EB tresos classic AUTOSAR training
- EB tresos Safety Products

Chapter overview

- Background and concept “Freedom from Interference”
- EB tresos Safety Products
  - TimE Protection
  - E2E Protection
  - EB tresos Safety RTE
  - EB tresos Safety OS
- Usage of EB tresos Safety Products

Background and Concept for “Freedom from Interference”

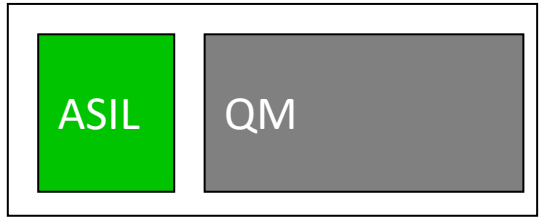
„Mixed SIL Systems“ as typical use case

Software mix in typical ECUs:

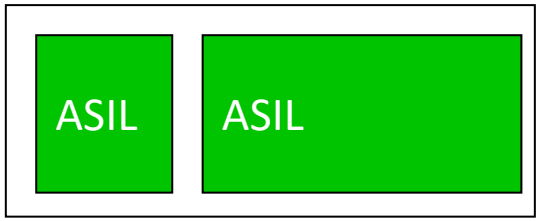
- QM Functions
- Safety Functions (ASIL)
- Safety Integrity Functions (ASIL)
- Basic Software, reused standard Software
- Black Box Software or Software from 3rd party

The majority of functions on an ECU is not safety related and thus QM classified

Only a minority of function is „Safety Software“ (ASIL classified)

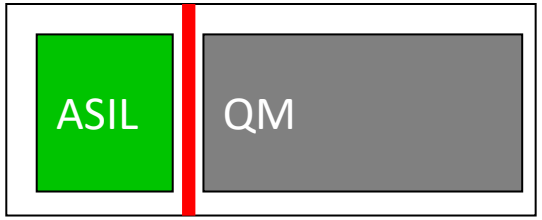


How to mix QM and ASIL Software?



Develop the complete ECU in conformance to highest ASIL of any function within the ECU (“ASIL Lift-up Effect”)

- high development effort
- failure propagation possible



Use mechanism to realize “Freedom from Interference”

- Avoids or detects propagation of failures
- Saves effort
  - application of ASIL-x development methods only where needed
  - re-use of existing QM software

Freedom from Interference

Memory

- Unintended writing to memory of another partition
- Register/Configuration corruption due to unintended writing to processor registers

CPU Time

- Blocking of partitions
- Wrong allocation of processor execution time

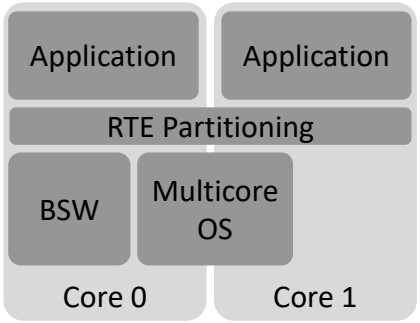
Communication

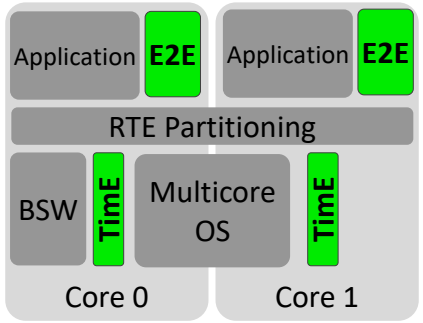
- Loss of communication
- Insertions of messages
- …

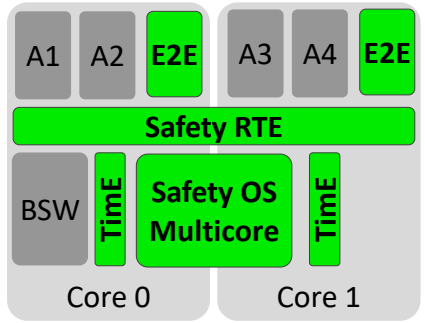
Usage of EB tresos Safety Products

Scalable Safety Solution

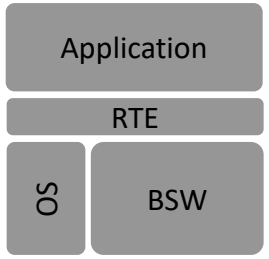
Multicore

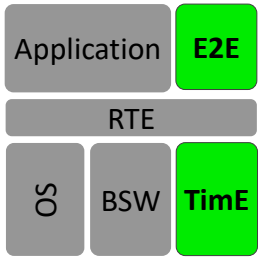


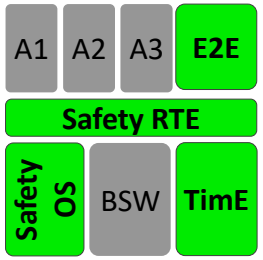




Singlecore

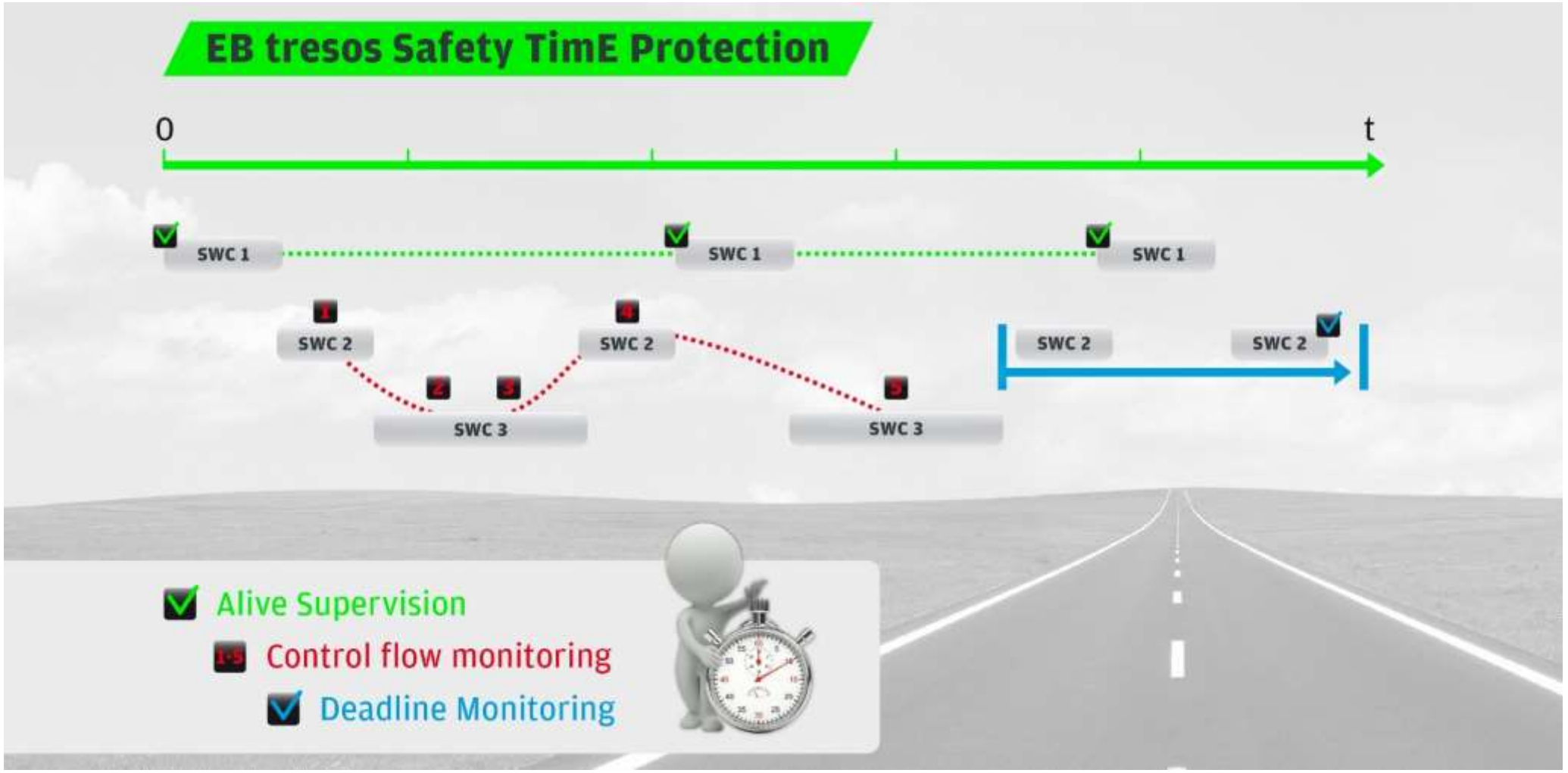






QM ASIL-A ASIL-B ASIL-C ASIL-D

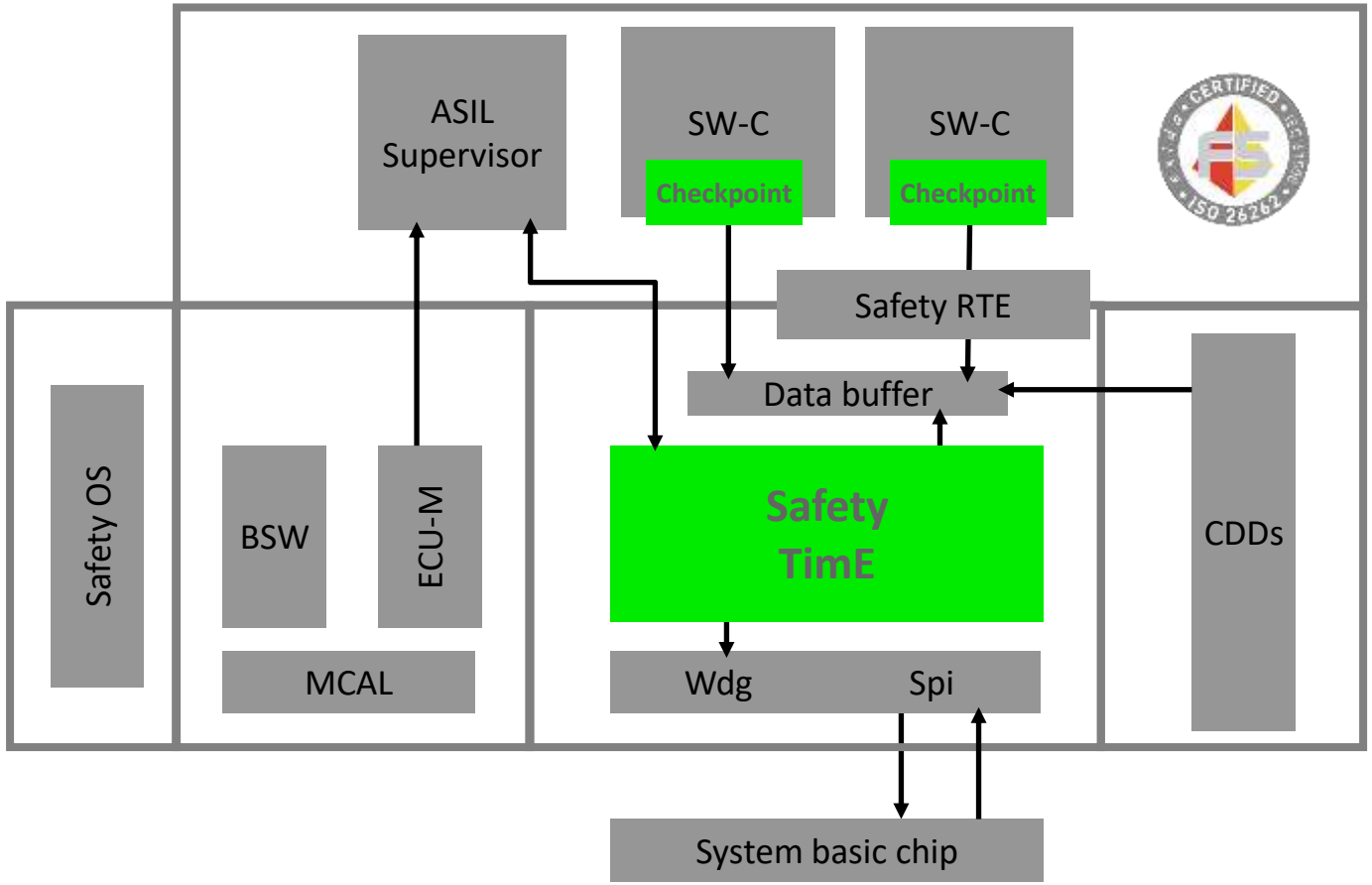
EB tresos Safety TimE Protection in a nutshell



EB tresos Safety TimE Protection

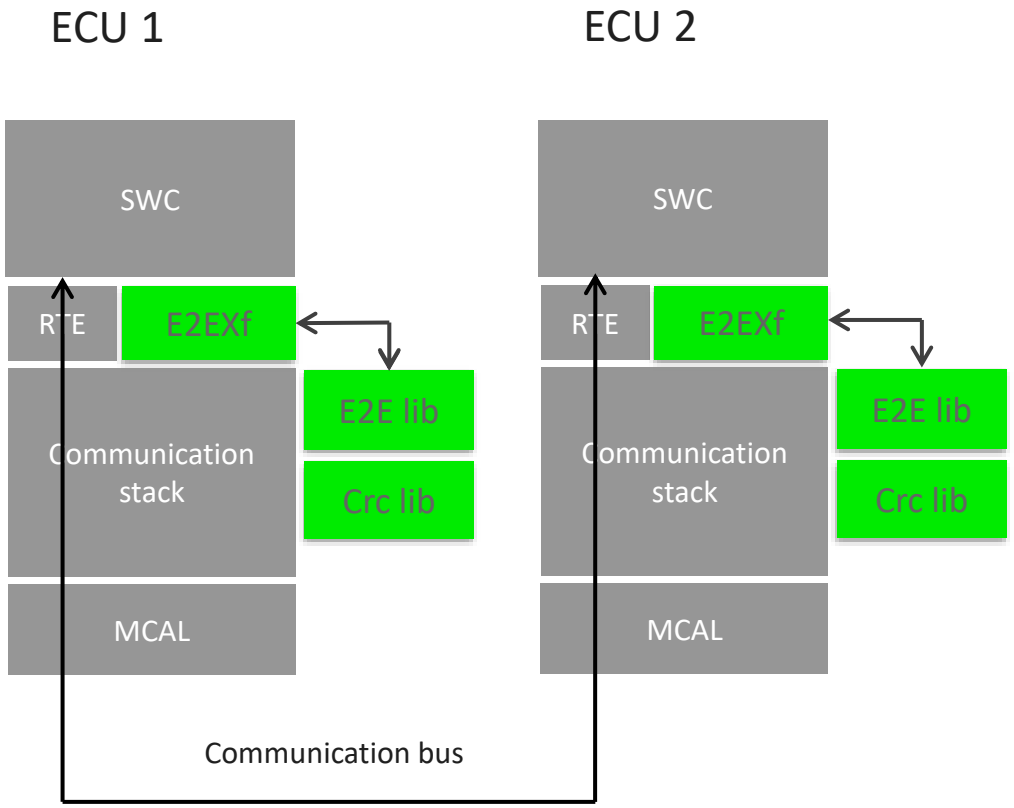
Key features

- **Alive supervision**
- **Enhanced deadline monitoring**
  TimE monitors not only checkpoints reached but also upcoming checkpoints
- **Control flow monitoring**
  Supports multiple control flows
- Optional **smooth error reaction**, allows error recovery **without a reset**
- Multi-core extension



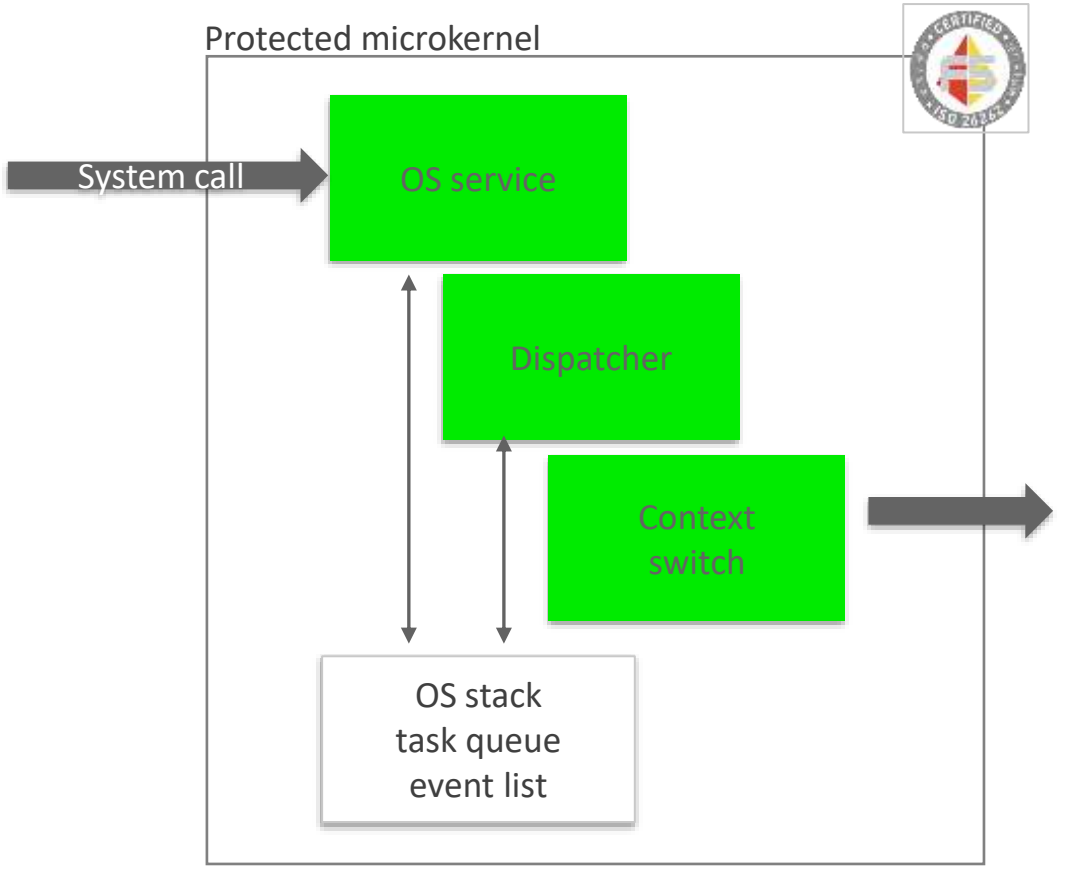
EB tresos E2E Protection Transformer

- **E2E Transformer** (E2EXf) allows to use E2E protection **transparent to the SWC-ECU allocation**
- **Import of system configuration** for E2E Protection according to AUTOSAR 4.2
- Support for different use cases:
  - S/R with **COMXF** and E2EXf **via Com**
  - S/R with **SOME/IP** and E2EXf via **LdCOM**
  - **Profile 1a/1c and 4/5/6/7** with 32-bit CRC, designed for large data as used with Ethernet
  - Support for **major OEMs**

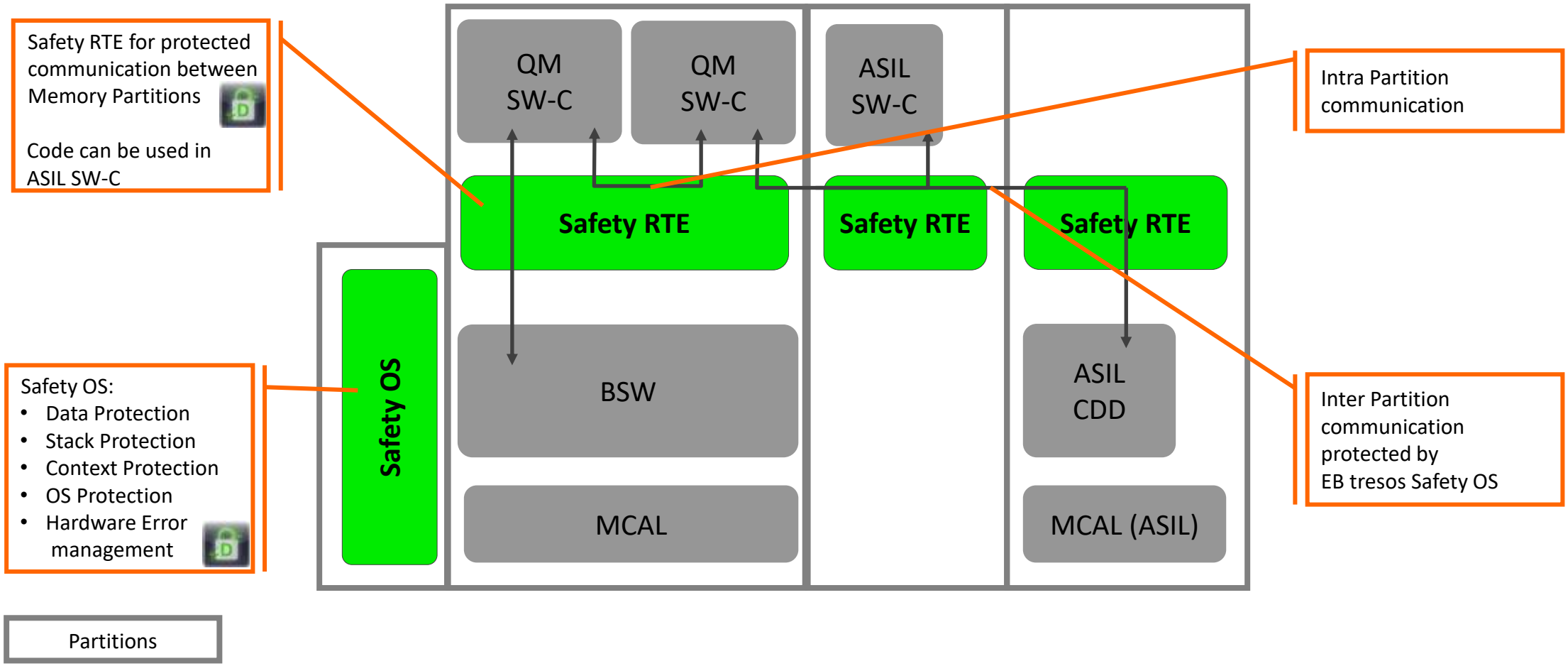


EB tresos Safety OS

- **Protected microkernel**
  Ensures FFI between OS services and other software
- Flexible memory partitioning scheme
  - As many memory regions per context as numbers of MPU region descriptors available
  - Flexible assignment of shared regions
  - Read and execution protection possible
  - Full memory protection in privileged CPU mode
- OS kernel protection via MPU
- Stack overflow protection using MPU
- Non-privileged/privileged mode separation



EB tresos Safety OS and Safety RTE



Get in touch!

Elektrobit

sales@elektrobit.com
www.elektrobit.com