KWB RS-485 Interface

Protokollanalyse

Stand 15.01.2017

Dirk Abel (dirk.abel@live.de)

nach intensiver Vorarbeit von:

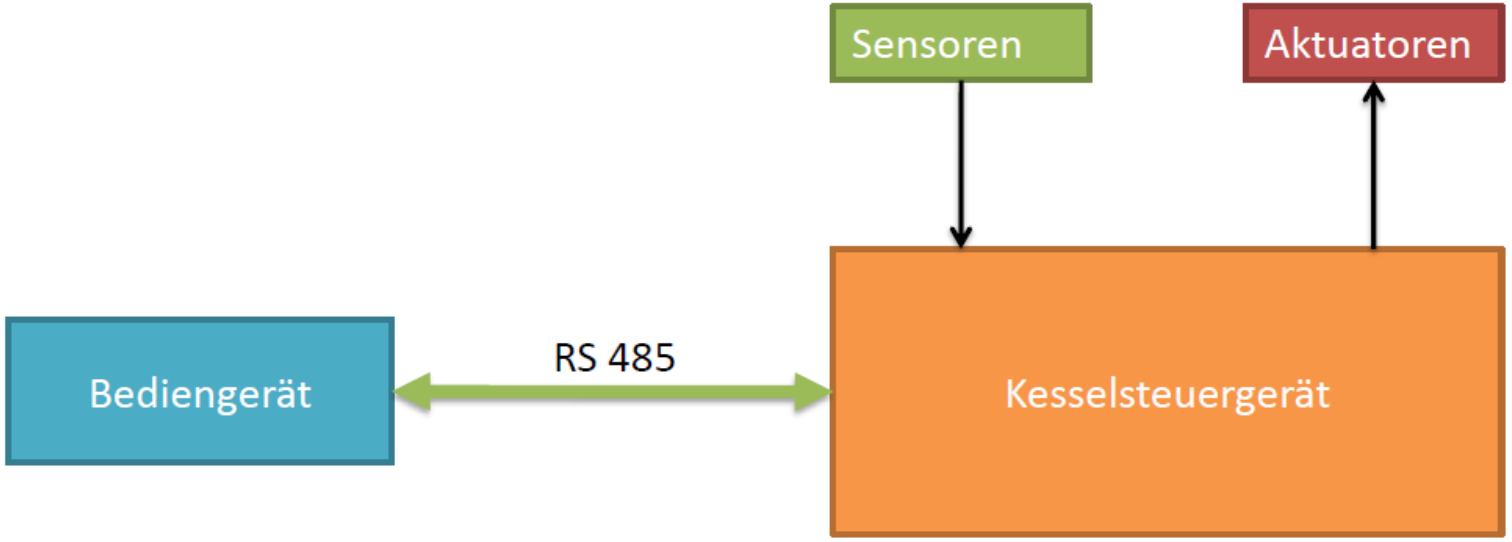
- Thomas T. (thomas_t33) (hat die Protokollanalyse initiiert und dieses Dokument ursprünglich erstellt)
- Martin Leitner (martinleitner75) für die CRC Berechnung
- Markus Heberling (markus_h62) und haros (Gast) für das Phyton Skript, das mir bei der Analyse der fehlenden Parameter sehr geholfen hat
- vielen anderen, siehe: https://www.mikrocontroller.net/topic/274137

Physikalische Parameter

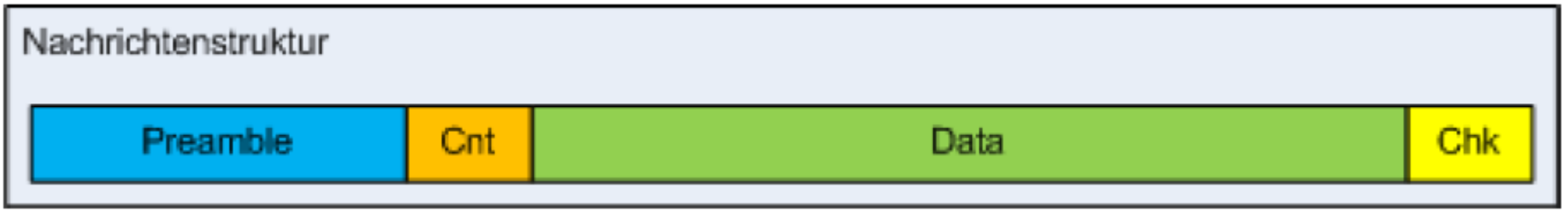
- RS-485
- Baudrate: 19200
- Databits: 8
- Parity: None
- Stopbits: 1

Topologie

- Das Kesselsteuergerät ist „dumm“. Es nimmt als I/O-Modul die Sensoren auf und steuert die Aktoren an.
- Das Bediengerät ist intelligent und steuert den kompletten Ablauf.
- Das Bediengerät empfängt vom Kesselsteuergerät die Werte der Sensoren (Temperaturen, Zustände)
- Über das Bediengerät werden die Aktuatoren (Pumpen, Mischer, Klappen, etc.) direkt gesteuert.



Protokoll



- Preamble: Die Nachrichten beginnen immer mit einer eindeutigen Bytefolge
- Cnt: Danach folgt ein Byte das von 64 bis 127 in Schritten von +1 durchzählt
- Data: Die eigentlichen Nutzdaten, variable Länge möglich, da Werte identisch mit der Preamble durch Hinzufügen von Bytes verhindert werden müssen
- Chk: Prüfsumme

Nachrichtentypen

Bisher wurden 2 Nachrichtentypen identifiziert

- CtrlMsg vom Bediengerät an das Kesselsteuergerät: beinhaltet Steuerkommandos
- SenseMsg vom Kesselsteuergerät an das Bediengerät: beinhaltet Sensorinformationen

Eine Nachricht beginnt immer mit dem Wert „2“. Kommt eine „2“ innerhalb einer Nachricht vor, so wird sie durch eine folgende „0“ als Header „entwertet“. Diese „0“ wird im Datenpaket ignoriert, sie ist nicht Bestandteil der Nachricht.

CtrlMsg

		LSB	Bit						MSB
		0	1	2	3	4	5	6	7
Byte	1	2 (Header)							
	2	16 (Länge der Nachricht)							
	3	17 (ID der Nachricht)							
	4	Zähler: 64-127 in +1 Inkrementen							
	5								
	6	Zündung	Brandschutzklappe	Alarm 2	Alarm 1	Leistung	Boiler 0 Pumpe	HK2 Pumpe	HK1 Pumpe
	7	Ascheaustragung	Reinigung	Rücklaufmischer ein	Rücklaufmischer zu	HK2 Mischer ein	HK2 Mischer zu	HK1 Mischer ein	HK1 Mischer zu
	8					Hauptreials	Raumaustragung		
	9	Rücklaufpumpe 0-100% = 0-255							
	10	Gebläsestufe 0-50 = 0-255							
	11	Saugzugstufe 0-50 = 0-255							
	12	Stokerantrieb ein 0 => 3							
	13	Stokerantrieb ein 0 => 232							
	14	Stokerantrieb ein 0 => 3							
	15	Stokerantrieb ein 0 => 232							
	16	Prüfsumme							

SenseMsg

		LSB			Bit				MSB
		0	1	2	3	4	5	6	7
Byte	1	2 (Header)							
	2	2 (Header)							
	3	51 (Länge der Nachricht)							
	4	16 (ID der Nachricht)							
	5	Zähler: 64-127 in +1 Inkrementen							
	6								
	7								
	8								
	9		Klixon Raumaustragung	Füllstandssensor	Klixon Stoker	Endschalter BS Klappe	Türkontakt	Extern 2	Extern 1
	10	Sicherheitsthermostat	RFK Taste	TÜB Stoker					
	11	HK1 Vorlauf Temperatur							
	12								
	13	Rücklauf Temperatur							
	14								
	15	Boiler 0 Temperatur							
	16								
	17	KesselTemperatur							
	18								
	19	Puffer 2 (unten) Temperatur							
	20								
	21	Puffer 1 (oben) Temperatur							

	22	
	23	Außen Temperatur
	24	
	25	Rauchgas Temperatur
	26	
	27	Kesselsteuergerät Temperatur
	28	
	29	HK1 Fernverstellung Temperatur
	30	
	31	HK2 Fernverstellung Temperatur
	32	
	33	HK2 Vorlauf Temperatur
	34	
	35	keine Ahnung! Bei mir immer zwischen 68.0-70.0 (ganze Schritte)
	36	
	37	keine Ahnung! Bei mir immer zwischen 28.0-29.0 (ganze Schritte)
	38	
	39	immer 130.0 - vermutlich Temp-Sensor auf Steckmodul 1
	40	
	41	immer 130.0 - vermutlich Temp-Sensor auf Steckmodul 1
	42	
	43	immer 130.0 - vermutlich Temp-Sensor auf Steckmodul 1
	44	
	45	immer 50.0 wie Frrnversteller HK1&2 - höchstwahrscheinlich Fernverst. HK0 auf Steckmodul 1
	46	
	47	
	48	
	49	
	50	
	51	Prüfsumme

- Der Datenbereich beginnt ab dem 6.Byte
- Der Datenbereich unterteilt sich in mehrere Bereiche
- Die ersten 5 Bytes im Datenbereich beinhalten einige Sensor-/Schalter-/Kontaktzustände, danach folgen 18 Temperaturwerte, gefolgt von weiteren 4 Bytes unbekannter Bedeutung
- Die Temperaturwerte werden als 16bit „signed integer“ übertragen und beinhalten eine Nachkommastelle. Der Wert muss daher durch zehn geteilt werden.

```
Temperatur = (signed short)( data[n] * 256 + data[n+1] ) // in Zehntel Grad
```

Aufschlüsselung nach Anschlüssen des Kesselsteuergerätes

Klemme	Name	friendly Name	Typ	Python Skript
1	Zündung	Zündung Pellets	Relais	
1	Luftgebläse	Luftgebläse	Phasenanschnitt	Control Byte 5 Stufe 50=255
1	Brandschutzklappe	Brandschutzklappe	Relais	Control Byte 1 Bit 1
1	Stoker	Stoker	Relais	Control Byte 7:0->3|8:0->232|9:0->3|10:0->232
2	Raumaustragung	Raumaustragung Knickschnecke	Reais	Control Byte 3 Bit 6
3	Wärmetauscherreinigung	Wärmetauscherreinigung	Relais	Control Byte 3 Bit 4
4	Saugzuggebläse	Saugzuggebläse	Phasenanschnitt	Control Byte 6 Stufe 50=255
5	Relais VB-Trafo	Ascheaustragung	Relais	Control Byte 2 Bit 0
6	Sicherheitsthermostat	Sicherheitsthermostat	Sensor Kontakt	Sense Byte 4 Bit 0
7	Leistung	Leistungsanforderung Zusatzkessel	Relais	Control Byte 1 Bit 4
7	Störung 1	Störung 1	Relais	Control Byte 1 Bit 3 (invertiert - normal angezogen)
7	Störung 2	Störung 2	Relais	Control Byte 1 Bit 2
8	Boilerpupe	Boilerpupe	Relais	Control Byte 1 Bit 5
9	HK-Mischer 2 zu	über zwei Relais gesteuert, das erste schaltet die	Relais	Control Byte 2 Bit 4 (Freigabe) Bit5=1 (zu)
9	HK-Mischer 2 auf	Spannung auf das 2. Diese steuert "auf" oder "zu"	Relais	Control Byte 2 Bit 4 (Freigabe) Bit5=0 (auf)
10	HK-Pumpe 2	HK-Pumpe 2	Relais	Control Byte 1 Bit 6
11	HK-Mischer 1 zu	über zwei Relais gesteuert, das erste schaltet die	Relais	Control Byte 2 Bit 6 (Freigabe) Bit7=1 (zu)
11	HK-Mischer 1 auf	Spannung auf das 2. Diese steuert "auf" oder "zu"	Relais	Control Byte 2 Bit 6 (Freigabe) Bit7=0 (auf)
12	HK-Pumpe 1	HK-Pumpe 1	Relais	Control Byte 1 Bit 7
13	Klixon Raumaustragung	Temperaturüberwachung Zuführschneckenmotor	Sensor Kontakt	Sense Byte 3 Bit1

14	RL-Mischer zu	über zwei Relais gesteuert, das erste schaltet die	Relais	Control Byte 2 Bit 2 (Freigabe) Bit3=1 (zu)
14	RL-Mischer auf	Spannung auf das 2. Diese steuert "auf" oder "zu"	Relais	Control Byte 2 Bit 2 (Freigabe) Bit3=0 (auf)
15	Kessl Bypass Pumpe	Rücklaufanhebung über Pumpe	Phasenanschnitt	Control Byte 4 Stufe 50=255
16	Verorgungsspannung		-	
17	Türkontaktschalter	Türkontakt Asche? (bei mir gebrückt)	Sensor Kontakt	Sense Byte 3 Bit 5
18	Klixon Stoker	Temperaturüberwachung Stoker Motor	Sensor Kontakt	Sense Byte 3 Bit 3
19	Endschalter BS-Klappe	Endschalter Brandschutzklappe Stoker	Sensor Kontakt	Sense Byte 3 Bit 4
20	Temperaturüberwachug Stoker	Rückbranderkennung Stokerkanal	Sensor Kontakt	Sense Byte 4 Bit 2
21	Extern 2	Fernanforderung	Sensor Kontakt	Sense Byte 3 Bit 6
22	Extern 1	Fernabschaltung, z.B. Temperaturüberwachung	Sensor Kontakt	Sense Byte 3 Bit 7
23	Füllstandssensor	Pellets im Stokerkanal	Sensor Kontakt	Sense Byte 3 Bit2
24	RFK-Taste	Rauchfangkehrer-Taste (Volllast)	Sensor Kontakt	Sense Byte 4 Bit 1
25	RS485 Anschluss extern		-	
26	RS485 Anschluss Kesselbediengerät		-	
27	Fernverstellung HK1	Analoges Raumbediengerät HK1	Sensor	Sense Byte 23+24
28	VL-Fühler HK1	HK1 Vorlauf Tempratur	Sensor	Sense Byte 5+6
29	Boilerfühler	Warmwasserboiler Temperatur	Sensor	Sense Byte 9+10
30	Pufferfühler 1	Pufferfühler oben	Sensor	Sense Byte 15+16
31	Fernverstellung HK2	Analoges Raumbediengerät HK2	Sensor	Sense Byte 25+26
32	VL-Fühler HK2	HK2 Vorlauf Tempratur	Sensor	Sense Byte 27+28
33	RL-Fühler	Rücklauftemperatur	Sensor	Sense Byte 7+8
34	Pufferfühler 2	Pufferfühler unten	Sensor	Sense Byte 13+14
35	Außenfühler	Außenfühler	Sensor	Sense Byte 17+18
36	nicht bestückt	-	-	-
37	nicht bestückt	-	-	-
38	Kesselfühler	Kesselwassertemperatur	Sensor	Sense Byte 11+12
39	Rauchgasfühler	Rauchgastemperatur	Sensor	Sense Byte 19+20

-	Temperatur Steuerung	Temperatur Steuerung im Kessel	Sensor	Sense Byte 21+22
-	Hauptrelais	Hauptrelais	Control	Control Byte 3 Bit 4
	Saugturbine	habe ich nicht	Control?	keine Änderung
	Filterreinigung	habe ich nicht	Control?	keine Änderung

CRC Berechnung

Die CRC Berechnung gelingt im Großteil der Fälle, mit einer Ausnahme, wenn die CRC 253 ist, wird eine CRC von 2 berechnet. Ich vermute, dass ist bewusst so „hingelogen“ von KWB, damit nicht noch eine weiter „2“ im Protokoll vorhanden ist. Die invertieren die CRC in diesem Fall einfach.

```
int Checksum(unsigned char* data, unsigned char length)
{
    int i;
    unsigned char crc = 0;

  crc = data[0];    // = 0x02
  for (i = 1; i < length; i++)
  {
    crc = rotl(crc, 1);
    if (crc + data[i] > 255)
    {
      crc = crc + data[i] + 1;
    }
    else
      crc = crc + data[i];

  }
  return crc;
}
```

Python Script

Hier die Protokolldaten für das Python Skript von Markus Heberling (markus_h62) und haros (Gast)

```
aaSignalMaps[16] = {
    #Name: Type='b'(bit), Offset, Bit
    #Name: Type='s'(signed)/'u'(unsigned), Offset, Length, Factor, Unit
    'Klixon Raumaustr.'    : ('b',3,1),
    'Füllstandssensor'     : ('b',3,2),
    'Klixon Stoker'        : ('b',3,3),
    'Endsch. BS Klappe'    : ('b',3,4),
    'Türkontakt'           : ('b',3,5),
    'Extern 2'             : ('b',3,6),
    'Extern 1'             : ('b',3,7),
    'Sicherheitsthermos.'  : ('b',4,0),
    'RFK Taste'            : ('b',4,1),
    'TÜB Stoker'           : ('b',4,2),
    'T_Vorlauf_HK1'        : ('s', 5, 2, 0.1,'°C'),
    'T_Rücklauf_Kessel'    : ('s', 7, 2, 0.1,'°C'),
    'T_Boiler'             : ('s', 9, 2, 0.1,'°C'),
    'T_Kessel'             : ('s',11, 2, 0.1,'°C'),
    'T_Puffer 2 (unten)'   : ('s',13, 2, 0.1,'°C'),
    'T_Puffer 1 (oben)'    : ('s',15, 2, 0.1,'°C'),
    'T_Aussen'             : ('s',17, 2, 0.1,'°C'),
    'T_Rauchgas'           : ('s',19, 2, 0.1,'°C'),
    'T_Steuerung'          : ('s',21, 2, 0.1,'°C'),
    'T_Fernverst. HK1'     : ('s',23, 2, 0.1,'°C'),
    'T_Fernverst. HK2'     : ('s',25, 2, 0.1,'°C'),
    'T_Vorlauf_HK2'        : ('s',27, 2, 0.1,'°C'),
    #'irgendwas internes 1' : ('s',29, 2, 1,'?'), # 68.0-70.0 ganzzahlige Schritte
    #'irgendwas internes 2' : ('s',31, 2, 1,'?'), # 28.0-29.0 ganzzahlige Schritte
    #'T_Steckmodul 1'       : ('s',33, 2, 1,'?'), # immer 130.0 - vermutlich Temp-Sensor auf Steckmodul 1
    #'T_Steckmodul 1'       : ('s',35, 2, 1,'?'), # immer 130.0 - vermutlich Temp-Sensor auf Steckmodul 1
    #'T_Steckmodul 1'       : ('s',37, 2, 1,'?'), # immer 130.0 - vermutlich Temp-Sensor auf Steckmodul 1
    #'T_Fernverst. HK0'     : ('s',39, 2, 1,'?')} # immer 50.0 wie Frnversteller HK1&2 - vermutlich Fernverst. HK0
    }
```

```
aaSignalMaps[17] = {

    #Name: Type='b'(bit), Offset, Bit
    #Name: Type='s'(signed)/'u'(unsigned), Offset, Length, Factor, Unit
    'Byte 1 Bit 0'           : ('b',1,0),
    'Brandschutzklappe'      : ('b',1,1),
    'Alarm 2'                : ('b',1,2),
    'Alarm 1'                : ('b',1,3),
    'Leistungsausgang'       : ('b',1,4),
    'Pumpe_Boiler'           : ('b',1,5),
    'Pumpe_HK2'              : ('b',1,6),
    'Pumpe_HK1'              : ('b',1,7),
    'Ascheaustragung'        : ('b',2,0),
    'Reinigung'              : ('b',2,1),
    'RL_Mischer ein'         : ('b',2,2),
    'RL_Mischer 0-auf|1-zu'  : ('b',2,3),
    'HK2_Mischer ein'        : ('b',2,4),
    'HK2_Mischer 0-auf|1-zu' : ('b',2,5),
    'HK1_Mischer ein'        : ('b',2,6),
    'HK1_Mischer 0-auf|1-zu' : ('b',2,7),
    'Zündung'                : ('b',3,0),
    #'Byte 3 Bit 1'           : ('b',3,1),
    #'Byte 3 Bit 2'           : ('b',3,2),
    #'Byte 3 Bit 3'           : ('b',3,3),
    'Hauptrelais'            : ('b',3,4),
    #'Byte 3 Bit 5'           : ('b',3,5),
    'Raumaustragung'         : ('b',3,6),
    #'Byte 3 Bit 7'           : ('b',3,7),
    'Rücklaufpumpe'          : ('u',4,1,0.3921,'%'),
    'Gebläsestufe'           : ('u',5,1,0.1960,'Stufe'),
    'Saugzugstufe'           : ('u',6,1,0.1960,'Stufe')}
```