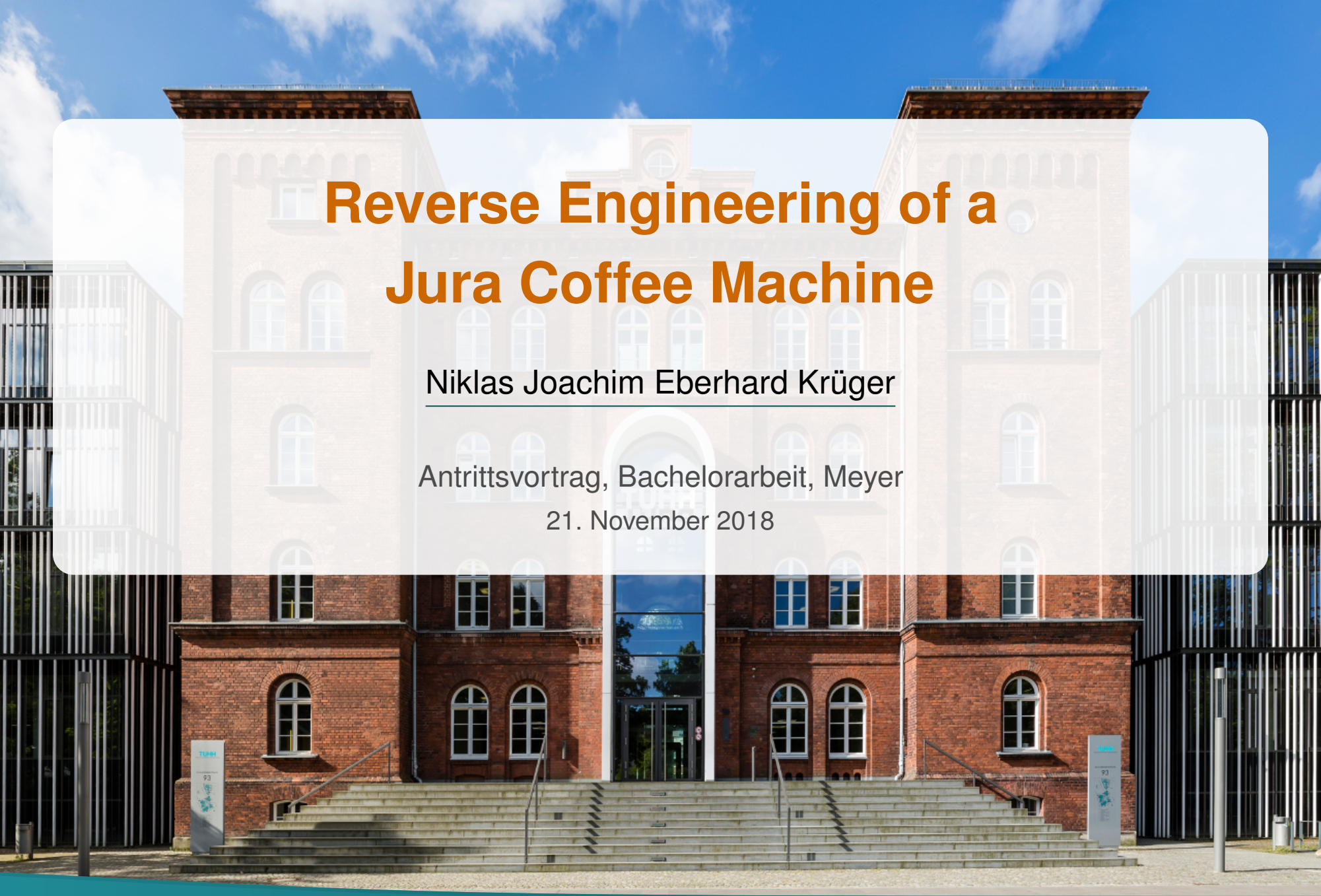


Reverse Engineering of a Jura Coffee Machine

Niklas Joachim Eberhard Krüger

Antrittsvortrag, Bachelorarbeit, Meyer

21. November 2018

Studiendekanat ET / IT
Technische Universität Hamburg

TUHH

Übersicht


jura
SWISS MADE
IMPRESSA S9
P
N


jura
SWISS MADE
IMPRESSA S9
GND
TX
RX
+5V
GND
RxD
TxD
SCL
SDA
AREF
GND
13
12
~11
~10
~9
8
7
~6
~5
4

Verkabelung

- Über eine serielle Schnittstelle kommunizieren Kaffee-Maschine und Arduino, sowie Arduino und PC
- Arduino kodiert die ASCI Befehle um in UART[1] Bytes, welche Kaffee-Maschine vesteht und vice versa
- Linux bindet den Arduino über /dev/ttyACM0 ein
  Die Baudrate liegt bei 9600

[1] Universal Asynchronous Receiver Transmitter

Kommandos

- AN: Betriebszustand
- FA:<id> Bezugstaste
- FN:<id> Steuerungskomponente
- IC: Eingabe Status*
- PM: Play music, easter egg*
- RE:<address> Liest 2 Byte EEPROM Speicher
- RR:<address> Liest eine Zeile Ram
- RT:<address> Liest eine Zeile EEPROM
- TY: Maschinen Typ
- WE:<address>,<value> Schreibt 2 Byte in EEPROM
- ?M3 Aktiviere Inkassomudus
- ?M1 Deaktiviere Inkassomodus
- ?D<row><8 chars> Row-te Displayzeile
- ...

* ggf. nicht alles implementiert

Kommandos

- AN: Betriebszustand
- FA:<id> Bezugstaste
- FN:<id> Steuerungskomponente
- IC: Eingabe Status*
- PM: Play music, easter egg*
- RE:<address> Liest 2 Byte EEPROM Speicher
- RR:<address> Liest eine Zeile Ram
- RT:<address> Liest eine Zeile EEPROM
- TY: Maschinen Typ
- WE:<address>,<value> Schreibt 2 Byte in EEPROM
- ?M3 Aktiviere Inkassomudus
- ?M1 Deaktiviere Inkassomodus
- ?D<row><8 chars> Row-te Displayzeile
- ...

* ggf. nicht alles implementiert

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

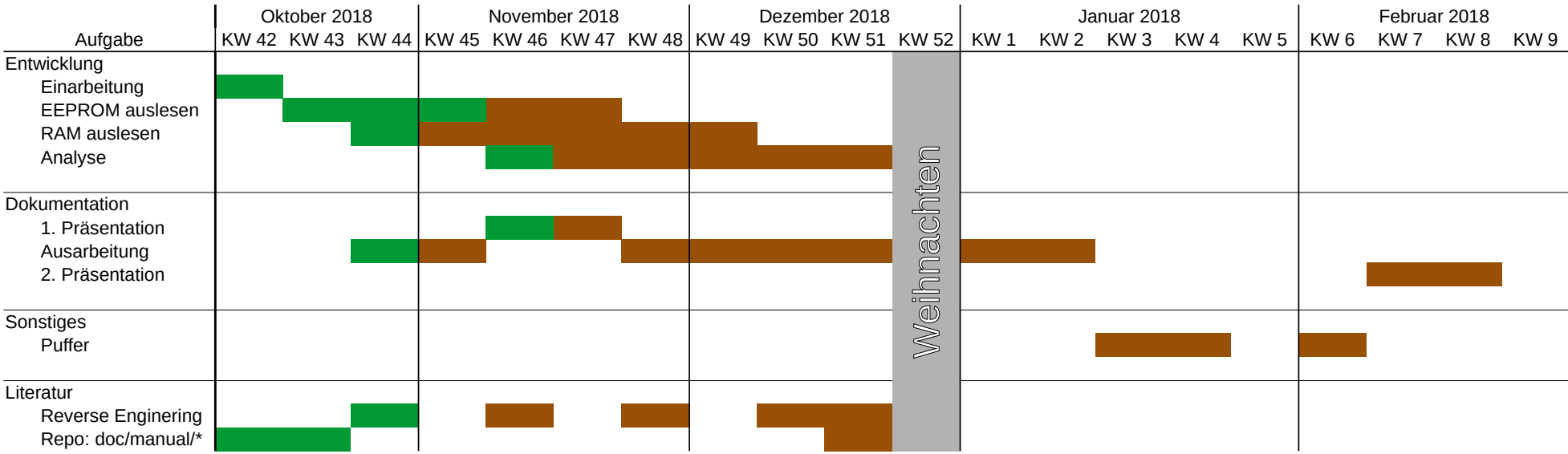
Aufgabenstellung / Thema

- Reverse Engineering des Speichers
- Welches Wort / Byte / Bit speichert welche Information?
- Zugang zum Speicher:
  - direkt: Während des Betriebs schwierig
  - seriell: Über die vorhandene Schnittstelle, langsam

Vorgehen

- EEPROM und Ram über ein Skript auslesen
- Nach möglichst elementaren Veränderungen wiederholen
- Zustände und Speicherbereiche, sowie deren Bedeutung für die Kaffeemaschine ermitteln
- Ausbauen mithilfe weiterer Literatur
- Reverse Engineering im allg. hierzu in Relation setzen
- Ausblick: EEPROM gezielt (fern-)steuern
  - Per Knopfdruck wird der Kaffee nach eigenen Präferenzen zubereitet
  - Profile für Wasser-, Pulvermenge, Temperatur, ...

Zeitplan


Aufgabe
Oktober 2018
KW 42 KW 43 KW 44
November 2018
KW 45 KW 46 KW 47 KW 48
Dezember 2018
KW 49 KW 50 KW 51 KW 52
Januar 2018
KW 1 KW 2 KW 3 KW 4 KW 5
Februar 2018
KW 6 KW 7 KW 8 KW 9
Entwicklung
Einarbeitung
EEPROM auslesen
RAM auslesen
Analyse
Dokumentation
1. Präsentation
Ausarbeitung
2. Präsentation
Sonstiges
Puffer
Literatur
Reverse Enginering
Repo: doc/manual/*
Weihnachten

Vielen Dank für die Aufmerksamkeit!