

Echtzeitsysteme

Einleitung

Lehrstuhl Informatik 4

17. Oktober 2011

Gliederung

- 1 Historischer Bezug
 - Das erste Echtzeitrechensystem
 - SAGE – Der Nachfolger
 - Heutige Echtzeitsysteme
- 2 Echtzeitbetrieb
 - Definition
 - Realzeitbetrieb
 - Termine
 - Deterministische Ausführung
- 3 Aufbau und Abgrenzung
 - Struktur dieser Vorlesung
 - Fokus: Rechtzeitigkeit
- 4 Zusammenfassung

Whirlwind I

Das erste Echtzeitrechensystem

Zweck: Flugsimulator
(Ausbildung von Bomberbesatzungen)

Auftraggeber: U.S. Navy

Auftragnehmer: MIT

Laufzeit: 1945 – 1952



(Quelle: Alex Handy from Oakland, Nmibia)

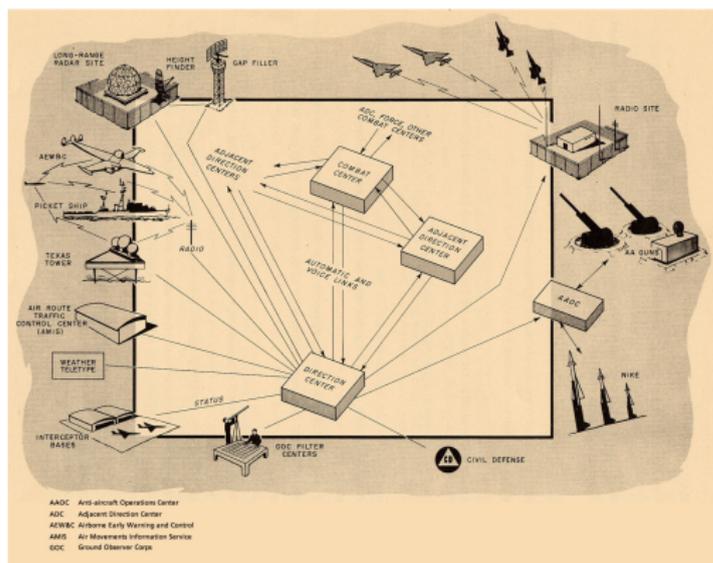
Bauweise: Digitalrechner, bit-parallele Operationen, 5000 Röhren, 11000 Halbleiterdioden, magnetischer Kernspeicher, Röhrenmonitore, Lichtgriffel

später: Nutzung durch die U.S. Air Force im SAGE

SAGE – Semi-Automatic Ground Environment

Erstes verteiltes Echtzeitrechensystem als Schöpfung des „Kalten Krieges“

Automatisiertes Kontroll- und Abwehrsystem für feindliche Bomber



- 27 Installationen
 - verteilt über die USA
 - *Nonstop*-Betrieb
 - 25 Jahre
- Kopplung durch Datenfernleitungen
 - Telefonleitungen
 - Internet-„Mutter“
- pro Installation...
 - 100 Konsolen
 - 500 KLOC Ass.

🔗 Entwicklung eines leistungsfähigeren Nachfolgers: Whirlwind II

SAGE und AN/FSQ-7 alias „Whirlwind II“

Daten AN/FSQ-7 alias „Whirlwind II“:



SAGE Bedienstation

Auftraggeber: U.S. Air Force

Auftragnehmer: MIT, später IBM

Bauweise: 55000 Röhren, 2000 m^2 , 275
Tonnen, 3 MW, 75 KIPS

(Quelle: Steve Jurvetson from Menlo Park, USA)

Betriebsdaten SAGE:

Installation: 22 - 23 Stationen im Zeitraum 1959 - 1963

Betrieb: bis 1983 (Whirlwind I bis 1979)

Nachfolgesysteme: z.B. AWACS

Kosten: 8 – 12 Milliarden \$ (1964), entspricht ca. 55 Milliarden \$ (2000)

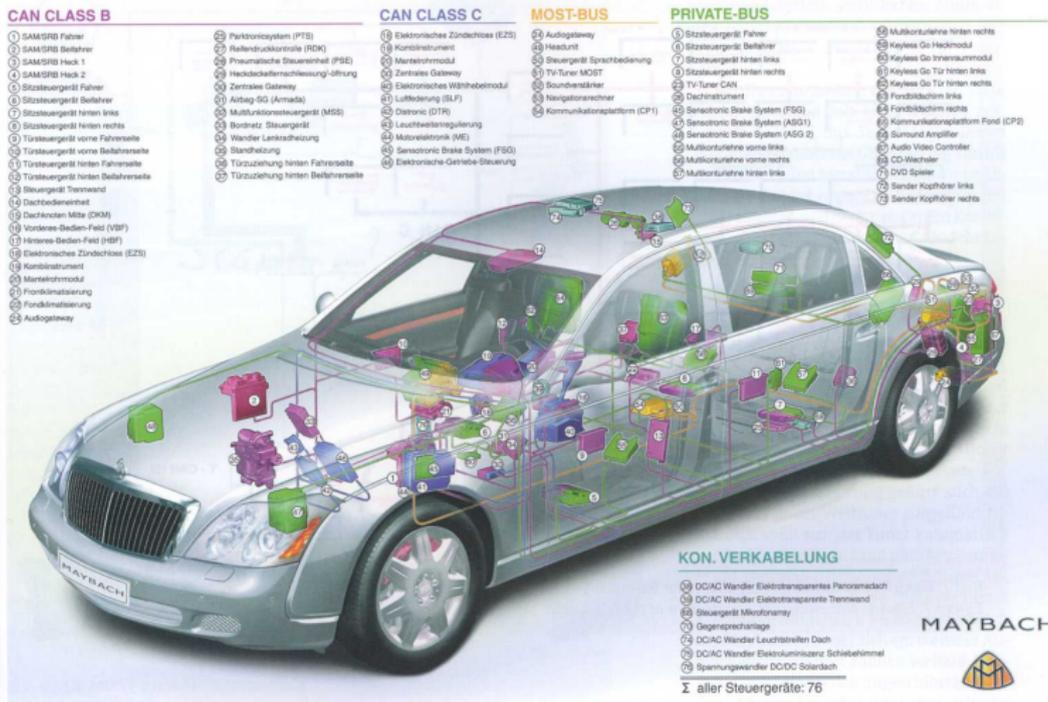
Moderne Echtzeitsysteme

Wo immer Rechensysteme mit ihrer physikalischen Umwelt interagieren ...



Spezialzweckssysteme (Forts.)

Verteiltes System auf Rädern



(Quelle: DaimlerChrysler [1])

Gliederung

- 1 Historischer Bezug
 - Das erste Echtzeitrechensystem
 - SAGE – Der Nachfolger
 - Heutige Echtzeitsysteme
- 2 **Echtzeitbetrieb**
 - Definition
 - Realzeitbetrieb
 - Termine
 - Deterministische Ausführung
- 3 Aufbau und Abgrenzung
 - Struktur dieser Vorlesung
 - Fokus: Rechtzeitigkeit
- 4 Zusammenfassung

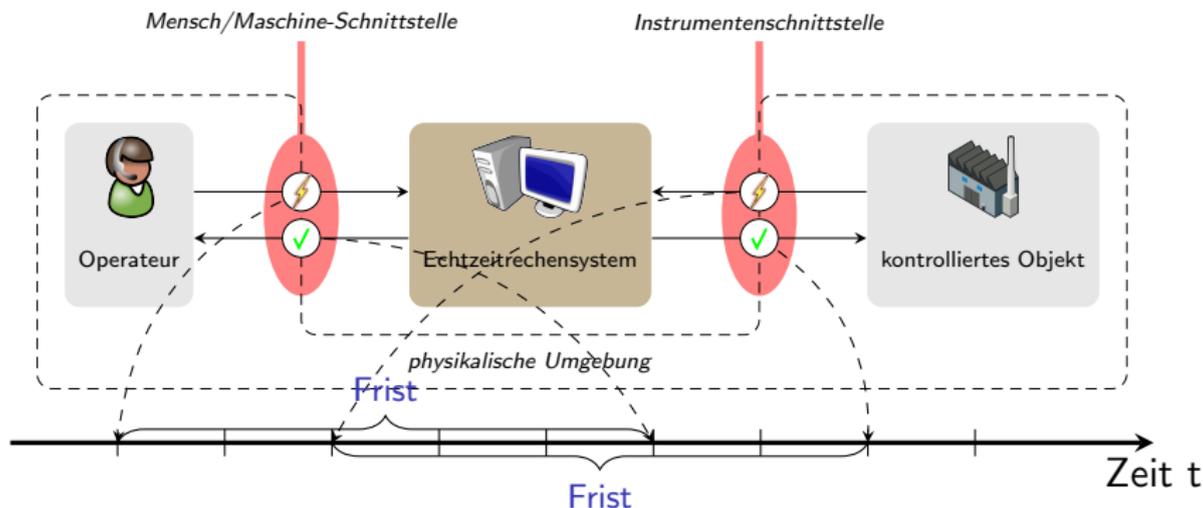
DIN 44300

Ereignis- oder zeitgesteuerte Programmverarbeitung

- *Echtzeitbetrieb ist ein Betrieb eines Rechensystems, bei dem Programme zur Verarbeitung anfallender Daten ständig betriebsbereit sind derart, dass die Verarbeitungsergebnisse innerhalb einer vorgegebenen Zeitspanne verfügbar sind.*
- *Die Daten können je nach Anwendungsfall nach einer zeitlich zufälligen Verteilung oder zu vorbestimmten Zeitpunkten anfallen.*

Komponenten eines Echtzeitsystems

Echtzeitrechnungssystem und seine Umgebung



- das Echtzeitrechnungssystem berechnet als Reaktion auf Stimuli bzw. **Ereignisse** (engl. *event*) der Umgebung **Ergebnisse**
- der Zeitpunkt, zu dem ein Ergebnis vorliegen muss, wird als **Termin** oder **Frist** (engl. *deadline*) bezeichnet

Verarbeitung von Programmen in Echtzeit

Realzeitverarbeitung (engl. *real-time processing*)

Echtzeitbetrieb bedeutet **Rechtzeitigkeit**

- korrektes Systemverhalten hängt nicht nur von den logischen Ergebnissen der Berechnungen ab
- zusätzlicher Aspekt ist der **physikalische Zeitpunkt** der Erzeugung und Verwendung der Berechnungsergebnisse
- den Rahmen stecken der Eintrittspunkt des Ereignisses und die entsprechende Frist ab

☞ Termine hängen dabei von der Anwendung ab

wenige Mikrosekunden z.B. Drehzahl- und Stromregelung bei der Ansteuerung von Elektromotoren

einige Millisekunden z.B. Multimedia-Anwendungen (Übertragung von Ton- und Bildmaterial)

Sekunden, Minuten, Stunden z.B. Prozessanlagen (Erhitzen von Wasser)

Geschwindigkeit impliziert nicht unbedingt Rechtzeitigkeit

Zuverlässige Reaktion des Rechensystems auf Umgebungsereignisse

Geschwindigkeit liefert keine Garantie, um rechtzeitig Ergebnisse von Berechnungen abliefern und Reaktionen darauf auslösen zu können

- asynchrone Programmunterbrechungen (engl. *interrupts*) können **unvorhersagbare Laufzeitvarianzen** verursachen
- schnelle Programmausführung ist bestenfalls hinreichend für die rechtzeitige Bearbeitung einer Aufgabe

Zeit ist keine intrinsische Eigenschaft des Rechensystems

- die im Rechner verwendete Zeitskala muss mit der durch die Umgebung vorgegebenen identisch sein

☞ die **Terminvorgaben** der Umgebung gelten als weich, fest oder hart

Konsequenzen überschrittener Termine

Verbindlichkeit von Terminvorgaben

weich (engl. *soft*) auch „schwach“

- das Ergebnis verliert mit zunehmender Terminüberschreitung an Wert (z.B. Bildrate bei Multimediasystemen)
- Terminverletzung ist tolerierbar

fest (engl. *firm*) auch „stark“

- das Ergebnis wird durch eine Terminüberschreitung wertlos und wird verworfen (z.B. Abgabetermin einer Übungsaufgabe)
- Terminverletzung ist tolerierbar, führt zum Arbeitsabbruch

hart (engl. *hard*) auch „strikt“

- eine Terminüberschreitung kann zum Systemversagen führen und eine „Katastrophe“ hervorrufen (z.B. Airbag)
- Terminverletzung ist keinesfalls tolerierbar

Arten von Echtzeitsystemen

Fest \longleftrightarrow Hart

fest/hart \mapsto Terminverletzung ist nicht ausgeschlossen¹

- die Terminverletzung wird vom Betriebssystem erkannt

fest \rightsquigarrow plangemäß weiterarbeiten

- das Betriebssystem bricht den Arbeitsauftrag ab
- der nächste Arbeitsauftrag wird gestartet
- ist transparent für die Anwendung

hart \rightsquigarrow sicheren Zustand finden

- das Betriebssystem löst eine **Ausnahmesituation** aus
- die Ausnahme ist **intransparent für die Anwendung**
- die **Anwendung** behandelt diese Ausnahme

¹Auch wenn Ablaufplan und Betriebssystem auf dem Blatt Papier Determinismus zeigen, kann das im Feld eingesetzte technische System von Störeinflüssen betroffen sein, die ggf. die Verletzung auch eines harten Termins nach sich ziehen.

Arten von Echtzeitsystemen (Forts.)

Radikale Unterschiede im Systementwurf zeichnen sich ab. . .

hard real-time computer system

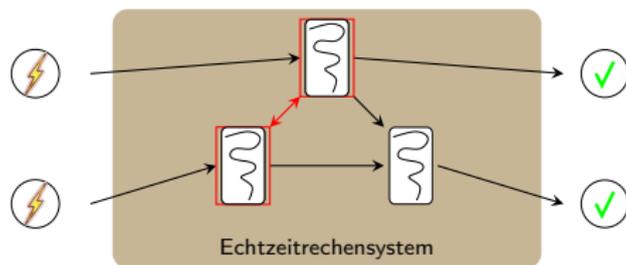
- ein Rechensystem, das mind. einen strikten Termin erreichen muss
 - garantiert unter allen (spezifizierten) Last- und Fehlerbedingungen
 - das Laufzeitverhalten ist ausnahmslos deterministisch
- typisch für ein **sicherheitskritisches Echtzeitrechensystem**
 - engl. *safety-critical real-time computer system*

soft real-time computer system

- ein Rechensystem, das keinen strikten Termin erreichen muss
- es ist erlaubt, gelegentlich Termine zu verpassen

Herausforderung: Gewährleisten von Rechtzeitigkeit

Ereignisbehandlungen müssen termingerecht abgearbeitet werden



Ereignisse aktivieren Ereignisbehandlungen

- Wie viel Zeit benötigt die Ereignisbehandlung **maximal**?
- Lösung des trivialen Falls ist (scheinbar) einfach, wenn man die **maximale Ausführungszeit** der Ereignisbehandlung kennt.

Reale Echtzeitsysteme sind **komplex**

- mehrere Ereignisbehandlungen \leadsto Konkurrenz
 - Verwaltung gemeinsamer Betriebsmittel, allen voran die CPU.
- Abhängigkeiten zwischen verschiedenen Ereignisbehandlungen

Vorhersagbarkeit des Laufzeitverhaltens

Echtzeitsysteme sind (schwach, stark oder strikt) deterministisch

Determiniertheit

Bei ein und derselben Eingabe sind verschiedene Abläufe zulässig, alle Abläufe liefern jedoch stets das gleiche Resultat.

- Transparenz von Programmunterbrechungen
 - *Interrupts verursachen* vom „normalen Ablauf“ verschiedene *ausnahmebedingte Abläufe*
 - Verzögerungen in der Programmausführung wirken sich nicht nachteilig aus
- Terminvorgaben der Umgebung werden eingehalten

Determinismus

Zu jedem Zeitpunkt ist bestimmt, wie weitergefahren wird.

Spezialzweckbetrieb

Verhalten von Echtzeitanwendungen [4, S. 25]

☞ deterministische Abarbeitung von Ereignisbehandlungen

rein zyklisch \leadsto nur periodische Ereignisbehandlungen, Abfrage-Betrieb

- nahezu konstanter Betriebsmittelbedarf von Periode zu Periode

meist zyklisch \leadsto überwiegend periodische Ereignisbehandlungen

- das System muss auf externe Ereignisse reagieren können

asynchron/vorhersagbar \leadsto kaum periodische Ereignisbehandlungen

- aufeinanderfolgende Aktivierungen können zeitlich stark variieren
- Zeitdifferenzen haben eine obere Grenze oder bekannte Statistik

asynchron/nicht vorhersagbar \leadsto aperiodische Ereignisbehandlungen

- Anwendungen reagieren auf asynchrone Ereignisse
- hohe, nicht deterministische Laufzeitkomplexität einzelner Ereignisbehandlungen

Gliederung

- 1 Historischer Bezug
 - Das erste Echtzeitrechensystem
 - SAGE – Der Nachfolger
 - Heutige Echtzeitsysteme
- 2 Echtzeitbetrieb
 - Definition
 - Realzeitbetrieb
 - Termine
 - Deterministische Ausführung
- 3 **Aufbau und Abgrenzung**
 - **Struktur dieser Vorlesung**
 - **Fokus: Rechtzeitigkeit**
- 4 Zusammenfassung

Aufbau der Vorlesung

Orientiert sich vor allem

- an der Ausprägung des Spezialzweckbetriebs ...
- und den Eigenschaften der Ereignisse und ihrer Behandlungen,
- blickt aber auch über den Tellerrand.

Einleitung

Grundlagen

vorranggesteuerte
Systeme

taktgesteuerte
Systeme

Analyse

periodische Echtzeitsysteme

nicht-periodische Echtzeitsysteme

Rangfolge

Zugriffskontrolle

Exkurs: nicht-blockierende Synchronisation

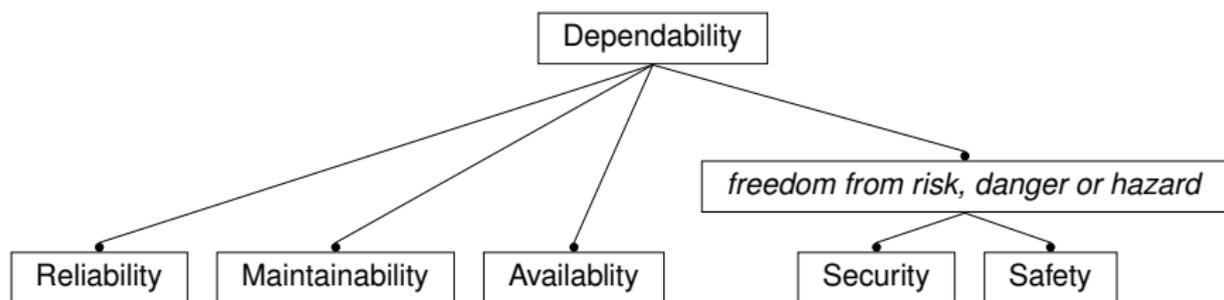
verteilte Echtzeitsysteme

Exkurs: WCET-Analyse

Zusammenfassung und Ausblick

Verlässlichkeit (engl. *dependability*)

Echtzeitsysteme sind häufig **sicherheitskritische Systeme** und erfordern ein hohes Maß an **Verlässlichkeit**. Verlässlichkeit selbst hat viele Gesichter ...



The trustworthiness of a computing system which allows reliance to be justifiably placed on the service it delivers. [3]

Zuverlässigkeit (engl. *reliability*)

Mittlere Betriebsdauer

- $R(t)$ die Wahrscheinlichkeit, dass ein System seinen Dienst bis zum Zeitpunkt t leisten wird, sofern es bei $t = t_0$ betriebsbereit war
- Annahme: eine **konstante Fehlerrate** von λ Fehler/Stunde
 - Zuverlässigkeit zum Zeitpunkt t : $R(t) = \exp(-\lambda(t - t_0))$
 - mit $t - t_0$ gegeben in Stunden
 - Inverse der Fehlerrate $1/\lambda$ ist die *mean time to failure* (MTTF)

ultra-hohe Zuverlässigkeit wenn $\lambda \leq 10^{-9}$ Fehler/Stunde gefordert ist

- Beispiel: elektronisch gesteuerte Bremsanlage im Automobil
 - das Kfz sei durchschnittlich eine Stunde täglich in Betrieb
 - dann darf jährlich nur ein Fehler pro eine Million Kfz auftreten
- andere Beispiele sind Eisenbahnsignalanlagen, Kernkraftwerk- und Flugüberwachungssysteme

Wartbarkeit (engl. *maintainability*)

Mittlere Reparaturdauer

- $M(d)$ die Wahrscheinlichkeit, dass das System innerhalb Zeitspanne d nach einem reparierbaren (gutartigen) Fehler wieder hergestellt ist
- Ansatz: **konstante Reparaturrate** von μ Reparaturen/Stunde
 - die Inverse $1/\mu$ ist dann die *mean time to repair* (MTTR)

Fundamentaler Konflikt zwischen Zuverlässigkeit und Wartbarkeit:

- ein wartbares System erfordert einen modularen Aufbau
 - kleinste ersetzbare Einheit (engl. *smallest replaceable unit*, SDU)
 - über Steckverbindungen lose gekoppelt mit anderen SDUs
 - dadurch ist jedoch eine höhere (physikalische) Fehlerrate gegeben
 - darüberhinaus verbuchen sich höhere Herstellungskosten
- ein zuverlässiges System ist aus einem Guss gefertigt. . .

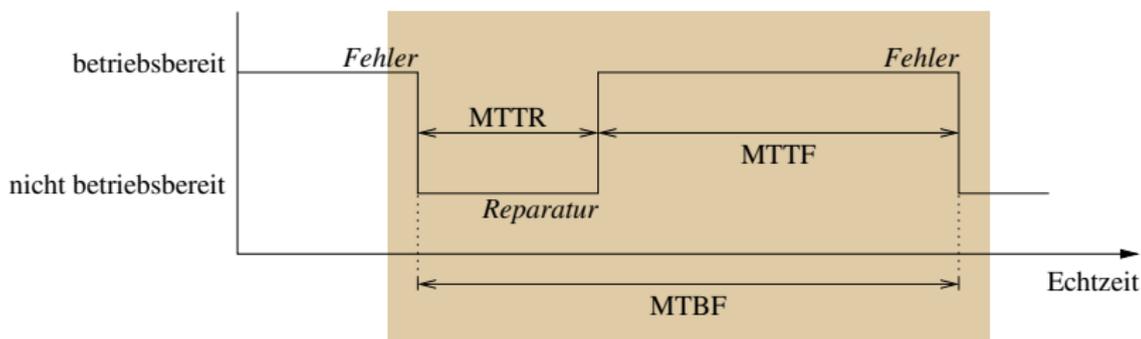
Beim Entwurf von Produkten für den Massenmarkt geht die Zuverlässigkeit meist auf Kosten von Wartbarkeit.

Verfügbarkeit (engl. *availability*)

MTTF und MTTR im Zusammenhang

Maß zur Bereitstellung einer Funktion vor dem Hintergrund eines abwechselnd korrekt und fehlerhaft arbeitenden Systems

- Zeitanteil der **Betriebsbereitschaft**: $A = MTTF / (MTTF + MTTR)$
- $MTTF + MTTR$ auch kurz: *mean time between failures* (MTBF)



☞ hohe Verfügbarkeit bedeutet kurze MTTR und/oder lange MTTF

Sicherheit \mapsto *Security* und *Safety*

Robustheit des Echtzeitrechnensystems stärken

security Schutz von Informationen und Informationsverarbeitung vor „intelligenten“ Angreifern

- allgemein in Bezug auf **Datenbasen** des Echtzeitsystems
 - Vertraulichkeit (engl. *confidentiality*)
 - Datenschutz (engl. *privacy*)
 - Glaubwürdigkeit (engl. *authenticity*)
- speziell z.B. Diebstahlsicherung: Zündungssperre im Kfz
 - Kryptographie (engl. *cryptography*)

safety Schutz von Menschen und Sachwerten vor dem Versagen technischer Systeme

- Zuverlässigkeit trotz **bösartigen** (engl. *malign*) **Fehlerfall**
 - Kosten liegen um Größenordnungen über den Normalbetrieb
- Abgrenzung von unkrit., gutartigen (engl. *benign*) Fehlern
- oft ist Zertifizierung (engl. *certification*) erforderlich

Verlässlichkeit ↔ Komplexität

Automobil eine Bestandsaufnahme vom Jahr 2005 ...

- etwa 90 % der Innovationen im Auto bringt die Elektronik ein
 - gut 80 % davon sind Software
- etwa ein Drittel aller Pannen liegen an fehlerhafte Elektronik
 - gut 80 % davon sind Softwarefehler

Everything should be made as simple as possible, but no simpler. (Albert Einstein)

You know you have achieved perfection in design, not when you have nothing more to add, but when you have nothing more to take away. (Antoine de Saint Exupery)

Abgrenzung

Zusammenspiel von Rechtzeitigkeit und Verlässlichkeit

Verlässlichkeit **erfordert** Rechtzeitigkeit!

- Verpasste Termine stellen Fehler dar.
- Diese Fehler müssen ggf. erkannt oder maskiert werden.

Andererseits: Rechtzeitigkeit **erfordert** Verlässlichkeit!

- Fehler können zum Verpassen eines Termins führen.
- Maskieren solcher Fehler hilft, die Rechtzeitigkeit zu gewährleisten.

 Betrachtung der Rechtzeitigkeit unter Annahme des *fehlerfreien Falls*

- Verletzte Termine werden auf einer höheren Ebene behandelt.
- Toleranz gegenüber Fehlern dient der Verlässlichkeit.
 - Entsprechende Maßnahmen zum Erreichen von Fehlertoleranz werden also nicht durch harte Termine impliziert.

 Harte Echtzeitsysteme sind häufig auch äußerst verlässlich.

;-)

Gliederung

- 1 Historischer Bezug
 - Das erste Echtzeitrechensystem
 - SAGE – Der Nachfolger
 - Heutige Echtzeitsysteme
- 2 Echtzeitbetrieb
 - Definition
 - Realzeitbetrieb
 - Termine
 - Deterministische Ausführung
- 3 Aufbau und Abgrenzung
 - Struktur dieser Vorlesung
 - Fokus: Rechtzeitigkeit
- 4 Zusammenfassung

Resümee

Echtzeitbetrieb eines Rechensystems in seiner Umgebung

- Komponenten eines Echtzeitsystems:
 - Operateur, Echtzeitrechensystem, kontrolliertes Objekt
- Verhalten von Echtzeitanwendungen:
 - rein/meist zyklisch
 - asynchron und irgendwie/nicht vorhersagbar
- schwache, starke oder strikte Echtzeitbedingungen

Abgrenzung Fokus dieser Vorlesung liegt auf der **Rechtzeitigkeit**

- Rechtzeitigkeit und Verlässlichkeit bedingen sich oft gegenseitig
- Maßnahmen zu ihrem Erreichen sind grundverschieden:
 - Verlässlichkeit \rightsquigarrow Robustheit durch Fehlertoleranz
 - Rechtzeitigkeit \rightsquigarrow deterministisches Ablaufverhalten

Literaturverzeichnis

- [1] DAIMLERCHRYSLER AG:
Der neue Maybach.
In: *ATZ/MTZ Sonderheft* (2002), Sept., S. 125
- [2] DEUTSCHES INSTITUT FÜR NORMUNG:
DIN 44300: Informationsverarbeitung — Begriffe.
Berlin, Köln : Beuth-Verlag, 1985
- [3] IFIP:
Working Group 10.4 on Dependable Computing and Fault Tolerance.
<http://www.dependability.org/wg10.4>, 2003
- [4] LIU, J. W. S.:
Real-Time Systems.
Prentice-Hall, Inc., 2000. –
ISBN 0-13-099651-3