

Vaillant X6 Schnittstelle

Auf der mit X6 beschrifteten Buchse liegt ein RS232-Signal mit TTL-Pegeln an. Die Geräte kommunizieren mit 9600 Baud (8N1, keine Flusskontrolle). Normalerweise wird über diese Buchse ein PC angeschlossen, auf dem das Programm vrDIALOG ausgeführt wird, oder ein Kommunikationsmodul für das vrNetDIALOG-System.

Eine Beta-Version des Programms vrDIALOG findet man mit Google (<http://www.google.de/#q=vrDIALOG+site%3Awww.vaillant.pl>) (Stand 10.01.11). Die Kommunikation des Programms mit dem Heizgerät lässt sich mit entsprechenden Tools beobachten.

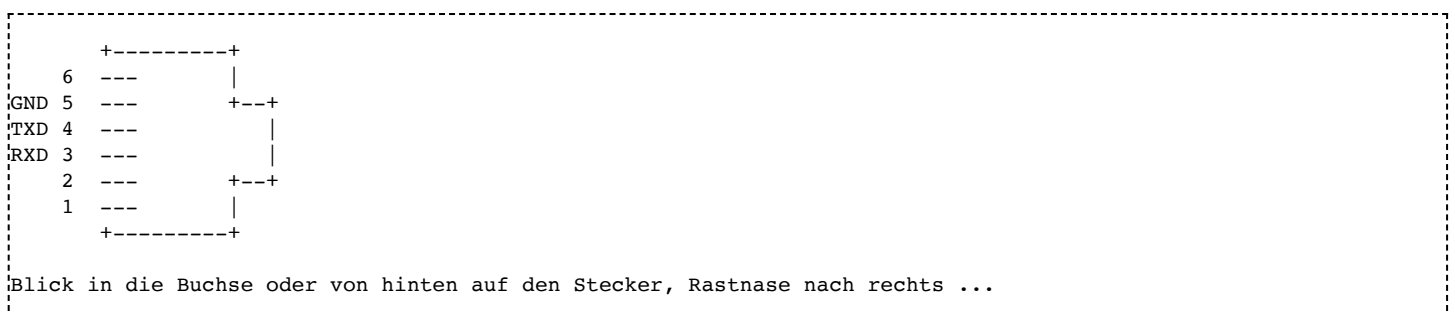
Solange es kein spezielles Modul für das Ethersex-System gibt, kann YPort verwendet werden. Das Heizgerät kann dann von eigener Software aus oder mit Hilfe eines gemappten COM-Ports auch von vrDIALOG aus angesprochen werden.

Alle Informationen ohne Gewähr. Durch Kommunikation über die X6-Schnittstelle kann man die Konfiguration des Geräts ändern. Dadurch ist ein sicherer und gefahrloser Betrieb möglicherweise nicht mehr gegeben. Es kann zu Sach- und Personenschäden kommen. Die Verwendung aller Informationen erfolgt auf eigene Gefahr!

Inhaltsverzeichnis

- 1 Belegung
- 2 Protokoll
 - 2.1 Aufbau der Nachrichten
 - 2.2 Prüfsumme
 - 2.3 Befehle
 - 2.3.1 Liste der Befehle
 - 2.3.2 Andere Befehle
 - 2.3.2.1 07 02 00 00 00 04 C4
 - 2.4 Antworten des Geräts
 - 2.4.1 Normale Antworten
 - 2.4.2 Andere Antworten
 - 2.5 Kodierung von Werten
 - 2.5.1 Temperaturen
 - 2.5.2 Sensorstatus
 - 2.5.3 Schaltzustand
- 3 Links

Belegung



Protokoll

Die Kommunikation scheint immer vom angeschlossenen PC (oder Ethersex?) auszugehen. Die Nachrichten in beide Richtungen haben ein ähnliches Format:

Es gibt kein Zeilenende wie CR oder CR+LF.

Aufbau der Nachrichten

Alle Nachrichten haben ein gemeinsames Format:

Bytes	1	2	3 ... n-1	n
	+	+	+	+
	Len	?	Data	Chk
	+	+	+	+
Byte 1	Gesamtlänge der Nachricht ("n" Bytes, Längenbyte, Nachrichtentyp und Prüfsumme sind dabei mitgezählt)			
Byte 2	Sowas wie ein Nachrichtentyp: 0x00 Normale Nachrichten 0x01 Fehlermeldung Checksum-Fehler? 0x02 ? - Verwendet bei der Abfrage der Version des Heizgeräts 0x03 Fehlermeldung? 0x0a ? - Verwendet bei der Abfrage der Version des Reglers 0x80 Änderung von Parametern			
Byte 3	Daten, beinhalten die eigentliche Anforderung an das Gerät, die angeforderten			
... n-1	Werte, oder sonstige Informationen.			
Byte n	Prüfsumme			

Prüfsumme

Zur Berechnung der Checksum werden die Bytes nacheinander XOR-verknüpft und das Zwischenergebnis dann jeweils um 1 bit nach links verschoben:

```
sub checksum
{
my $string = $_[0];
my $checksum;

for (my $i = 0; $i < length($string); $i++)
{
if ($checksum & 0x80)
{
$checksum = ($checksum << 1 | 1) & 0xFF;
# ???
$checksum = $checksum ^ 0x18;
}
else
{
$checksum = $checksum << 1;
}
$checksum = $checksum ^ ord(substr($string, $i, 1));
}
return $checksum;
}
```

Den Quelltext darf gerne mal jemand in C konvertieren ;-) ...

Beim Finden des Algorithmus waren kurze Nachrichten wie 03 03 05 und 03 01 07 nützlich. Es fiel dann aber auf, dass die Berechnung immer dann zu einem anderen Ergebnis führt, wenn das Zwischenergebnis im Verlauf der Berechnung größer als FFh (127) wird. In der Nachricht 07 00 00 00 98 05 cc ist dies erst beim letzten

Datenbyte der Fall. Von dort konnte man also zurückrechnen, was man am Zwischenergebnis ändern muss, um letztendlich auf die gleiche Prüfsumme zu kommen wie das Gerät. Diese Änderung ist genau ein XOR mit 18h. Siehe auch [1] (<http://coding.derkeiler.com/Archive/General/comp.arch.embedded/2008-06/msg00256.html>) und [2] (<http://www.gamefaqs.com/console/nes/file/563408/47175>).

Ich sehe gerade, dass sich da schon jemand anderes mit beschäftigt hat. Er kommt im Prinzip zum gleichen Ergebnis: <http://ab-log.ru/smart-house/heating-automation/vaillant-rs232> (russisch).

Befehle

Die bekannten Befehlsnachrichten sind 7 Byte lang und haben einen einheitlichen Aufbau. Dem 1 Byte langen Befehl werden zwei Null-Bytes vorangestellt, dann folgt ein Byte, das die Länge der erwarteten Daten angibt:

```
00 00 98 05
```

Der resultierende String wird nach dem oben geschilderten Aufbau von Nachrichten verpackt. Dabei ist das noch unbekannte Byte 2 ebenfalls "00h". Es ergibt sich:

```
07 00 00 00 98 05 CC
```

Was das Byte angeht, das die Datenlänge angibt, bin ich noch nicht ganz sicher. Mein Gerät scheint es nicht allzu ernst zu nehmen. Verändert man das entsprechende Byte in der Anfrage, sendet weiterhin die ursprüngliche Anzahl von Bytes und somit eine andere Zahl von Bytes als angefordert:

```
07 00 00 00 98 03 CA  
08 00 02 2A FD D5 00 37
```

Liste der Befehle

Befehl	Funktion	Datenbytes	Typ
01h	Sollwert Brauchwassertemperatur	2	Ein Analogwert (2 byte)
02h	?	2	Ein Analogwert (2 byte)
03h	Unbekannter Statuswert	1	Status (F0h/0Fh)
04h	Sollwert Speicher	2	Ein Analogwert (2 byte)
05h	Flammsignal	1	Status (F0h/0Fh)
06h	Fehlerspeicher?	28	Fehlerspeicher
07h	?	1	Status (F0h/0Fh)
08h	Sommer/Winter-Schalter	1	Status (Sommer/Winter)
09h	?	2	Ein Analogwert (2 byte)
0Ah	?	2	Ein Analogwert (2 byte)
0Bh	?	2	Ein Analogwert (2 byte)
0Ch	?	2	Ein Analogwert (2 byte)
0Dh	?	1	Status (F0h/0Fh)
0Eh	Status Raumthermostat	1	Status (00h/01h)
16h	Brauchwassersensor	3	Ein Analogwert (2 byte) + ein Sensorstatus
17h	Speichertemperatur	3	Ein Analogwert (2 byte) + ein Sensorstatus
18h	Vorlauftemperatur	3	Ein Analogwert (2 byte) + ein Sensorstatus
19h	?	2	Ein Analogwert (2 byte)
1Fh	Anzahl GFA Störungen	1	Ein Analogwert (1 byte)
20h	Anzahl STB Abschaltungen	1	Ein Analogwert (1 byte)
21h	?	1	Ein Analogwert (1 byte)
22h	?	2	Ein Analogwert (2 byte)
23h	?	2	Ein Analogwert (2 byte)
24h	Drehzahlsollwert	2	Ein Analogwert (2 byte)
25h	Sollwert Vorlauf Ext. Regler 7-8-9	2	Ein Analogwert (2 byte)
26h	?	2	Ein Analogwert (2 byte)
28h	?	2	Ein Analogwert (2 byte)
29h	?	2	Ein Analogwert (2 byte)
2Eh	?	2	Ein Analogwert (2 byte)
32h	?	2	Ein Analogwert (2 byte)
38h	Verbleibende Brennersperrzeit	1	Ein Analogwert (1 byte)
39h	Sollwert Vorlauftemperatur	2	Ein Analogwert (2 byte)
3Ah	?	2	Ein Analogwert (2 byte)
3Ch	?	1	Status (00h/01h)
3Dh	?	1	Ein Analogwert (1 byte)
3Eh	?	1	Status (00h/01h)
3Fh	Status externe Heizungspumpe	1	Status (00h/01h)
40h	?	1	Status (00h/01h)
42h	Stellung VUV	1	Status (?)

43h	?	1	Status (00h/01h)
44h	Status interne Heizungspumpe	1	Status (00h/01h)
45h	?	1	Status (00h/01h)
46h	?	1	Status (F0h/0Fh)
47h	?	1	Status (F0h/0Fh)
48h	Status Gasmagnetventil	1	Status (F0h/0Fh)
49h	Status Zünder	1	Status (F0h/0Fh)
4Bh	?	2	Ein Analogwert (2 byte)
4Ch	?	1	Ein Analogwert (1 byte)
4Dh	?	1	Status (F0h/0Fh)
4Eh	?	1	Status (F0h/0Fh)
4Fh	?	1	Status (F0h/0Fh)
50h	?	1	Status (F0h/0Fh)
51h	?	1	Status (F0h/0Fh)
53h	Status Unbekannt	1	Status (F0h/0Fh)
54h	?	1	Status (00h/01h)
55h	?	2	Ein Analogwert (2 byte)
57h	?	1	Status (00h/01h)
58h	Anforderung Warmwasser C1/C2	1	Status (00h/01h)
5Bh	?	1	Status (00h/01h)
5Ch	?	2	Ein Analogwert (2 byte)
5Dh	?	1	Status (00h/01h)
5Eh	?	1	Status (00h/01h)
5Fh	?	1	Status (00h/01h)
63h	Wasserpumpennachlaufzeit nach Speicherladung	1	Ein Analogwert (1 byte)
64h	Wasserpumpennachlaufzeit nach Heizbetrieb	1	Ein Analogwert (1 byte)
65h	Korrekturwert Aussentemperatur	1	Ein Analogwert (1 byte)
66h	Speicherladezeit	1	Ein Analogwert (1 byte)
68h	?	8	?
69h	?	1	Ein Analogwert (1 byte)
6Ah	Aussentemperatur	3	Ein Analogwert (2 byte) + ein Sensorstatus
6Bh	Ext. Vor-/Rücklauftemperatur	3	Ein Analogwert (2 byte) + ein Sensorstatus
6Ch	Heizungsteillast	1	Ein Analogwert (1 byte)
6Dh	?	1	Status (00h/01h)
6Eh	?	1	Ein Analogwert (1 byte)
6Fh	Zähler 3 Zündversuche	1	Ein Analogwert (1 byte)
70h	?	1	Status (00h/01h)
71h	Status Speicherfreigabe Schaltuhr	1	Status (00h/01h)
72h	?	1	Status (00h/01h)
73h	?	2	Ein Analogwert (2 byte)

74h	?	1	Status (00h/01h)
75h	?	1	Status (00h/01h)
76h	?	3	Ein Analogwert (2 byte) + ein Sensorstatus
77h	?	1	Status (F0h/0Fh)
7Ah	?	1	Status (00h/01h)
7Bh	?	1	Status (00h/01h)
7Ch	?	2	Ein Analogwert (2 byte)
81h	?	2	Ein Analogwert (2 byte)
82h	?	1	Status (00h/01h)
83h	Drehzahlistwert	2	Ein Analogwert (2 byte)
89h	?	1	Status (00h/01h)
8Eh	?	1	Status (00h/01h)
8Fh	?	9	?
98h	Rücklauftemperatur	5	Zwei Analogwerte (2 x 2 byte) + ein Sensorstatus
99h	?	1	Ein Analogwert (1 byte)
9Ah	Unbekannter Temperaturwert	5	Zwei Analogwerte (2 x 2 byte) + ein Sensorstatus
9Bh	?	1	Status (00h/01h)
9Dh	Offset Warmstartsollwert	1	Ein Analogwert (1 byte)
9Eh	Status Speicherladepumpe	1	Status (00h/01h)
9Fh	?	2	Ein Analogwert (2 byte)
A0h	?	1	Ein Analogwert (1 byte)
A1h	Sollwert interne Heizungspumpe	1	Status (00h/01h)
A2h	?	2	Ein Analogwert (2 byte)
A3h	?	3	Ein Analogwert (2 byte) + ein Sensorstatus
A4h	?	2	Ein Analogwert (2 byte)
A5h	Max. Vorlauftemperatur	1	Ein Analogwert (1 byte)
A6h	?	1	Ein Analogwert (1 byte)
A7h	?	1	Ein Analogwert (1 byte)
A8h	?	1	Ein Analogwert (1 byte)
A9h	Unbekannter Wert	1	Ein Analogwert (1 byte)
AAh	?	1	Status (00h/01h)
ABh	?	1	Ein Analogwert (1 byte)
ACh	?	2	Ein Analogwert (2 byte)
ADh	?	1	Status (F0h/0Fh)
AEh	?	1	Ein Analogwert (1 byte)
AFh	Status Zirkulationspumpe	1	Status (00h/01h)
B0h	?	1	Status (00h/01h)
B2h	?	1	Status (00h/01h)
B3h	Status Rücklaufregelung	1	Status (00h/01h)
B4h	?	1	Status (00h/01h)

B6h	Speichertemperatur unten	3	Ein Analogwert (2 byte) + ein Sensorstatus
B7h	Kollektortemperatur (nein!)	3	Ein Analogwert (2 byte) + ein Sensorstatus
B8h	Kollektortemperatur	3	Ein Analogwert (2 byte) + ein Sensorstatus
B9h	?	2	Ein Analogwert (2 byte)
C3h	Hyterese Solarpumpe	1	Ein Analogwert (1 byte)
CAh	?	2	Ein Analogwert (2 byte)
D4h	?	3	Ein Analogwert (2 byte) + ein Sensorstatus
D5h	?	1	Status (00h/01h)
D6h	?	1	Status (00h/01h)

Andere Befehle

Nicht alle Befehle passen in das genannte Schema.

07 02 00 00 00 04 C4

Fragt nach angeschlossenen Geräten? In meinem Fall meldet das Gerät anscheinend seine Versionsnummer, die von vrDIALOG als "0153_07.00" angezeigt wird:

```
07 02 00 00 00 04 C4
08 00 00 99 07 00 14 96
```

Bei diesem Befehl ist die Anzahl der zurückgelieferten Bytes nicht gleich dem als viertem Bytes gesendeten Wert "04". Weiterhin hat das unbekannte Byte 2 den Wert "02h".

Antworten des Geräts

Das Gerät antwortet mit Nachrichten, die den oben angegebenen Aufbau haben. Dabei das unbekannte Byte 2 anzugeben, ob es sich um eine "normale" Antwort ("00h") oder um eine andere Antwort handelt.

Normale Antworten

Bei normalen Antworten hat Byte 2 den Wert "00h". Ab Byte 3 folgenden dann die angeforderten Daten. Hierbei werden verschiedene Kodierungen verwendet. Analogwerte werden in einem oder zwei Bytes kodiert, je nach Befehl werden ein oder zwei derart kodierte Analogwerte zurückgegeben. Für Statusmeldungen scheint es verschiedene Kodierungen zu geben, die jeweils ein Byte verwenden.

Andere Antworten

Nachricht	Bedeutung
03 00 06	Bestätigung Parameteränderung
03 01 07	Checksummenfehler?
03 03 05	Nicht unterstützt, nicht vorhanden?

Kodierung von Werten

In den Antworten des Heizgeräts sind verschiedene Informationen kodiert. Vermutlich ist das Format der zurückgelieferten Daten eindeutig mit dem anfordernden Befehl verbunden.

Temperaturen

Es scheint zwei Möglichkeiten zu geben, Temperaturen zu kodieren. Sollwerte (Grenzwerte?) sind teilweise in einem Byte kodiert, während andere Sollwerte und Messwerte in zwei Bytes kodiert sind: Das zuerst gesendete Byte ist das höherwertige Byte. Der erhaltene Zahlenwert entspricht der Temperatur in $1/16^{\circ}\text{C}$. Negative Werte werden in Zweikomplement-Darstellung übertragen.

Beispiel

```
52h = 82d => 82 °C  
0230h = 560d => 560/16 °C = 35,00 °C  
FF21h = -223d => -223/16 °C = -13,94 °C
```

Sensorstatus

```
00 = kein Fehler  
55 = Kurzschluss  
AA = Unterbrechung
```

Schaltzustand

```
F0 = Inaktiv  
0F = Aktiv
```

oder

```
00 = Inktiv  
01 = Aktiv
```

Links

- <http://www.hx7.net/vaillant/> - liest Daten per EBUS mit vrDialog aus und stellt sie mit RRDTool grafisch dar
- <http://ab-log.ru/smart-house/heating-automation/vaillant-rs232> (Google Übersetzung (<http://translate.google.de/translate?u=http%3A%2F%2Fab-log.ru%2Fsmart-house%2Fheating-automation%2Fvaillant-rs232&sl=ru&tl=de&hl=&ie=UTF-8>)) - liest Daten per X6 aus, beschreibt auch, wie man Parameter ändert.

Abgerufen von „http://old.ethersex.de/index.php?title=Vaillant_X6_Schnittstelle&oldid=4743“

-
- Diese Seite wurde zuletzt am 7. Februar 2011 um 22:39 Uhr bearbeitet.