

MICROSAR Safe

- A  and **TTTech** Solution -

ISO 26262 ...

- ▶ ... is based on the generic safety standard IEC 61508.
- ▶ ... is a safety standard specific for the automotive industry,
- ▶ ... comprises an approach based on risks / hazards which are associated with the system to be developed.
- ▶ ... demands technical measures for the system itself
- ▶ ... demands measures for the engineering processes applied during development.
- ▶ ... has been released in 2011.

Safety Standard ISO 26262

- Goals:
1. Avoid failures
 2. Make unavoidable failures safe

Determine Risk (ASIL = Automotive Safety Integrity Level)

Product Measures

Technical measures against **random** HW failures:

- ▶ Redundancy
- ▶ Diagnostics
- ▶ Self-tests
- ▶ ...

Technical measures against **systematic** HW and SW failures:

- ▶ Redundancy
- ▶ Diagnostics
- ▶ Self-tests
- ▶ ...
- ▶ Modular HW/SW architecture
- ▶ Architecture patterns
- ▶ Defensive programming
- ▶ ...

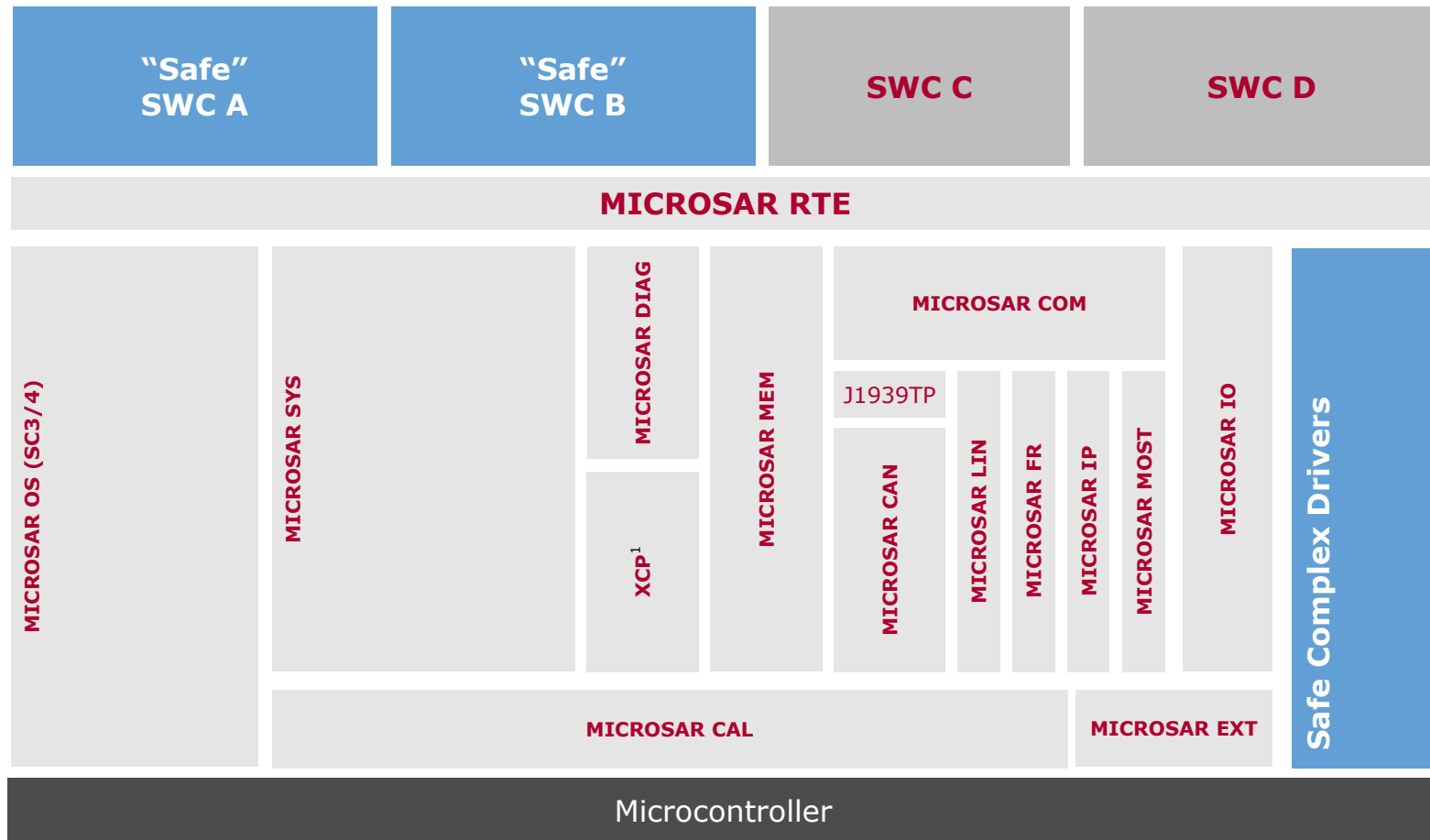
Development Process

Methodological measures to ensure the application of a safety-conform development process:

- ▶ Design methods
- ▶ Analysis techniques
- ▶ Test methods
- ▶ Safety case
- ▶ Configuration management
- ▶ ...

SafeExecution

Topic



Safety Mechanism

Safety Related Function

Autosar Basic SW Component

Non-safety related Function

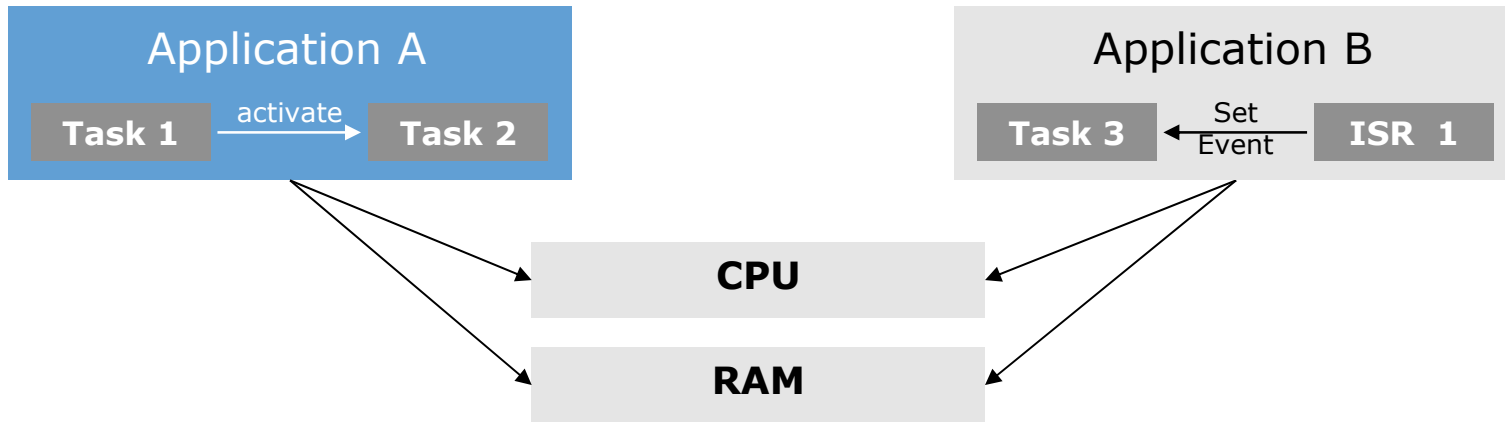


The **safety mechanisms**

- ▶ detect and handle interference faults
 - > in the basic SW
 - > in the application SW
 - > in the hardware (partly)
- ▶ and thus allow the coexistence of SW with different integrity levels

SafeExecution

Freedom from Interference



Threat

Memory corruption

- ▶ Tasks affect safety related memory

Insufficient execution time

- ▶ QM task blocks CPU
- ▶ OS does not provide CPU slot

Solution

Memory encapsulation & Context save

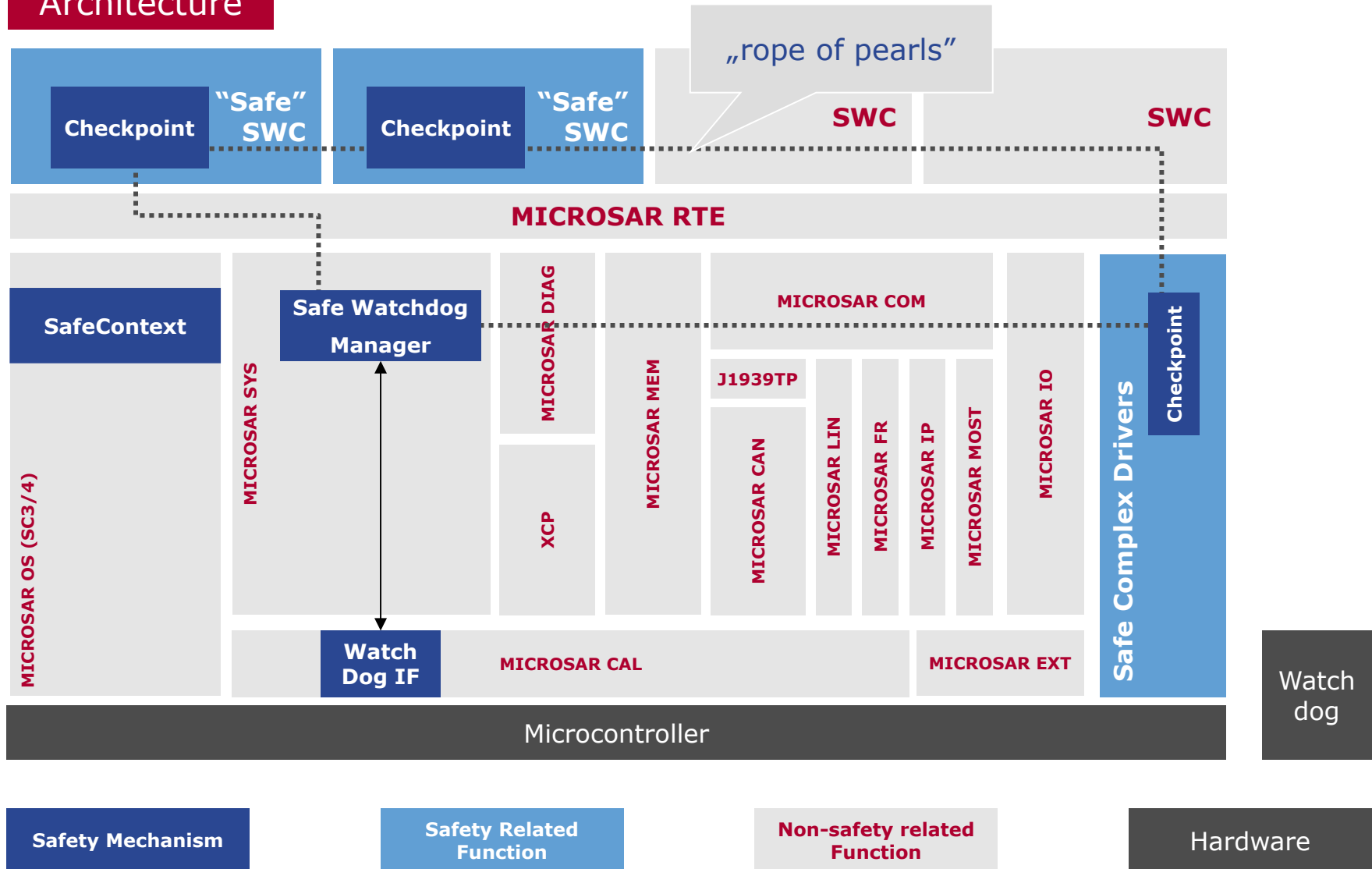
- ▶ Safety relevant tasks run in separated memory segments
- ▶ Memory Protection Unit (MPU)
- ▶ OS SC3 (QM) incl. SafeContext (ASIL D)

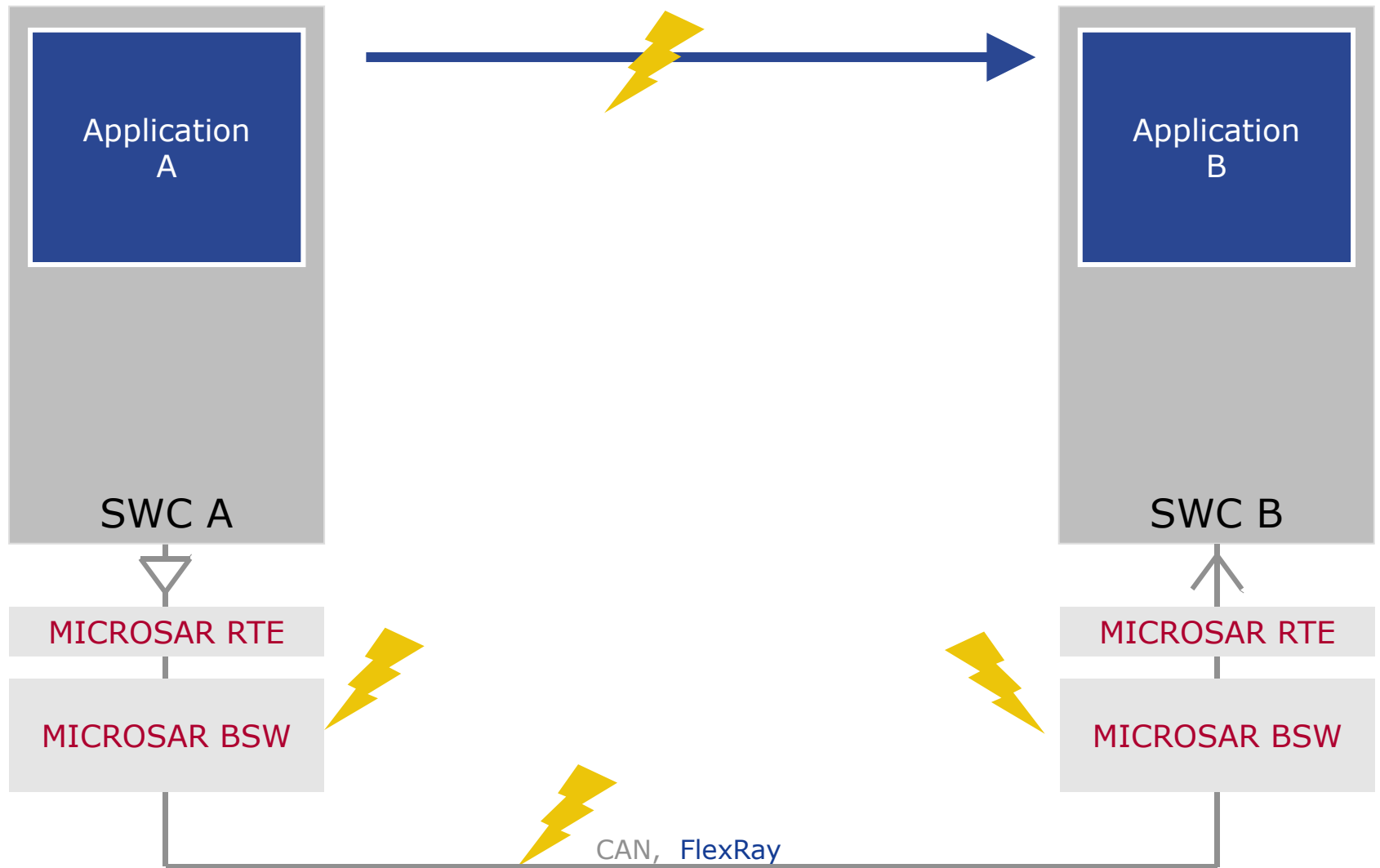
Program Flow Monitoring

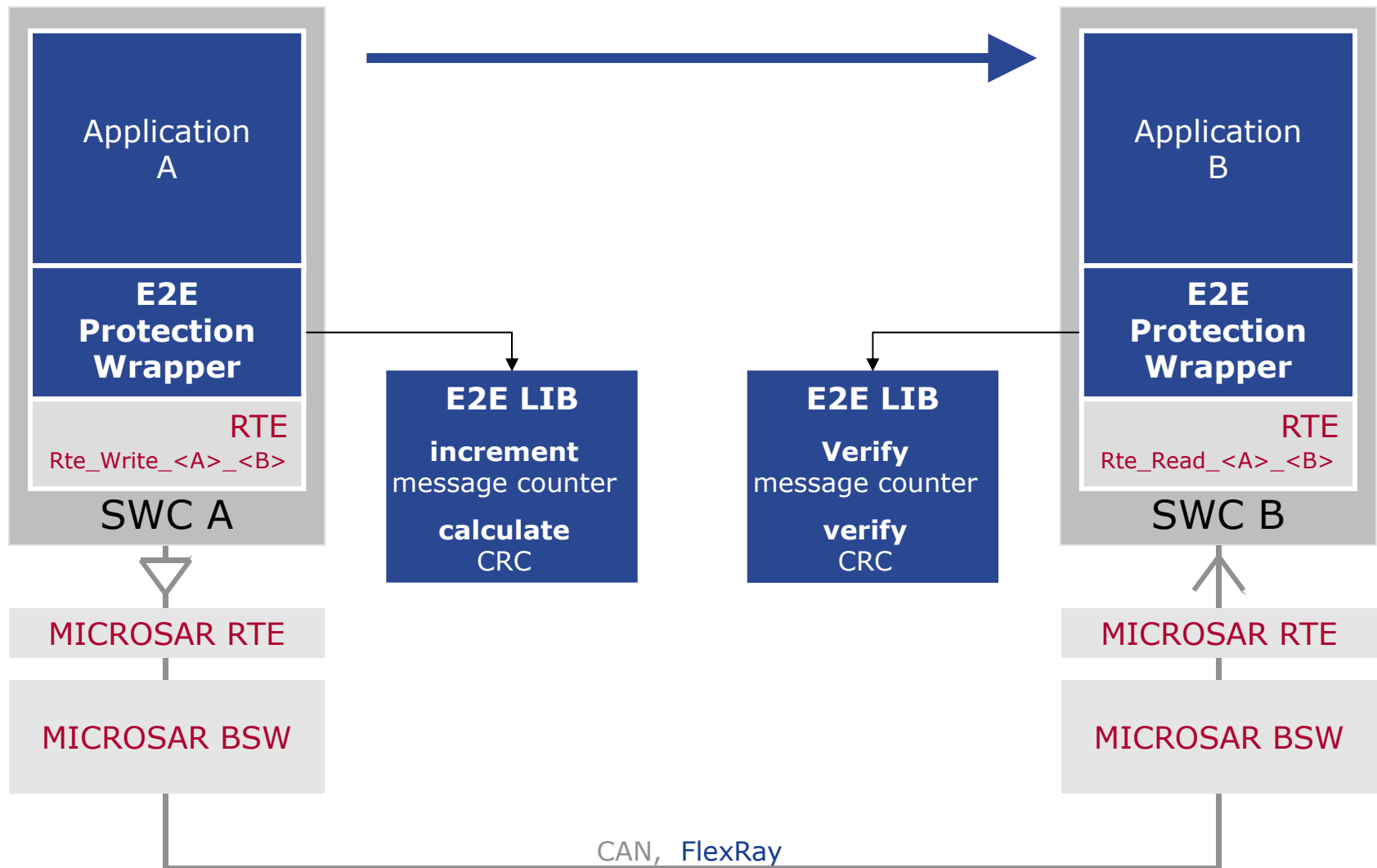
- ▶ Checks correct execution of safety relevant tasks
- ▶ Supervision by independent HW Watchdog (e.g. challenge/response)
- ▶ compliant to AUTOSAR 4.0

SafeExecution

Architecture

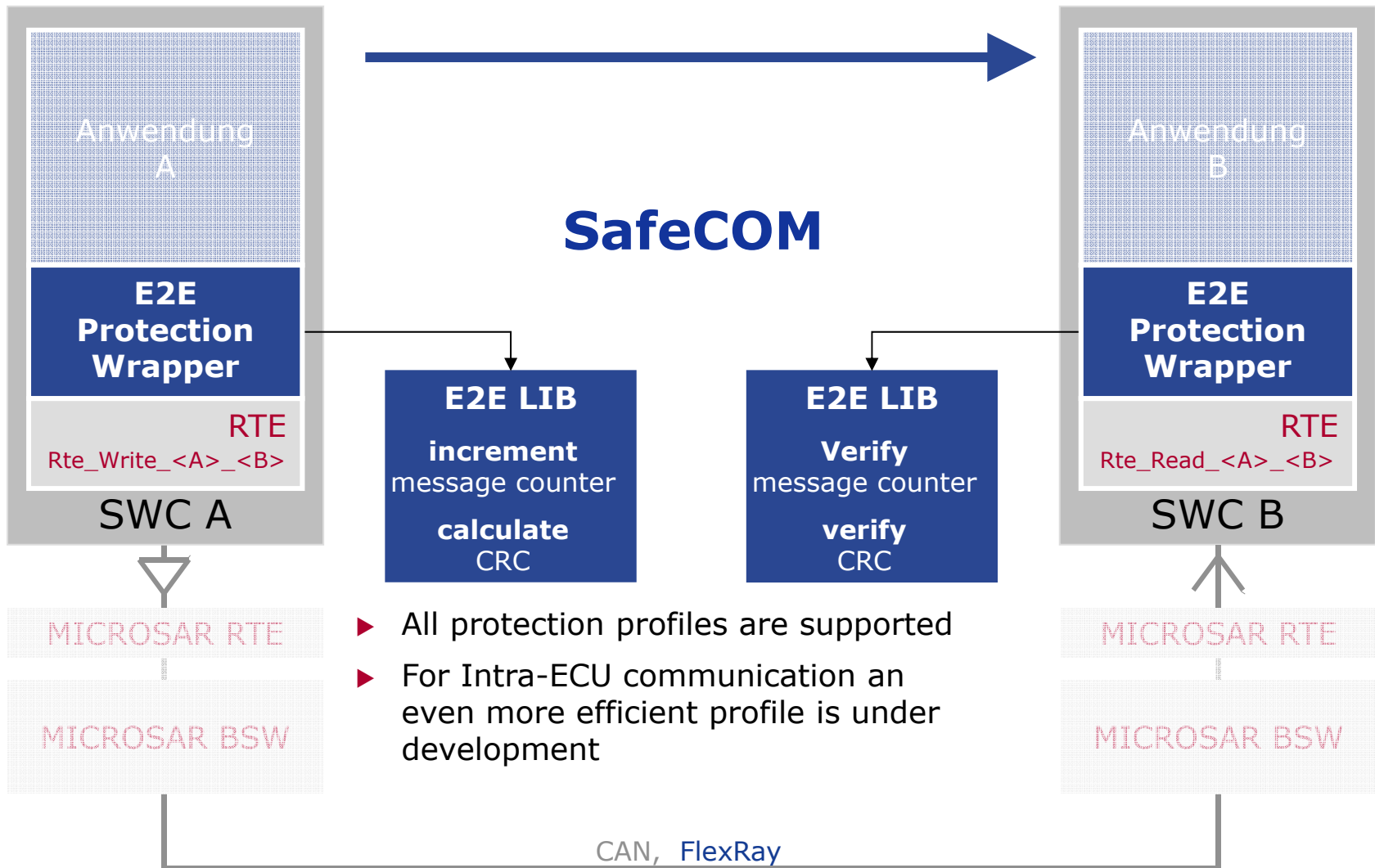






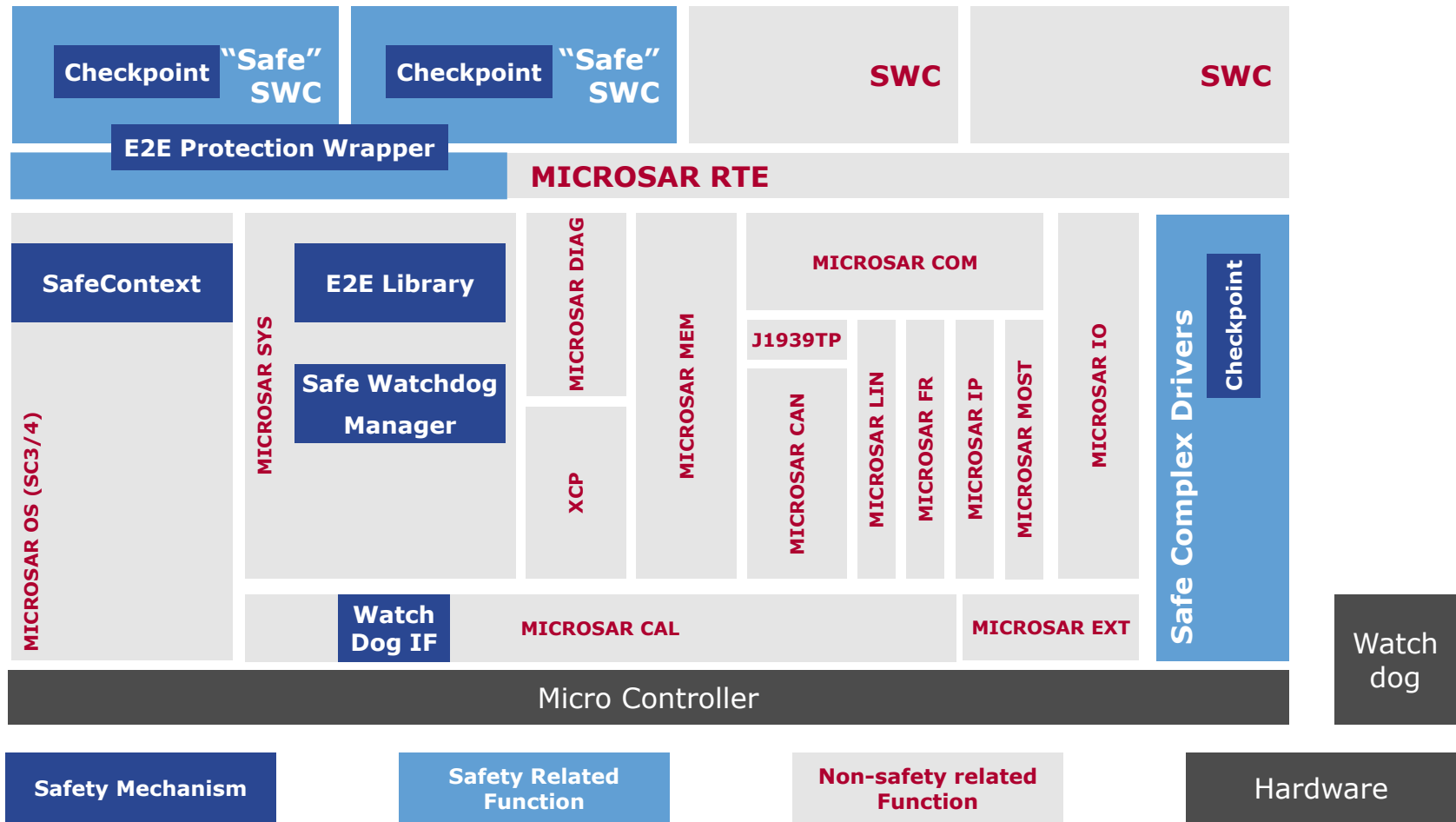
SafeCOM

Solution



MICROSAR Safe

- ▶ ... is the AUTOSAR basic software (incl. RTE) of Vector
- ▶ ... combined with safety mechanisms developed by TTTech **SafeExecution** and **SafeCOM**



Safety Standard ISO 26262

- Goals:
1. Avoid failures
 2. Make unavoidable failures safe

Determine Risk (ASIL = Automotive Safety Integrity Level)

Product Measures

Technical measures against **random** HW failures:

- ▶ Redundancy
- ▶ Diagnostics
- ▶ Self-tests
- ▶ ...

Technical measures against **systematic** HW and SW failures:

- ▶ Redundancy
- ▶ Diagnostics
- ▶ Self-tests
- ▶ ...
- ▶ Modular HW/SW architecture
- ▶ Architecture patterns
- ▶ Defensive programming
- ▶ ...

Development Process

Methodological measures to ensure the application of a safety-conform development process:

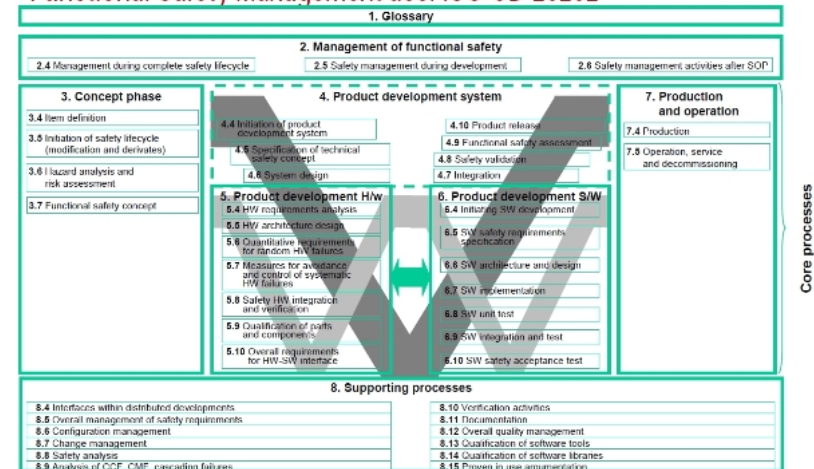
- ▶ Design methods
- ▶ Analysis techniques
- ▶ Test methods
- ▶ Safety case
- ▶ Configuration management
- ▶ ...

MICROSAR Safe

Qualification according to ISO 26262

- ▶ Tasks for ISO 26262 projects
 1. Safety management
 2. Hazard and risk analysis
 3. Definition of safety goals
 4. ...
 5. Classification of tools used
 6. ...
- ▶ Safety elements out of context
 - ▶ Developed according to ASIL-D
 - ▶ Certified by TÜV or similar organization
 - ▶ Integration according to Safety Manual
- ▶ QM Software
 - ▶ No special process required – after risk analysis

Functional Safety Management acc. ISO CD 26262



MICROSAR Safe

- ▶ ... allows the coexistence of software with different integrity levels
- ▶ ... detects and inhibits violations regarding runtime or memory (Freedom of Interference)
- ▶ ... protects communication end-to-end
- ▶ All modules with safety mechanisms are
 - ▶ developed according to ASIL-D
 - ▶ delivered with a Safety Manual
 - ▶ certified by TÜV or comparable organization
- ▶ Related tools are developed and qualified according to the appropriate Tool Confidence Level (TCL)

Vector and TTTech support their customers to develop an optimal safety concept up to ASIL-D

- ▶ We will send you the slides of this webinar.
- ▶ 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 them to **all participants**.
- ▶ Contact data for additional questions, product information or presentation :
 - ▶ Helmut.brock@vector.com
 - ▶ +49 (0) 711 80670 400
 - ▶ embedded@de.vector.com

Thank you for your attention.

For detailed information please have a look at:

www.vector.com

www.tttech.com

Authors:

Helmut Brock

Carsten Weich

Joachim Kalmbach