Digitale Bus-Systeme in Kraftfahrzeugen: Funktion und Störbarkeit durch Funksender

Dipl.-Ing. Erich H. Franke, DK6II

erich.franke@afusoft.com

Was Flugzeugen recht ist, ist modernen Kraftfahrzeugen billig. Personen- und Lastkraftwagen, Omnibusse und Sonderfahrzeuge enthalten immer mehr und zunehmend komplexere Elektronik, die mehr und mehr über Bus-Systeme miteinander kommunizieren. Auf der anderen Seite wollen wir leistungsfähige Kommunikationstechnik benutzen. Funksender von Kurzwelle bis in den hohen UHF-Bereich, alte CB- und neue Digitalfunkgeräte, Telematik-Boxen und natürlich Mobiltelefone aller Ausfertigungen. Damit stellt sich für alle, die solche Geräte in Fahrzeugen verbauen die Frage nach der Verträglichkeit. Dieser Beitrag zeigt den Stand der Technik auf der Fahrzeugseite und beleuchtet die Aspekte der Störbarkeit.

Königsbach-Stein, im Juni 2013

Einführendes

Mancher Funkamateur kann ein Lied davon singen.

Als Pendler, Geschäftsreisender oder professioneller Fahrer verbringt man ein gerütteltes Maß seiner kostbaren Zeit notgedrungen in seinem Auto oder Sattelzug zu. Was liegt also näher, im Zeitalter grenzenloser Kommunikation auch an diesem Ort QRV zu sein.

Doch dabei tut sich eine unerwartete Hürde auf. Selbst wenn man das beste Equipment besitzt, Transceiver und Antennen, ob nun gekauft oder ehrenvoll selbst gebaut, so verbieten plötzlich Herstellervorgaben den Betrieb der Funkanlage während der Fahrt.

Ärgerlich, so möchte man meinen.

Doch wie häufig steckt hinter diesem Verbot ein Körnchen Logik. In unserem Fall wächst das Körnchen unter Umständen zu einem richtiggehenden Felsblock aus!

Was steckt also dahinter?

Nun! Jeder Insider weiß, dass moderne Fahrzeuge inzwischen mehr und mehr einem Computer auf Rädern gleichen. Und dieser besteht, anders als unser heimischer PC, in Wahrheit aus einer Vielzahl unterschiedlicher Prozessoren, den „*Steuergeräten*“, die dauernd miteinander kommunizieren müssen, damit das ganze Gebilde auch wirklich funktioniert.

Diese Idee ist nicht wirklich neu. Jede Industrieanlage ist so ähnlich aufgebaut und natürlich auch Flugzeuge, Seeschiffe und militärische Waffensysteme.

Was das heimische Auto dabei so besonders macht, ist der Kostendruck, dem sich die Hersteller unterwerfen um ihre Profitabilität zu sichern. Auf der anderen Seite wächst gleichzeitig der Anspruch der Autokäufer nach immer mehr Komfort, was die Anzahl der Funktionen regelrecht explodieren lässt.

Selbstverständlich ist es nicht wirklich zulässig, den guten alten VW Käfer Baujahr 1960 mit einem Fahrzeug moderner Bauart zu vergleichen. Doch kann uns dieser Vergleich das Dilemma zeigen, in dem die Entwickler heutzutage stecken.

Früher wurden die Anbaugeräte, wie Lampen, Hupe und Zündung mit einzelnen Adern in einem Kabelbaum versorgt und geschaltet. Beispielsweise führten einzelne Drähte vom Lichtschalter zu den Scheinwerfern, dem Rücklicht und der Instrumentenbeleuchtung. Manchmal waren dazu auch Schalter mit vielen Einzelkontakten notwendig, Flachstecker, Sicherungen und vieles mehr und das war aufwändig, fehleranfällig und teuer in der Montage.

In einem modernen Fahrzeug wären darüber hinaus armdicke Kabelbäume notwendig, was aufgrund der Rohstoffkosten – am Beispiel des Kupfers – und der Kosten für die Verkabelungsarbeit nicht mehr sinnvoll abzuhandeln wäre.

Inzwischen ist es tatsächlich billiger und einfacher, ein Steuergerät bei den Rückleuchten zu montieren, das nur noch mit Spannung versorgt wird und ‚lokal' die Verbraucher über kurze Kabel schaltet. Der ‚Lichtschalter' von damals meldet sich dann bei einem anderen Steuergerät am Armaturenbrett und teilt diesem mit, dass der Fahrer die Scheinwerfer einzuschalten wünscht.

Nun muss das Steuergerät am Armaturenbrett eigentlich nur noch dem Gerät bei den Rückleuchten mitteilen, was es zu tun hat.

Und diese Meldung erfolgt dann als Datensatz über ein so genanntes „Bus-System".

Das klingt doch eigentlich ganz gut, oder? Nun ja, zumindest so lange, wie alles reibungsfrei funktioniert. Wir werden gleich darauf zu sprechen kommen.

Ein weiterer Aspekt tangiert die Betriebssicherheit (engl. *Integrity*).

Reichte bei dem bereits erwähnten Käfer noch ein einfacher Unterbrecherkontakt und ein Zündverteiler, so besitzen die Motoren moderner Fahrzeuge immer ausgefeiltere Systeme insbesondere zur Verbrauchs- und Emissionsreduktion. Lastabhängig elektronisch geregelte Einspritzanlage, adaptive Kennfelder für die Zündung, ausgefuchste Abgasreinigungsanlagen. Diese Teile müssen in Echtzeit kommunizieren. Funktioniert diese Kommunikation nicht – auch zeitweise – dann stottert der Motor. Klingt das vertraut?

In den U.S.A. hatte ich einmal ein System gesehen, das vom Hubschrauber aus mittels eines extrem starken Mikrowellengenerators Autos aus der Luft „abschießen" konnte. In Wahrheit erzeugte man mit dieser Einrichtung eine Art Mini-EMP, der die Motorsteuerung des Opfers lahm legte.

Es gibt dabei allerdings noch etwas zu bedenken, und das tangiert die Sicherheit (engl. *Safety*) von Fahrzeug und Passagieren weitaus stärker als wenn Motor oder vielleicht auch nur die elektrische Sitzverstellung nicht mehr so richtig will.

Mehr und mehr greifen die im Fahrzeug vernetzten Steuergeräte direkt in das Fahrverhalten ein.

E-Gas, also das Gaspedal, dessen Stellung durch elektrische Signale übertragen wird ist dabei noch das harmloseste.

Es gibt inzwischen in einer Reihe von Fahrzeugen adaptive Fahrwerke, deren Federungsverhalten in Echtzeit von einem Steuergerät verstellt wird. Der altehrwürdige Stoßdämpfer hat immer öfter ausgedient.

Dann wäre noch die adaptive Bremsanlage als Nachfolger des alt bekannten ABS zu nennen. Hier agieren die Steuergeräte als elektronische Bremsassistenten, die nach Bedarf die Bremse loslassen oder fester drücken.

Das Neueste auf diesem Gebiet - quasi als Krone automotiver Schöpfung - ist die elektronische Lenkung.

Was man beim Airbus als Fly-by-wire bezeichnet taucht zunehmend auch in Mittelklassefahrzeugen auf. Das Lenkrad betätigt dabei nur noch ein Drehgeber und teilt dem hydraulischen oder elektrischen Antrieb der Radlenkung über ein Bussystem mit, wohin das Fahrzeug denn nun fahren soll.

Und spätestens hier muss man sich ernsthaft die Frage nach der Störbarkeit derartiger Systeme stellen. Und zwar nicht unter dem Aspekt von Hardware-Ausfällen, sondern unter Umständen auch bei Störungen durch Kurzwellensender großer Leistung.

Die Krake Bussystem

Bis ca. ins Jahr 2000 konkurrierten mehrere Arten von Datenbusse miteinander. Aus dem Amerikanischen und Japanischen Raum gab es Systeme, die auf den ehrwürdigen seriellen Schnittstellen basierten.

Das K-Line-Interface gemäß ISO 9141 findet sich beispielsweise heute eher bei älteren Baujahren. Es handelt sich dabei im Grundsatz um eine serielle, bidirektionale Ein-Draht-Schnittstelle, bei dem alle Teilnehmer von Versorgungsspannung hart gegen Masse „ziehen". Die Datenübertragung ist nicht besonders sicher, mit 10,5 kBit/s auch nicht übermäßig schnell und ähnelt ein wenig – wenn auch nicht ganz – dem EIB aus der Gebäudeautomatisierung.

Ähnlich verhält es sich mit dem inzwischen veralteten Automotive Interface Bus gemäß SAE J.1850, der in der Fahrzeugdiagnose Verwendung findet.

Im Flugzeugbau, vor allem bei Kampfflugzeugen gibt es den MIL-Bus (MIL-STD 1553), der in der zivilen Avionik durch den ARINC Bus (429) abgelöst ist.

Dieser besitzt bewährte Verfahren zur Störungsvermeidung, wie zum Beispiel Doppelung (Redundanz) von Systemkomponenten und Datenverbindungen und die Härtung gegen elektromagnetische Einflüsse, insbesondere durch den EMP bzw. NEMP.

Der MIL-Bus besitzt als Besonderheit die ‚Echtzeitfähigkeit'.

Unter ‚Echtzeit' versteht man in diesem Zusammenhang, wenn man *exakt vorhersehen* kann, wie lange die Übertragung eines Datensatzes benötigt und nicht, wie oft fälschlicherweise angenommen wird, dass die Übertragung möglichst schnell erfolgt.

Die ‚Echtzeitfähigkeit' ist eine wichtige Voraussetzung dafür, dass man *direkte* Regelprozesse wie am Motor oder am Fahrwerk über einen Bus überhaupt durchführen kann.

Sie setzt voraus, dass die Übertragungszeit einer Nachricht selbst bei Störungen oder Daten-‚Kollisionen' auf dem Bus vorhersehbar bleibt.

Deshalb ist beispielsweise das klassische Netzwerk (Local Area Network, LAN) mit den wohl bekannten Internet-Protokollen (IP) ohne weitergehende Maßnahmen für Echtzeitanwendungen ungeeignet, da Telegrammwiederholungen im Kollisionsfall das Zeitverhalten unvorhersehbar machen.

Daher hat sich heutzutage eine Technologie durchgesetzt, die aus der Deutschen Automobilindustrie entsprang: Der CAN-Bus gemäß SAE J.2284.

Yes, we CAN

Der CAN-Bus wurde von BOSCH als „Car Area Network" definiert und hat sich inzwischen als Quasi-Standard in der Automobilbranche etabliert. Mehr und mehr nutzen auch andere Gebiete den Bus als Grundlage für verteilte Steuerungen. So auch in der Industrie- und Gebäudeautomatisierung, z.B. CANOpen-Lift für Aufzüge.

Der CAN-Bus besitzt ein paar interessante Eigenschaften, die ihn für den industriellen und automotiven Einsatzfall geeignet machen.

Zum Ersten adressiert der CAN-Bus keine Geräte. Er adressiert Botschaften!

Als Beispiel: Im IP-Protokoll legt die so genannte MAC-Adresse (Media Access Code) fest, wer eine Botschaft an wen sendet.

Ein nettes Beispiel dafür zeigt der bekannte Sketch des Komikers Otto Waalkes über *»Die Vorgänge im menschlichen Körper beim Ärgern«*:

»*Leber an Großhirn: Wo bleibt'n der Alkohol?* «

Im grundlegenden CAN-Bus-Protokoll (CAN RAW) stattdessen gibt es keine Geräteadressen.

Hier sind lediglich ‚Botschaften' nebst den dazu gehörenden Parametern definiert.

Jede Botschaft wird durch ihre Nummer, ihre ‚ID' gekennzeichnet.

Diese ID kann, je nach Version in CAN 2.0 A elf beziehungsweise in CAN 2.0 B auch neunundzwanzig Bit umfassen.

	D	x	x	D	D	x	x	x	R	x	R	R	R
Bit	1	11	1	1	1	4	0..64	15	1	1	1	7	3
	Start of Frame	Identifier	Remote transmission Bit	Identifier Extension Bit	reserved	Data length Code (DLC)	Data (0..8 Byte)	Check (CRC)	CRC Delimiter	Acknowledge Time Slot (ACK)	ACK Delimiter	End of Frame	Padding

11-Bit-ID: Anzahl Bit pro Rahmen: 47..111

	D	x	x	R	x	x	D	D	x	x	x	R	x	R	R	R
Bit	1	11	1	1	18	1	1	1	4	0..64	15	1	1	1	7	3
	Start of Frame	Identifier	Remote request Bit	Identifier Extension Bit	Extended identifier	Remote Transmission Bit	reserved	reserved	Data length Code (DLC)	Data (0..8 Byte)	Check (CRC)	CRC Delimiter	Acknowledge Time Slot (ACK)	ACK Delimiter	End of Frame	Padding

29-Bit-ID: Anzahl Bit pro Rahmen: 67..131

Bei 250 kBit/s rund 2000 voll beladene Rahmen pro Sekunde

Physikalisch ist der CAN-Bus ein Zwei-Leiter-System, an dem eine Reihe von Teilnehmern angeschlossen sind.

Alle Teilnehmer sind dabei zunächst gleichberechtigt: Wenn einer sendet, dann hören es alle anderen.

Nach der Konvention wird jede ID eigentlich nur von einem bestimmten Sender auf den Bus gelegt. Jedes Gerät kann nach Herzenslust am Bus zuhören und alle ID herausfiltern, für die es sich interessiert.

In einem fiktiven Beispiel könnte einer angenommenen ID 123 als Quelle das Gaspedal zugeordnet sein.

Damit könnte das Pedal seine Stellung zwischen 0 und 100% melden und jeder, der sich für die Gaspedalstellung interessiert würde sie hören.

ID	Daten
0130	F4 08 A4 00 E3 00 00 00
0070	18 00 00 01 07 00 00 00
0094	44 30 80 00 80 00 00 8F

Beispiel für CAN 2.0A (11 Bit ID)

ID	Daten
0CF00400	F1 B2 B2 08 43 03 FF FA
18FEF100	F3 00 00 00 01 00 03 00
18FEF200	31 01 00 00 FF FF FF FF
0CF00300	D0 FF 39 FF FF FF FF FF

Beispiel für CAN 2.0B (29 Bit ID)

Die fiktive Gaspedalstellung würde dann in die Nutzdaten hineincodiert werden. Im „rohen CAN" können bis zu acht Nutzdaten-Byte pro Botschaft übertragen werden. Diese werden oft als „Parameter" bezeichnet.

Soweit also die gute Nachricht.

Nun kommt aber der Pferdefuß:

Niemand kann mit Bestimmtheit sagen, welche Funktion eine bestimmte ID, beispielsweise unsere ID 123 auslöst!

Die Vergabe der ID ist nämlich einzig und alleine dem Designer des jeweiligen Autos vorbehalten.

Will heißen, dass im „rohen“ CAN-Bus ein und dieselbe ID in verschiedenen Fahrzeugen durchaus völlig unterschiedliche Funktionen haben kann.

Außerdem wird der normale Fall, dass eine ID immer nur von ein und demselben Gerät auf den Bus gelegt wird technisch nicht erzwungen.

Es ist eben nur eine Konvention, damit Gateways wissen, welche ID sie über Busgrenzen weiterleiten müssen.

Um es mit Thomas Jefferson zu sagen: »*Zur Freiheit gehört Verantwortung!* «.

In unserem Fall gehört zur Freiheit, alles auf dem Bus senden zu können zur Verantwortung nur CAN-ID zu senden die man auch wirklich senden darf und zu „wissen“, was eine bestimmte ID im Gesamtsystem auslöst!

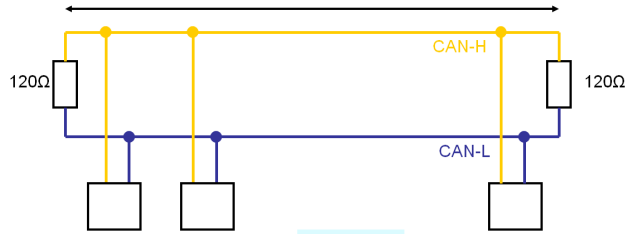
Wie man sich leicht denken kann ist es also keine wirklich gute Idee, ‚piratenmäßig‘ eine ID in den Bus einzuspeisen, womöglich auch noch während der Fahrt, obgleich einem technisch niemand daran hindert!

Ach ja! Und da wäre dann noch die „störende Beeinflussung“ durch elektromagnetische Felder von der Antenne unseres Kurzwellensenders…

Elektrisches

Physikalisch gesehen ist der CAN-Bus ein Zwei-Leiter-System. Die Leitungen werden als CAN-H (HIGH) und CAN-L (LOW) bezeichnet.

Die beiden Leitungen sind an beiden Enden des Busses mit einem Widerstand von jeweils 120 Ohm abgeschlossen. In Nutzfahrzeugen werden die Leitungen auch schon einmal verdrillt, was aus Gründen der Störresistenz durchaus sinnvoll ist.



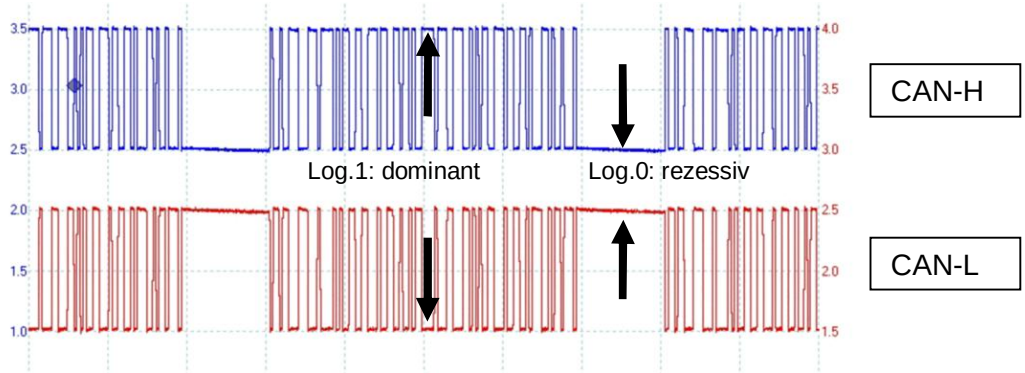
Verwendet werden zu 5-Volt kompatible Pegel in einer interessanten Weise:

Ein „dominantes“ Bit zieht CAN-H aus der Ruhelage auf 3,5 Volt. Auf CAN-L zieht das gleiche dominante Bit die Leitung gegen 1,5 Volt.

Ein „rezessives“ Bit lässt die jeweilige Leitung los. Damit stellen sich auf CAN-H und CAN_L ca. 2,5 Volt ein.

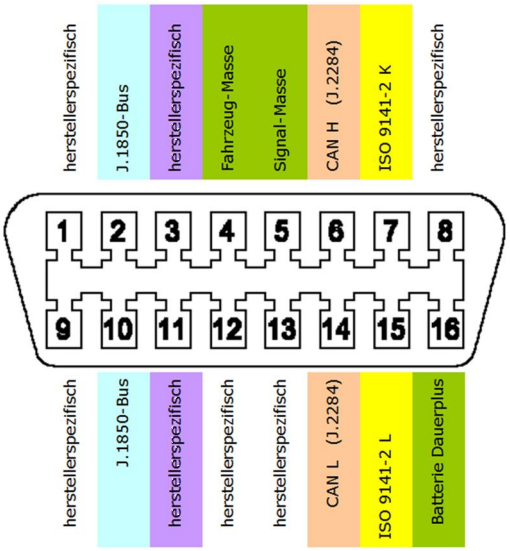
Durch diese „Gegenphasigkeit“ werden die Abstrahlungen durch den Bus minimiert, vor allem, wenn die Leitungen verdrillt sind.

Auf diese Weise lassen sich darüber hinaus typische Fehler wie: »Kurzschluss nach V_{CC}«, »Kurzschluss nach Masse« oder auch Unterbrechungen der Leitungen detektieren und ggf. auch verkraften.



Das ist immerhin mehr als bei manch anderem Bus-System, obgleich niemand garantiert, dass der Entwickler des Autos das auch wirklich macht.

So ist man in gewisser Weise zum Glauben gezwungen.



Der Trick mit den dominanten und rezessiven Bit ist notwendig, um eine Kollisionsvermeidung in Quasi-Echtzeit zu erreichen.

Da sich – wie der Name schon sagt – ein dominantes Bit gegen ein rezessives Bit durchsetzt und weil jeder Sender gleichzeitig auf dem Bus mithört, so muss ein unterlegener Sender sofort mit der Einspeisung aufhören, sobald er einen „dominanteren“ Sender bemerkt.

Als Faustregel kann man sagen, dass ID mit mehr „dominanten“ HIGH-Bits eine höhere Priorität auf dem Bus bekommen und Kollisionen, wie wir sie vom LAN her kennen sollten *eigentlich* nicht auftreten.

Die Bitrate auf dem Bus ist nicht wirklich definiert. Inzwischen haben sich jedoch in der Fahrzeugtechnik Bitraten von 125kBit/s, 250kBit/s, 500kBit/s und 1MBit/s durchgesetzt.

Die erlaubten Kabellängen sind, wie man sich denken kann, abhängig von der Bitrate, vor allem, damit die Kollisionserkennung funktioniert. Im *worst case* müssen sich zwei Bus-Teilnehmer, die eine ID auf den Bus legen sich trotzdem innerhalb eines einzigen Bit noch gegenseitig hören.

Wir unterscheiden bei den Bus-Längen momentan folgende Fälle.

Der „low speed“ Bus (LS CAN) mit Bitraten ≤125kBit/s erlaubt Kabellängen bis zu 500m. Ihn findet man in großen Fahrzeugen, beispielsweise mit Anhängern oder externen Fahrgestellen wie Langholztransporter oder in Industrieanlagen.

Als „medium speed“ Bus (MS CAN) bezeichnet man Busse mit Bitraten ≤250kBit/s. Hier sind Kabellängen von bis zu 100m zulässig.

Der „high speed“ Bus (HS CAN) mit Raten ≤1MBit/s erlaubt immerhin noch Längen bis zu 40m.

Normatives

Auf den CAN-Bus als „rohen“ Informationsträger sind ID mit 11 und 29 Bit definiert.

Es gibt nun eine Reihe von Protokollen, die auf dem reinen CAN RAW aufsetzen, um damit beispielsweise größere Datenmengen als die bereits erwähnten acht Nutzbytes zu transportieren oder um doch eine Art von Geräteadressierung zu ermöglichen.

Ein guter Bekannter aus der Autowelt ist die On-Board Diagnostic (OBD).

OBD, genauer gesagt OBD-2 CAN definiert einen Satz wenigstens teilweise standardisierter Abfragen an die Fahrzeugelektronik.

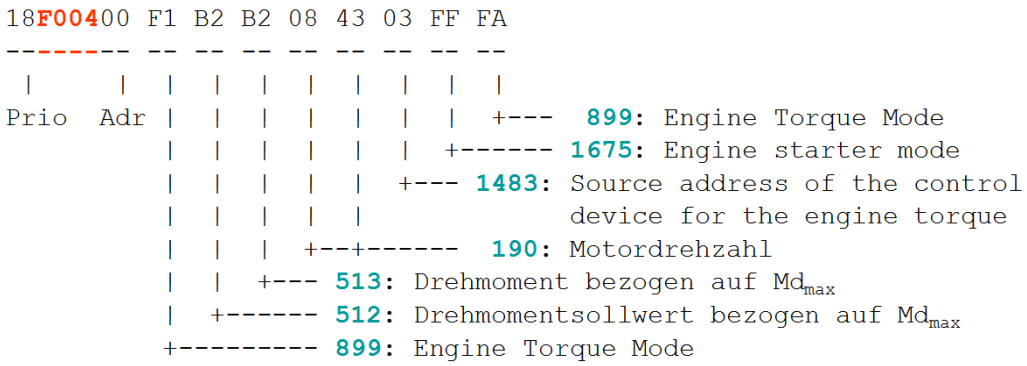
OBD-2 definiert diese Abfragen als „Challenge-Response“-Protokoll. Man muss definiert fragen und bekommt auch nur eine – theoretisch – klar definierte Antwort.

Die Abgasuntersuchung moderner Fahrzeuge verwendet das Protokoll, um das Fahrzeug zu fragen, ob es denn die Bestimmungen einhält.

Technisch erfolgt die Abfrage über den CAN-Bus unter einem weitgehend standardisierten Identifier 0x7DF.

Bei Nutzfahrzeugen hat sich der SAE-Standard J.1939 etabliert. Dieser setzt auf CAN 2.0 B (29 Bit) auf. Jede Botschaft überträgt immer acht Nutzbytes. Damit ist der Verkehr auf dem Bus streng deterministisch.

Die ID enthält die so genannte „Parameter Group Number“ (PGN). Wie der Name schon sagt sind in jeder PGN eine Reihe von Parametern enthalten, die aus historischen Gründen als SPN („Suspect Parameter Number“) bezeichnet werden.



Beispiel für eine J.1939-Botschaft: PGN F004

So enthält beispielsweise die in der hexadezimalen 29-Bit-ID 0x18**F004**00 enthaltene PGN 0xF004 in den Byte 4 und 5 die SPN 190, die die aktuelle Motordrehzahl anzeigt.

Darauf basiert ein weiterer aus der Nutzfahrzeugtechnik bekannter Sub-Standard FMS („Fahrzeug Management System“).

FMS schreibt eigentlich vor, dass die Schnittstelle ein Gateway enthält. Damit sollte der Fahrzeuginterne CAN-Bus von störenden Beeinflussungen geschützt werden, indem er von dem abfragenden Geräte elektrisch und protokolltechnisch isoliert wird.

Das erscheint wie ein Schritt in die richtige Richtung, doch es ist fraglich, ob sich alle Hersteller daran halten.

Gefährliches

Wer schon einmal sein SSB-Signal in einem Audio-Verstärker wiedergefunden hat oder gehört hat, wie sein Mobiltelefon in den PC-Lautsprechern quäkt, der ahnt, was ich mit „störender Beeinflussung“ meine.

Nun sind es aber nicht diese kleinen Unschönheiten, welche den Entwicklern in den Fahrzeugen Sorge bereiten.

Schließlich ist es nur eine Frage der Feldstärke, beziehungsweise der in die Busleitungen eingekoppelten Pegel, ob hierdurch die Datenübertragung behindert, gestört oder verfälscht werden kann.

Letzteres ist für uns das infektiösere Übel.

Die Entwickler des CAN-Bus haben zwar eine ganze Reihe Vorkehrungen getroffen um unschöne Effekte zu vermeiden. Beispielsweise die galvanische Trennung von Bussen unterschiedlicher Funktion.

In den Fahrzeugen gibt es zum Einen den sicherheitskritischen Bus für die Motor- und Fahrwerksteuerung, der schnelle und potentiell gefährliche Transaktionen in Echtzeit steuert.

Daneben gibt es den Bus für die „Komfort-Funktion“, also Klimaanlage, Fensterheber und Sitzverstellung, der für die Sicherheit des Fahrzeugs weniger wichtig ist. Unter Umständen existiert dann noch ein "Entertainment-Bus" für Audio-, Video und Navigation.

In den meisten Fahrzeugen werden diese Busse elektrisch getrennt, so dass sich Daten nicht vermischen können.

Oft laufen diese unterschiedlichen Busse auch mit verschiedenen Bitraten.

Die symmetrische Auslegung als terminiertes System in Verbindung mit der gegenphasigen Ansteuerung selbst bei nicht verdrillten Leitungen ohne Abschirmung eine recht ordentliche Störungsunterdrückung.

Ein Störsignal müsste in CAN-H und CAN-L also genau gegenphasig wirken, um eine Verfälschung zu bewirken.

Zudem enthält das Telegramm selbst eine Prüfinformation in Form eines CRC.

Die traurige Wahrheit jedoch lautet: Imitationen von CAN-Bus-Botschaften kommen im Alltag trotzdem immer wieder einmal vor! Vor allem in elektronisch „rauer“ Umgebung.

Wie immer ist alles nur eine Frage der Wahrscheinlichkeit, ob zu einem Zeitpunkt der CRC eben doch einmal passt, und ein verfälschtes Telegramm auf dem Bus erscheint.

Nun ist es zum Glück nicht so, dass bereits ein einziges fehlerhaftes Telegramm auf dem CAN-Bus zum Totalausfall der gesamten Fahrzeugelektronik führt.

Zum Beispiel werden wichtige Botschaften sogar mehrfach pro Sekunde wiederholt. Diese zum Teil massive Redundanz stellt sicher, dass sich kritische Situationen oft mehr oder minder wie von selbst entschärfen.

Allerdings gibt es auch genügend Gegenbeispiele, die durchaus zu kuriosen Effekten führen können.

Im Fahrzeug des Verfassers beispielsweise fällt sporadisch und unvorhersehbar, jedoch mit unangenehmer Häufigkeit die Geschwindigkeits-Regelanlage (‚Tempostat‘) aus. Fährt man dann auf einen Parkplatz und schaltet die Zündung ab, atmet drei Mal durch und fährt danach weiter, so scheint wieder alles perfekt zu funktionieren. Dies passiert von ganz alleine, also auch ohne dass Funkgeräte oder Mobiltelefone involviert wären.

Selbstredend, dass man diesen Effekt in der Werkstatt nicht nachvollziehen kann und das ist auch nicht notwendig. Jeder KFZ-Techniker kennt solche UFO-Phänomene und je nach nervlicher Stabilität muss man eben damit leben.

Nun ist dies aber kein Defekt und auch kein richtiger Software-Fehler. Er lässt sich – bei stehendem Fahrzeug selbstverständlich – auch durch Einspeisen eines verfälschten Datensatzes hervorrufen.

Damit liegt der Verdacht nahe, dass dieser Ausfall eher vom Geschehen auf dem CAN-Bus herrührt und zu einer Kategorie gehört, die sich eben *nicht* durch Redundanz repariert.

Dieses simple Beispiel zeigt, wie verwundbar diese Technik in Wahrheit ist, wenn tatsächlich massive elektromagnetische Einstrahlungen bzw. Einleitungen in die CAN-Busse auftreten.

In meinem Vortrag werde ich auf entsprechende Beispiele eingehen.

Was man weiterhin nach Möglichkeit vermeiden sollte ist, an den CAN-Bus des Fahrzeugs externe Hardware anzuschließen.

In den wenigsten Fällen sind die auf der OBD-Buchse aufgelegten CAN-Busse über ein Gateway isoliert. Aus Sicht der Hersteller ist dies auch gar nicht nötig, da die dauerhafte Anschaltung externen Gerätes sowieso nicht zulässig wäre.

Da gerade auf dem Gebiet telematischer Diebstahlschutzsysteme Sicherheitsstandards manchmal mit geradezu kindlicher Naivität ignoriert werden muss darauf hingewiesen werden: Die Busse sind vergleichbar mit dem Rückenmark eines Lebewesens.

Speisen wir unbedarft Daten ein, dann reagiert das System darauf. Im schlimmsten Fall katastrophal!

Wie das System im Ernstfall auf das Spektrum einer SSB-Aussendung bei einhundert Watt PEP reagiert, vermag ich nicht abzuschätzen. Die Messungen der elektromagnetischen Verträglichkeit gehen weitgehend von Dauerträgern aus.

Ausblick

Bus-Systeme sind ein nicht mehr wegzudenkender Bestandteil moderner Fahrzeuge mit dem Trend immer höherer Geschwindigkeit. Mehr und mehr der Bordsysteme verlassen sich (blind) auf die Funktionsfähigkeit dieser Datenpfade.

Leider begrenzen in gewisser Weise Kostenüberlegungen die Störsicherheit.

Daher betrachten die Fahrzeughersteller auch den Einbau gerade von besonders leistungsstarken Funksendern mit gewissem Misstrauen, was uns als Funkamateure nicht immer fröhlich stimmt.

Erfreulich ist jedoch, dass uns die moderne Kommunikationswelt mit ihren Mobiltelefonen in die Hände spielt, da diese in vielen Fällen systembedingt im Innern des Fahrgastraumes benutzt werden müssen.

Immer mehr Hersteller setzen beispielsweise auf die Anbindung des Mobiltelefons in der Tasche des Reisenden via Bluetooth, also quasi ein Autotelefon für Arme.

Durch diesen „Kunstkniff“ wird am Auto zwar Geld gespart, die Sende-Antenne des Telefons jedoch in das *Innere* des Fahrzeugs verschoben, was aus hochfrequenztechnischer Sicht ein Wenig fremdartig anmutet.

Umgekehrt sind die Fahrzeughersteller hierdurch mehr und mehr gezwungen, ihre Produkte gegen elektromagnetische Beeinflussung aus dem Fahrgastraum zu härten.

Wir müssen uns dabei allerdings die Frage stellen, inwieweit die Störungen durch Kurzwellensender höherer Leistung mit denen eines Mobiltelefons verglichen werden können.

Der pragmatische Ansatz ist, vor dem Einbau einer Funkanlage den Fahrzeughersteller zu befragen. Zumindest einige der Hersteller zeigen sich inzwischen sehr kooperativ und haben Einbauvorschriften veröffentlicht, denen man entnehmen kann, wo Massepunkte zu liegen haben, wo Antennen montiert und die Kabel verlegt werden können und wo Versorgungsspannung entnommen werden kann.

Unter Umständen kann solch eine Anfrage bzw. die Antwort des Herstellers darauf auch kaufentscheidend sein.

Direkte Eingriffe in die CAN-Busse sollten meiner persönlichen Meinung nach nicht erfolgen, selbst wenn der Hersteller Stein und Bein schwört, dass dabei „eigentlich gar nichts passieren kann“!

Dieser Beitrag war gedacht den Hintergrund ein wenig näher zu bringen.

Bleiben wir also gespannt wie sich die Verträglichkeit zwischen elektronischer Kommunikation und automobiler Zukunft weiterentwickelt.

Abkürzungen und Begriffe

ACK	Acknowledge; Hier: Bestätigungs-Bit
ADC	Analog Digital Converter; Analog Digital Wandler
CAN	Car Area Network
CRC	Cyclic Redundancy Code; Prüfinformation, die Fehler in einem Datensatz erkennen hilft
DAC	Digital Analog Converter; Digital Analog Wandler
EIB	Elektro Installations Bus
EMC	electromagnetic compatibility (->EMV)
EMP	Elektromagnetischer Puls
EMV	Elektromagnetische Verträglichkeit (->EMC)
ID	Identification (number)
IP	Internet Protocol
ISO	International Standardization Organization
KBA	Kraftfahrt-Bundesamt
MAC	Media Access Code
MIL STD	Military Standard
NEMP	Nuclear electromagnetic pulse
OBD	On-Board Diagnostic
PEP	Peak Envelop Power; Leistungsangabe: Hüllkurven-Spitzenleistung
PGN	Parameter Group Number; J.1939-Bezeichnung für eine Zusammenstellung von SPN
PID	Parameter Identification (code)
QRV	Internationale Q-Gruppe: „Ich bin sende- und empfangsbereit!“
SAE	Society of Automotive Engineers
SPN	Suspect Parameter Number; synonym für die Nummer eines bestimmten Parameters
SSB	Single Side Band; Einseitenband (-Aussendung)
TCP	Transfer Control Protocol
VW	Volkswagen

Quellen

[J1939] SAE J.1939-71, Copyright © 2008 SAE International

[DMK] Waalkes, Otto; „Der menschliche Körper“; z.B. in “Das vierte Programm”; 4/1976

Internet:

- http://www.motor-talk.de/forum
- http://en.wikipedia.org/wiki/OBD-II_PIDs
- http://hackingvolvo.blogspot.de/2012/11/our-mysterious-friend-can-bus.html
- http://www.obd-2.de/carcode/tech_conn.html
- http://marco.guardigli.it/2010/10/hacking-your-car.html