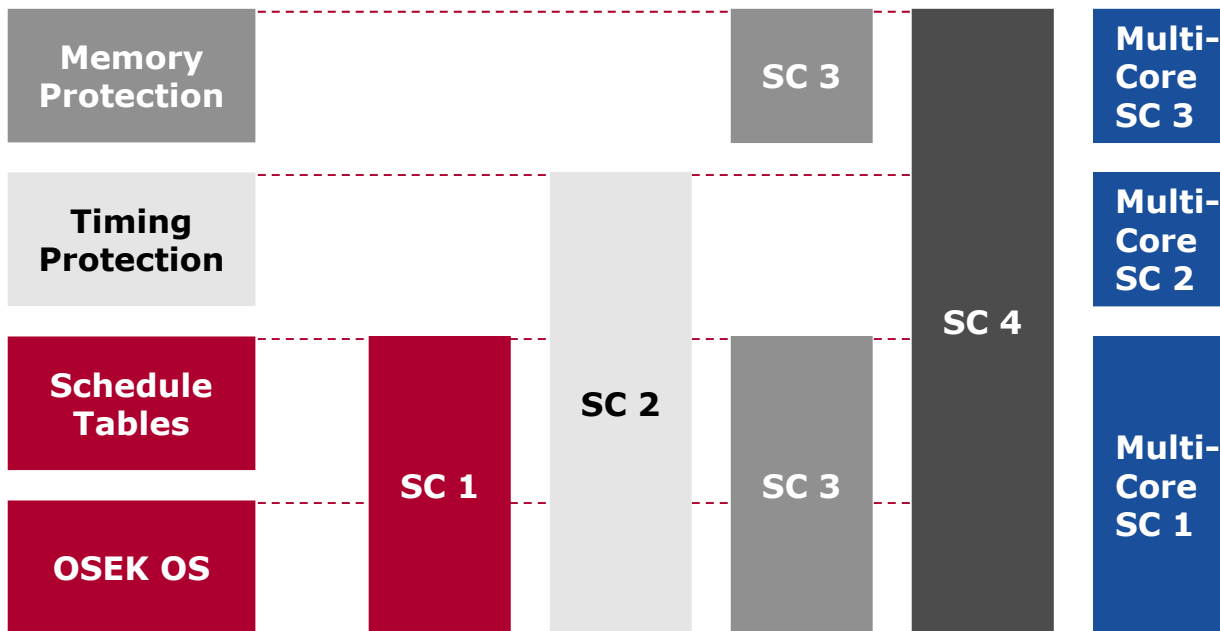


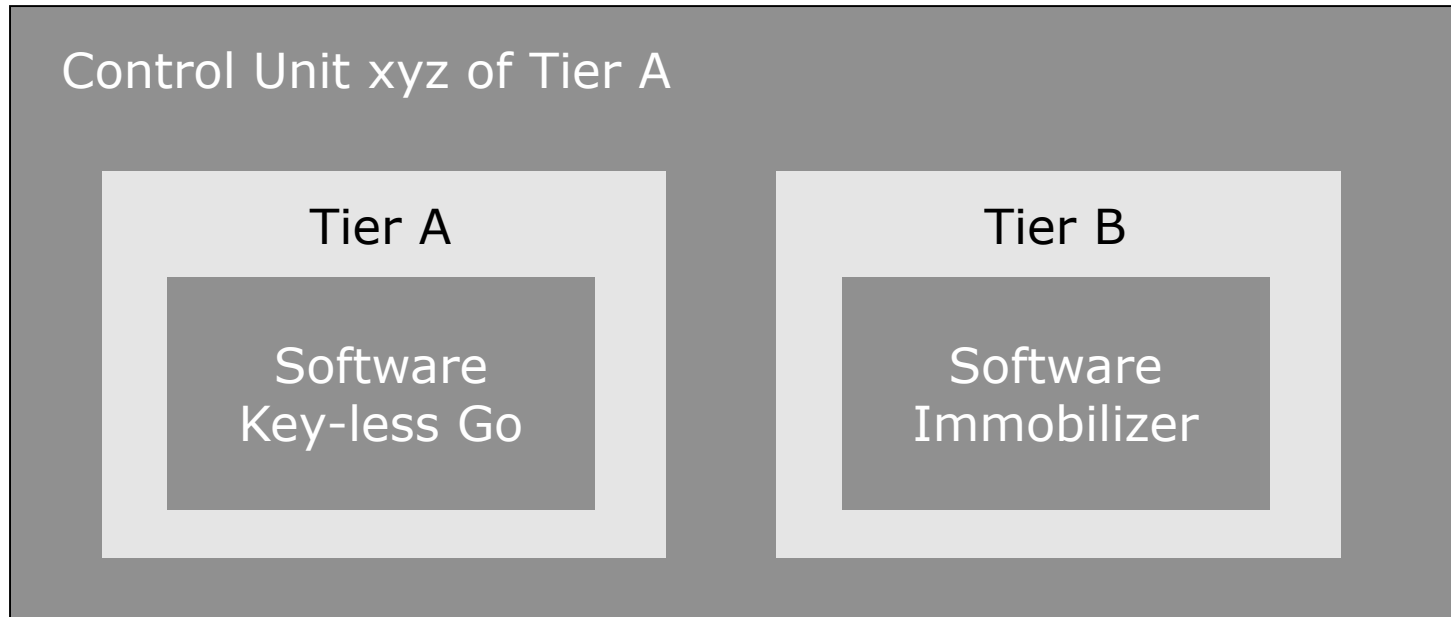


MICROSAR-OS

Memory and Timing Protection

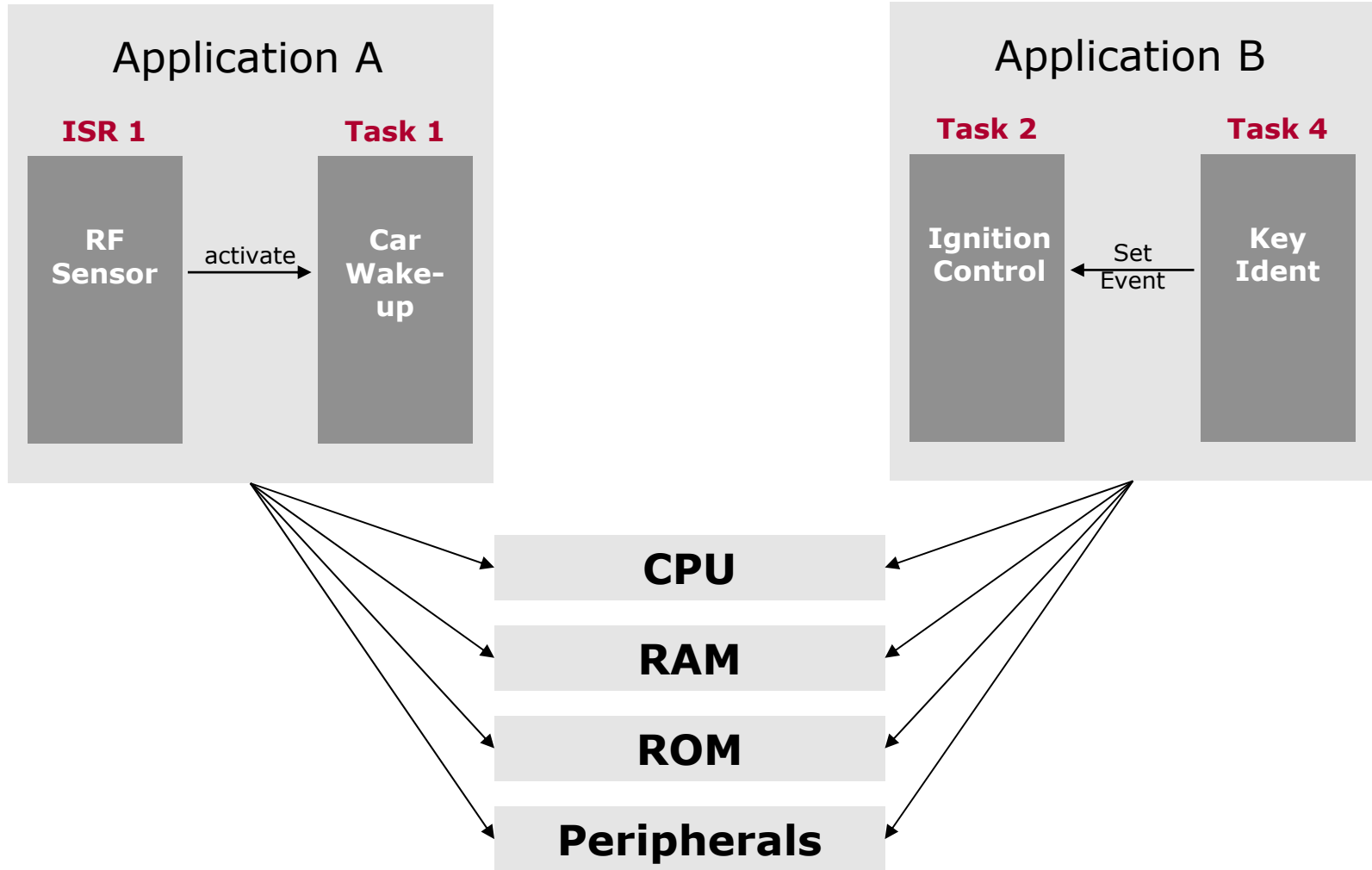
- ▶ AUTOSAR **extends** the OSEK/VDX standard of operating systems.
- ▶ AUTOSAR Add-ons are segmented into Scalability Classes (SC).





Who is liable in case auf fault?

Goal: freedom of interference

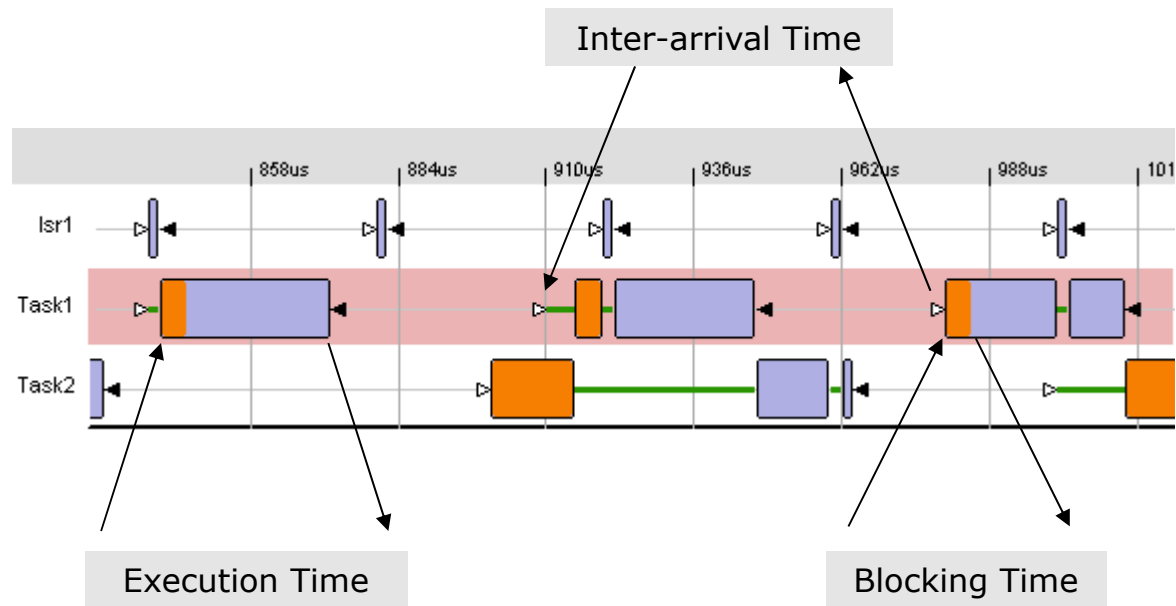


- ▶ The application shall finalize the data evaluation in due time, i.e.
 - ▶ Sufficient CPU time has to be available
 - ▶ CPU time is provided in due time
 - ▶ The application is not interrupted too long
- ▶ The supervision shall detect the cause for a missing of deadlines

Timing Protection

Concept

- ▶ The following characteristics of a task or ISR (only category 2) are measured and monitored
 - ▶ Execution Budget
 - ▶ Lock Budget
 - ▶ Time Frame – Inter-arrival Time



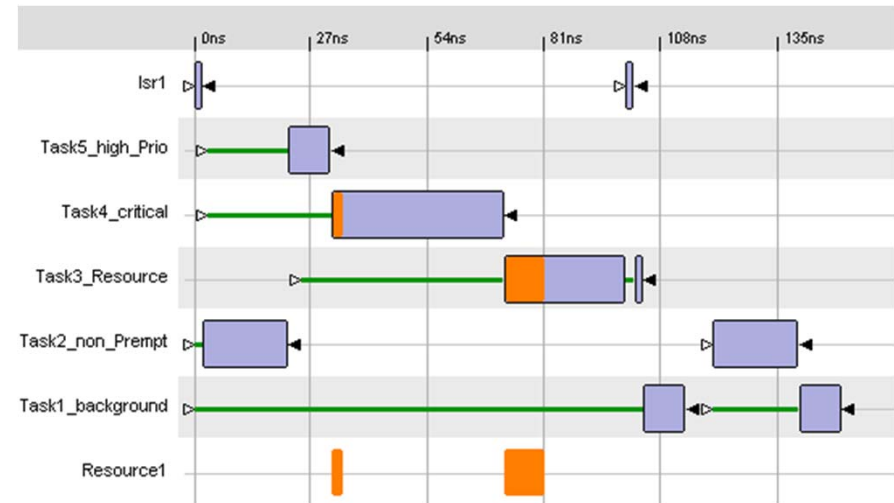
- ▶ Whenever a time budget is exceeded the operating system will invoke the Protection Hook
- ▶ The return value defines on the reaction of the operating system:
 - ▶ Continue operation
 - ▶ Terminate the Task / ISR owing the exceeded time budget
 - ▶ Terminate the defective Application (optional with re-start)
 - ▶ Terminate the complete control unit (Shutdown)

Timing Protection

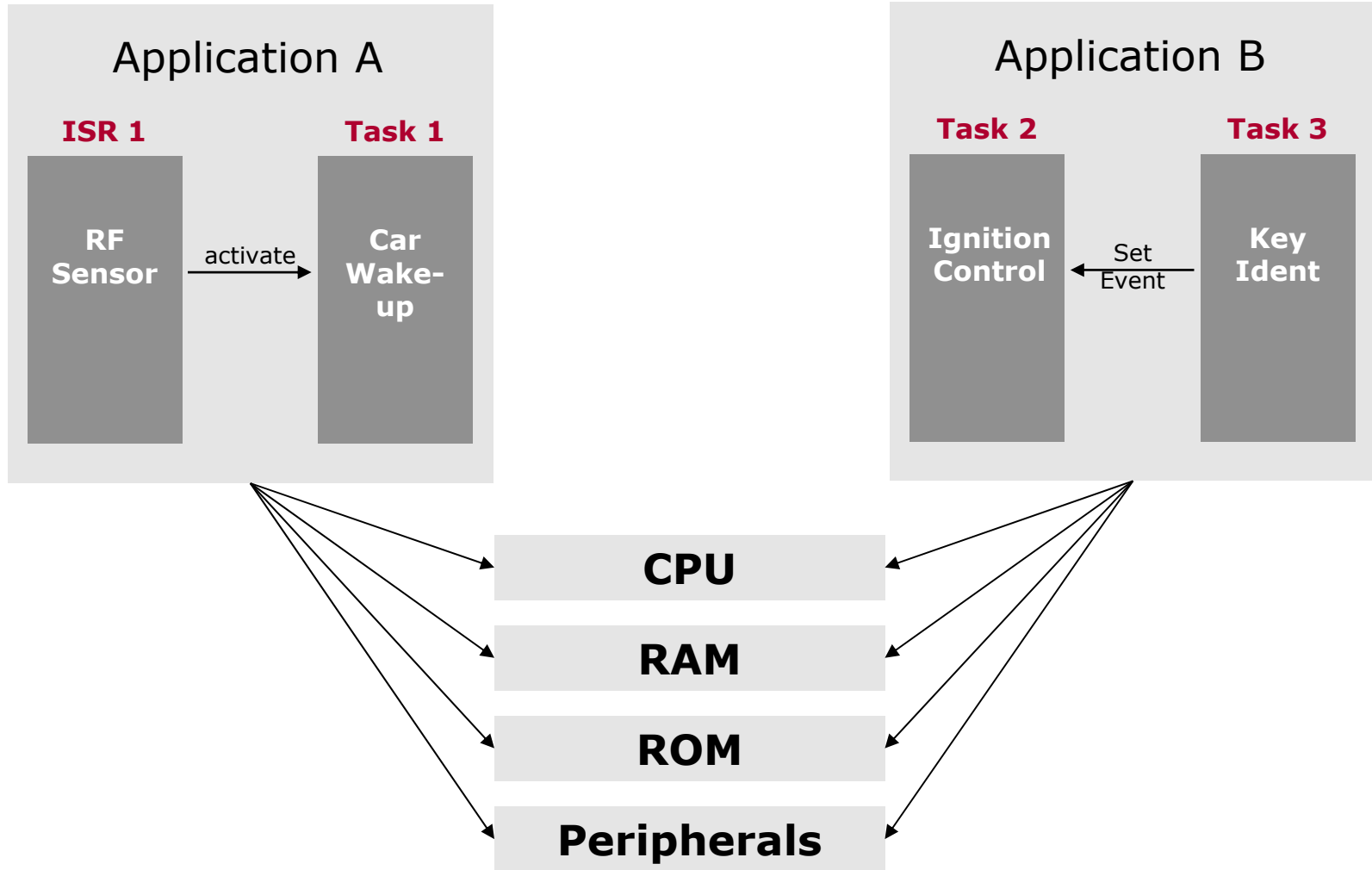
Development Process



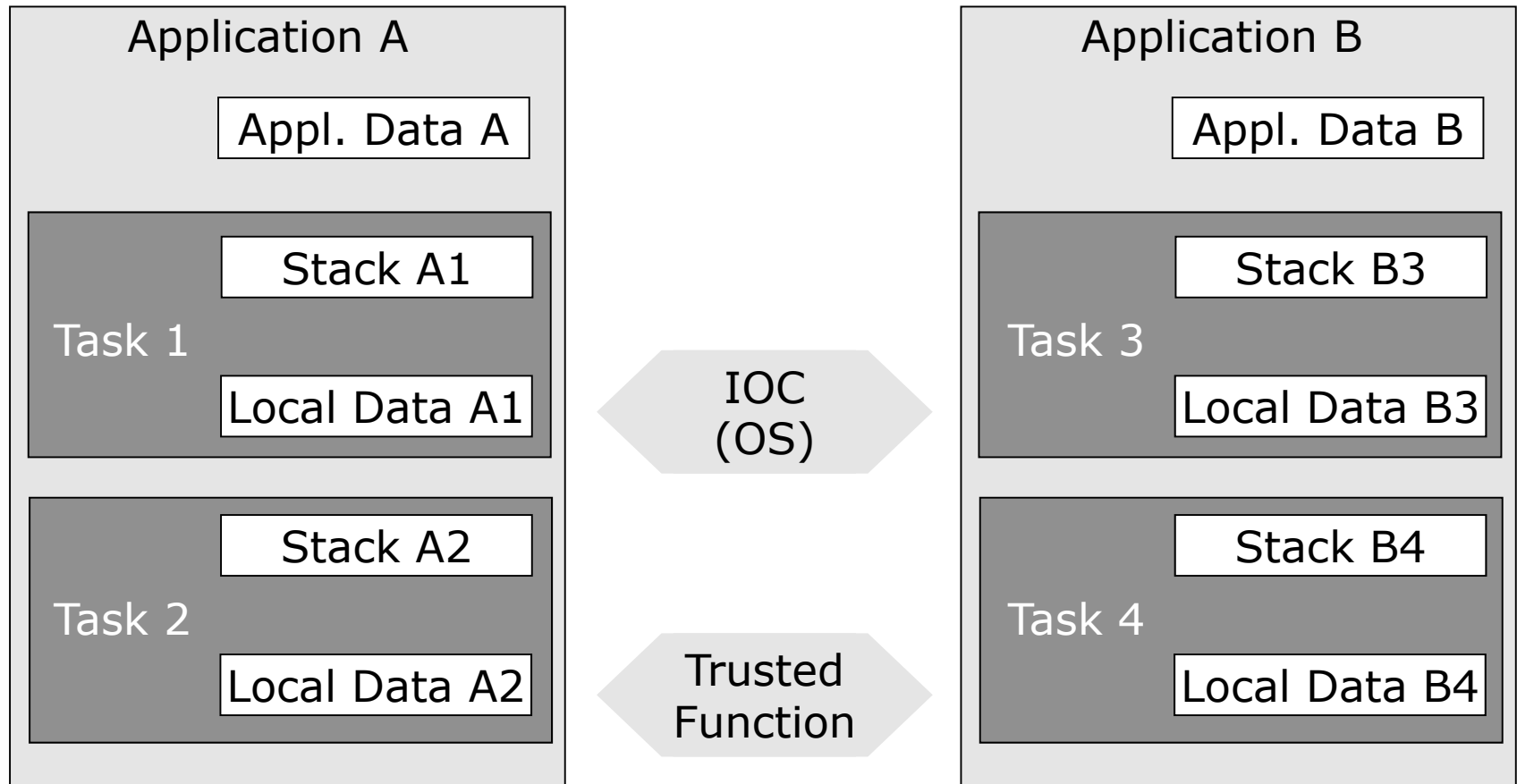
- ▶ A system function is provided to read the measured values
 - ▶ Execution Time = Maximum of all measured execution times of a task or ISR since Start-OS
 - ▶ Blocking Time = Maximum of all measured times of a task or ISR since Start-OS
 - ▶ Inter-arrival Time = Minimum for a Task or ISR since Start-OS
- ▶ Design – Have all Tasks (ISRs) to be monitored?
 - ▶ No, only
 - > Critical Tasks
 - > Non-preemptive Tasks
 - > Tasks with high Priority
 - > Tasks using Resources and / or disabling of Interrupts



Memory Protection

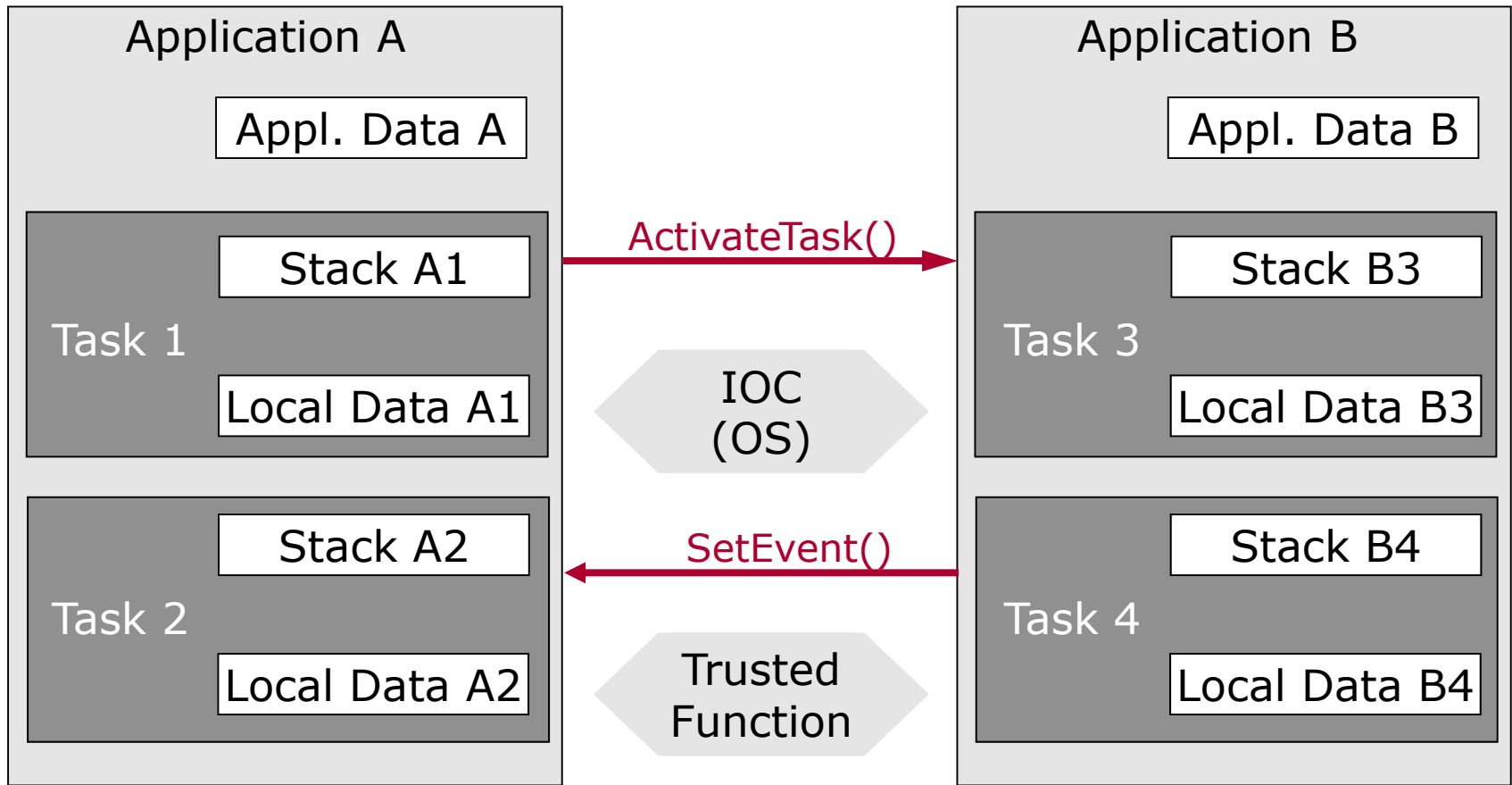


Memory Protection



- ▶ What is the configuration of memory protection like?
 - ▶ The Configuration is depending on hardware and compiler / linker.
 - ▶ OS elements have to be assigned to Applications (e.g. using Davinci Developer)
 - ▶ The generator generates Linker Include files (if possible)
- ▶ Design
 - ▶ Have all tasks or applications to be monitored?
 - > All non-trusted applications have to be monitored.
 - ▶ How are functions handled, that are called by various applications?
 - > Functions are running in the context of the calling task, i.e. application.
 - > The Function must not use static variables.
- ▶ Reaction in case of fault
 - ▶ The MPU refuses the access and invokes an exception
 - ▶ The operating system invokes the Protection Hook with `E_OS_PROTECTION_MEMORY`

Service Protection



- ▶ Service Protection is included by SC3 and SC4
- ▶ Protected are the operating system elements
 - ▶ Task
 - ▶ Counter
 - ▶ Alarm
 - ▶ Resource
 - ▶ ScheduleTable

- ▶ The webinar series about operating systems
 - ▶ 2011-10-25 MICROSAR OS - a pre-emptive realtime multitasking operating system
 - ▶ 2011-11-09 TimingAnalyzer – schedulability analysis of task runtime
 - ▶ 2011-11-22 Memory and runtime protection of the MICROSAR OS operating system
 - ▶ 2011-11-29 Introduction to the multi-core operating system from Vector
- ▶ Registration to the upcoming Webinars and the list of recorded Webinars:
http://www.vector.com/vi_webinars_en.html
- ▶ The overview of Vector's training services:
http://www.vector.com/vi_training_en.html
- ▶ We stay online for some more minutes to answer your questions. Please write your questions in the **Q&A window** and submit it to **all**.
- ▶ Contact data for additional questions, product information or presentation :
 - ▶ helmut.brock@vector.com
 - ▶ +49 (0) 711 80670 385
 - ▶ 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

Author:

Helmut Brock

Vector Informatik GmbH

Ingersheimer Str. 24

70499 Stuttgart