Verifikation von Spezifikationsmodellen mit Intervall-Petri-Netzen

Vesselka Duridanova
Thorsten Hummel
Olga Fengler
Wolfgang Fengler
Technische Universität Ilmenau
Institut für Theoretische und Technische Informatik
Fachgebiet Rechnerarchitektur
email: wolfgang.fengler@tu-ilmenau.de

TU Ilmenau

Gliederung

1. Motivation
2. Message Sequence Charts / Intervall-Petri-Netze
3. Formale Analyse des Intervall-Petri-Netzes
4. Anwendungsbeispiel
5. Zusammenfassung / Ausblick

Motivation

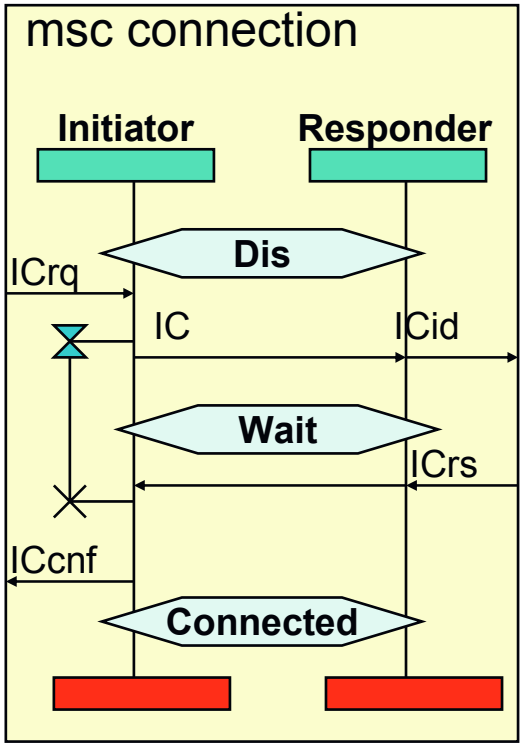
Eingebettete Systeme:

- Komplexe Hard- und Softwaresysteme
- Einhaltung harter zeitlicher Restriktionen
- Berücksichtigung in frühen Entwurfs-phasen
- Konsequente Verifikation in allen Entwurfsphasen

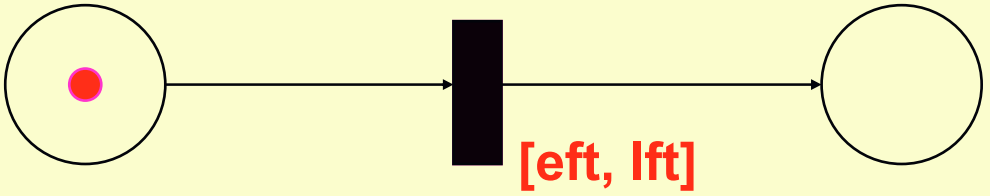
↗ Erhöhung der Entwurfsqualität, Verkürzung der Entwurfszeiten

Message Sequence Charts (MSC)

- Beschreibung von:
  - Funktionalität
  - Verhalten
  - Interaktion durch Nachrichten
- Nachrichtenaustausch meist asynchron
- Instanzen:
  - Hardware
  - Softwareprozesse
  - Benutzer
- Darstellungsdimensionen:
  - Vertikal – klassische Zeitachse
  - Horizontal – Spezifizierung der betrachteten Objekte
- Zeitbehaftete MSCs
  - Zeitkonstrukte mit Nachrichten verbunden
  - Zeitbedingungen neben Lebenslinie
  - Zeitintervalle möglich



Intervall-Petri-Netze



- Jeder Transition wird ein Zeitintervall zugeordnet, innerhalb dessen die Transition feuern kann

t[a,b] 0 <= eft<= lft **eft** → earliest firing time (Startzeit)

lft → latest firing time (Stoppzeit)

- Transition schaltfähig, wenn Startzeit erreicht
- Wenn Stoppzeit erreicht wird, gerät die Transition in Schaltzwang

Analyse von Pfaden im Erreichbarkeitsraum

- parametrische Darstellung von Transitionssequenzen
- Berechnung von optimalen Zeitparametern

Überführung von MSC in Intervall-Petri-Netze

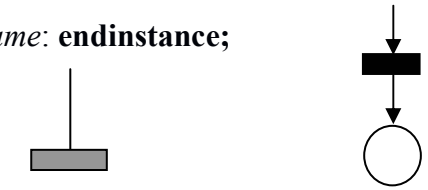
- **Vorteile**
  - Unterstützung von modularer Strukturierung
  - Vereinfachung von Hierarchiebildung
  - Vereinfachung von Analysetechniken
  - automatische Überführung und Analyse von Zeitanforderungen in MSC ohne detaillierte Kenntnisse des Petri-Netz-Formalismus
- **Nachteile**
  - IPN komplexer und unübersichtlicher

Überführung von MSC in Intervall-Petri-Netze

- Ausgangspunkt sind MSCs im Textformat nach Z.120
- Umwandlung durch einen Parser
- Übersetzung der MSC-Grundelemente in IPN-Teilnetze
- Bearbeitung der textlichen Darstellung des MSC in mehreren Durchgängen

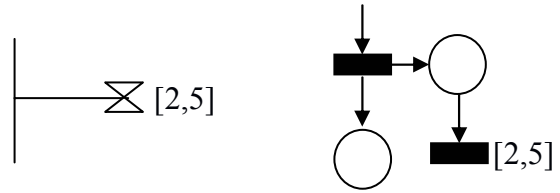
InstanzName: **instance** *Name*;

InstanzName: **endinstance;**



InstanzName: **action** ‘*Name*‘;

InstanzName: **set** *Name*, *Zeitwert*;



Analyse von Intervall-Petri-Netzen

- Verfolgung der Pfade im Erreichbarkeitsgraphen
- Analyse von Prozesseigenschaften mit vertretbarem Rechenaufwand
- Gegeben:
  - Anfangszustand
  - Transitionssequenz
- Zwei Schritte:
  - Berechnung der Folgezustände ohne Berücksichtigung der Zeitintervalle
  - Bildung von Zustandsklassen unter Berücksichtigung der Transitionsintervalle

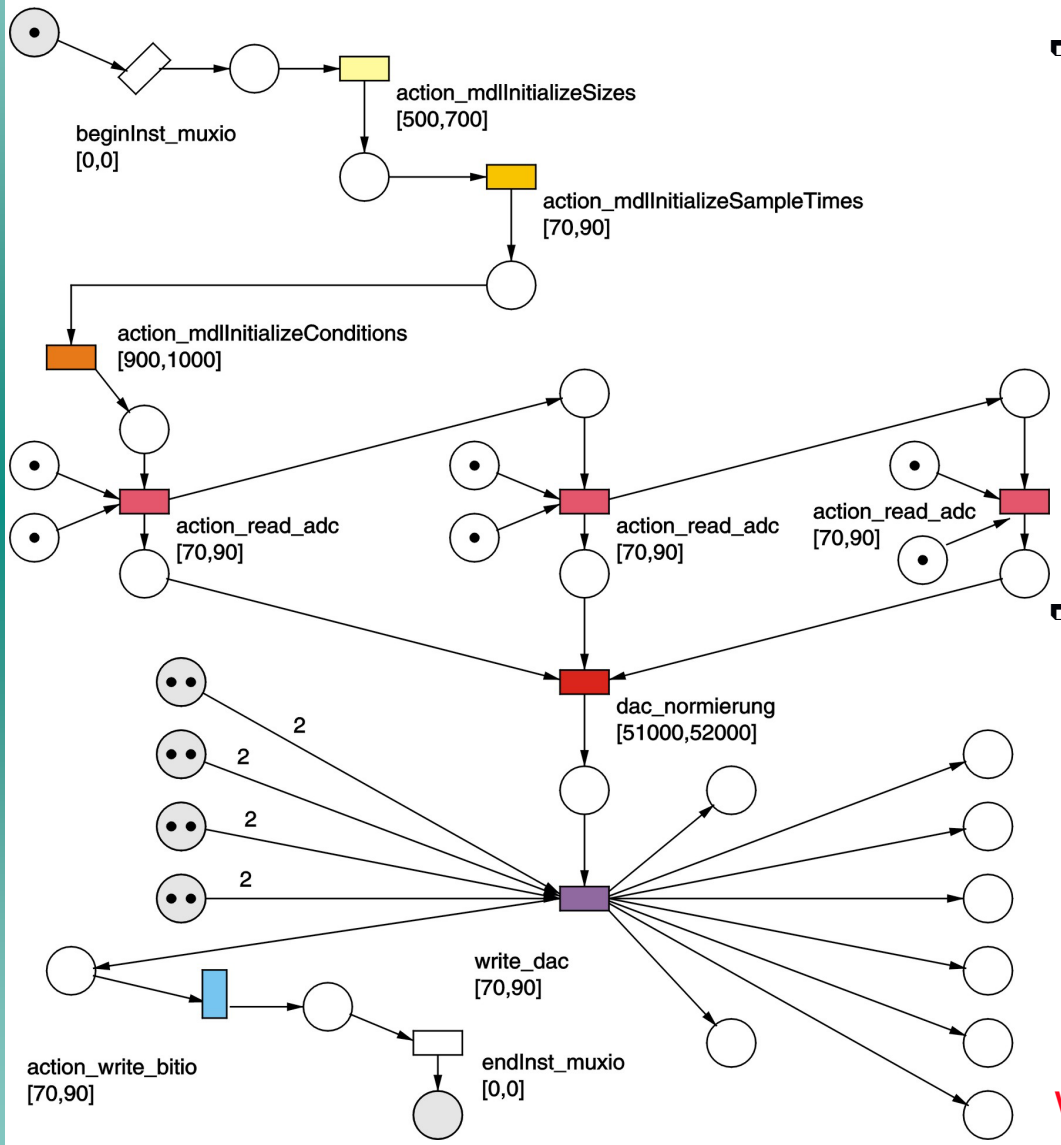
Zustandsklasse: Folge von Zuständen und Zustandsübergängen

Überprüfung von Zeitanforderungen mit Intervall-Petri-Netzen

- σ mit den angegebenen Zeiten ausführbar
- σ erfüllt angegebene Zeiteinschränkungen (deadline-Bestimmung)
- kürzeste und längste Dauer (worst-case-Bestimmung)
- Berechnung von Zeitintervallen für die Transitionen, so dass eine σ ausführbar ist
- Berechnung von Zeitintervallen für die Transitionen, so dass ein bestimmter Zustand (lifelock) nicht erreicht werden kann

$\sigma \rightarrow$ Transitionssequenz

Analyse von Pfaden in einem IPN

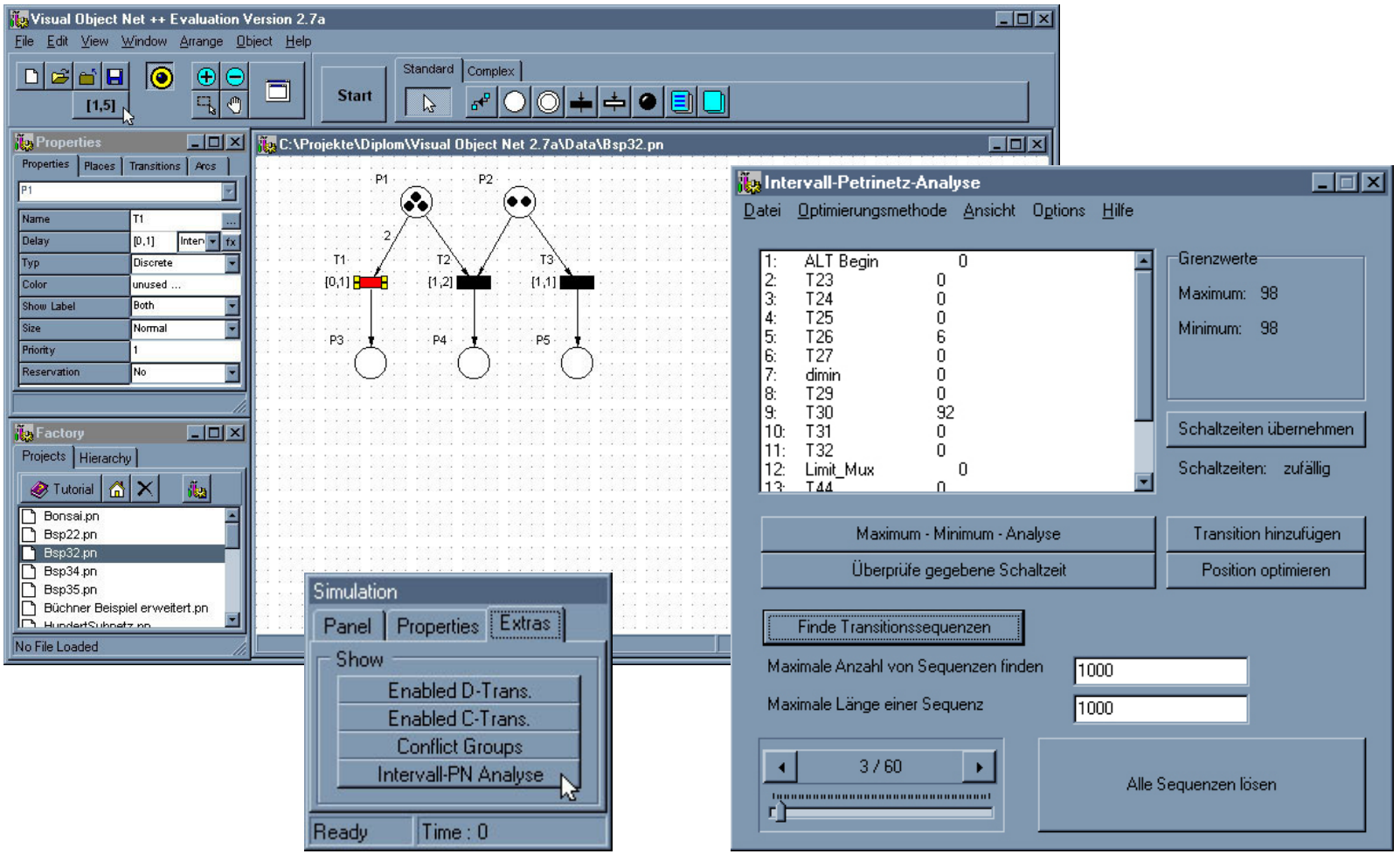


- **feste Zeiten**
  - **✓Bestimmen, ob die Dauer einer Transitionssequenz unter einer Zeitmarke bleibt (deadline)**
  - **✓ Bestimmung der kürzesten und längsten Dauer einer Transitionssequenz (worst case Werte)**
- **variable Zeiten**
  - **✓Bestimmung von optimalen Werten für die noch nicht festgelegten Zeiten, so dass die gesamte Transitions-sequenz unter einer Zeitmarke bleibt.**

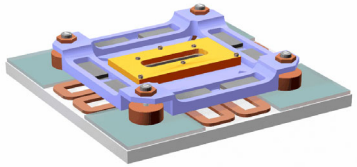
worst case [52820, 54240]

Toolunterstützung

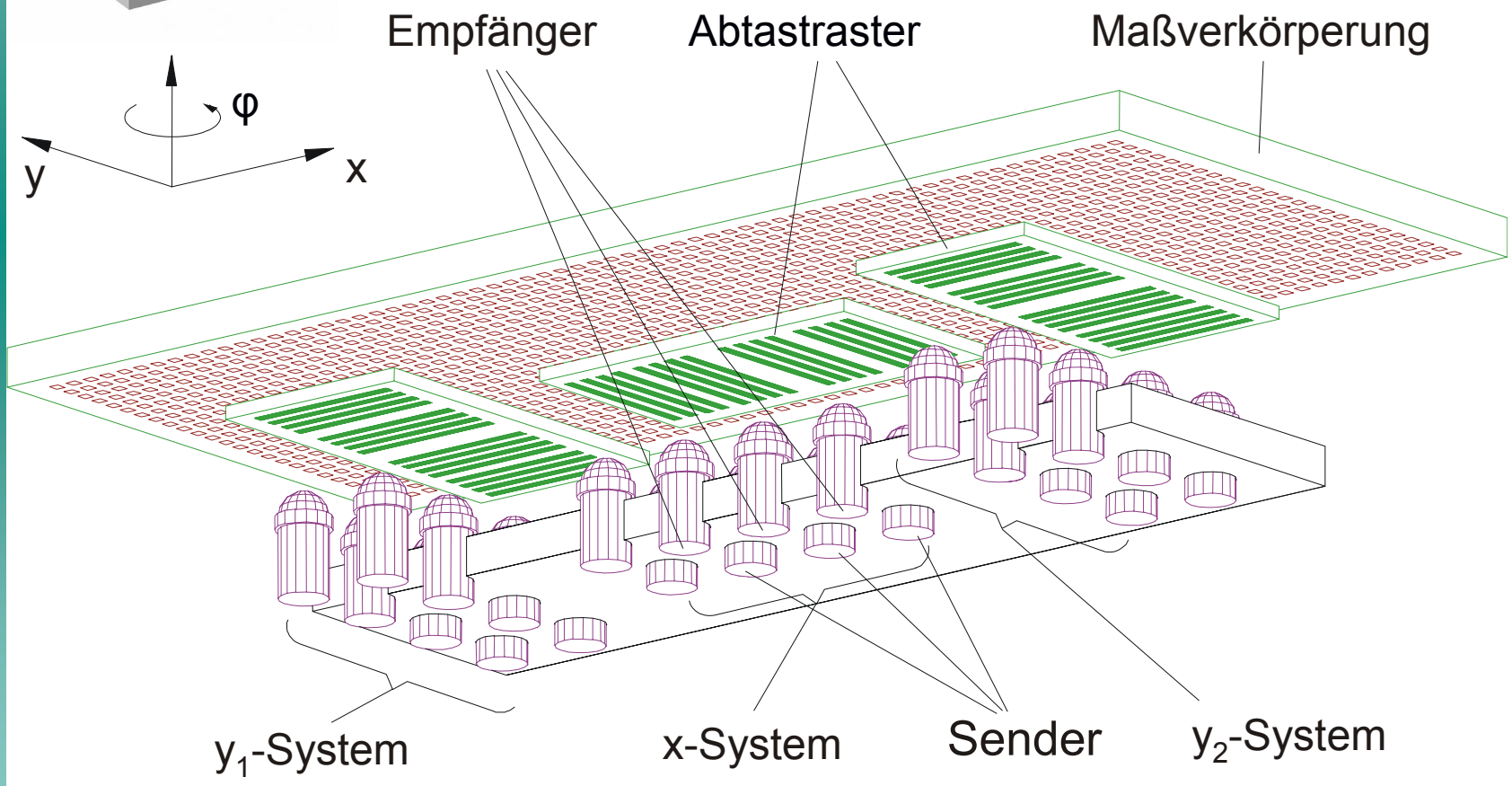
- **Erweiterte Version von VisualObjectNet++**



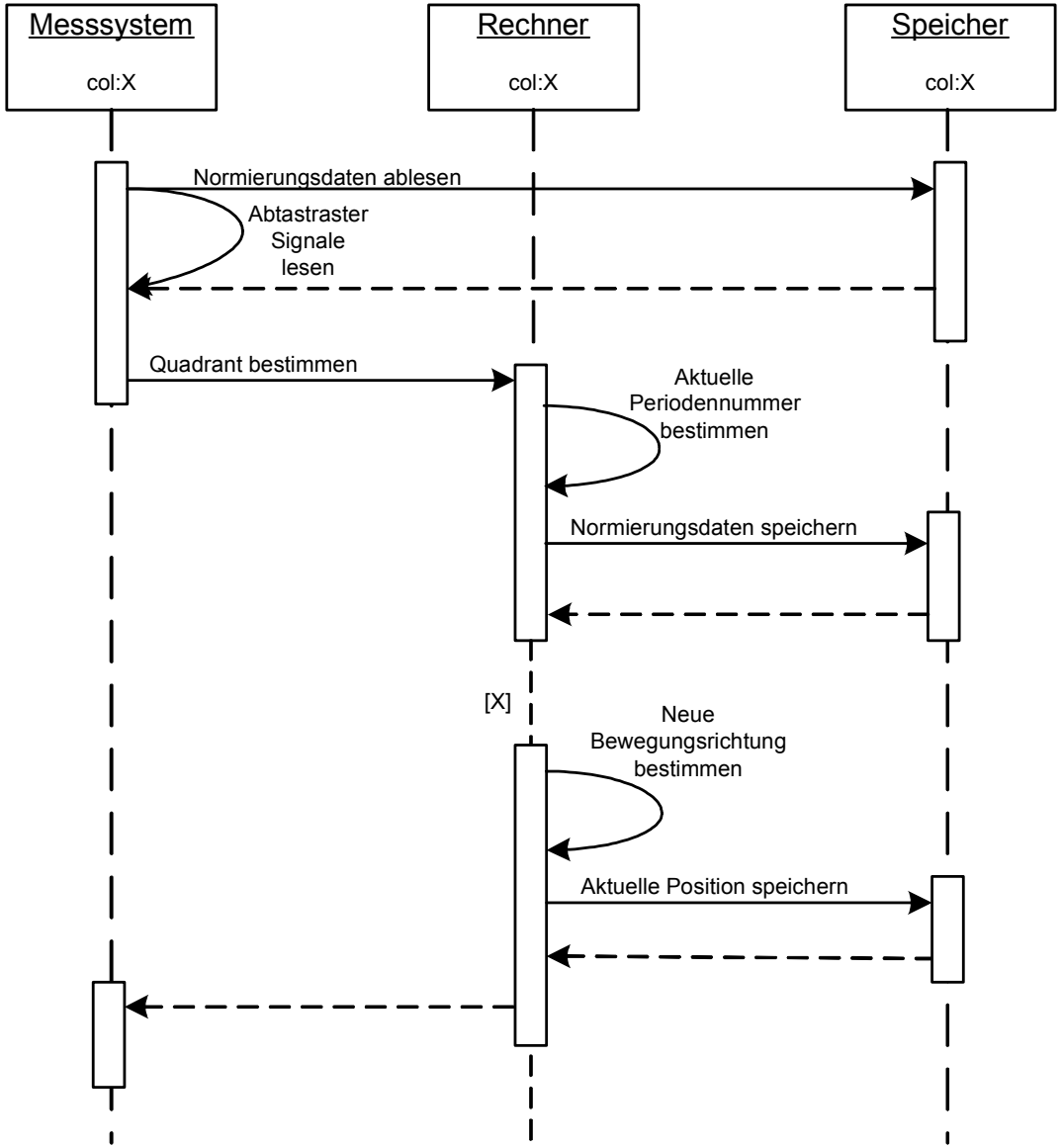
Anwendungsbeispiel



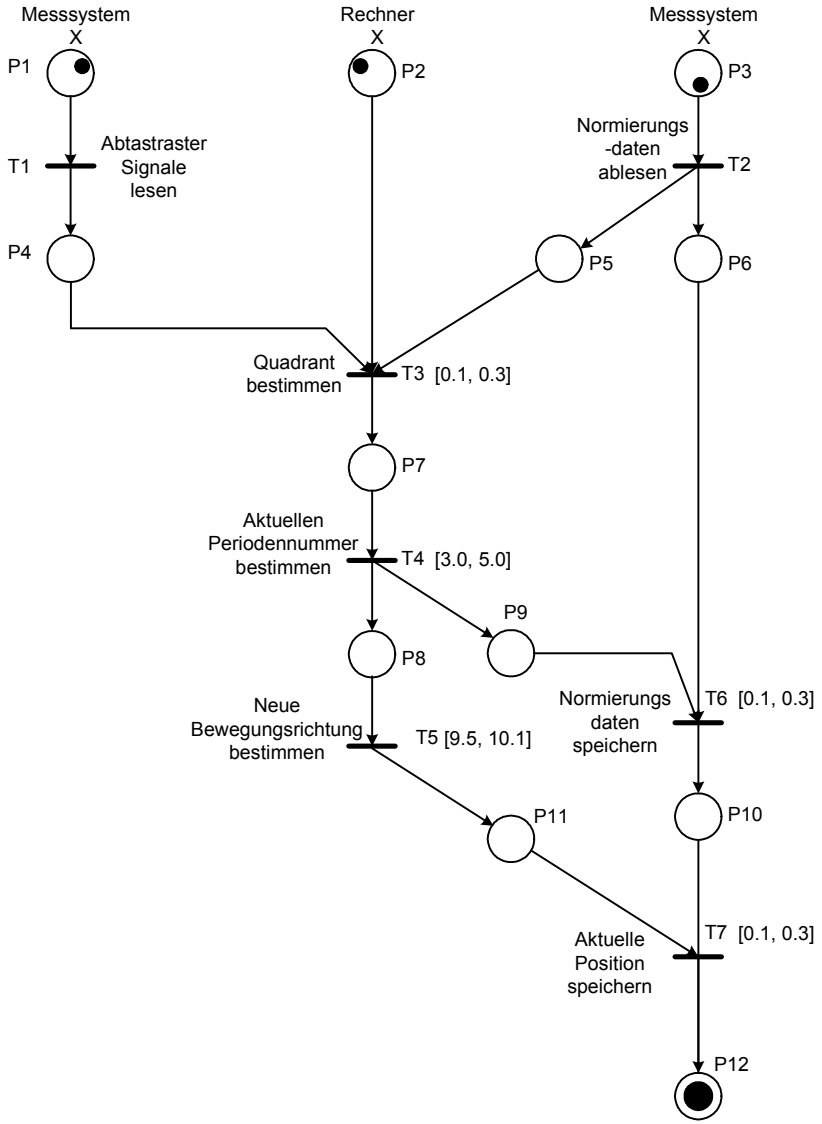
Mehrkoordinatenmesssystem



Message Sequence Chart des Beispielsystems



Intervall-Petri-Netz des Beispielsystems



Zusammenfassung - Ausblick

- Frühzeitige Kontrolle der Einhaltung zeitlicher Eigenschaften komplexer eingebetteter Systeme
- Erweiterung des Entwurfswerkzeuges „VisualObjectNet++“
  - Automatische Umwandlung von MSCs in Intervall-Petri-Netze
  - Formale Analyse von Intervall-Petri-Netzen
- Formale Verifikation von SoC-Entwürfen auf Systemebene