Digitale Bus-Systeme in Kraftfahrzeugen

Funktion und Störbarkeit durch Funksender

Dipl.-Ing. Erich H. Franke, DK6II
erich.franke@afusoft.com

58. Weinheimer UKW-Tagung 2013

Hardware

- CAN-Bus
  - Abgeschlossener Zwei-Draht-Bus
  - Heute mehr oder minder gut standardisiert

- K-Line
  - Serielles, bidirektionelles Ein-Draht-Interface
  - Initialisierung: Line-Break oder 5 Baud (!)
  - Betrieb meist bei 10,5 kBit/s
  - Eher Veraltet

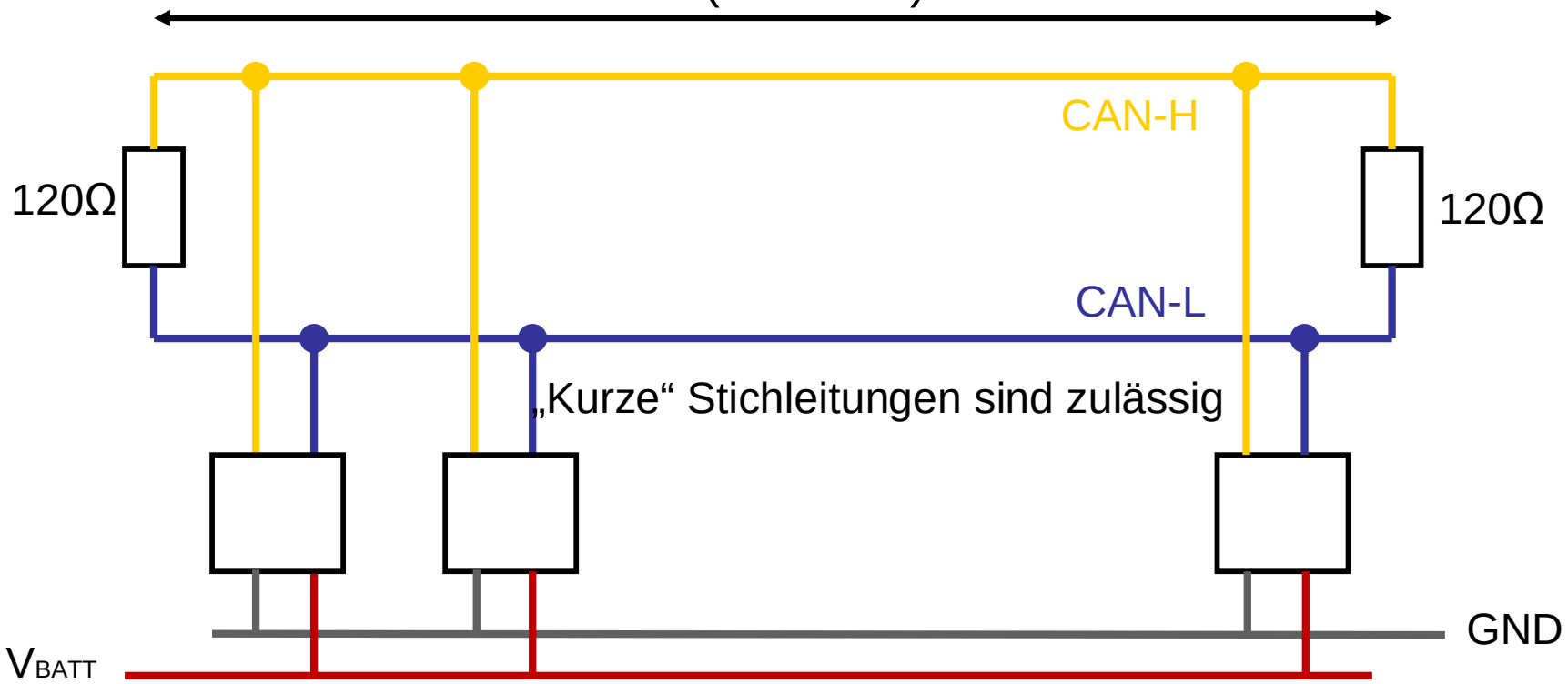
CAN Basics

- 120 Ohm terminierter Zweidrahtbus, 5V
- Fehlererkennung durch CRC
- Bitraten
  - Low Speed (LS) bis 125 kBit/s, Medium Speed (MS) bis 250 kBit/s
  - High Speed (HS) 500 kBit/s .. 1 MBit/s
- Jede „Botschaft" besitzt eine ID
  - CAN 2.0A: 11 Bit ID , CAN 2.0B: 29 Bit ID
- Eine „rohe" Botschaft trägt bis zu acht Datenbyte

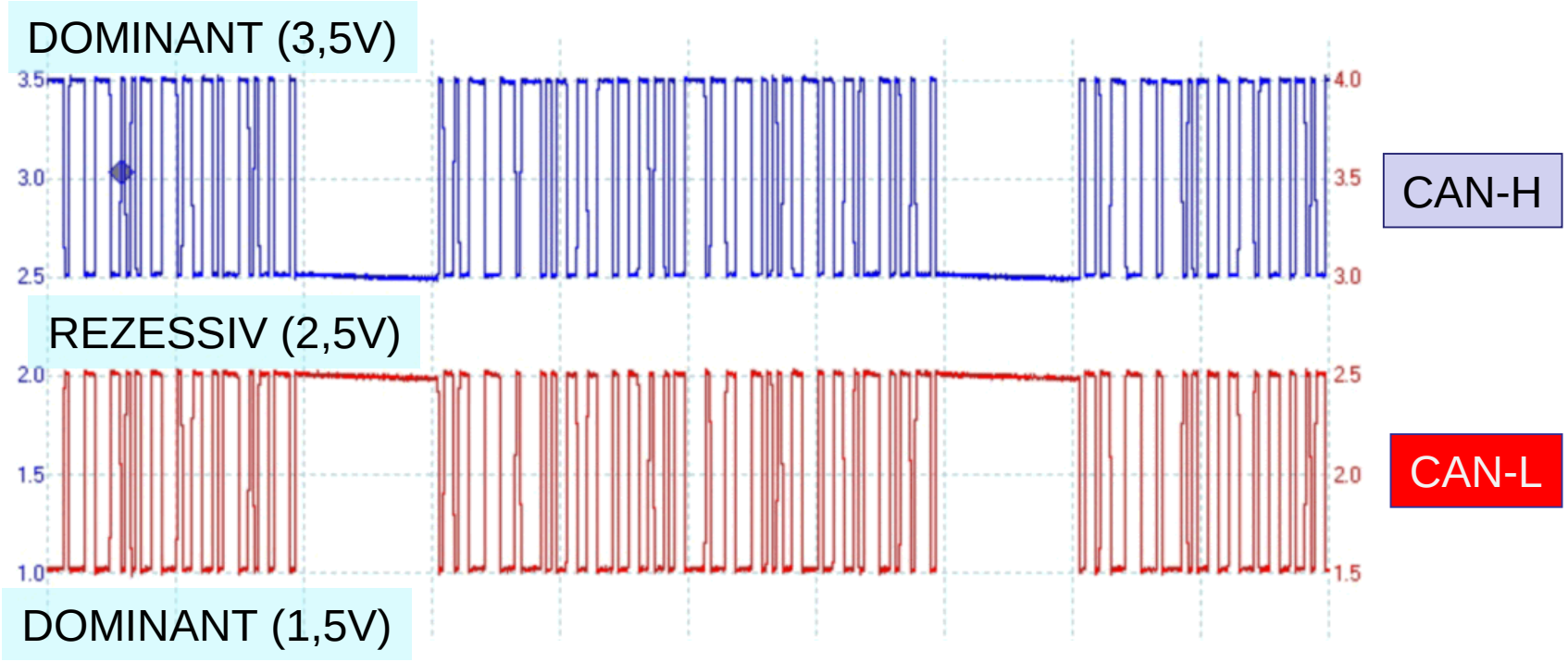
CAN Basics

Der Bus ist terminiert.
Die Leitungen sind manchmal verdrillt

LS CAN (<125kBit/s) : 500m
MS CAN (<250kBit/s) : 100m
HS CAN (<1MBit/s) : 40m



CAN Basics



Die Ansteuerung erfolgt gegenphasig.
Zweck ist die Störungsunterdrückung.

	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

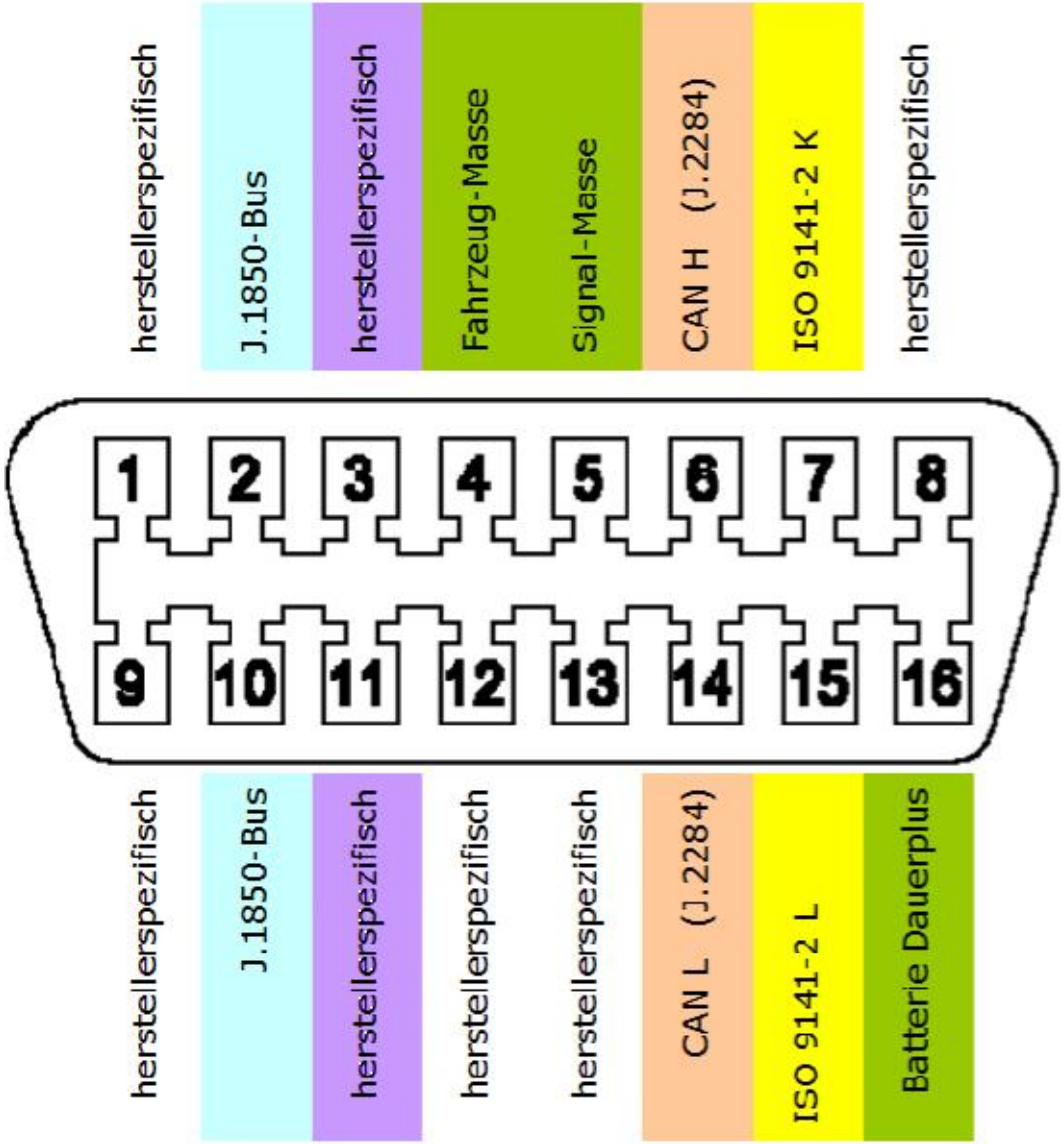
11-Bit-ID: Anzahl Bit pro Rahmen: 47..111

	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

Diagnosebuchse im Fahrzeug (J.1962)



CAN-Bus = Rückenmark?

- Alle Teilnehmer hören auf dem CAN-Bus passiv mit.

- Jede ID sollte eindeutig einem Sender zugeordnet sein.

- Was auch immer man tut:
  Es wirkt sich sofort auf die Bordsysteme aus.

CAN-Bus = Rückenmark?

- Ein CRC ist kein Allheilmittel!
- Es ist nicht ausgeschlossen, dass hochfrequente Einstreuungen zu Imitationen führen!
- Es besteht immer die Gefahr, dass beim Stecken und Trennen Glitches auftreten die Telegramme stören oder imitieren.
- Der CAN-Bus an der OBD-Buchse ist <u>NICHT</u> notwendigerweise durch ein Gateway geschützt.

CAN-Bus = Rückenmark?

- Der Schutz vor Fehlauslösungen erfolgt auf Applikationsebene
- Niemand garantiert, dass Hersteller Sicherheitsmaßnahmen eingebaut haben!
- Während der Fahrt dort zu manipulieren ist wahrhaftig keine gute Idee!

Protokoll-Schichten

- SAE J.1939
  - Standardisierte Identifier für Motorsteuerungen
  - Nur über CAN
- OBD („On Board Diagnosis“)
  - „weicher“ Standard
  - Früher: Häufig K-Line. Heute: Mehr und mehr CAN-Bus
  - „Eingebaute ASU“
- FMS
  - Nur CAN
  - Datenübernahme für Telematik bei LKW

CAN ist nicht CAN

Beispiel: CAN 2.0A: 11-Bit ID:

(0x000 .. 0x7FF)

```
 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
0310    00 00 00 00 FF 00 00 36
```

- Jede ID muss gemäß Standard eindeutig einem Sender am Bus zugeordnet sein.
- Verletzen wir diese Regel, gibt es Probleme bei der Arbitrierung!

CAN ist nicht CAN

Beispiel: CAN 2.0B: 29-Bit ID:
(0x00000000.. 0x1FFFFFFF)

```
   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
```

- Es existieren Protokolle, die auf dem „Raw CAN“ aufsetzen:
  - z.B. CANOpen, SAE J.1939, CAN-OBD
  - Derivate wie z.B. CANOpen-Lift

Documented CAN

In SAE J.1939 sind die Dateninhalte recht gut dokumentiert.
Setzt auf 29-Bit-ID mit acht Datenbyte auf. Ggf. durch 0xFF aufgefüllt.

Die ID enthält die „Parameter Group Number“ (**PGN**)

```
18F00400 F1 B2 B2 08 43 03 FF FA
-------- -- -- -- -- -- -- -- --
 |      |  |  |  |  |  |  |  |
Prio  Adr |  |  |  |  |  |  |  +---  899: Engine Torque Mode
          |  |  |  |  |  |  +------ 1675: Engine starter mode
          |  |  |  |  |  +--- 1483: Source address of the control
          |  |  |  |  |             device for the engine torque
          |  |  |  +--+------  190: Motordrehzahl
          |  |  +--- 513: Drehmoment bezogen auf Md_max
          |  +------ 512: Drehmomentsollwert bezogen auf Md_max
          +--------- 899: Engine Torque Mode
```

In den Daten sind Messwerte („Parameter“, **SPN**) enthalten

Semi-Documented CAN

- Die „On-Board-Diagnosis“ (OBD-2) definiert Nutzdaten über die so genannte „Parameter ID“ (PID)

- Abfrage erfolgt über ein Query-Response-Protokoll – Also immer aktiv!

- Aber:
  - Nur ein Teil der PID ist definiert. Viele PID sind herstellerabhängig und undokumentiert.

OBD Query

Beispiel: Abfrage der Kühlertemperatur

```
ID          Daten
---  ------------------------
7DF  02 01 05 55 55 55 55 55
      |  |  |  |  |  |  |  |
      |  |  |  +--+--+--+--+--- Padding (0x55)
      |  |  +---- PID 05 = Engine Coolant Temperature
      |  +------- Mode 01: Current Data
      +---------- 2 Parameter Bytes are Following
```

- OBD-2 definiert 0x7DF als gemeinsamer 11-Bit-Identifier für alle Abfragen.
- Nicht 100% standardisiert

OBD Response

Beispiel: Meldung der Kühlertemperatur

```
ID          Daten
---  -----------------------
7E8  03 41 05 82 55 55 55 55
      |  |  |  |  |  |  |  |
      |  |  |  |  +--+--+--+--- Padding (0x55)
      |  |  |  +- Value: 0x82=130 -> 130-40=90°C
      |  |  +---- PID 05 = Engine coolant temperature
      |  +------- Mode+0x40: 41: Current Data
      +---------- 3 Parameter Byte following
```

- OBD-2 definiert 0x7e8 als gemeinsamer 11-Bit-Identifier für die abgefragten Werte.
- Dieser Identifier kann aber auch andere Werte annehmen, die mit der Adresse des Fahrzeug-Steuergerätes variieren…

Documented OBD

- OBD soll als „Eingebaute ASU“ dienen: Das Fahrzeug sagt dem TÜV: „Mir geht es gut…“
  - Long/Short Term Fuel Trim (06..09)
  - Div. „Pollution related“ Messwerte: Lamda-Sonde / Oxygen Sensor / Cat. Purge (13..3F)
  - „Distance Travelled with malfunction indicator on“ (21)
  - Diverse Momentanwerte (Ladedruck, Temperatur, Drehzahl, Spannung, Pedalstellung)

Undocumented OBD

- Mit OBD sollte man *eigentlich* nichts kaputt machen können… …aber:
  - Betrieb während der Fahrt unzulässig da potentiell gefährlich!

- Fahrzeughersteller können eigene PID implementieren:
  - Nur ein paar Dutzend PID sind im Standard definiert. Der Rest ist herstellerabhängig.
  - Es ist durchaus möglich, dass beim Stochern in PIDs Unerfreuliches geschieht.

Even More Undocumented CAN

- In PKW werden oft proprietäre „rohe“ CAN-Parameter benutzt.
  - CAN-ID verändern sich u.U. sogar innerhalb einer Fahrzeugfamilie
  - Bitraten inzwischen 250kBit/s und 500kBit/s (Tendenz steigend)
  - Verschiedene CAN-Busse
  - CAN-Botschaften können durchaus in das Fahrverhalten eingreifen…
    z.B. 4C-Fahrwerk, Power-Steering

Exploring CAN

- Wo ist der CAN-Bus zu finden?
  - OBD-Stecker (Pin 6/14), ggf. (3/12)
  - Kabelanschluss
    (nicht genormt, nicht empfohlen…)
    - z.B. manche VW:
      - Orange/Violett: Infotainment Bus
      - Orange/Grün: Komfortsysteme
      - Orange/Schwarz: Motor/Fahrwerk ☹
- Welche Bitrate?
- Welche ID-Länge?

Exploring CAN

Und nun der harte Teil: Beobachten…

Beispiel: S80 Steering Wheele Module (250kBit/s, Comfort-Bus)

(nach Olaf, http://hackingvolvo.blogspot.de/2012/11/poking-bits.html)

```
ID          Daten
---   -----------------------
466   C0 00 00 01 1F 40 40 7F
       |  |  |  |  |  |  |  |
       |  |  |  |  |  |  |  +- Audio-Buttons
       |  |  |  |  |  |  +---- immer 0x40 (???)
       |  |  |  |  +--+------- Cruise control buttons
       |  |  |  +-------------- Rolling counter on change (0..7)
       |  +--+----------------- Immer Null (???)
       +----------------------- Rolling cntr on msg (00, 40, 80, C0)
```

Exploring CAN

Olafs Erkenntnisse auf seinem VOLVO.

Bei meinem ist es ein ganz klein Wenig anders… ☺

Byte 5 und 6: Cruise Control Buttons:

```
1f 40    nothing pressed
1e 41    cruise main button
0f 50    0/zero
17 48    reload/return to previously set speed
1d 42    + speed
1b 44    - speed
```

Byte 8: Audio Buttons

```
7f       nothing pressed
77       volume up
7b       volume down
7d       forward
7e       backward
```

Quellen

- 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

Vy 73

Bis zum nächsten Mal

Erich H. Franke

DK6II

erich.franke@afusoft.com