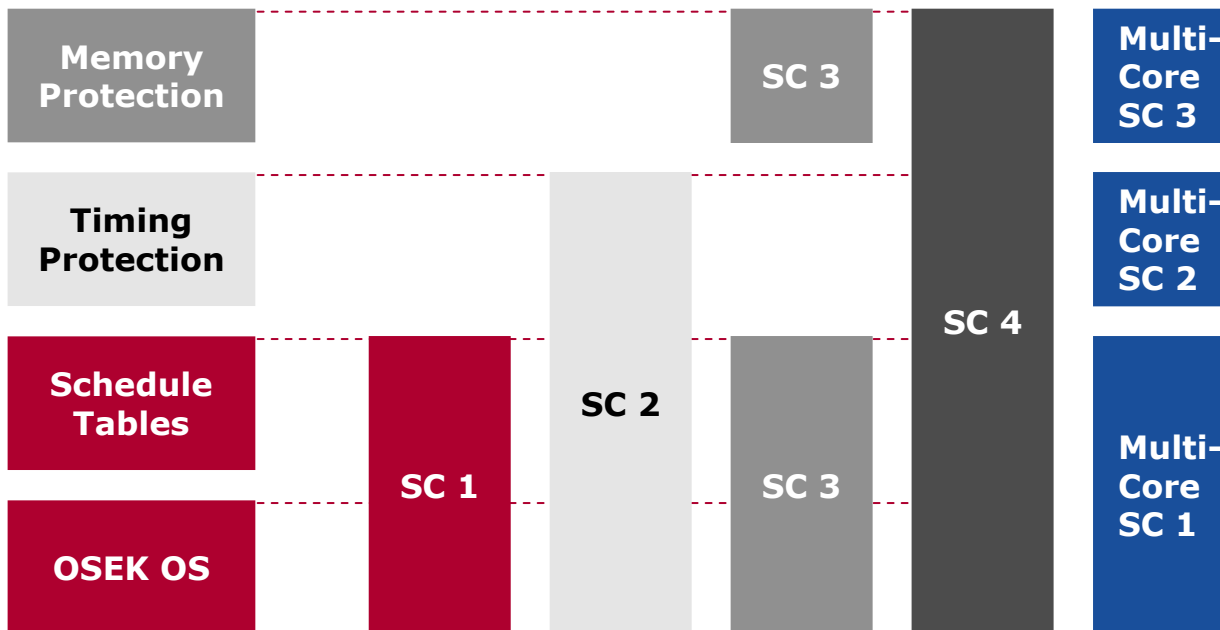


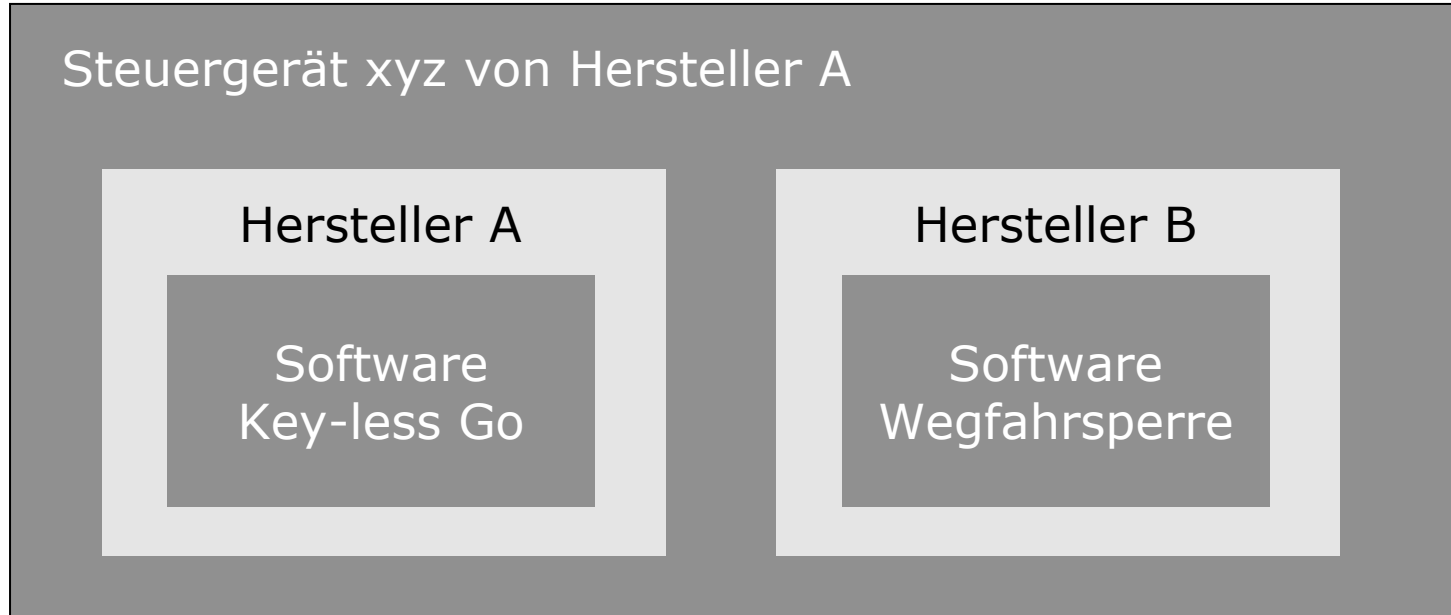


# MICROSAR-OS

## Speicher- und Laufzeitschutz

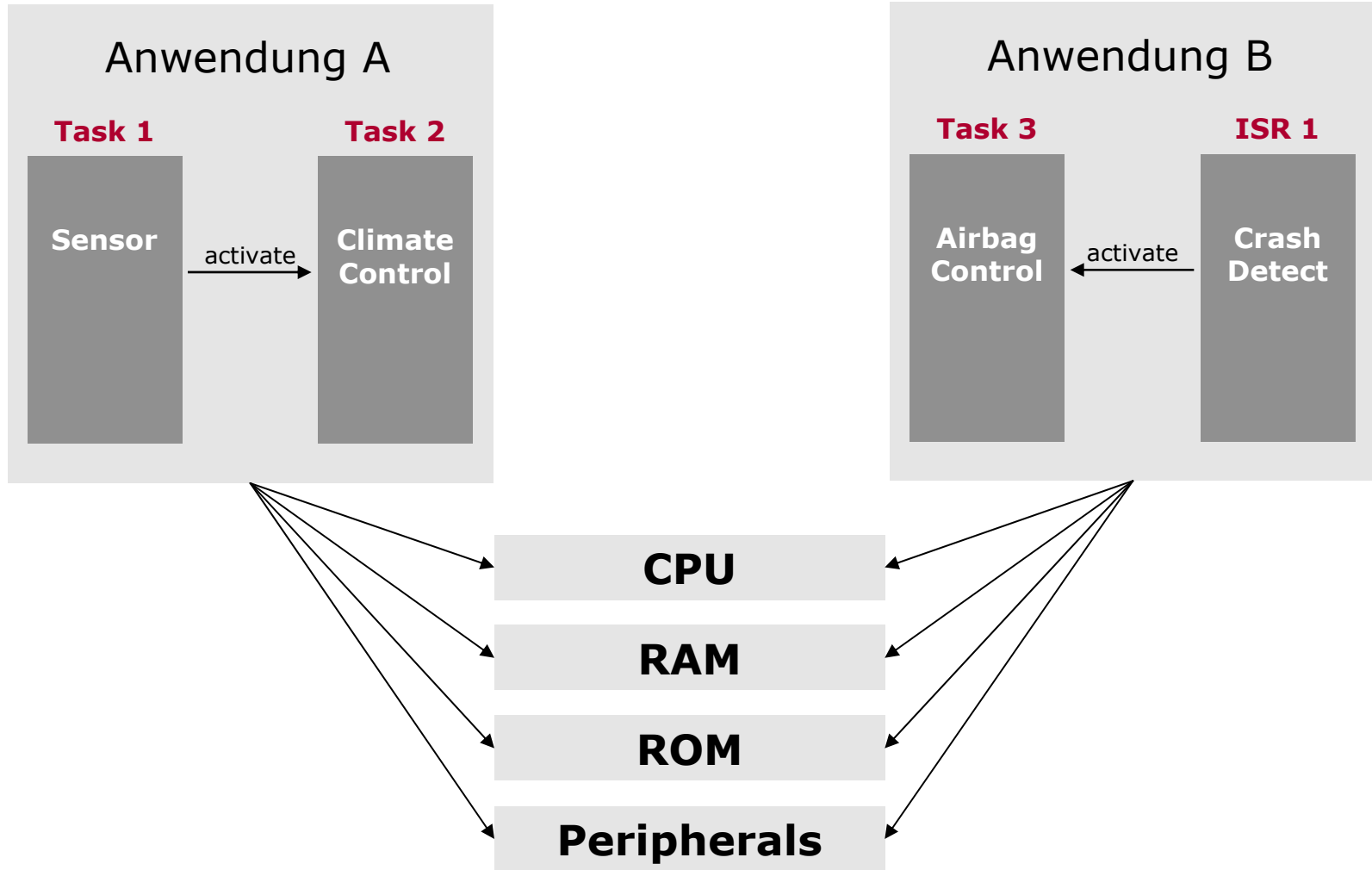
- ▶ AUTOSAR **erweitert** den OSEK/VDX Betriebssystem Standard
- ▶ Die AUTOSAR Erweiterungen sind in Scalability Klassen (SC) zusammengefasst.





Wer haftet im Fehlerfall?

Zielsetzung: Gegenseitige Störung vermeiden

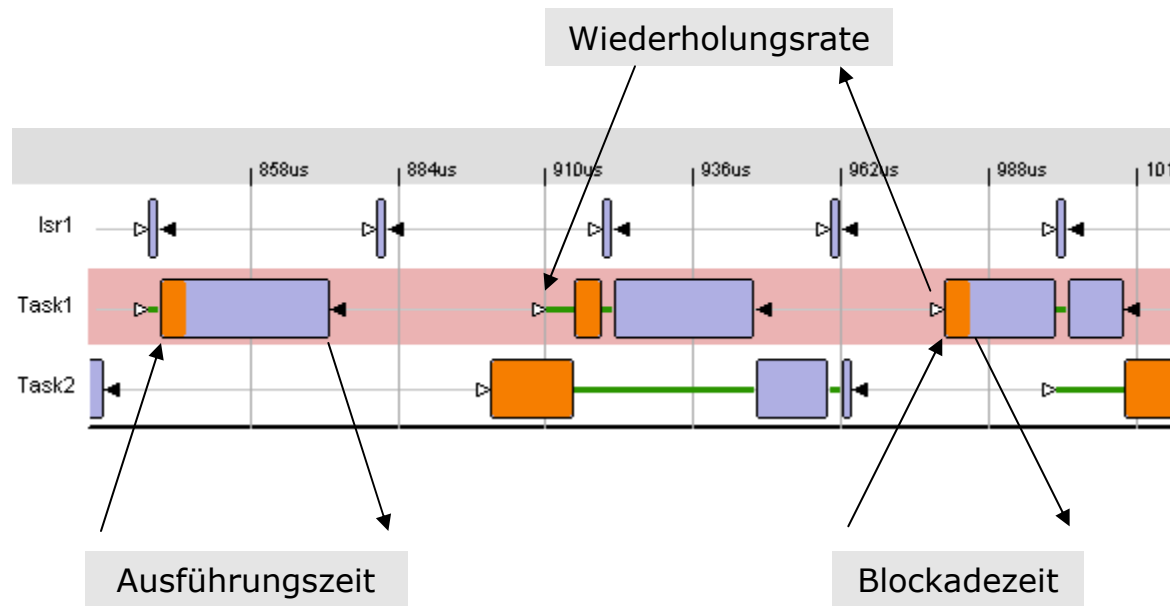


- ▶ Die Anwendung soll die Berechnung rechtzeitig abschließen können, d.h.
  - ▶ Es wird ausreichend Rechenzeit zur Verfügung gestellt
  - ▶ Die Rechenzeit wird rechtzeitig bereitgestellt
  - ▶ Die Anwendung wird nicht zu lange unterbrochen
- ▶ Die Überwachung soll die Ursache feststellen, nicht den Schaden

# Timing Protection

## Funktionsweise

- ▶ Es werden die folgenden drei Eigenschaften einer Task oder ISR (nur Kategorie 2) überwacht
  - ▶ Ausführungszeit (Execution Budget)
  - ▶ Blockadezeit (Lock Budget)
  - ▶ Wiederholungsrate (Time Frame)

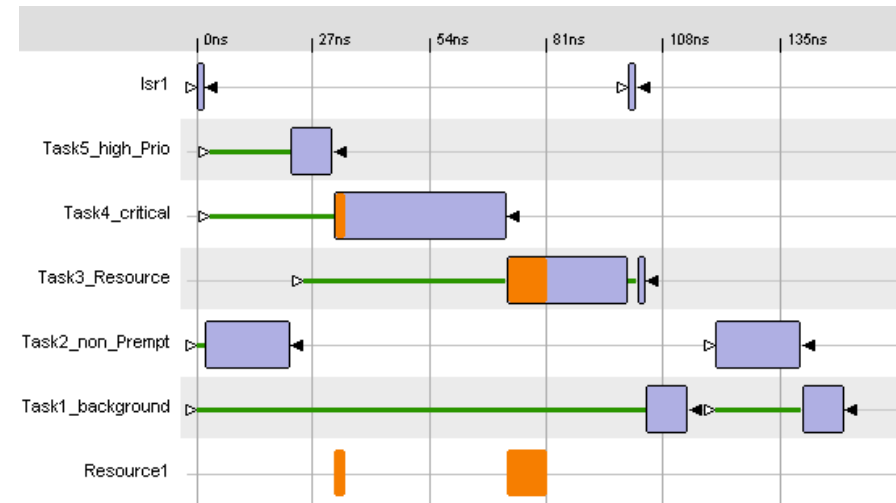


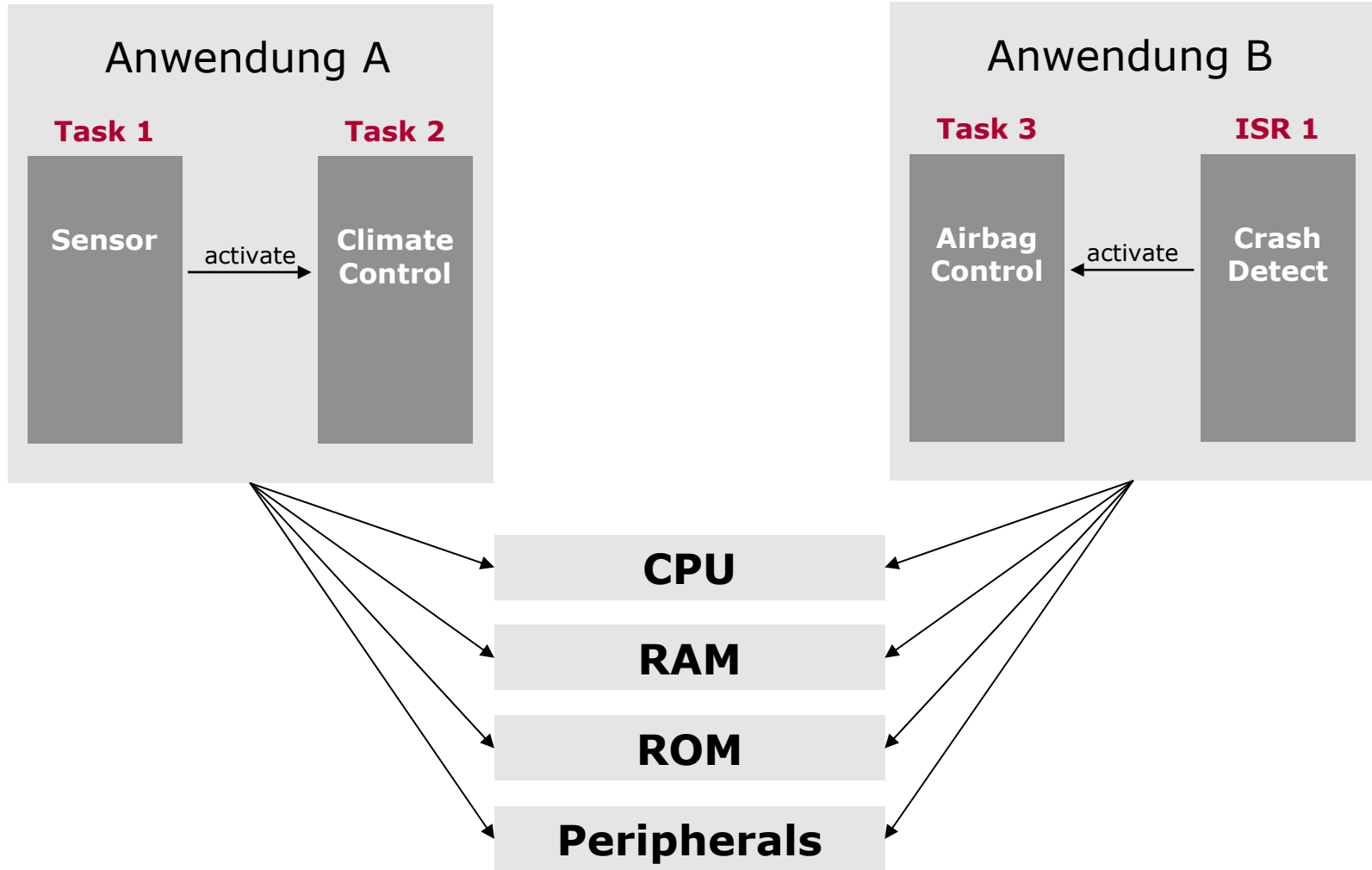
- ▶ Bei Überschreitung eines der Zeitbudgets wird die Protection Hook angesprungen
- ▶ Über den Rückgabewert wird entschieden, wie das System weiterarbeiten soll:
  - ▶ Normal weiterarbeiten
  - ▶ Die defekte Task / ISR beenden
  - ▶ Die defekte Application beenden (evtl. mit Neustart)
  - ▶ Das gesamte Steuergerät beenden (Shutdown)

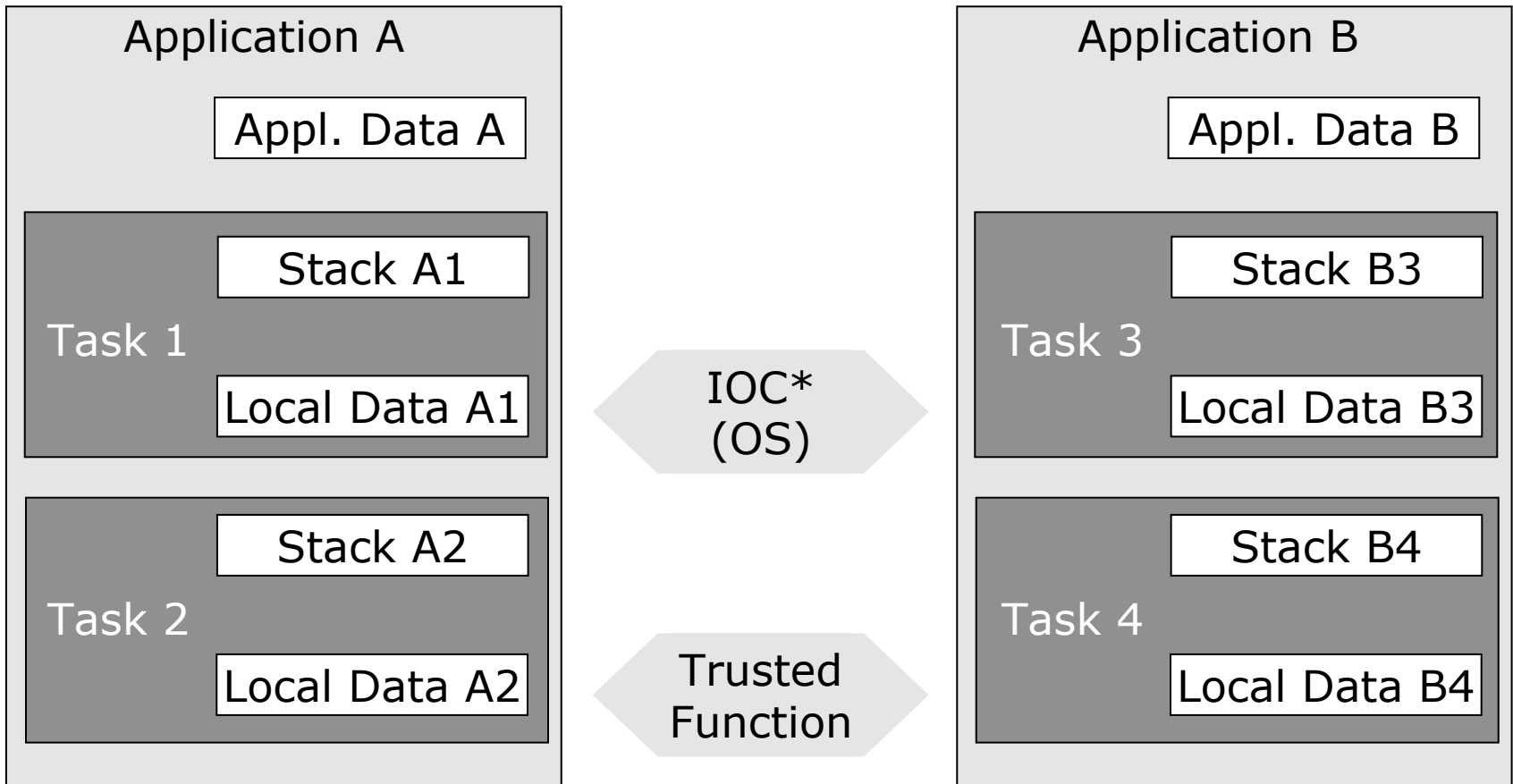




- ▶ Über eine Systemfunktion können die Messwerte ausgelesen werden
  - ▶ Execution Time = Maximum aller gemessenen Laufzeiten einer Task/ISR seit Start-OS
  - ▶ Blocking Time = Maximum der Messwerte einer Task/ISR seit Start-OS
  - ▶ Interarrival Time = Minimum für eine Task/ISR seit Start-OS
- ▶ Design - Müssen alle Tasks (ISRs) überwacht werden?
  - ▶ Nein, nur
    - > Kritische Tasks
    - > Non-preemptive Tasks
    - > Tasks mit hoher Priorität
    - > Tasks mit Ressourcen und/oder Interruptsperrern

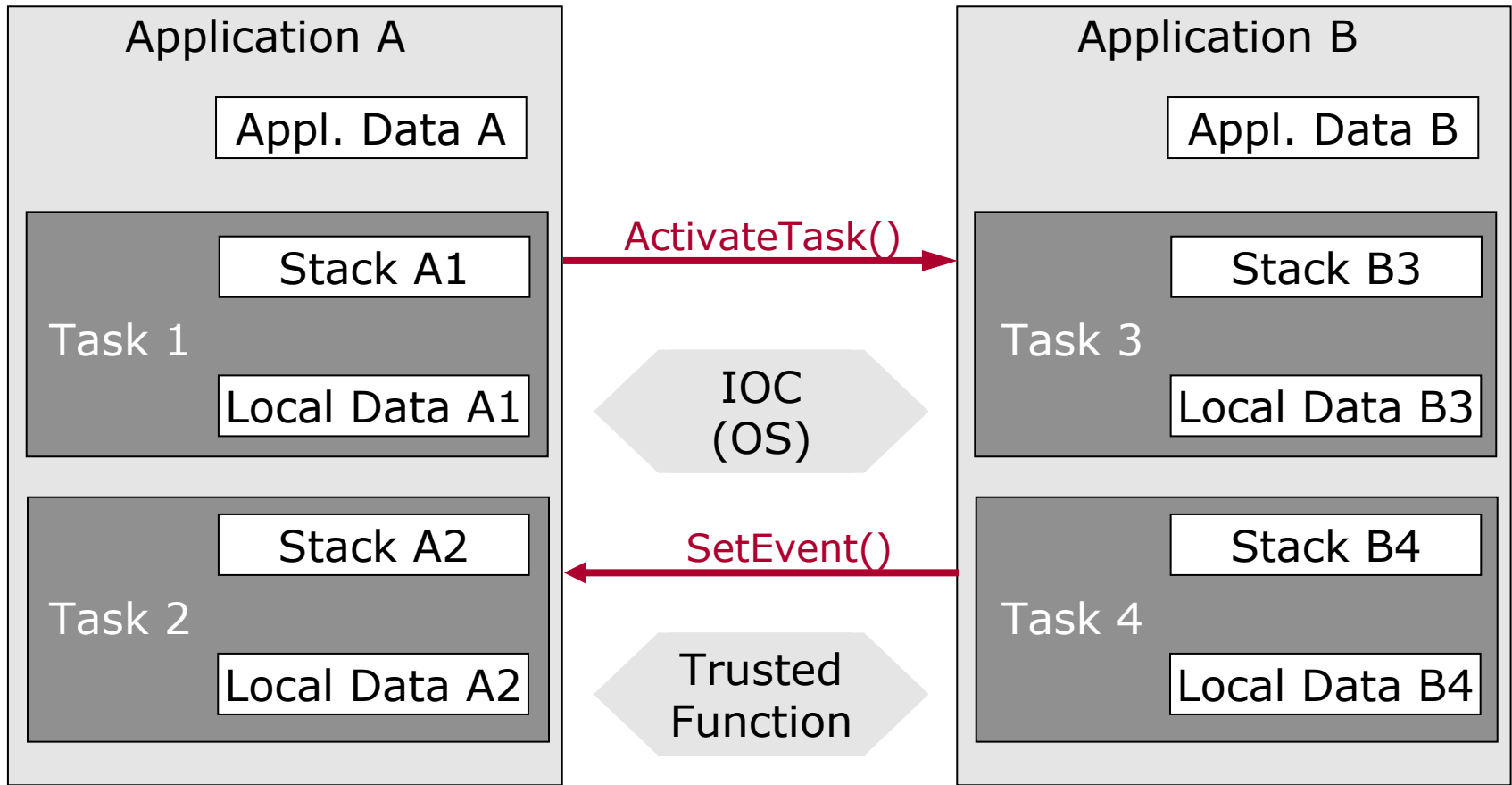






- ▶ Wie wird der Speicherschutz eingerichtet?
  - ▶ Abhängig von Hardware und Compiler/Linker
  - ▶ Zuordnung der OS Elemente zu Applications (geschieht im Davinci Developer)
  - ▶ Generator erzeugt Linker-Include Dateien (so weit möglich)
- ▶ Design
  - ▶ Müssen alle Tasks/Applications überwacht werden?
    - > Alle non-trusted Applications müssen überwacht werden.
  - ▶ Was gilt für Funktionen, die in mehreren Applications aufgerufen werden?
    - > Funktionen laufen im Kontext der aufrufenden Task d.h. Application.
    - > Funktion darf keine static Variablen enthalten
- ▶ Reaktion im Fehlerfall
  - ▶ Die MPU verweigert den Zugriff und erzeugt eine Exception
  - ▶ OS springt in die ProtectionHook mit dem Fehler E\_OS\_PROTECTION\_MEMORY

# Service Protection



- ▶ Service Protection ist Bestandteil von SC3 und SC4
- ▶ Geschützt wird auf OS Element Ebene
  - ▶ Task
  - ▶ Counter
  - ▶ Alarm
  - ▶ Resource
  - ▶ ScheduleTable

- ▶ Die Webinar-Reihe zum Thema Betriebssysteme:
  - ▶ 2011-03-22 MICROSAR OS - ein präemptives Echtzeit-Multitasking-Betriebssystem
  - ▶ 2011-03-29 TimingAnalyzer – Schedulability-Analyse von Task-Laufzeiten
  - ▶ 2011-04-12 Speicher- und Laufzeitschutz für das Betriebssystem MICROSAR OS
  - ▶ 2011-04-21 Vorstellung des Multi-Core Betriebssystems von Vector
  
- ▶ Anmeldung zu den kommenden Webinaren und Aufzeichnung der bereits gehaltenen Webinare:  
[http://www.vector.com/vi\\_webinare\\_de.html](http://www.vector.com/vi_webinare_de.html)
  
- ▶ Das Schulungs-Angebot von Vector:  
[http://www.vector.com/vi\\_training\\_de.html](http://www.vector.com/vi_training_de.html)
  
- ▶ Für Ihre Fragen bleiben wir noch einige Minuten online. Bitte stellen Sie ihre Fragen im Q&A-Fenster.
  
- ▶ Kontaktdaten für weitere Fragen, Produktdetails oder –vorführungen:
  - ▶ [helmut.brock@vector.com](mailto:helmut.brock@vector.com)
  - ▶ +49 (0) 711 80670 385
  - ▶ [embedded@de.vector.com](mailto:embedded@de.vector.com)

Thank you for your attention.

For detailed information about Vector  
and our products please have a look at:

[www.vector.com](http://www.vector.com)

Author:

Helmut Brock

Vector Informatik GmbH

Ingersheimer Str. 24

70499 Stuttgart