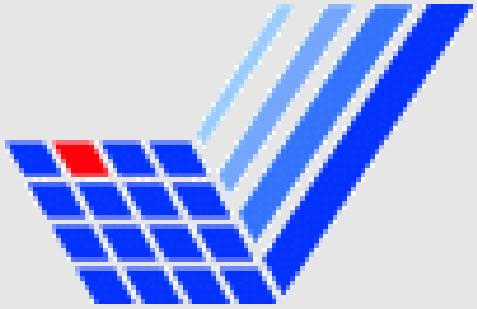
Verteilte Echtzeitsysteme

Sabrina Hecke

sabrina.hecke@uni-dortmund.de

PG AutoLab
Seminarwochenende 21.-23. Oktober 2007



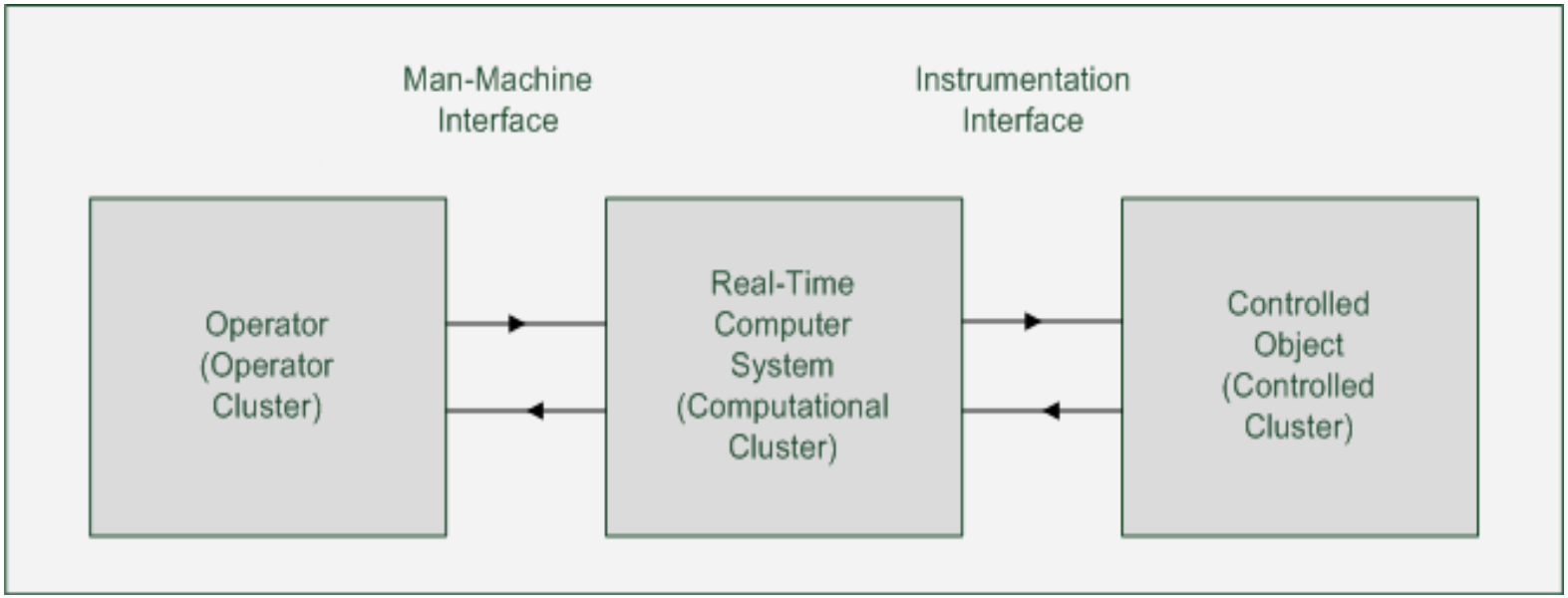
Überblick

- Was sind Echtzeitsysteme?
  - Real Time Task
  - Scheduling
- Verteilte Echtzeitsysteme
- Systemarchitektur
- Echtzeitkommunikationssysteme
  - Flusskontrolle
  - Protokolle
- Fehlertolerante Systeme

Was sind Echtzeitsysteme ?

- Korrektes Verhalten eines Echtzeit-Computersystems abhängig von logischem Ergebnis und der Zeit
- Echtzeit-Computersystem Teil eines größeren Systems → Echtzeitsystem
- Zwei Typen von Echtzeitsystemen
  - Ereignisgesteuerte Echtzeitsysteme
  - Zeitgesteuerte Echtzeitsysteme

Was sind Echtzeitsysteme?



Was sind Echtzeitsysteme? - Echtzeittask

- Nebenläufige Tasks führen gewünschte Funktion aus
- Ausführung eines sequentiellen Programms

- Periodische Tasks
  - Wiederholte Ausführung alle T Zeiteinheiten(Periode)
- Aperiodische Tasks
  - Tritt unvorhersehbar auf
- Sporadische Tasks
  - Zeitliche Abstand zwischen zwei Ausführungen eines Tasks ist begrenzt
- Echtzeittasks besitzen Deadline

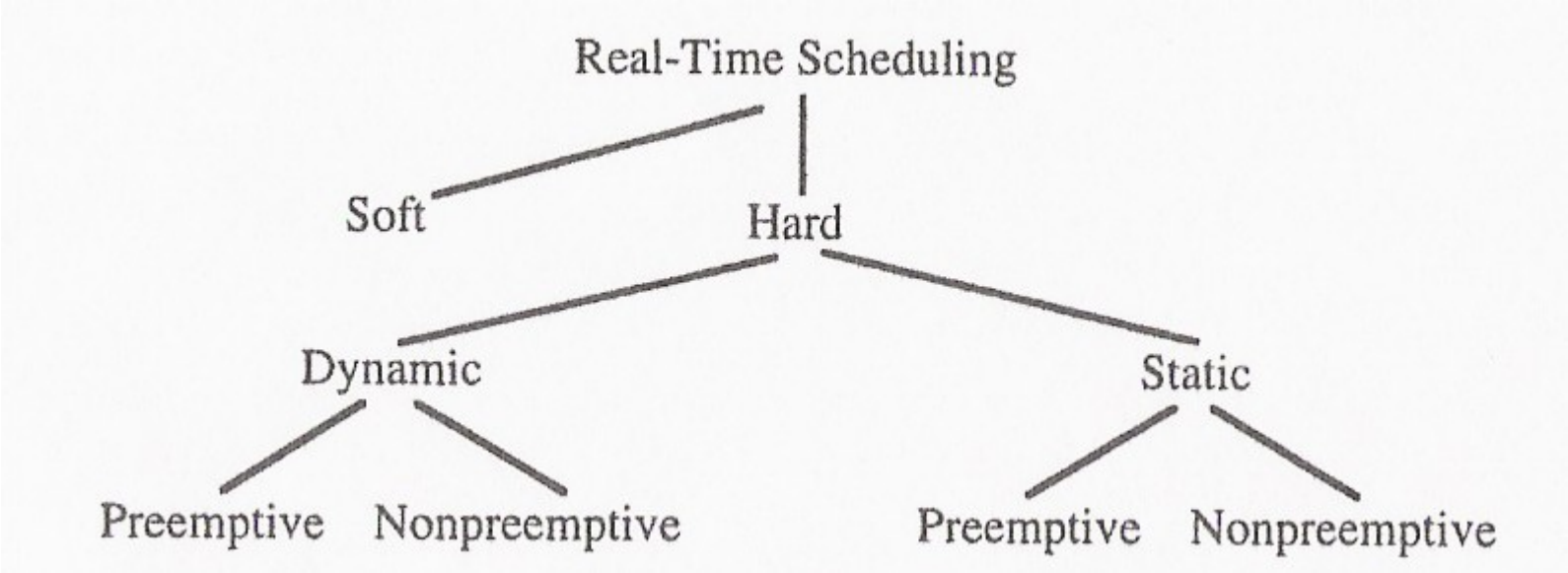
Was sind Echtzeitsysteme? - Echtzeittask

- Drei Kategorien von Echtzeittasks
  - **weich:** Das nicht Einhalten der Deadline hat keine Konsequenzen
  - **fest:** bei nicht Einhalten der Deadline hat Ergebnis keinen Nutzen mehr
  - **hart:** Das nicht Einhalten der Deadline führt zu einer Katastrophe

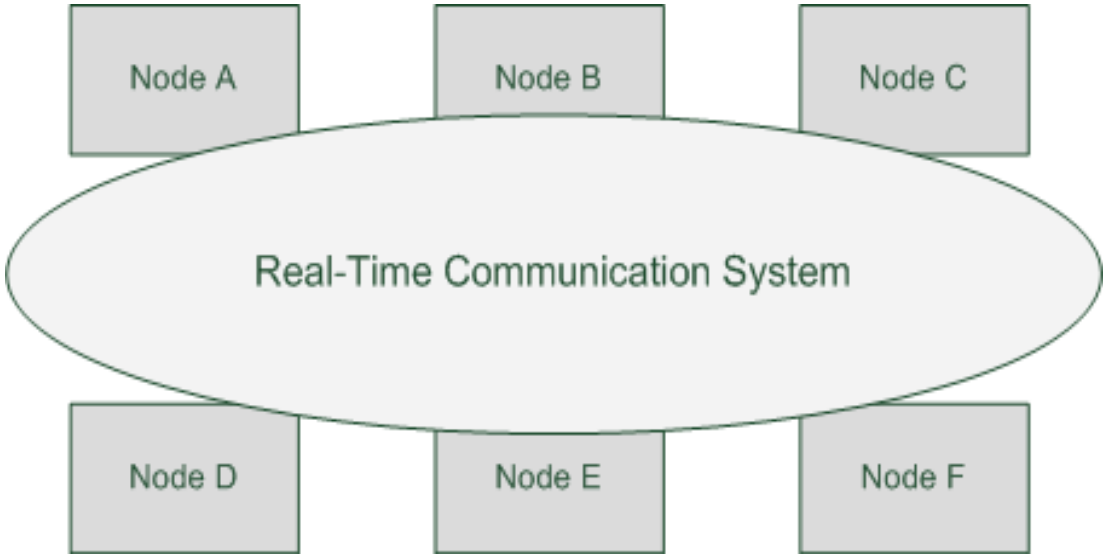
- besteht Echtzeitcomputersystem aus mind. einem harten Echtzeittask => hartes Echtzeitcomputersystem oder sicherheitskritisches Echtzeitcomputersystem
- Kein harter Echtzeittask => weiches Echtzeitcomputersystem

Was sind Echtzeitsysteme? - Scheduling

- Scheduling Problem beschäftigt sich mit Alloziierung von Ressourcen, um Zeitanforderungen der Tasks zu erfüllen



Verteilte Echtzeitsysteme



Verteilte Echtzeitsysteme

- Anforderungen
  - **Komponierbarkeit:** Kritischer Punkt bei Systemdesign ist das Integrieren der Subsysteme zu großem System. Spezifizierte und getestete Eigenschaften dürfen nicht verloren gehen.
  - **Skalierbarkeit:** System ist offen gegenüber Veränderungen und hat keine vordefinierten Einschränkungen im Bezug auf Erweiterbarkeit
  - **Zuverlässigkeit:** auftretende Fehler müssen behandelt werden → Fehlertoleranz

- Messwerte der Zuverlässigkeit (Dependability)
  - Ausfallsicherheit (Reliabality)
  - Sicherheit (Safety)
  - Wartbarkeit (Maintainability)
  - Verfügbarkeit (Availability)
  - Sicherheit (Security)

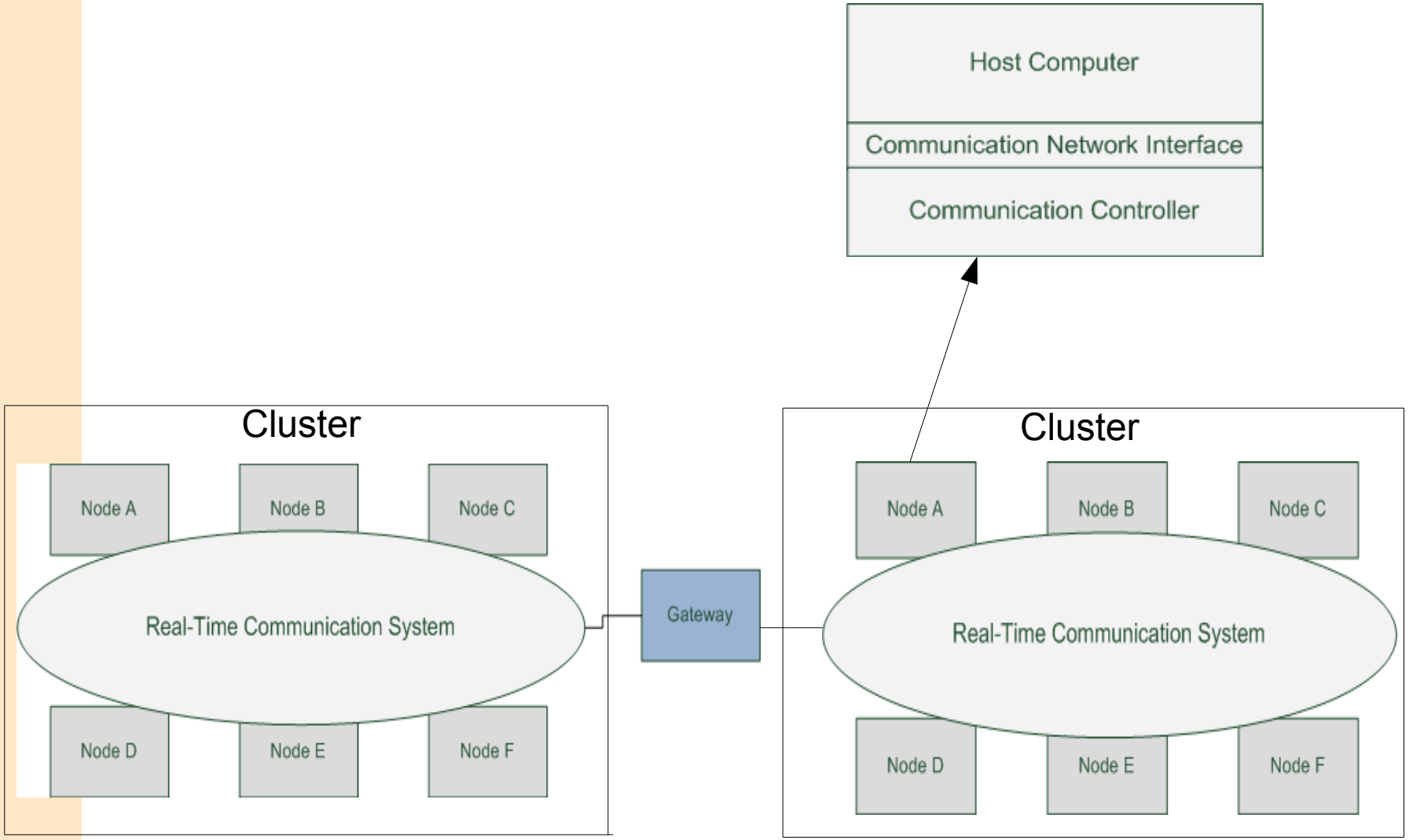
Verteilte Echtzeitsysteme

- Ausfallsicherheit
  - Ist eine Funktion $0 \leq R(t) \leq 1$, dass das System korrekt während des Intervalls $[t_0, t]$ funktioniert unter der Annahme, dass das System zum Zeitpunkt t_0 korrekt arbeitete.
- Sicherheit (Safety)
  - Wahrscheinlichkeit $0 \leq S(t) \leq 1$, dass ein System entweder korrekt arbeitet oder seine Funktion auf eine Art und Weise beendet, so dass nicht die Funktionsweise anderer Systeme gestört oder Menschen gefährdet werden.
- Verfügbarkeit
  - Wahrscheinlichkeit $0 \leq A(t) \leq 1$, dass ein System zum Zeitpunkt t korrekt arbeitet.

Verteilte Echtzeitsysteme

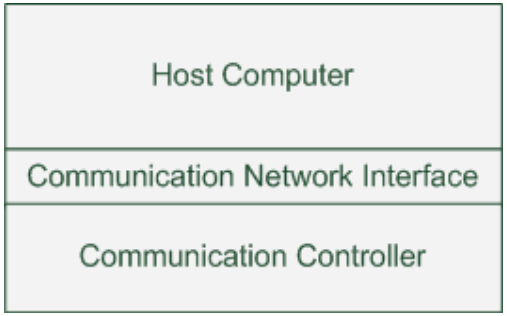
- Wartbarkeit
  - Wahrscheinlichkeit M(t), dass ein fehlerhaftes System innerhalb einer Zeitdauer t repariert werden kann.
- Sicherheit (Security)
  - Fähigkeit eines Systems in Hinblick auf Datenschutz und das Verhindern vor unautorisiertem Zugriff auf das System

Systemarchitektur



Systemarchitektur

- Knoten
  - Hardware-Software Einheit mit wohldefinierter Funktion innerhalb des verteilten Computersystems



- FTU
  - Abstraktion zur Verwirklichung von Fehlertoleranz durch Replikation
  - Besteht aus einer Menge von replizierten Knoten
- Cluster
  - Menge von FTUs
- Gateway
  - Austausch von relevanten Informationen zwischen Cluster

Echtzeitkommunikationssystem

- Flusskontrolle
  - Kontrolliert Geschwindigkeit des Informationsflusses zwischen Sender und Empfänger
- Zwei Typen von Flusskontrolle
  - Implizite Flusskontrolle
    - Es wird festgelegt,wann Nachrichten gesendet werden
    - Fehlerentdeckung beim Empfänger
  - Explizite Flusskontrolle
    - Empfänger sendet nach Erhalt der Nachricht ACK
    - Fehlerentdeckung beim Sender

Echtzeitkommunikationssystem

- Protokolle
  - Event-Triggered Protokoll
    - Protokollausführung wird durch Event beim Sender ausgeführt
    - Fehlerentdeckung liegt beim Sender
    - Benötigt explizite Flusskontrolle
  - Time Triggered Protokoll
    - Sendezeitpunkt einer Nachricht ist festgelegt
    - Fehlerentdeckung beim Empfänger

Fehlertolerante Systeme

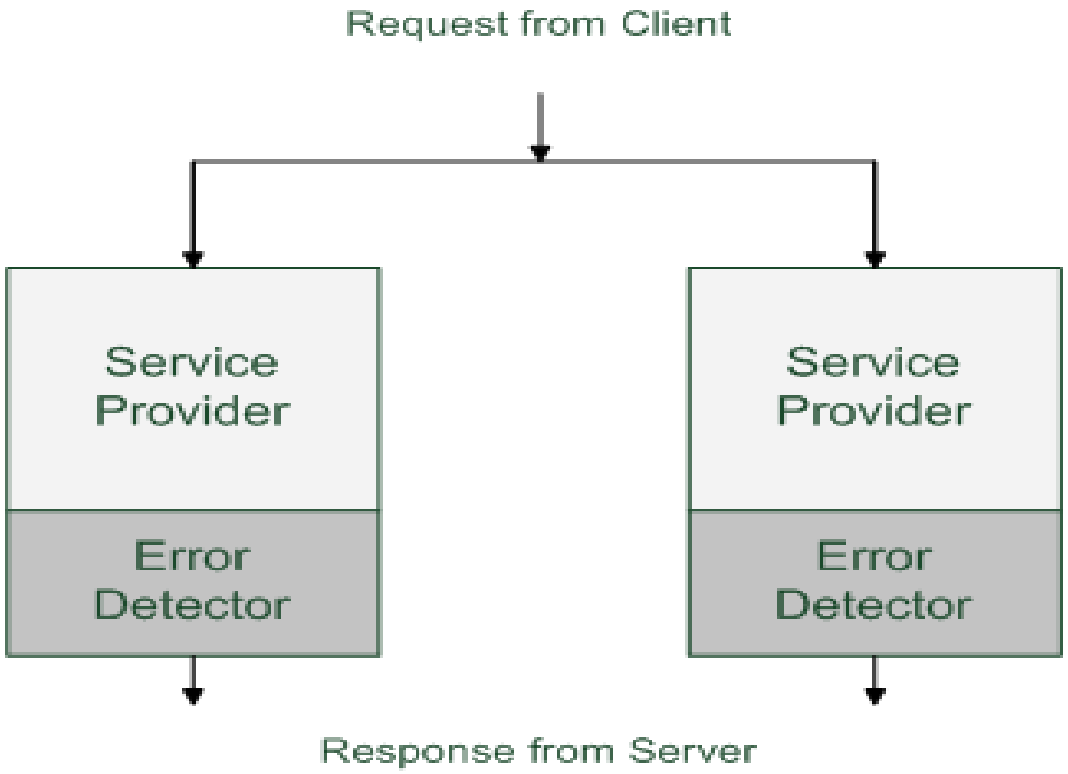
- Motivation:
  - In einem Echtzeitsystem können Fehler auftreten
    - Verlust einer Nachricht
    - Fehlerhafte Nachricht
    - Ausfall eines Knotens
- Fehlertoleranz:
  - Hard- und Software-Fehler sollten das Echtzeitsystem nicht zum Totalausfall führen

Fehlertolerante Systeme

- Fehlertoleranz wichtig, denn Komponentenfehler führen zu einer Katastrophe
- Fehlerentdeckung:
  - über festgelegte Constraints oder Wissen über das korrekte Verhalten der Berechnung
  - Vergleich von zwei redundanten Kanälen
- Fehler müssen schnell angezeigt werden
  - Schnittstelle zwischen Knoten und Kommunikationssystem wird dazu verwendet (Fault/error containment region)
- FTU (Fault-Tolerant Unit, FTU)
  - Realisiert Fehlertoleranz durch Replikation

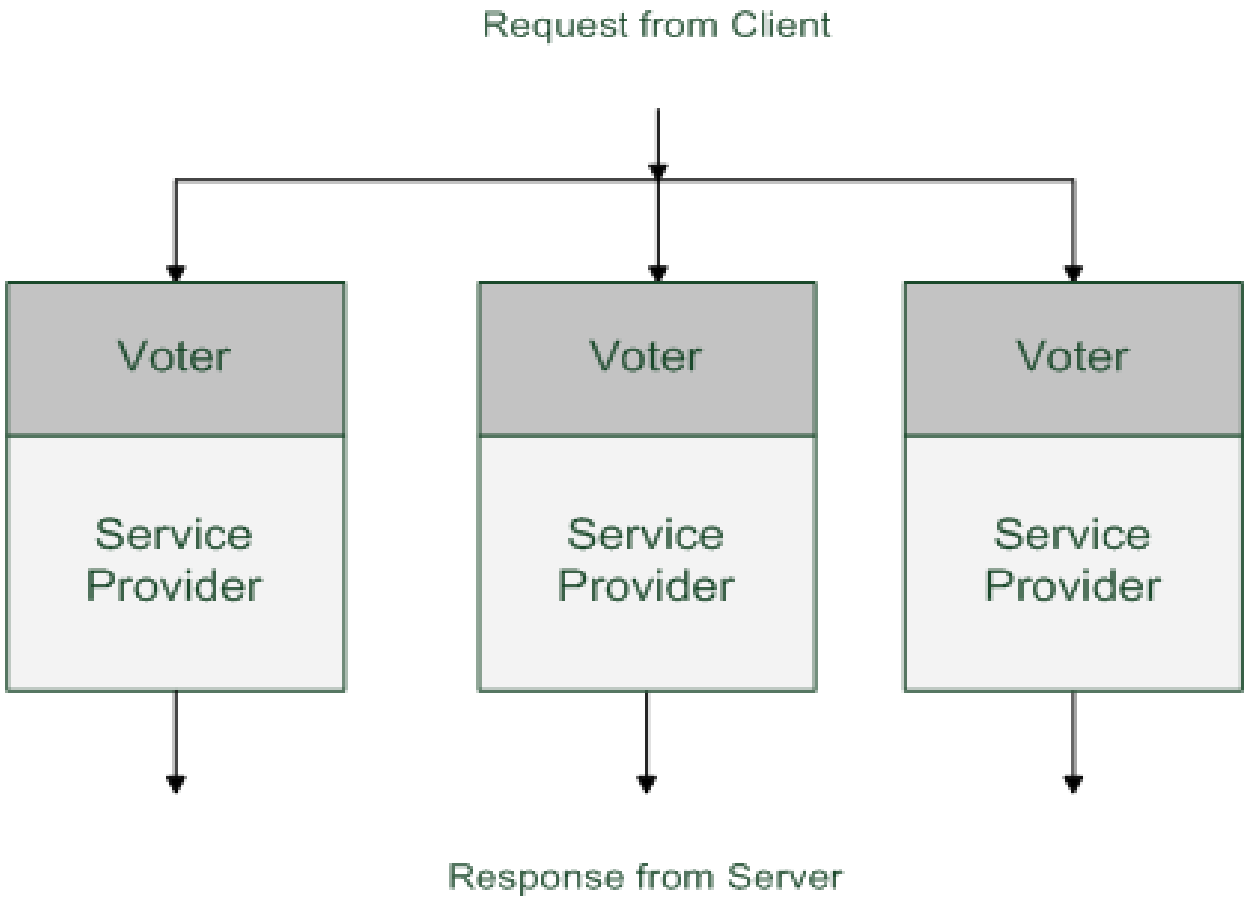
Fehlertolerante Systeme

- Fail Silent Knoten



Fehlertolerante Systeme

- Triple Modular Redundancy



Literatur

- Kopetz, H.(2001), Real-Time Systems: Design Principles for Distributed Embedded, Kluwer Academic Publishers
- Marwedel, P.(2003), Embedded System Design, Kluwer Academic Publishers