An PEARL orientiertes Echtzeit-PES für sicherheitsgerichtete Anwendungen

Martin Skambraks

FernUniversität in Hagen
Fachbereich Elektrotechnik und Informationstechnik

Vorrangige Entwurfsrichtlinie

„Fortschritt ist der Weg
vom Primitiven
über das Komplizierte
zum Einfachen“

(K. Biedenkopf, 1994)

Vortragsinhalte

1. Erläuterung unserer Ziele
   - Einschränkungen aufgrund des Sicherheitsstandards IEC 61508
   - Arten verfügbarer PES
2. Vorstellung eines neuartigen PES-Konzeptes
   - Arbeitsweise
   - Hardware Realisierung
   - Integration in ein ganzheitliches Sicherheitskonzept

Einschränkungen aufgrund des Sicherheitsstandards

IEC 61508 (Teil 3):

Auszug aus Tabelle B.1 (Entwurfs- und Codierungsrichtlinien)

Verfahren / Maßnahme	SIL 1	SIL 2	SIL 3	SIL 4
1 Verwendung von Codierungs-Richtlinien	++	++	++	++
2 Keine dynamischen Objekte	+	++	**++**	**++**
3a Keine dynamischen Variablen	---	+	**++**	**++**
3b Online-Test der Installation von dynamischen Variablen	---	+	++	++
4 Eingeschränkte Verwendung von Interrupts	+	+	**++**	**++**
5 Eingeschränkte Verwendung von Pointern	---	+	**++**	**++**
6 Eingeschränkte Verwendung von Rekursionen	---	+	++	++
7 Keine unbedingten Sprünge in Programmen in höherer Programmiersprache	+	++	++	++

Auszug aus Tabelle A.9 (Software Verifikation)

Verfahren / Maßnahme	SIL 1	SIL 2	SIL 3	SIL 4
Formaler Beweis	---	+	+	**++**

Arten verfügbarer PES

- Die derzeit in sicherheitskritischen Anwendungen eingesetzten PES können in zwei Klassen eingeteilt werden:
  - zyklisch arbeitende PES
  - task-basierte PES

Arten verfügbarer PES

zyklisch arbeitende PES:

- o Programmausführung in Zyklen konstanter Dauer
- o vollständige Ausführung des Programmcodes in jedem Zyklus
- ⊕ Hardware-Struktur und Zeitverhalten inhärent einfach
- ⊖ Programmierstil nicht problemorientiert
- ⊖ prozessabhängiger Programmfluss nur eingeschränkt möglich
- ⊖ umfangreiche Algorithmen führen zu langer Zyklusdauer
- ⊖ Handhabung mehrerer Rechenprozesse mit unterschiedlichen bzw. variierenden geforderten Bearbeitungsintervallen schwierig

→ werden den Anforderungen einer Sicherheitszertifizierung bestens gerecht, Einsatzfeld jedoch auf einfache Steuerungsaufgaben beschränkt

Arten verfügbarer PES

Task-basierte PES

- o unterbrechungsgesteuerte Programmausführung
- ⊕ prozessabhängige Programmflüsse unterliegen geringeren Einschränkungen
- ⊕ asynchrone Bearbeitung mehrerer Tasks möglich
- ⊕ problemorientierter Programmierstil
- ⊖ erfüllt nicht die Anforderungen der IEC 61508-3 für SIL-3 bzw.-4
- ⊖ hohe Komplexität der Hardware, des Betriebssystems und des Zeitverhaltens insgesamt

→ Einsatzfeld weniger stark eingeschränkt als bei zyklisch arbeitenden PESs, jedoch hoher Aufwand bei der Sicherheitszertifizierung

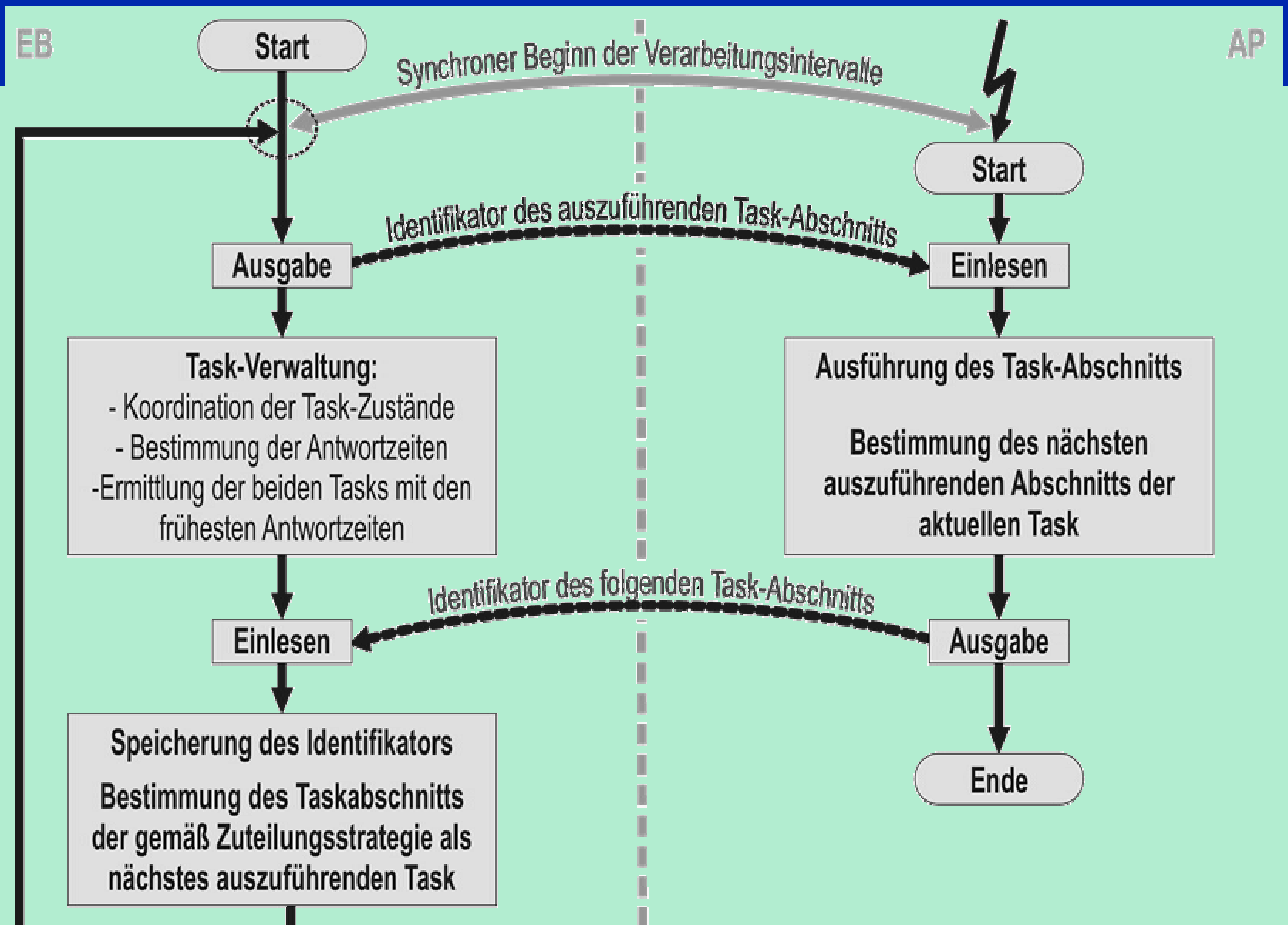
Zielsetzung

- PES, welches die Vorteile beider PES-Kategorien vereint
  - Task-basierte Echtzeitausführung
    - problemorientierte Software-Entwicklung
    - Unterstützung von beliebig prozessgesteuerten Ablaufpfaden
    - geringe Einschränkung des möglichen Einsatzfeldes
  - Taskausführung ohne asynchrone Unterbrechungen
    - Erfüllung aller Anforderungen der IEC 61508
    - einfache Architektur
    - einfaches Zeitverhalten

Task-Ausführung ohne asynchrone Unterbrechungen

- Trennung von Anwendungsprozessor (AP) und Echtzeit-betriebssystem (EB)
  - AP: anwendungsspezifische Software
  - EB: Taskverwaltung und Zuteilung des Anwendungsprozessors gemäß der Strategie der nächsten Antwortzeiten
- Quantelung der Zeit in diskrete *Verarbeitungsintervalle*
- Tasks setzen sich aus *Task-Abschnitten* zusammen
  - vollständig ausführbar innerhalb eines Verarbeitungsintervalls
  - nicht unterbrechbar
  - Datenaustausch zwischen Task-Abschnitten nur über Datenspeicher möglich
  - Abschnitte einer Task können in beliebig prozessgesteuerter Reihenfolge verarbeitet werden

Task-Ausführung ohne asynchrone Unterbrechungen



Vorteile

- Vereinfachung der Systemarchitektur und des Zeitverhaltens
  - Prozessor ohne Unterbrechwerk, keine speziellen Mechanismen zur Synchronisation notwendig, keine Unterscheidung zwischen unterbrechbaren und nicht unterbrechbaren Programmteilen
  - ? Vereinfachung der Zuteilbarkeitsanalyse
- Betriebssystem von geringem Umfang
  - ? kann als Digitalschaltung in Hardware umgesetzt werden
  - ? kurze Antwortzeiten ohne Gliederung in Schichten erreichbar
  - ? UTC-konforme Zeitverarbeitung direkt möglich
  - ? **Einheitliches Konzept**
    - zur Erkennung von Fehlern und Ausfällen,
    - zum Neuaufsetzen im laufenden Betrieb und
    - zur einflusslosen Überwachung.
- Ring-basiertes, zyklisches Kommunikationsverfahren
  - geringe Komplexität, geringer Verdrahtungsaufwand und hohe Zuverlässigkeit
  - ? alle Systemkomponenten arbeiten zyklisch synchron

Zusammenfassung

- Einschränkungen aufgrund der IEC 61508
  - Keine dynamischen Objekte oder Variablen für SIL3/4
  - Eingeschränkte Verwendung von Unterbrechungen und Zeigern für SIL3/4
  - Verifikation mit formalen Methoden für SIL4
- PES-Klassen
  - zyklisch arbeitende PES werden den Sicherheitsanforderungen bestens gerecht, Einsatzfeld jedoch eingeschränkt
  - Task-basierte PES entsprechen eigentlich nicht den Anforderungen der IEC 61508 an SIL 3 und SIL 4
- Neuartiges PES-Konzept
  - Task-basierte Programmausführung ohne asynchrone Unterbrechungen
  - ganzheitliches Konzept zur Fehlererkennung, zum Neuaufsetzen im laufenden Betrieb und zur einflusslosen Überwachung.
  - Ring-basiertes Kommunikationsverfahren

Vielen Dank für Ihre Aufmerksamkeit!

Martin Skambraks