Reverse Engineering eines Kaffeevollautomaten

Niklas Joachim Eberhard Krüger

Abschlussvortrag, Bachelorarbeit, Meyer

6. März 2019

Studiendekanat ET / IT
Technische Universität Hamburg

TUHH

Übersicht

1. Aufbau und Kommunikation
2. Speicher
3. Vorgehen
4. Ergebnisse
5. Terminologie „Reverse Engineering“
6. Live Vorführung

1

Aufbau und Kommunikation

Zugriff direkt oder über die UART Schnittstelle

Direkte Speicherabfrage:

- Aktives Eingreifen verursacht Kurzschlüsse im Betrieb

Serielle UART Schnittstelle:

- Vorteil: RAM und EEPROM Abfrage im laufenden Betrieb
- Nachteil: Zeitintensiv

  $\Rightarrow$ kein konsistenter Speicherauszug
- Nachteil: Hemmt das interne Bussystem


jura
SWISS MADE
IMPRESSA S9
P
N

Probleme bei der seriellen Kommunikation

- Initialisierung benötigt mehrere Anläufe
- Kaum reproduzierbares Fehlverhalten beim direkten Zugriff auf die Gerätedatei
- Initialisierte Umgebung ließ sich nicht über `stty -F /dev/ttyACM0` nachbauen
- $\Rightarrow$ *libserial*-Library

2

Speicher

EEPROM

Adresse

DEC	HEX	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		0x00	0x01	0x02	0x03	0x04	0x05	0x06	0x07	0x08	0x09	0x0A	0x0B	0x0C	0x0D	0x0E	0x0F
0	0x00																
16	0x10	RE:00 (2 Byte Wort lesen,0x00-0xFF)															
32	0x20	re:0000 (2 Byte = 4 HEX Antwort)															
48	0x30																
64	0x40	RT:00 (eine Reihe = 32 Byte lesen, 0x00-0xF0) (32 Byte = 64 HEX Antwort)															
80	0x50	rt:00010001000600010001000000004000F000000000000000000001000F0000000E															
96	0x60																
112	0x70	WE:00,0001 (Schreibe an Adresse, den Wert)															
128	0x80	ok:															
144	0x90																
160	0xA0																
176	0xB0																
192	0xC0																
208	0xD0	1 Kästchen ≡ 1 Byte															
224	0xE0	je 0x00-0xFF = 00-255															
240	0xF0																

∑ 512 Byte

RAM

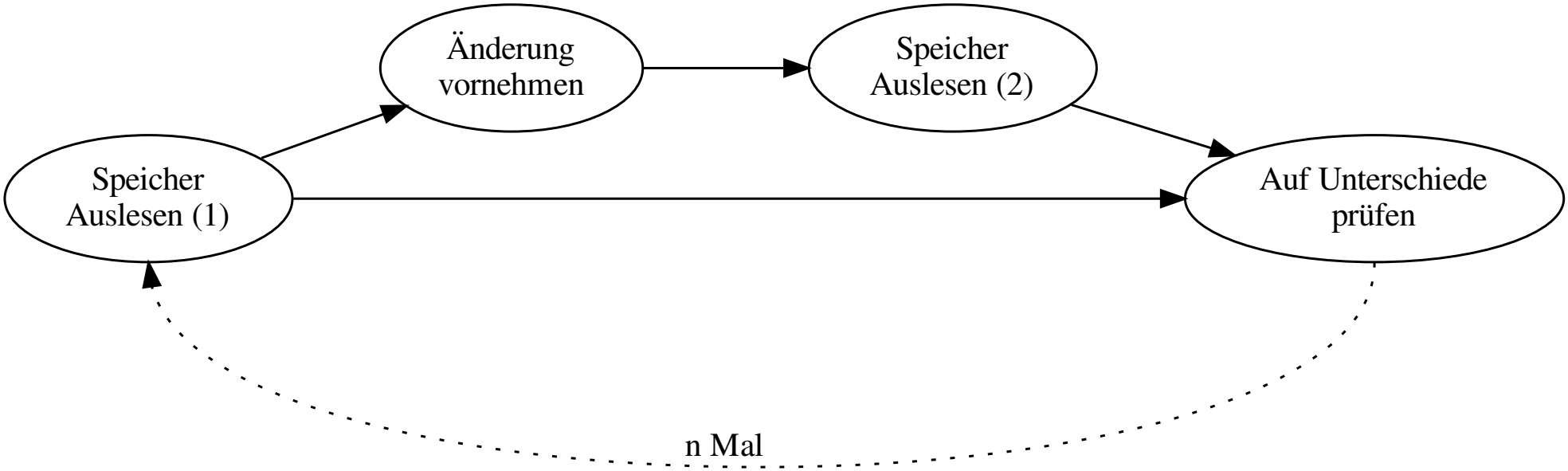
Adresse

DEC	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
HEX	0x00	0x01	0x02	0x03	0x04	0x05	0x06	0x07	0x08	0x09	0x0A	0x0B	0x0C	0x0D	0x0E	0x0F
0 0x00																
16 0x10		RR:00 (eine Reihe = 16 Byte lesen, 0x00-0xF0)														
32 0x20		rr:0002040000000000006A000102000058 (32 HEX Antwort)														
48 0x30																
64 0x40																
80 0x50																
96 0x60																
112 0x70																
128 0x80																
144 0x90																
160 0xA0																
176 0xB0																
192 0xC0																
208 0xD0		1 Kästchen ≡ 1 Byte														
224 0xE0		je 0x00-0xFF = 00-255														
240 0xF0																

∑ 256 Byte

Vorgehen

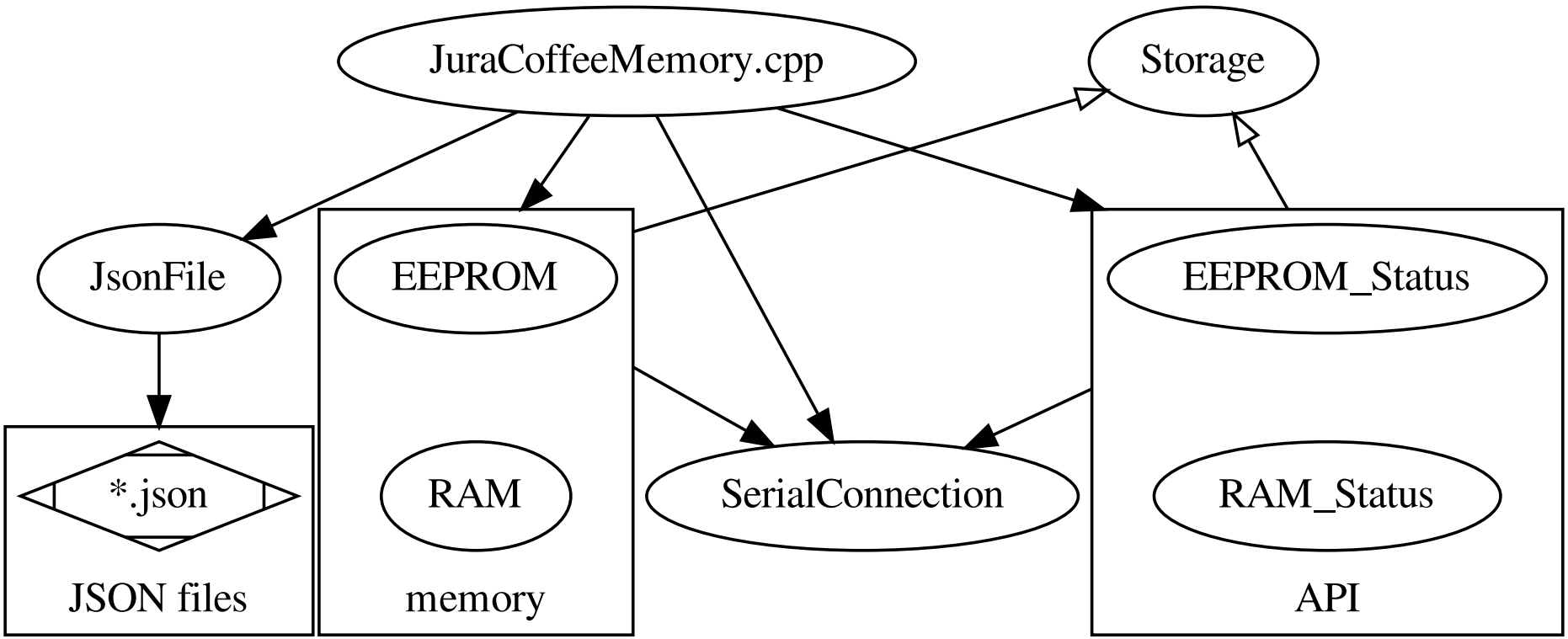
Standardverfahren



Weitere Ansätze

- Regelmäßige Unregelmäßigkeiten im RAM ausgeblendet
- Zähler im EEPROM verändert
- ASCII Tabelle für Zeichensatz des Displays angewendet

Implementierung in C++

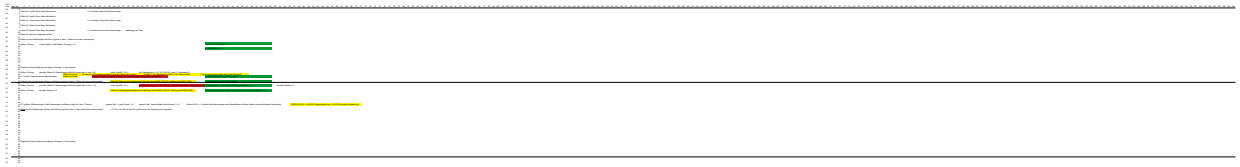


4

Ergebnisse

EEPROM

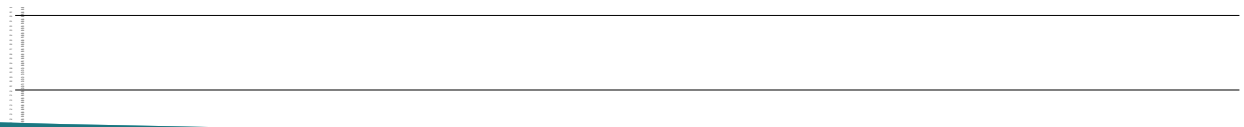
EEPROM



HEX Pos.	Byte \ Bit	0	1	2	3	4	5	6	7
00	0								
	1	Zähler für 1 große Tasse übers Bohnenfach							
01	2								
	3	Zähler für 2 große Tasse übers Bohnenfach							
02	4								
	5	Zähler für 1 kleine Tasse übers Bohnenfach							
03	6								
	7	Zähler für 2 kleine Tasse übers Bohnenfach							
04	8								
	9	Zähler für Spezial-Tasse übers Bohnenfach							
05	10								
	11	Zähler für jeden neu eingesetzten Filter							
06	12								
	13	Zähler für alle Zubereitungen mit Pulver (egal ob 1 oder 2, Zähler wird immer inkrementiert)							
07	14								
	15	Spülen / Rinsing			Gesamtzähler Anzahl Spülen / Rinsing (+=1)				
08	16								
	17								
09	18								
	19								
0A	20								
	21								
0B	22								
	23								
0C	24								
	25	Teeportion? (keine Änderung bei weiteren Bezügen => kein counter)							
0D	26								
	27	Spülen / Rinsing			partieller Zähler für Zubereitungen (zählt nicht jedes mal => max +=1)				
0E	28								
	29	+=1 bei der Zubereitung eines Spezialkaffees							
0F	30								
	31	Zähler für alle Zubereitungen (Pulver und Bohnen) (egal ob 1 oder 2, Zähler wird immer inkrementiert)							
10	32								
	33	Spülen / Rinsing			partieller Zähler für Zubereitungen (zählt nicht jedes mal => max +=1)				
11	34								
	35	Spülen / Rinsing			bei jeder Spülung +=1				
12	36								
	37								
13	38								
	39								
14	40								
	41	??? größere Zählersprünge für alle Zubereitungen mit Bohnen (egal ob 1 oder 2 Tassen)							
15	42								
	43	Zähler für alle Zubereitungen (Pulver und Bohnen) (egal ob 1 oder 2, Zähler wird immer inkrementiert)							
16	44								

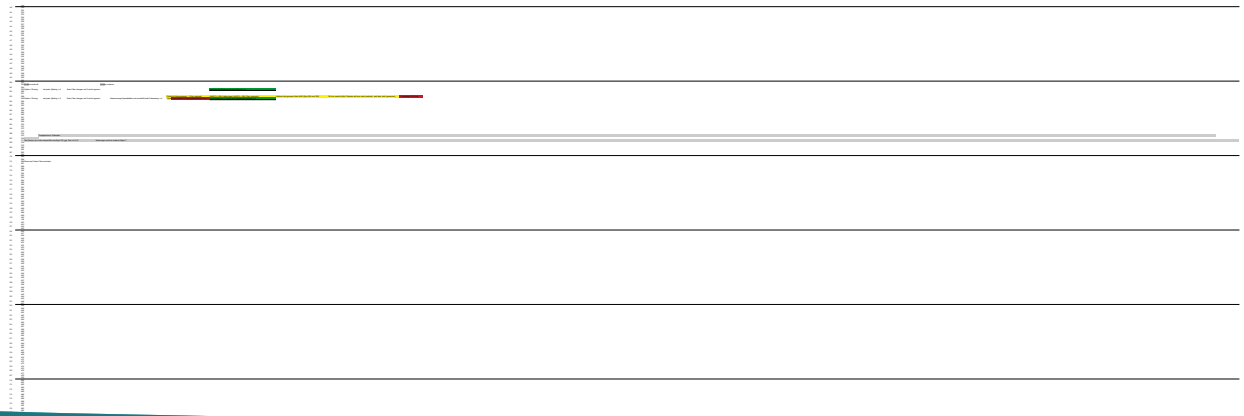
HEX Pos.	Byte \ Bit	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	5
00	0																																											
	1							+=1 auch beim Setzen der Wassermenge																																								
01	2																																												
	3																																												
02	4																																												
	5							+=1 auch beim Setzen der Wassermenge																																								
03	6																																												
	7																																												
04	8																																												
	9							+=1 auch beim Setzen der Wassermenge								unabhängig vom Filter																															
05	10																																												
	11																																												
06	12																																												
	13																																												
07	14																																												
	15																															Am Ende der Reinigung +=1												
08	16																																											
	17																															In der Reinigung +=1												
09	18																																											
	19																																												
0A	20																																												
	21																																												
0B	22																																												
	23																																												
0C	24																																												
	25																																												
0D	26																																												
	27												siehe „Byte/Bit“ 33 (=)						Bei Zubereitung nr. 3,4,7,10,13,16,19 (~ jede 3. Zubereitung?!)																												
0E	28																																												
	29																																												
0F	30																																												
	31												Zähler für Reinigungsankündigung nach Bezügen (bis 0x00DB (219) OK, Meldung ab 0x00DC (220))																															
10	32																																												
	33												siehe „Byte/Bit“ 27 (=)						Bei Zubereitung nr. 3,4,7,10,13,16,19 (~ jede 3. Zubereitung?!, bei Einstellung d																												
11	34																																												
	35												Zähler für Reinigungsankündigung nach Spülungen (bis 0x00B3 (179) OK, Meldung ab 0x00B4 (180))																															
12	36																																												
	37																																												
13	38																																												
	39																																												
14	40																																												
	41												eeprom Tag1 „1 große Tasse“ +=6						eeprom Tag2 „Spezial Kaffee (ohne Bohnen)“ +=6																												
15	42																																												
	43												+??? da > als Wert an Byte 31 (wird nicht bei der Reinigung zurück gesetzt)																															
16	44																																												

HEX Pos.	Byte \ Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	5
17	45																																																				
	47																																																				
18	48																																																			
	49																																																				
19	50																																																			
	51																																																				
1A	52																																																			
	53																																																			
1B	54																																																		
	55																																																			
1C	56																																																		
	57																																																			
1D	58																																																		
	59																																																			
1E	60																																																		
	61																																																			
1F	62																																																		
	63																																																			

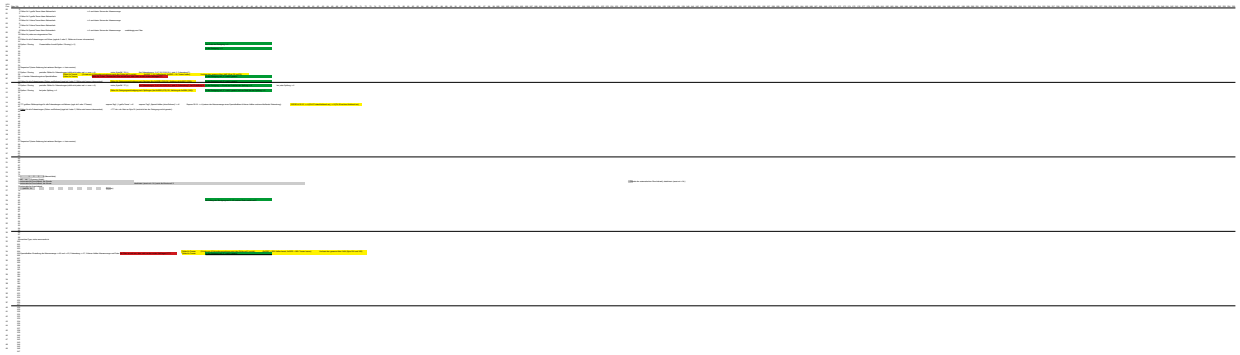


EEPROM

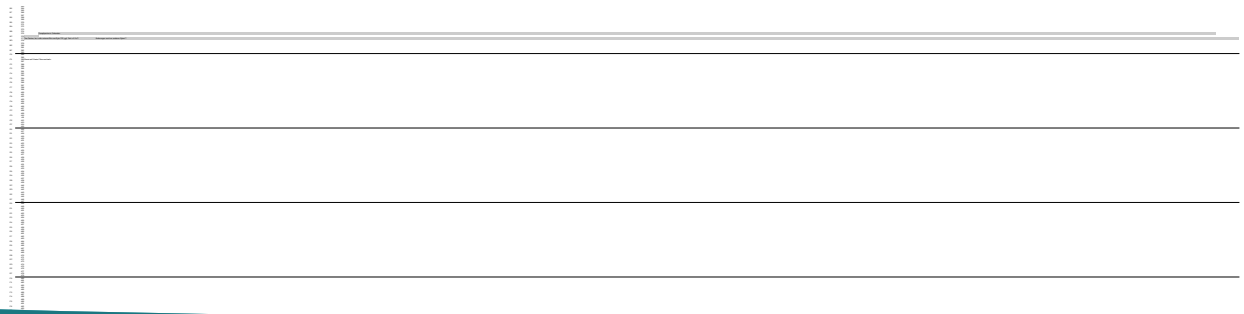
	69	
23	70	
	71	
24	72	-- 1 2 3 4 (Wasserhärte)
	73	off on (Economy Mode)
25	74	automatische Einschaltzeit, die Stunde
	75	automatische Einschaltzeit, die Minute deaktiviert (reset mit <N>) setzt die Minute auf 0
26	76	automatische Ausschaltzeit
	77	-.- (d0.5h 1h 9h (max)
27	78	
	79	
28	80	
	81	



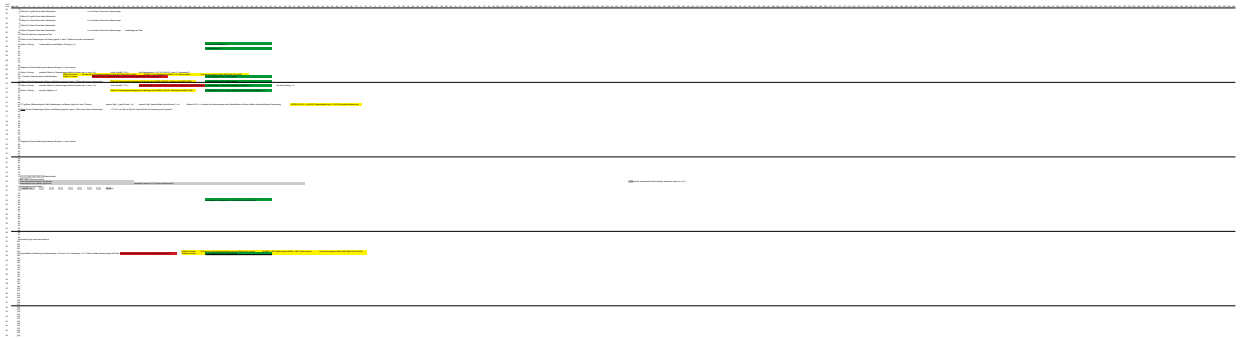
EEPROM



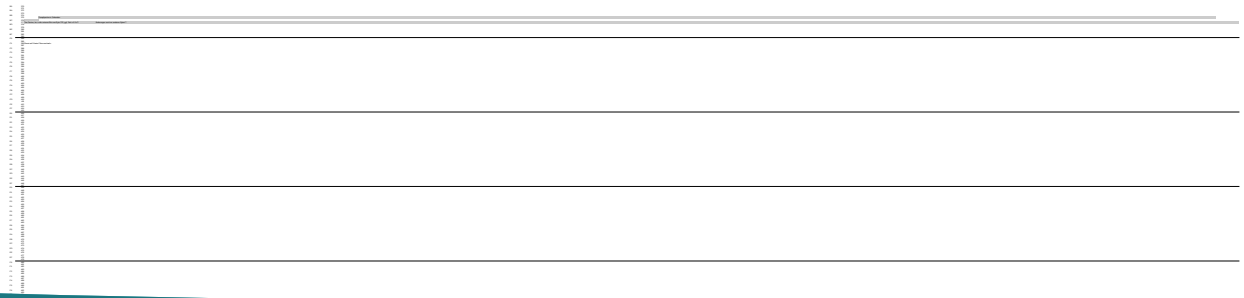
	251	Einschaltvorgänge (counter)				
7E	252					
	253					
7F	254					
	255					
80	256					
	257					
81	258					
	259	Deutsch (Sprache) immer in 16 Bit Schritten		Italienisch	Niederländisch	Spanisch
82	260	???				
	261	Pulvermenge einer kleinen Tasse: 0=min, 28=max	in Bit weisen Stufen einstellbar		Reset [N] stellt auf den Standardwert: 5	
83	262	???				
	263	Pulvermenge einer großen Tasse: 0=min, 28=max	in Bit weisen Stufen einstellbar		Reset [N] stellt auf den Standardwert: 8	
84	264	???				
	265	Pulvermenge einer Spezialtasse: 0=min, 28=max	in Bit weisen Stufen einstellbar		Reset [N] stellt auf den Standardwert: 11	
85	266					
	267	Temp Temp Temperatur Temperatur hoch, Spezialtasse			Standardwert wahrscheinlich: 0 (alle drei Bitts auf 0)	
86	268				Standardwert wahrscheinlich: 0	
	269	Wassermenge einer kleinen Tasse	anschließende manuelle Korrektur, 5 Bit Schritte in 29 Stufen einstellbar (+-14 Stufen von der Mitte aus => +- 70 Nachjustierung möglich)		Reset [N] stellt auf den Standardwert: 180	
87	270				Reset [N] stellt auf den Standardwert: 1	
	271	Wassermenge eienr großen Tasse	anschließende manuelle Korrektur, 5 Bit Schritte in 29 Stufen einstellbar (+-14 Stufen von der Mitte aus => +- 70 Nachjustierung möglich)		Reset [N] stellt auf den Standardwert: 84	
88	272				Reset [N] stellt auf den Standardwert: 1	
	273	Wassermenge einer Spezialtasse	anschließende manuelle Korrektur, 5 Bit Schritte in 29 Stufen einstellbar (+-14 Stufen von der Mitte aus => +- 70 Nachjustierung möglich)		Reset [N] stellt auf den Standardwert: 124	
89	274					
	275					



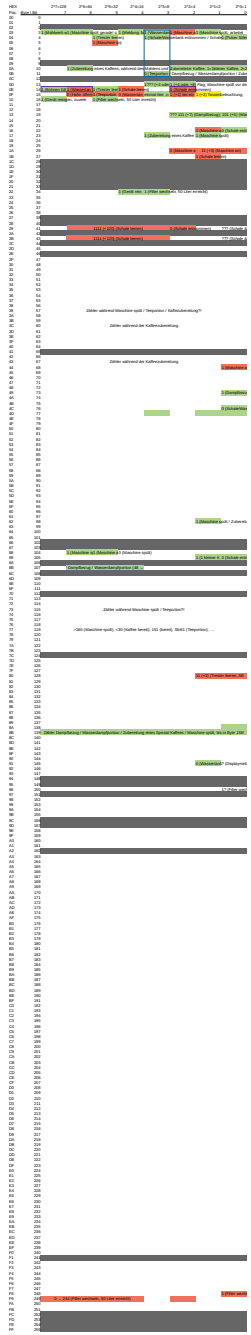
EEPROM



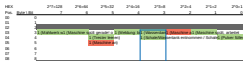
B0	352						
	353	incasso mode off			incasso mode on		
B1	354						
	355	Spülen / Rinsing	bei jeder Spülung +=1	Beim Filter einlegen auf 0 zurück gesetzt			Am Ende der Reinigung bei der Spülung +=1
B2	356						
	357						
B3	358					Zähler für Wassermenge → Filter wechseln	(0x01F3 = 499: Kaffee bereit; 0x01F4 = 500: Filter wechseln)
	359	Spülen / Rinsing	bei jeder Spülung +=1	Beim Filter einlegen auf 0 zurück gesetzt	Wassermenge Spezialkaffee und anschließende Zubereitung +=1	Zähler Tassenzähler nur bei eingeschaltetem Filter???	In der Reinigung +=10 und am Ende bei der Spülung +=1
B4	360						
	361						
B5	362						
	363						
B6	364						
	365						
B7	366						
	367						
B8	368						
	369						
B9	370						
	371						
BA	372						
	373						
BB	374						
	375	Dampfportion in Sekunden					
BC	376						
	377	Tee Portion, bis in die unteren Bits von Byte 376, ggf. Zeit in 0.1s?!		Änderungen auch an anderen Bytes!?			
BD	378						



RAM



RAM

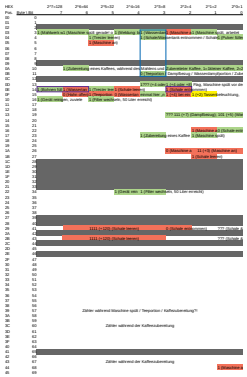


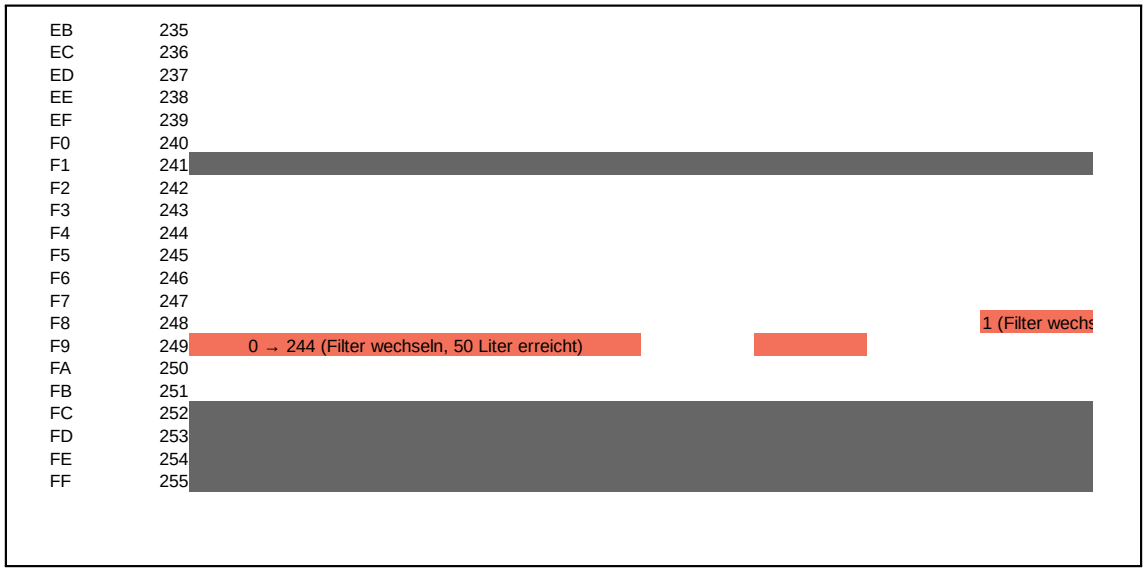
HEX Pos.	Byte \ Bit	2^7=128 7	2^6=64 6	2^5=32 5	2^4=16 4	2^3=8 3	2^2=4 2	2^1=2 1	2^0=1 0
00	0								
01	1								
02	2								
03	3	1 (Mahlwerk w	1 (Maschine spült gerade! o		1 (Meldung: b	1 (Wasserdam	1 (Maschine a	1 (Maschine spült, arbeitet	
04	4			1 (Trester leeren)		1 (Schale/Wassertank entnommen / Schale		1 (Pulver füller	
05	5			1 (Maschine an)					
06	6								
07	7								
08	8								
09	9								
0A	10		1 (Zubereitung eines Kaffees, während des			Mahlens und	Zubereiteter Kaffee, 1=1kleiner Kaffee, 2=2		
0B	11					0 (Teeportion /	Dampfbezug / Wasserdampfportion / Zube		
0C	12								
0D	13					1??? (+4 oder	1 (+4 oder +8)	Flag, Maschine spült vor de	
0E	14	1 (Bohnen füll	1 (Wassertan	1 (Trester leer	1 (Schale leeren)		1 (Schale entnommen)		
0F	15		0 (Hahn offen)	1 (Teeportion	0 (Wassertan	einmal hier „n	1 (+4) bei ein	1 (+2) Tassenbeleuchtung,	
10	16	1 (Gerät reinigen, zuviele		1 (Filter wechseln, 50 Liter erreicht)					
11	17								
12	18								
13	19						??? 111 (+7) (Dampfbezug); 101 (+5) (Was		
14	20								
15	21								
16	22							1 (Maschine a	0 (Schale entr
17	23					1 (Zubereitung eines Kaffee		1 (Maschine spült)	
18	24								
19	25								
1A	26						0 (Maschine a	11 (+3) (Maschine an)	
1B	27							1 (Schale leeren)	
1C	28								
1D	29								
1E	30								
1F	31								
20	32								
21	33								
22	34			1 (Gerät rein	1 (Filter wechseln, 50 Liter erreicht)				
23	35								
24	36								
25	37								
26	38								
27	39								
28	40								
29	41		1111 (+120) (Schale leeren)			0 (Schale entnommen)		??? (Schale &	
2A	42								
2B	43		1111 (+120) (Schale leeren)					??? (Schale &	
2C	44								
2D	45								
2E	46								
2F	47								

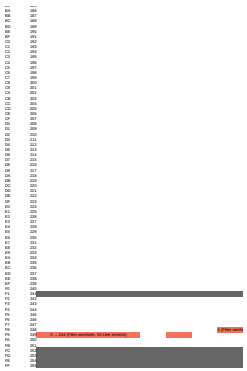
RAM

61	97	
62	98	1 (Maschine spült / Zubereitu
63	99	
64	100	
65	101	
66	102	
67	103	
68	104	1 (Maschine s 1 (Maschine a 0 (Maschine spült)
69	105	1 (1 kleiner K 0 (Schale entr
6A	106	
6B	107	Dampfbezug / Wasserdampfportion (48 →
6C	108	
6D	109	
6E	110	
6F	111	
70	112	
71	113	
72	114	
73	115	Zähler während Maschine spült / Teeportion?!
74	116	
75	117	
76	118	
77	119	>160 (Maschine spült), <30 (Kaffee bereit), 151 (bereit), 55/61 (Teeportion), …
78	120	
79	121	
7A	122	
7B	123	
7C	124	
7D	125	
7E	126	
7F	127	
80	128	11 (+3) (Trester leeren, AB
81	129	
82	130	
83	131	
84	132	
85	133	
86	134	
87	135	
88	136	
89	137	
8A	138	
8B	139	Zähler Dampfbezug / Wasserdampfportion / Zubereitung eines Spezial Kaffees / Maschine spült, bis in Byte 138!
8C	140	
8D	141	

RAM



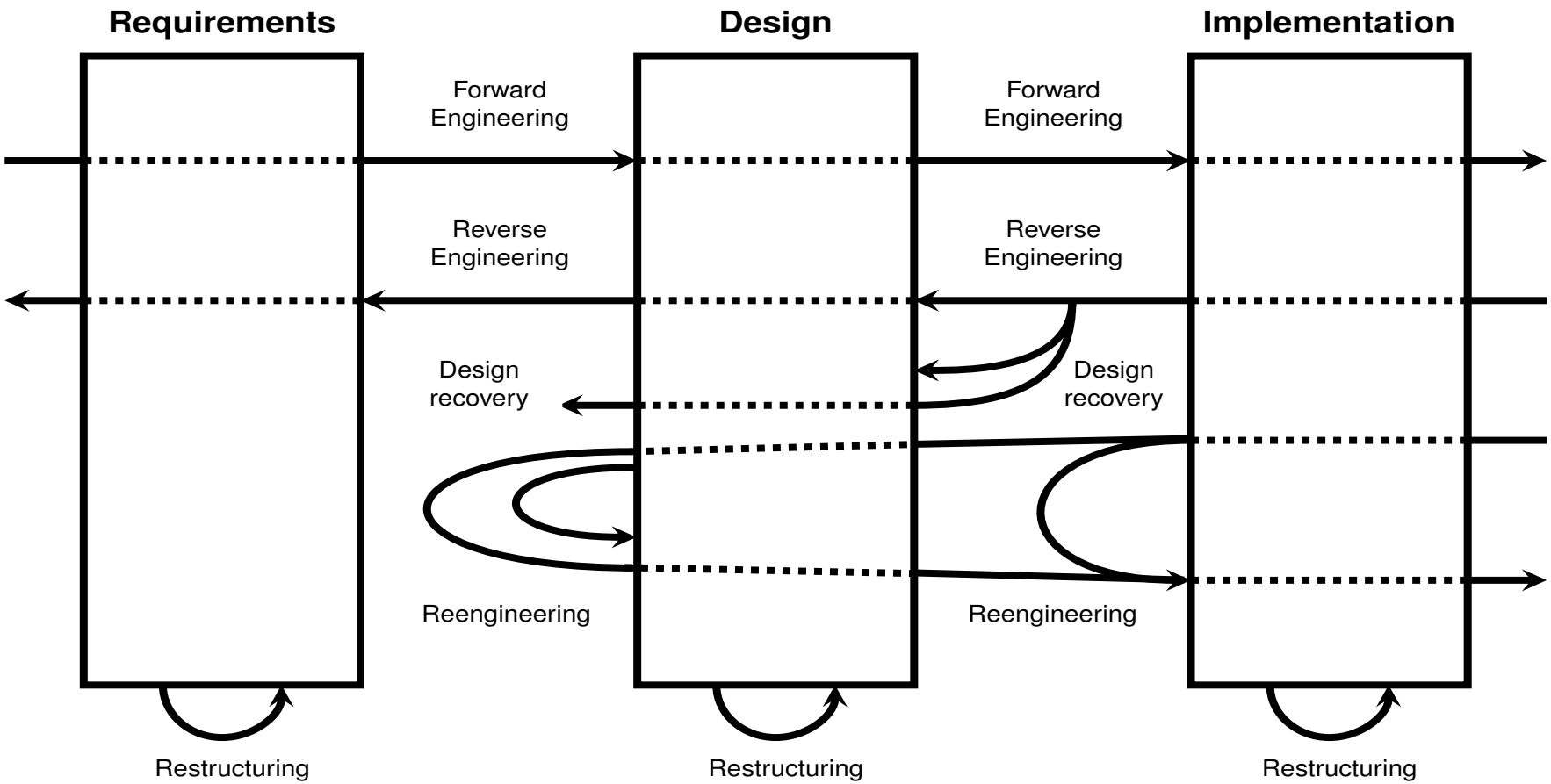

EB 235
EC 236
ED 237
EE 238
EF 239
F0 240
F1 241
F2 242
F3 243
F4 244
F5 245
F6 246
F7 247
F8 248
F9 249
FA 250
FB 251
FC 252
FD 253
FE 254
FF 255
1 (Filter wechs
0 → 244 (Filter wechseln, 50 Liter erreicht)



Terminologie „Reverse Engineering“

Begriffe

- Forward Engineering
- Reverse Engineering
- Redocumentation
- Design Recovery
- Restructuring
- Reengineering

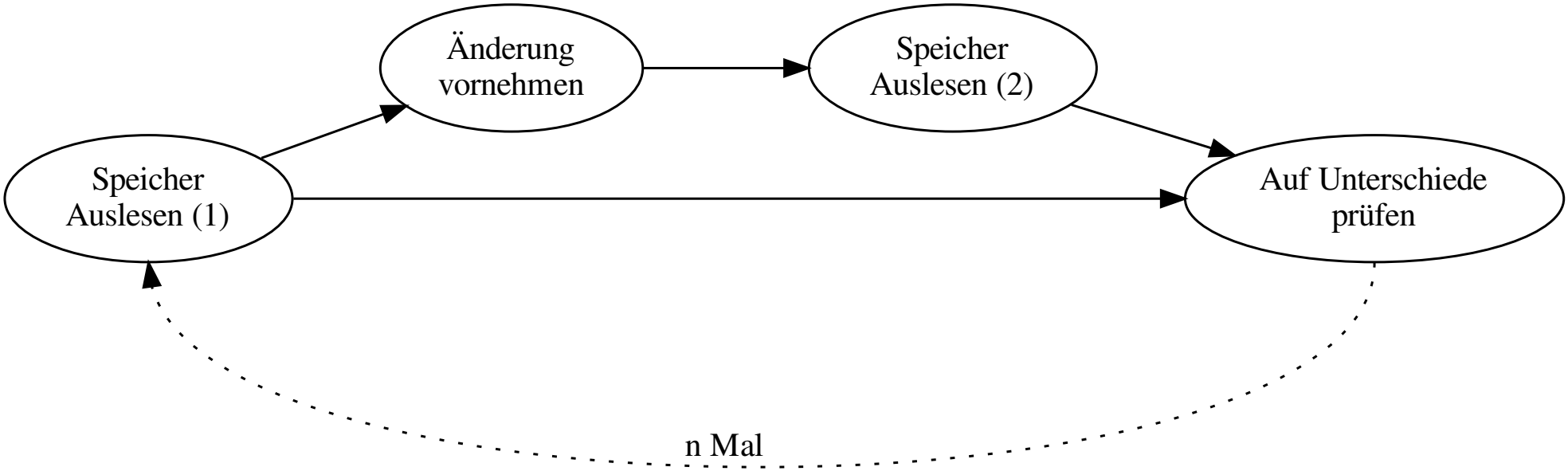


Live Vorführung


jura
SWISS MADE
IMPRESSA S9
P
N

```
Main Menu
Please make your selection
1 - EEPROM Skript
2 - Ram Skript
3 -
4 - Send a command
5 -
6 - Dump EEPROM
7 - Dump RAM
8 -
9 - Options
0 - Analyse existing dumps
Q / q / quit / exit - To leave
Selection: 1
Scanning [####################################] 100%
EEPROM: Enter a command to the coffee maschine, pr
ess only <Enter> to continue, <S> to print the las
t dump or <Q> to quit: AN:01
ok:
Scanning [####################################] 100%
Say what you've changed: Machine turned on
Sorry, no Bytes are changed ;(
000A0007002A0007004C0005001C005C0001000000000000100
08002F0000004400A0003600000000022000A900000000000
```

Standardverfahren



	0x00	0x01	0x02	0x03	0x04	0x05	0x06	0x07	0x08	0x09	0x0A	0x0B	0x0C	0x0D	0x0E	0x0F
0x00	00	02	74	00	04	00	00	00	00	FA	00	01	10	00	10	5A
0x10	00	00	0A	00	00	00	00	00	00	00	04	02	32	04	03	08
0x20	15	15	00	00	00	00	00	19	07	78	29	78	35	01	00	40
0x30	00	00	08	00	00	00	00	00	00	00	00	00	A2	00	00	20
0x40	00	00	00	A2	00	10	00	00	11	00	C0	00	01	00	00	01
0x50	00	08	00	00	00	00	00	00	10	00	00	00	00	00	02	00
0x60	02	92	00	EC	00	00	07	04	10	00	20	10	25	00	00	06
0x70	06	00	00	00	00	00	00	A2	00	00	04	00	0E	00	00	00
0x80	00	00	00	00	00	00	80	00	01	2A	0B	40	00	00	FE	00
0x90	06	96	00	00	07	43	02	2C	00	00	00	00	1A	84	00	71
0xA0	00	38	1C	00	00	0F	00	E6	01	0A	01	BE	02	22	17	D4
0xB0	0B	EA	08	98	07	3A	05	DC	04	4C	03	E8	00	14	01	2C
0xC0	00	10	00	00	00	00	0C	14	03	C0	00	00	00	1E	00	00
0xD0	00	DC	00	B4	06	72	06	40	01	90	50	32	10	00	08	04
0xE0	80	A0	64	5D	28	5F	08	0D	02	00	04	00	06	97	00	00
0xF0	00	8D	03	00	00	01	32	24	00	00	00	00	A0	F1	04	A9

	0x00	0x01	0x02	0x03	0x04	0x05	0x06	0x07	0x08	0x09	0x0A	0x0B	0x0C	0x0D	0x0E	0x0F
0x00	00	02	4C	00	04	00	00	00	00	75	00	01	11	00	00	5A
0x10	00	00	0A	00	00	00	00	00	00	00	04	00	0C	01	00	0C
0x20	2C	58	00	00	00	00	00	19	19	05	01	05	01	01	02	40
0x30	00	00	08	00	00	00	00	00	00	00	00	00	A2	00	00	20
0x40	00	00	00	A2	00	10	00	00	11	00	C0	00	01	00	00	01
0x50	00	08	00	00	00	00	00	00	10	00	00	00	00	00	02	00
0x60	02	92	00	EC	00	00	05	00	10	00	20	10	25	00	00	06
0x70	06	00	00	00	00	00	00	A2	00	00	04	00	07	00	00	00
0x80	00	00	00	00	00	00	80	00	01	2A	0B	40	00	00	FE	00
0x90	06	96	00	00	07	5C	02	3D	00	00	00	00	2C	00	00	71
0xA0	00	38	24	00	00	0F	00	E6	01	0A	01	BE	02	22	17	D4
0xB0	0B	EA	08	98	07	3A	05	DC	04	4C	03	E8	00	14	01	2C
0xC0	00	10	00	00	00	00	0C	14	03	C0	00	00	00	1E	00	00
0xD0	00	DC	00	B4	06	72	06	40	01	90	50	32	10	00	08	04
0xE0	80	A0	64	5D	28	5F	08	0D	02	00	04	00	06	97	00	00
0xF0	00	68	03	00	00	01	32	24	00	00	00	00	A1	17	08	60

	0x00	0x01	0x02	0x03	0x04	0x05	0x06	0x07	0x08	0x09	0x0A	0x0B	0x0C	0x0D	0x0E	0x0F
0x00	00	02	4C	00	04	00	00	00	00	75	00	01	11	00	**00**	5A
0x10	00	00	0A	00	00	00	00	00	00	00	04	**00**	0C	01	00	0C
0x20	2C	58	00	00	00	00	00	19	19	**05**	01	**05**	01	01	02	40
0x30	00	00	08	00	00	00	00	00	00	00	00	00	A2	00	00	20
0x40	00	00	00	A2	00	10	00	00	11	00	C0	00	01	00	00	01
0x50	00	08	00	00	00	00	00	00	10	00	00	00	00	00	02	00
0x60	02	92	00	EC	00	00	05	00	10	00	20	10	25	00	00	06
0x70	06	00	00	00	00	00	00	A2	00	00	04	00	07	00	00	00
0x80	00	00	00	00	00	00	80	00	01	2A	0B	40	00	00	FE	00
0x90	06	96	00	00	07	5C	02	3D	00	00	00	00	2C	00	00	71
0xA0	00	38	24	00	00	0F	00	E6	01	0A	01	BE	02	22	17	D4
0xB0	0B	EA	08	98	07	3A	05	DC	04	4C	03	E8	00	14	01	2C
0xC0	00	10	00	00	00	00	0C	14	03	C0	00	00	00	1E	00	00
0xD0	00	DC	00	B4	06	72	06	40	01	90	50	32	10	00	08	04
0xE0	80	A0	64	5D	28	5F	08	0D	02	00	04	00	06	97	00	00
0xF0	00	68	03	00	00	01	32	24	00	00	00	00	A1	17	08	60

```
{
        "amount_1_big_coffee_with_beans" :
        {
                "value" : 10
        },
        "amount_1_small_coffee_with_beans" :
        {
                "value" : 42
        },
        "amount_2_big_coffees_with_beans" :
        {
                "value" : 7
        },
        "amount_2_small_coffees_with_beans" :
        {
                "value" : 7
        },
        "amount_coffee_preparations_until_next_cleaning" :

        {
                "default" : 0,
                "max" : 219,
                "min" : 0,
                "value" : 68
        },
        "amount_filter_replacements" :
        {
                "value" : 5
        },
        "amount_ground_1" :
        {
                "default" : 0,
                "max" : 15,
                "min" : 0,
                "value" : 0
        },
        "amount_ground_2" :
        {
                "default" : 0,
                "max" : 959,
                "min" : 0,
                "value" : 0
        },
```

Small Coffee	
Powder quantity	2
Water quantity	1
Temperature (+1)	7

Cookie | Brew 1 | Brew 2

Big Coffee	
Powder quantity	0
Water quantity	1
Temperature (+2)	7

Cookie | Brew 1 | Brew 2

Special Coffee	
Powder quantity	0
Water quantity	1
Temperature (+4)	7

Cookie | Brew

Water and Steam	
Water hardness	4
Filter	8
Steam portion	20
Tea portion	450

Machine	
Machine type	1
Language	0
Economy mode	1
Incasso mode	0

Time switches	
Autom. off in [h]	10
Autom. on at [h]	128
Autom. on at [m]	0

Messages

On	off
Tray missing	off
Empty drip tray	off
Empty grounds	off
Fill water	off
Clean machine	off
Rinsing before switching off	0
Cup illumination	off
Replacing filter	off
Tap closed	on
Fill powder	off
Fill beans	off

Working

Coffee is made	off
Brew coffee type	0
Brew step1: grinder	off
Brew step2: pumping coffee	off
Rinsing unit	off
Steam portion	off
Tea portion	off

Counting states

Coffee	**#**
1 small coffee	42
2 small coffees	7
1 big coffee	9
2 big coffees	7
1 special coffee	75
pulver coffees	28
Machine	**#**
Starts	153
Filter replacements	5
Rinsings	83
Using	**%**
Amount of ground	67%
	99%
Coffee preparations until next cleaning	122%
Rinsings until next cleaning	25%

Vielen Dank für die Aufmerksamkeit!