



V1.0.20240930

Embedded Software Engineering 1

HS 2024 – Prof. Reto Bonderer

Autoren: Laurin Heitzer, Simone Stitz

<https://github.com/P4ntomime/EmbSW1>

Inhaltsverzeichnis

1	Embedded Systems – Allgemein	2			
1.1	Definition	2			
1.2	Beispiele	2			
1.3	Deeply Embedded System	2			
1.4	Betriebssysteme bei Embedded Systems	2			
1.5	Bare Metal Embedded System	2			
1.6	Zuverlässigkeit	2			
1.7	Verfügbarkeit	2			
1.8	Abstraktionsschichten	2			
2	Real-Time System (Echtzeitsystem)	2			
2.1	Definitionen	2			
2.2	Fehlverhalten eines Systems (failed system)	2			
2.3	Echtzeitdefinition – Verschiedene Echtzeitsysteme	3			
2.4	Determinismus (determinacy)	3			
2.5	Auslastung (utilization)	3			
2.6	Real-time Scheduling	3			
3	Modellierung eines Embedded Systems	3			
3.1	V-Modell für Software-Entwicklungszyklus	3			
3.2	Model Driven Development (MDD)	3			
3.3	Vorgehen bei der Modellierung	3			
3.4	Systemgrenze definieren & Systemprozesse finden	3			
3.5	Verteilungen festlegen	3			
			3.6	Systemprozesse detaillieren	4
4	Hardware-Software-Codesign	4			
4.1	Ziele	4			
4.2	Anforderungen für praktische Anwendungen	4			
4.3	Spezifikationssprachen	4			
4.4	Virtuelle Prototypen	4			
4.5	X-in-the-loop	4			
4.6	Entwicklungsplattformen	5			
5	Zustandsbasierte Systeme	5			
5.1	Asynchrone vs. synchrone FSM	5			
5.2	Finite State Machines (FSM)	5			
5.3	State-Event-Diagramm (Zustandsdiagramm)	5			
5.4	Zustandstabelle	5			
6	Statecharts	5			
6.1	Nachteile von State-Event-Diagrammen	5			
6.2	Definitionen	5			
6.3	Hierarchie	5			
6.4	Default-State	5			
6.5	History	5			
6.6	Parallelität	5			
6.7	Timers	5			
6.8	Beispiel – Armbanduhr als Statechart	5			

1 Embedded Systems – Allgemein

1.1 Definition

Ein Embedded System...

- ist ein System, das einen Computer beinhaltet, selbst aber kein Computer ist
- besteht üblicherweise aus Hardware (Mechanik, Elektronik) und Software
- ist sehr häufig ein Control System (Steuerung, Regelung)

Ein Embedded System beinhaltet typischerweise folgende Komponenten:

- Sensoren
- Mikrocomputer
- Hardware (Mechanik, Elektronik)
- Aktoren
- Software (Firmware)

1.1.1 Charakterisierung von Embedded Systems

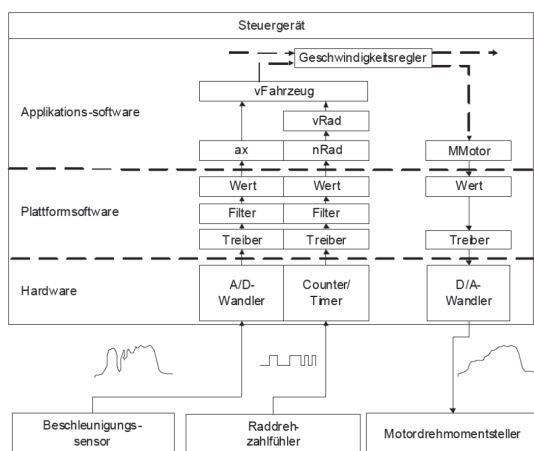
Embedded Systems können (**müssen aber nicht**) folgende Eigenschaften haben:

- **reactive systems:** Reaktive Systeme interagieren mit ihrer Umgebung
- **real-time systems:** Echtzeitsysteme haben neben funktionale Anforderungen auch definierbaren zeitlichen Anforderungen zu genügen
- **dependable systems:** Verlässliche Systeme sind Systeme, welche (sehr) hohe Zuverlässigkeitsanforderungen erfüllen müssen
- **Weitere (häufige) Anforderungen:**
 - kleiner Energieverbrauch
 - kleine physikalische Abmessungen
 - Lärm, Vibration, etc.

1.1.2 Typischer Aufbau

Ein gutes Design beinhaltet unterschiedliche Abstraktionsschichten → Layer

⇒ Siehe Abschnitt 1.8



1.2 Beispiele

Fahrrad-Computer

- GPS-Navigation
- Geschwindigkeits- und Trittfrequenzmessung
- Pulsmesser
- Drahtlosübertragung (ANT+)
- Interface zu elektronischer Gangschaltung
- Barometer, Thermometer
- Trainingsassistent
- Display

Auto

- Sicherheitsrelevante Aufgaben
 - ABS, ASR
 - Motorenregelung
 - Drive-by-wire
 - Autonom fahrende Autos
 - Unterhaltung / Komfort
 - Radio / CD / etc.
 - Navigation
 - Klima
 - Mehrere Netzwerke
 - CAN, LIN, Ethernet
 - Echtzeitteile und andere
 - Von einfachsten μ Cs bis DSPs und GPUs
- ⇒ Auto ist ein riesiges Embedded System

Weitere Beispiele

- Smartphone
- Mobile Base Station
- CNC-Bearbeitungszentrum
- Hörgerät

1.3 Deeply Embedded System

- 'Einfaches' Embedded System, mit **minimaler Benutzerschnittstelle**, üblicherweise mit **keinerlei GUI** und **ohne Betriebssystem**
- Beschränkt auf **eine** Aufgabe (z.B. Regelung eines physikalischen Prozesses)
- Muss oft zeitliche Bedingungen erfüllen ⇒ Echtzeitsystem

1.3.1 Beispiele – Deeply Embedded System

- Hörgerät
- ABS-Controller
- etc...
- Motorenregelung
- 'Sensor' im IoT

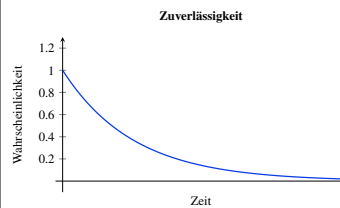
1.4 Betriebssysteme bei Embedded Systems

- Es kommen Betriebssysteme wie (Embedded) Linux oder Android zum Einsatz
⇒ **Achtung: Linux und Android sind nicht echtzeitfähig!**
- Wenn Echtzeit verlangt wird: real-time operating systems (RTOS)
 - Beispiele: Zephyr, Free RTOS (Amazon), TI-RTOS (Texas Instruments), etc.

1.5 Bare Metal Embedded System

- Es kommt **keinerlei Betriebssystem** zum Einsatz
- Bare Metal Embedded Systems sind recht **häufig**, insbesondere bei **Deeply Embedded Systems**
- Bare Metal Embedded Systems stellen besondere Ansprüche an Programmierung

1.6 Zuverlässigkeit



- Je länger das System läuft, desto weniger zuverlässig ist es
- Die Wahrscheinlichkeit für einen Ausfall steigt stetig

Achtung: Hier ist nur die Alterung der Hardware berücksichtigt

1.7 Verfügbarkeit

Die Verfügbarkeit A (Availability) ist der Anteil der Betriebsdauer innerhalb dessen das System seine Funktion erfüllt.

$$\text{Verfügbarkeit} = \frac{\text{Gesamtzeit} - \text{Ausfallzeit}}{\text{Gesamtzeit}}$$

1.8 Abstraktionsschichten

- Bei μ C-Programmierung (Firmware) müssen oft Bitmuster in Register geschrieben werden
- Solche Register-Zugriffe dürfen **nicht** 'willkürlich' überall im Code erfolgen
⇒ schlecht lesbar, schlecht portierbar, fehleranfällig
- **Damit Code lesbarer und besser auf andere Plattform portierbar wird, beinhaltet jeder professionelle Code einen Hardware Abstraction Layer (HAL)**
- HAL führt **nicht** zum Verlust bei Laufzeit, wenn korrekt implementiert

1.8.1 Hardware-abstraction-layer (HAL)

- Trennt HW-Implementierung von SW-Logik
- Gleiche SW kann auf verschiedene HW verwendet werden ⇒ Portabilität
- HW-Komponenten können einfach ausgetauscht werden ⇒ Flexibilität

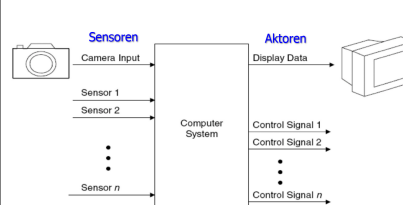
2 Real-Time System (Echtzeitsystem)

2.1 Definitionen

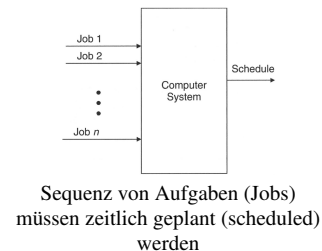
2.1.1 Real-Time System (Echtzeitsystem)

- Ein Echtzeitsystem ist ein System, das Informationen **innerhalb einer definierten Zeit (deadline)** bearbeiten muss.
⇒ Explizite Anforderungen an **turnaround-time** (Antwortzeit) müssen erfüllt sein
- Wenn diese Zeit nicht eingehalten werden kann, ist mit einer **Fehlfunktion** zu rechnen.

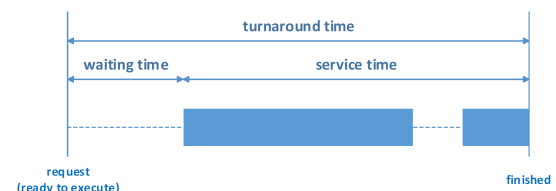
Typisches Echtzeitsystem



Repräsentation RT-System



2.1.2 Zeitdefinitionen (Task)



- **turnaround time:** (response time, Antwortzeit)
 - Startet, wenn der Task bereit zur Ausführung ist und endet, wenn der Task fertig abgearbeitet ist
 - Zeit zwischen dem Vorhandensein von Eingangswerten an das System (Stimulus) bis zum Erscheinen der gewünschten Ausgangswerte.
- **waiting time:** (Wartezeit)
 - Zeit zwischen Anlegen der Eingangswerte und Beginn der Abarbeitung des Tasks
- **service time:** (Bearbeitungszeit)
 - Zeit für Abarbeitung des Tasks ⇒ Unterbrechungen bzw. (preemptions) möglich

2.2 Fehlverhalten eines Systems (failed system)

- Ein fehlerhaftes System (failed system = missglücktes System) ist ein System, das nicht alle formal definierten Systemspezifikationen erfüllt.
- **Die Korrektheit eines RT Systems bedingt sowohl die Korrektheit der Outputs als auch die Einhaltung der zeitlichen Anforderungen.**

2.3 Echtzeitdefinition – Verschiedene Echtzeitsysteme

- **soft real-time system** (weiches Echtzeitsystem)
 - Durch Verletzung der Antwortzeiten wird das System **nicht** ernsthaft beeinflusst
 - Es kommt zu Komforteinbußen
- **hard real-time system** (hartes Echtzeitsystem)
 - Durch Verletzung der Antwortzeiten wird das System **ernsthaft beeinflusst**
 - Es kann zu einem kompletten Ausfall oder katastrophalem Fehlverhalten kommen
- **firm real-time system** (festes Echtzeitsystem)
 - Kombination aus soft real-time system und hard real-time system
 - Durch Verletzung einiger weniger Antwortzeiten wird das System nicht ernsthaft beeinflusst
 - Bei vielen Verletzungen der Antwortzeiten kann es zu einem kompletten Ausfall oder katastrophalem Fehlverhalten kommen

2.3.1 Beispiele verschiedener Echtzeitsysteme

System	Klassifizierung	Erläuterung
Geldautomat	soft	Auch wenn mehrere Deadlines nicht eingehalten werden können, entsteht dadurch keine Katastrophe. Im schlimmsten Fall erhält ein Kunde sein Geld nicht.
GPS-gesteuerter Rasenmäher	firm	Wenn die Positionsbestimmung versagt, könnte das Blumenbeet der Nachbarn platt gemäht werden.
Regelung eines Quadcopters	hard	Das Versagen der Regelung kann dazu führen, dass der Quadcopter ausser Kontrolle gerät und abstürzt.

2.4 Determinismus (determinacy)

Ein System ist deterministisch, wenn für jeden möglichen Zustand und für alle möglichen Eingabewerte **jederzeit der nächste Zustand und die Ausgabewerte definiert** sind.

Insbesondere race conditions können dazu führen, dass der nächste Zustand davon abhängt, 'wer das Rennen gewonnen hat und wie gross die Bestzeit ist', d.h. der nächste Zustand ist nicht klar bestimmt.

⇒ Nicht mehr deterministisch und nicht mehr echtzeitauglich

2.5 Auslastung (utilization)

Die (CPU-) Auslastung (utilization) ist der Prozentsatz der Zeit, zu der die XPU **nützliche (non-idle) Aufgaben** ausführt.

2.5.1 Berechnungen zur Auslastung (utilization)

Annahmen:

- System mit $n \geq 1$ periodischen Tasks T_i und Periode p_i
- Jeder Task T_i hat bekannte / geschätzte maximale (worst case) execution time e_i

Auslastungsfaktor eines Tasks

$$u_i = \frac{e_i}{p_i}$$

⇒ utilization factor

Gesamtauslastung des Systems

$$U = \sum_{i=1}^n u_i = \sum_{i=1}^n \frac{e_i}{p_i}$$

⇒ utilization

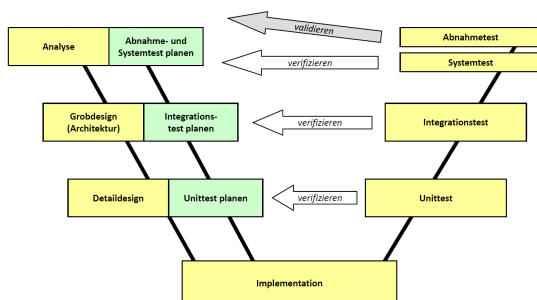
⇒ Bei 69 % Auslastung ist das 'theoretical limit'

2.6 Real-time Scheduling

- Alle kritischen Zeiteinschränkungen (deadlines, response time) sollen eingehalten werden
- Im Notfall muss der Scheduling Algorithmus entscheiden, um die kritischsten Tasks einhalten zu können.
 - Unter Umständen müssen dabei Deadlines von weniger kritischen Tasks verletzt werden.

3 Modellierung eines Embedded Systems

3.1 V-Modell für Software-Entwicklungszyklus



⇒ Nur Anforderungen (requirements) definieren, welche man auch testen kann!

3.2 Model Driven Development (MDD)

- Bei **modellbasierter Entwicklung** kommen in **allen Entwicklungsphasen** durchgängig Modelle zur Anwendung

- MDD geht davon aus, dass aus formalen Modellen lauffähige Software erzeugt wird ⇒ Codegeneratoren
 - Modelle werden traditionell als Werkzeug der Dokumentation angesehen
 - Unter Umständen wird zweimal dasselbe beschrieben (Code und Diagramm)
- ⇒ **unbedingt zu vermeiden!**

3.3 Vorgehen bei der Modellierung

1. **Systemgrenze definieren**
 - Kontextdiagramm: Use-Case-Diagramm
 - Kontextdiagramm: Sequenzdiagramm
2. **Systemprozess finden**
 - Kontextdiagramm: Use-Case-Diagramm
 - Kontextdiagramm: Sequenzdiagramm
3. **Verteilungen festlegen**
 - Verteilungsdiagramm (deployment diagram)
4. **Systemprozesse detaillieren**
 - Umgangssprachlicher Text
 - Sequenzdiagramm
 - Aktivitätsdiagramm
 - Statecharts
 - Code (C, C++, ...)

Strukturmodellierung (Statische Aspekte)

Modellierung der dynamischen Aspekte

3.4 Systemgrenze definieren & Systemprozesse finden

3.4.1 Systemgrenze definieren

Die Festlegung der Systemgrenze ist das Wichtigste und Allererste bei sämtlichen Systemen!

Man sollte sich die folgenden Fragen stellen und diese beantworten:

- Was macht das System, d.h. was liegt innerhalb der Systemgrenze?
 - Was macht das System **nicht**?
- Mit welchen Teilen ausserhalb des Systems kommuniziert das System?
- Welches sind die Schnittstellen zu den Nachbarsystemen (Umsystemen, peripheren Systemen)?

3.4.2 Systemprozesse finden (use-cases)

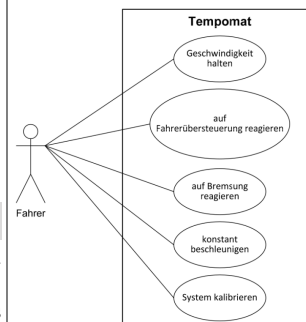
Da man sich noch immer in der **Analyse** befindet, sollen nur die **Anforderungen** definiert werden. Die Umsetzung ist Teil des Designs!

Um die Use-Cases zu identifizieren, sollte folgendes beachtet werden:

- Aussenbetrachtung des Systems (**oberflächlich!**)
 - Nicht komplizierter als nötig
- System als Blackbox betrachten
 - **Was** soll System können; (nicht: wie soll das System etwas machen)
- RTE-Systeme bestehen häufig aus nur einem einzigen Systemprozess
 - speziell wenn System 'nur' ein Regler ist

3.4.3 Kontextdiagramm: Use-Case Diagramm

Tempomat: zu detailliert



Tempomat: verbesserte Version



3.4.4 Kontextdiagramm: Sequenzdiagramm

- Speziell bei Systemen, deren Grenzen durch **Nachrichtenflüsse** charakterisiert werden können
- Details zu Sequenzdiagrammen siehe Abschnitt 3.6.1

3.5 Verteilungen festlegen

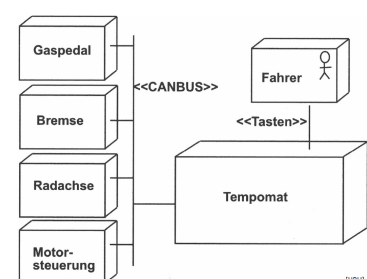
- Bei Embedded Systems werden häufig **mehrere Rechnersysteme** verwendet, um die verschiedenen Aufgaben zu erledigen
- Rechner sind örtlich verteilt und mittels Kommunikationskanal verbunden
 - ⇒ **Verteilte Systeme (distributed systems)**

3.5.1 Verteilungsdiagramm

Knoten: Darstellung der örtlichen Verteilung der Systeme
Knoten können auch hierarchisch aufgebaut sein

Linien: Physikalische Verbindungen der Knoten (Netzwerke, Kabel, Wireless, etc.)

Beispiel: Tempomat

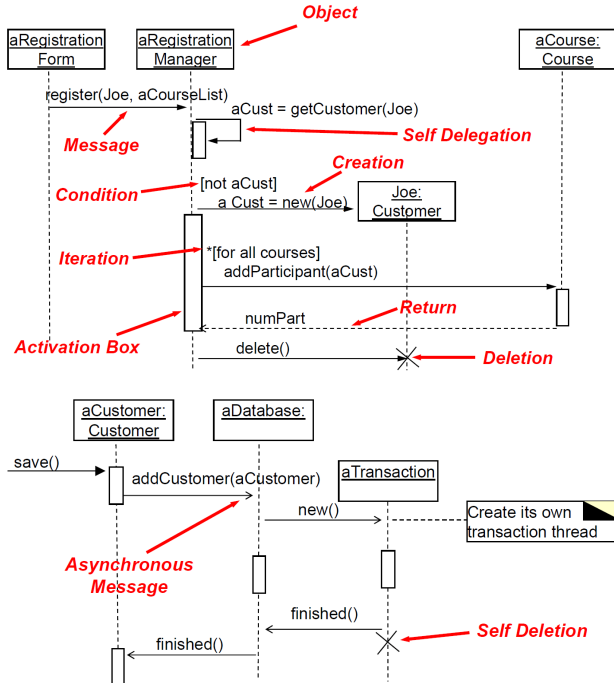


3.6 Systemprozesse detaillieren

- Die gefundenen Systemprozesse (use-cases) müssen genauer spezifiziert werden
 - Nicht detaillierter spezifizieren als sinnvoll / gefordert!**
 - Jede weitere Spezifizierung soll einen 'added value' liefern
- Verschiedene Detaillierungsstufen für verschiedene Zielgruppen
 - Auftraggeber: Überblick (z.B. in Form von Umgangssprachlichem Text)
 - Systementwickler: 'Normale Sicht' enthält mehr Details

3.6.1 Sequenzdiagramm

- Gute Darstellung für **Austausch von Meldungen** zwischen Objekten innerhalb einer **beschränkten Zeitdauer**
 - Nachrichtenflüsse
 - Kommunikationsprotokolle
- Ideal für...
 - kurze Zeitdauer
 - wenige Objekte
 - wenige Verschachtelungen
 - wenige Verzweigungen



Pfeiltyp	Semantik
	Synchrone Aufrufe
	Asynchrone Nachrichten
	Datenfluss

- Beim Zeichnen von Hand unbedingt die **Pfeilkonventionen** beachten!
- Diagramme generell nicht 'überladen'

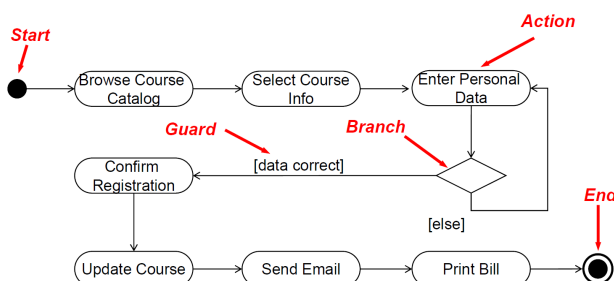
3.6.2 Kommunikationsdiagramm (Kollaborationsdiagramm)

- Kommunikationsdiagramm zeigt **dieselbe Information** wie Sequenzdiagramm
- Schwerpunkt: Informationsfluss** zwischen den Objekten
 - Beim Sequenzdiagramm liegt der Schwerpunkt auf dem zeitlichen Ablauf



3.6.3 Aktivitätsdiagramm

- Gut geeignet für ...
 - workflow modelling**
 - Sequenzielle Abläufe
 - Prozess- und Steuerfluss
 - Gleichzeitige Prozesse (fork, join)
- Weniger geeignet für ...
 - komplexe logische Bedingungen



4 Hardware-Software-Codesign

4.1 Ziele

- Entwurf (Design) **so lange wie sinnvoll** (nicht so lange wie möglich) **lösungsneutral**
- Systemdesign fördern**, statt separate Designs für Mechanik, Elektronik, Firmware, Software, etc., die sich unter Umständen auch widersprechen können
- Systemspezifikation erfolgt idealerweise mit Hilfe einer **eindeutigen Spezifikationssprache**, nicht in Prosa
- Die Spezifikation sollte simuliert (ausgeführt) werden können
- Implementationen können einfach geändert werden: HW ↔ SW
- Zielplattformen: diskrete Elektronik, ASIC, μ C, DSP, **FPGA**, Software

4.2 Anforderungen für praktische Anwendungen

- Methoden / Tools sollten beim Systemdesign nicht zu fachlastig sein
 - Methoden sollten für Elektronik-, Firmware- und wenn möglich auch Mechanik-entwickler anwendbar sein
- Wenn möglich gute Toolunterstützung
- (Automatische Synthese aus dem Modell)

4.3 Spezifikationssprachen

- Formale Sprachen sind eindeutig** (Prosa immer mehrdeutig)
- Spezifikation kann kompiliert und ausgeführt werden ⇒ Simulationen
- Die ausführbare Spezifikation dient als **Golden Reference** für die künftigen Entwicklungsschritte

Beispiele für Spezifikationssprachen

- SystemC (eine C++-Template Library)
- SysML
- SpecC
- SystemVerilog
- Esterel
- Matlab/Simulink
- Statecharts

4.4 Virtuelle Prototypen

- Die Simulation des Systems kann unterschiedlich stark detailliert werden
- Die simulierten Systeme sind Virtuelle Prototypen**
- Während der Entwicklung können einzelne (virtuelle) Teile des Prototyps laufend durch physische Teile ersetzt werden

4.5 X-in-the-loop

- Model-in-the-Loop (MIL):** vollständig als Modell vorliegender virtueller Prototyp
- Je mehr der Prototyp durch konkretere Implementationen ersetzt wird, spricht man von
 - Software-in-the loop (SIL)
 - Processor-in-the loop (PIL)
 - Hardware-in-the loop (HIL)

⇒ Test outputs werden jeweils mit **Golden Reference** verglichen



4.6 Entwicklungsplattformen

Als Entwicklungsplattformen eignen sich häufig **FPGA basierte Systeme**.

- Hardware mit VHDL
- Software/Firmware in C/C++
 - auf integriertem µC (z.B. Zynq von AMD/Xilinx) (Hard core)
 - auf Soft Core innerhalb FPGA (z.B. Nios II von Intel/Altera)

5 Zustandsbasierte Systeme

5.1 Asynchrone vs. synchrone FSM

- **Asynchron**
 - geänderte Inputsignale führen **direkt** zur Zustandsänderung
 - schneller, aber enorm anfällig auf Glitches
- **Synchron**
 - Inputsignale werden nur zu diskreten Zeitpunkten betrachtet ⇒ getaktete Systeme
- Softwareimplementationen sind eigentlich immer **synchron**, da Rechner getaktet sind
 - Rein softwareseitig besteht die Problematik der Asynchronizität nicht

5.2 Finite State Machines (FSM)



Eine FSM besitzt die folgenden Eigenschaften:

- Eine FSM befindet sich immer in einem **definierten Zustand**
- Die **Inputs X** bezeichnen üblicherweise **Ereignisse (Events)**
- Die **Outputs Y** werden oft auch **Actions** genannt
- Eine FSM benötigt immer **Speicherelemente** zur Speicherung des internen Zustands
 - Eine FSM ist ein sequenzielles und kein kombinatorisches System

Eine FSM kann auf zwei Arten dargestellt werden:

- State-Event-Diagramm
- Zustandstabelle

5.2.1 Mealy-Automat

- Nächster Zustand Z_{n+1} abhängig vom Input X und vom internen Zustand Z_n
 - $Z_{n+1} = f(Z_n, X)$
- Output Y ist abhängig vom internen Zustand Z_n **und vom Input X**
 - $Y = g(Z_n, X)$
- Actions liegen bei den Transitionen

5.2.2 Moore-Automat

- Nächster Zustand Z_{n+1} abhängig vom Input X und vom internen Zustand Z_n
 - $Z_{n+1} = f(Z_n, X)$
- Output Y ist **nur** abhängig vom internen Zustand Z_n
 - $Y = g(Z_n)$
- Actions liegen bei den Zuständen

⇒ Wenn immer möglich sollten Moore-Automaten verwendet werden

5.2.3 Medvedev-Automat

- Nächster Zustand Z_{n+1} abhängig vom Input X und vom internen Zustand Z_n
 - $Z_{n+1} = f(Z_n, X)$
- Output Y entspricht **entspricht direkt** internem Zustand Z_n
 - $Y = Z_n$
- Actions liegen bei den Zuständen

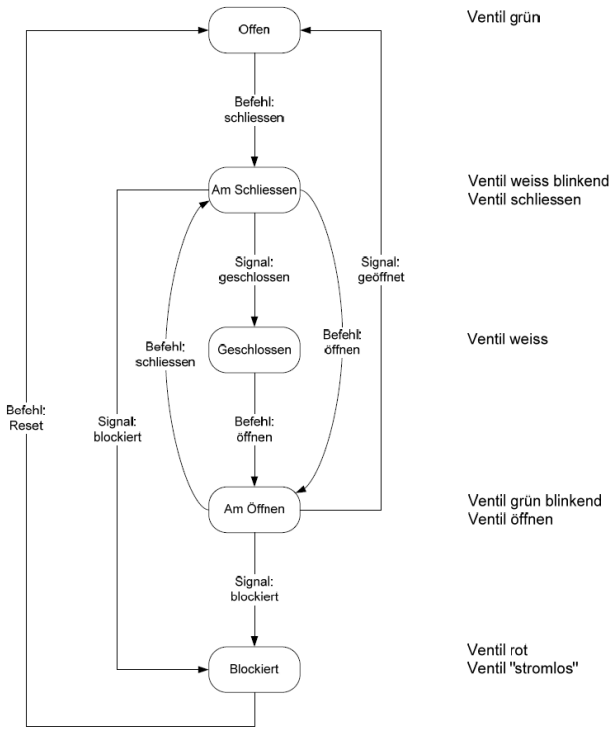
⇒ Wird hier nicht weiter behandelt...

5.3 State-Event-Diagramm (Zustandsdiagramm)

Ein State-Event-Diagramm ist eine grafische Möglichkeit, um eine FSM zu beschreiben. In einem State-Event-Diagramm gelten folgende Darstellungsformen

- **Zustände** werden mit einem **Kreis** gezeichnet
- **Ereignisse** werden mit **Pfeilen** zwischen Zuständen dargestellt (**Transitionen**)
- **Aktionen** werden entweder bei Zuständen oder bei Transitionen geschrieben (je nach Automatentyp)
- Ausführung einer Transition ist unendlich schneller
 - ⇒ Bei Modellierung sind Zwischenzustäde vorgehesen, z.B. 'closing', starting up'

Beispiel: State-Event-Diagramm – Moore Automat



5.4 Zustandstabelle

Nebst der grafischen Darstellung einer FSM mittels State-Event-Diagramm kann die FSM auch tabellarisch mittels Zustandstabelle beschrieben werden.

Beispiel: Zustandstabelle für Elektromotor

Momentaner Zustand	Ereignis	Nächster Zustand	Aktionen
AUS	EIN-Taste	Hochlaufen	Motor ausschalten Kühlung ausschalten Grüne Lampe aus Rote Lampe aus
Hochlaufen	Drehzahl_erreicht Signal	Drehzahl_ok	Motor einschalten Kühlung einschalten
	Aus-Taste	AUS	
	Wasserkühlung Störung	Störung	
Drehzahl_ok	Wasserkühlung Störung	Störung	Grüne Lampe anzeigen
	AUS-Taste	AUS	
Störung	RESET-Taste	AUS	Motor ausschalten Kühlung ausschalten Rote Lampe anzeigen

6 Statecharts

6.1 Nachteile von State-Event-Diagrammen

- Zustandsdiagramme sind flach (es gibt keine Hierarchie) ⇒ schnell unübersichtlich
- Es kann keine zeitliche Parallelität modelliert werden

6.2 Definitionen

6.2.1 Elemehte der Statecharts

6.3 Hierarchie

6.4 Default-State

6.5 History

6.5.1 Shallow History

6.5.2 Deep History

6.6 Parallelität

6.7 Timers

6.8 Beispiel – Armbanduhr als Statechart