Projekt ACOP-PC

Aircraft Operating System für den PC

Jan Peleska, Kirsten Berkenkötter

PROBE 11.5.2005

APEX (Application/EXecutive) Interface

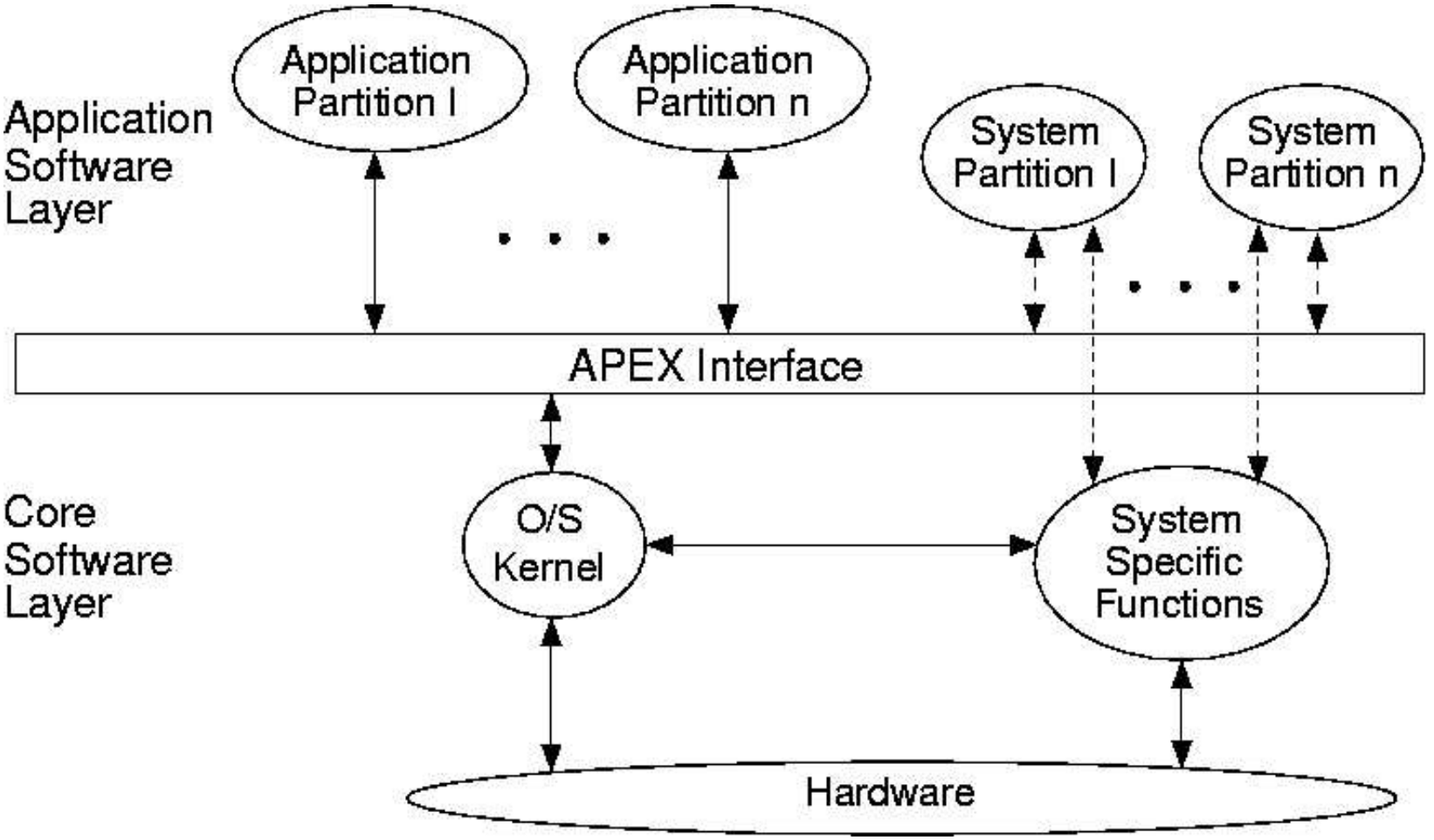
Schnittstelle zwischen Betriebsystem und Anwendungssoftware

- echtzeitfähig
- plattformunabhängig
- sprachunabhängig
- erweiterbar

Vorteile

- Portabilität
- Wiederverwendbarkeit
- Modularität
- Software verschiedener Sicherheitsstufen auf einer Plattform

APEX - Aufbau


Application Partition I
Application Partition n
System Partition I
System Partition n
Application Software Layer
APEX Interface
Core Software Layer
O/S Kernel
System Specific Functions
Hardware

APEX - Aufgaben

Partitionen und Prozesse

- Verwaltung
- Scheduling

Kommunikation zwischen Partitionen

- Messages
- Channels und Ports

Kommunikation innerhalb von Partitionen

- Blackboards
- Buffers
- Semaphore
- Events

APEX - Aufgaben

Zeitverwaltung

Speicherverwaltung

Überwachung (Health Monitor)

- Problemebene (Partition, Prozess, Modul)
- Fehlererkennung- und behandlung je nach Ebene

Konfigurationsmanagement

- Konfiguration von Partitionen (Speichergröße, Periode, Message Interface, ...)
- Konfiguration der Kommunikationswege zwischen Partitionen
- Konfiguration des Health Monitors

APEX – Beispiel Blackboard

Funktion

- Kommunikation innerhalb einer Partition
- speichert immer die letzte aktuelle Nachricht
- muss während der Initialisierungsphase angelegt werden

Routinen

- CREATE_BLACKBOARD
- DISPLAY_BLACKBOARD
- READ_BLACKBOARD
- CLEAR_BLACKBOARD
- GET_BLACKBOARD_ID
- GET_BLACKBOARD_STATUS

APEX – Beispiel Blackboard

Anlegen eines Blackboards mit CREATE_BLACKBOARD

- Eingabeparameter
  - BLACKBOARD_NAME Name des neuen Blackboards
  - MAX_MESSAGE_SIZE maximale Nachrichtenlänge
- Ausgabeparameter
  - BLACKBOARD_ID ID des neuen Blackboards
  - RETURN_CODE Fehlercode

Verhalten im Normalfall

- BLACKBOARD_ID eines (vorher nicht allokierten) Speicherbereichs wird zurückgeliefert
- internes Flag, das ein leeres Blackboard anzeigt, wird TRUE gesetzt
- RETURN_CODE = NO_ERROR

APEX – Beispiel Blackboard

Verhalten im Fehlerfall

- nicht genug Speicher
  RETURN_CODE = INVALID_CONFIG
- BLACKBOARD_NAME bereits belegt
  RETURN_CODE = NO_ACTION
- MAX_MESSAGE_SIZE inadequat
  RETURN_CODE = INVALID_PARAM
- das Betriebssystem ist nicht in der Initialisierungphase
  RETURN_CODE = INVALID_MODE

APEX – Beispiel Blackboard

Nachricht vom Blackboard lesen mit READ_BLACKBOARD

- Eingabeparameter
  - BLACKBOARD_ID — ID des zu lesenden Blackboards
  - TIME_OUT — maximale Wartezeit auf Nachricht
  - MESSAGE_ADDR — Adresse, an der die Nachricht abgelegt werden soll
- Ausgabeparameter
  - LENGTH — Länge der gelesenen Nachricht
  - RETURN_CODE — Fehlercode

Verhalten im Normalfall (Blackboard enthält eine Nachricht)

- die Nachricht wird in den Adressbereich von MESSAGE_ADDR kopiert
- die Länge der Nachricht wird in LENGTH abgelegt
- RETURN_CODE = NO_ERROR

APEX – Beispiel Blackboard

Verhalten in Normalfall (Blackboard enthält keine Nachricht)

- TIME_OUT = 0

  RETURN_CODE = NOT_AVAILABLE
- TIME_OUT = infinity
  - der aufrufende Prozess wird in den Zustand WAITING versetzt -> Scheduler
  - ein anderer Prozess legt eine Nachricht auf dem Blackboard ab -> READY
  - Nachricht wird in den Adressbereich von MESSAGE_ADDR kopiert
  - die Länge der Nachricht wird in LENGTH abgelegt

  RETURN_CODE = NO_ERROR
- 0 < TIME_OUT < unendlich
  - der aufrufende Prozess wird in den Zustand WAITING versetzt -> Scheduler
  - wenn der Timer abläuft ->

  RETURN_CODE = TIMED_OUT
  - wenn ein anderer Prozess eine Nachricht auf dem Blackboard ablegt -> READY
  - weiter wie bei Timeout unendlich ->

  RETURN_CODE = NO_ERROR

APEX – Beispiel Blackboard

Verhalten im Normalfall (Blackboard enhält keine Nachricht)

- präemptives Scheduling ist nicht möglich oder der aufrufende Prozess ist eine Fehlerbehandlungsroutine

  RETURN_CODE = INVALID_MODE

Verhalten im Fehlerfall

- ungültige BLACKBOARD_ID

  RETURN_CODE = INVALID_PARAM

- ungültiger TIME_OUT

  RETURN_CODE = INVALID_PARAM

APEX – Beispiel Sampling Port

Funktion

- Kommunikation zwischen Partitionen und Devices
- speichert immer die letzte aktuelle Nachricht (↔ Queuing Port)
- muss während der Initialisierungsphase angelegt werden

Routinen

- CREATE_SAMPLING_PORT
- WRITE_SAMPLING_MESSAGE
- READ_SAMPLING_MESSAGE
- GET_SAMPLING_PORT_ID
- GET_SAMPLING_PORT_STATUS

APEX – Beispiel Sampling Port

Anlegen eines Sampling Ports mit CREATE_SAMPLING_PORT

- Eingabeparameter
  - SAMPLING_PORT_NAME — Name des neuen Sampling Ports
  - MAX_MESSAGE_SIZE — maximale Nachrichtenlänge
  - PORT_DIRECTION — lesender oder schreibender Port
  - REFRESH_PERIOD — Sampling-Rate beim Lesen
- Ausgabeparameter
  - SAMPLING_PORT_ID — ID des neuen Sampling Ports
  - RETURN_CODE — Fehlercode

Verhalten im Normalfall

- SAMPLING_PORT_ID des Sampling Ports wird zurückgeliefert
- RETURN_CODE = NO_ERROR

APEX – Beispiel Sampling Port

Verhalten im Fehlerfall

- Port kann nicht angelegt werden (zu wenig Speicher, zu viele Ports, ...)
  RETURN_CODE = INVALID_CONFIG
- SAMPLING_PORT_NAME wurde in der Konfiguration nicht zugewiesen
  RETURN_CODE = INVALID_CONFIG
- SAMPLING_PORT_NAME wird bereits verwendet
  RETURN_CODE = NO_ACTION
- MAX_MESSAGE_SIZE inadequat
  RETURN_CODE = INVALID_CONFIG
- PORT_DIRECTION (lesend/schreibend) ist ungültig oder nicht konfiguriert
  RETURN_CODE = INVALID_CONFIG
- REFRESH_PERIOD ist ungültig
  RETURN_CODE = INVALID_CONFIG
- das Betriebssystem ist nicht in der Initialisierungphase
  RETURN_CODE = INVALID_MODE

APEX – Beispiel Sampling Port

Nachricht lesen mit READ_SAMPLING_MESSAGE

- Eingabeparameter
  - SAMPLING_PORT_ID — ID des Sampling Ports, von dem gelesen wird
  - MESSAGE_ADDR — Adresse, an der die Nachricht abgelegt werden soll
- Ausgabeparameter
  - LENGTH — Länge der gelesenen Nachricht
  - VALIDITY — Flag für gültige/ungültige Nachricht
  - RETURN_CODE — Fehlercode

Verhalten im Normalfall (Port enthält eine Nachricht)

- die Nachricht wird in den Adressbereich von MESSAGE_ADDR kopiert
- die Länge der Nachricht wird in LENGTH abgelegt
- wenn der Zeitstempel der Nachricht konsistent mit der Update-Rate ist: VALIDITY=VALID sonst INVALID
- RETURN_CODE = NO_ERROR

APEX – Beispiel Sampling Port

Verhalten in Normalfall (Sampling Port enthält keine Nachricht)

- VALIDITY=INVALID
- RETURN_CODE = NO_ERROR

Verhalten im Fehlerfall

- ungültige SAMPLING_PORT_ID
  RETURN_CODE = INVALID_PARAM
- PORT_DIRECTION ≠ DESTINY
  RETURN_CODE = INVALID_MODE

Projektziele

RETURN_C

Entwicklung eines APEX-konformen Betriebssystems auf Basis von Linux

- Modifikation des Linux-Kernels
- Systemcalls für Operationen des APEX-Interface

Formale Dokumentation des APEX-Interface

- Erweiterte Manual Pages
- Beschreibung der formalen Semantik (UML, CSP, Z, ...)

Test des Systems

- Entwicklung einer Teststrategie für das Betriebssystem
- Automatische Testdatengenerierung auf Basis der formalen Semantik