-rate detection.

Using the CanAnalyser set to the found bit-rates provides information on which nodes are using which bit-rate. This allows detecting the faulty configured devices.

If just device D communicates with 250 kbit/s (see Figure 2), the tools may also detect only one bit-rate as in the above described scenario with multiple misconfigured nodes.

If all nodes are configured to use 125 kbit/s, and node D is modified in a way to achieve a wide range drift of the bit-rate, the error rate shown in a simultaneously running CanAnalyser was lower than expected. The explanation for this is that the drift was not big enough to get close enough to other bit-rates. This was proven using an oscilloscope. Therefore, the test-software would need to use all bit-rates supported by the CAN controller, then setting the CanAnalyser set to all active bit-rates would show node D using several bit-rates.

Detecting the sources of error-frames

The CAN protocol is focused on providing robust communication independent from external influences. Therefore, CAN makes use of advanced error detection, error notification and error containment mechanisms, which are included in the protocol-engine of each node.

The only way to get more information on the node, which started the error-flag is using an oscilloscope. However, even with this, it is often not possible to identify the causing CAN node.

If passive error flags are visible on the oscilloscope, then the node transmitting this current CAN frame is destroying it. Therefore the CAN identifier can be used to select the causing device. However, in certain cases this does not help, e.g. if CAN remote frame, is destroyed.

For active error flags or in case of not possible detection using the above way, the oscilloscope can help detect the culprit. With oscilloscopes offering better bandwidth, higher sample rates and easy to use mask tests, it is also possible to detect the CAN node causing the error by only the starting edge of the error flag.

The allocation of a message due to a single signal edge is only possible if the signals from the different nodes differ to a certain extend. The signal difference is due to:

- Different layout and components used in devices, notably protection circuits have major impact on the signal form.
- Variances in components even in identical built nodes can cause the signal form to differ. Differences in resistors and capacitors lead to different signal levels (e.g. due to changing power supply of CAN transceiver, changing capacitance/impedance, etc.).
- Differences in voltage-supply and local EMI. If the power supply of the node is affected and offers inconsistent voltage levels, this can have ef-

fects on the CAN node (depending on node design), the same is true for disturbances that are on the voltage line and might affect devices via this way.

- The position on network cable also influence the signals, the signal form of distant devices differs from nodes close to the measurement device, even if the devices would have identical signal forms if connected directly to the measurement device.
- The position regarding other CAN nodes in a CAN network also affects the signal form significantly. CAN side local EMI effects do influence the signals significantly – and these EMI might also be due to specific CAN nodes, e.g., high power inverters.

To show the difference in signals, two nodes of the same making in an optimized laboratory network (10 m cable length, minimum external signal distortions and a 1 m distance for node B and a 9 m distance for node A to the oscilloscope) are measured (see Figure 3). It is easily possible to distinguish messages from different nodes by only one single signal edge as shown in Figures 4 to 6. To achieve this view a mid-range oscilloscope was used, with an external trigger on the recessive dominant signal edge. Each graph shows a timeline of 60 ns at a bit-rate of 500 kbit/s.

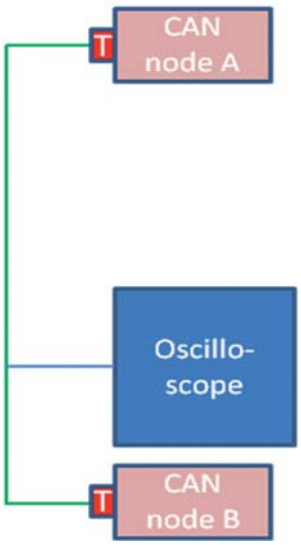

Figure 3: Test setup for node detection according to signal characteristics

Generating a signal-database

First, it is necessary to get each node's signal measured. Notably, the signal edge recessive-dominant is important. To get good results, the network should show the same behavior as during standard operation otherwise signals will look too different for good allocation to the different nodes.

When measuring, the oscilloscope needs to be triggered to the specific messages from the different nodes or it is necessary to verify that only the specific node to be measured is transmitting. Note that detaching other nodes from the network is not good, as this will also influence the CAN-signals.

Therefore a mid-range oscilloscope with internal or external CAN trigger capabilities should be used. Whether this signal is measured and stored by an oscilloscope or a PC-based tool with external sampling hardware is not relevant to the measurements. Either way, it is recommended that the used oscilloscope or sampling hardware should provide a bandwidth and sampling rate of more than 500 MHz. For basic CAN-analysis a lower-performance oscilloscope is suitable, but due to the fact that only a single edge needs to be analyzed in detail, a limited sampling performance will give poor results and it will be hard to identify the error generating CAN node. In addition, oscilloscopes with integrated mask generation and mask tests will ease the comparison of the different signals measured.

The easiest way to get this special signal edge from all nodes is to measure all messages in normal operation mode for a certain time. The oscilloscope should decode the Identifier of the messages and store the signal information to generate a kind of "signal database" for the checked CAN-network. With all nodes being measured, signal information can be stored in the oscilloscope's memory.

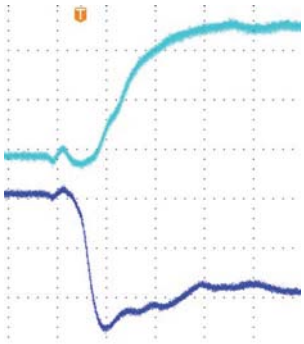

Figure 4: Node A (purple: CAN-low; blue: CAN-high)

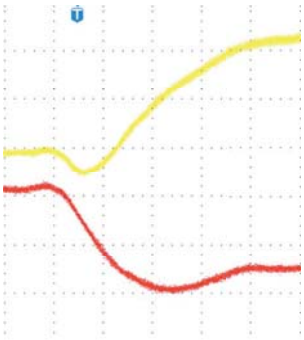

Figure 5: Node B (red: CAN-low; yellow: CAN-high)

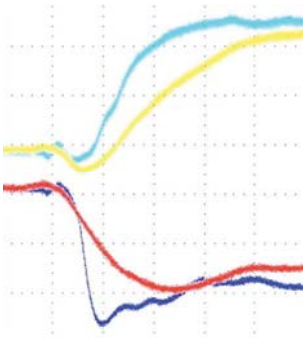

Figure 6: Node A (purple: CAN-low; blue: CAN-high) and node B (red: CAN-low; yellow: CAN-high) in overlay

This stored information now allows determining all messages transmitted by one single node by comparing the sampled signals. By verification of this message, signal-to-node assignment, the user can also check the quality of scan.

In addition, the questioned error flag should be sampled using the same oscilloscope and same settings. Notably, the signal edge recessive/dominant is important.

Now this sample is to be used to generate a signal mask, and by reloading the single node signal samples, it is possible to determine the best fitting signal. As this best fitting signal is calculated from the similarity of the signal masks, the quality of this solution could be calculated in fitting percent.

If the fitting percentage is high, then the sender of the error flag seems to be found. If the fitting percentage is low or if the measurement system is not able to find a node that fits, then the following might be cause:

- Several sent an error flag at the very same time due to detection of message data errors
- Other physical effects cause a global CAN failure, which results in all nodes starting the error flag.

In this case, the transmitting node as well as the physical characteristics of the CAN network need be examined in detail. The available signal samples and the complete sampled CAN error message will also help to find the reason of the error. In order to examine the node transmitting, the "destroyed" message either by checking the CAN-ID, or if the CAN-ID is destroyed or possibly used by several nodes (e.g. for CAN remote frames) by using the sampled signal edge of the data field for comparison with the already available "signal database". ◀