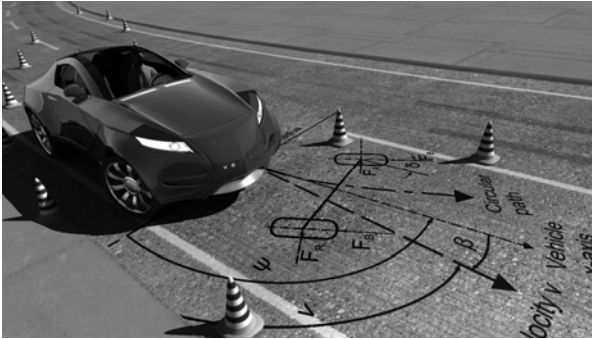


## **MICROSAR Safe**

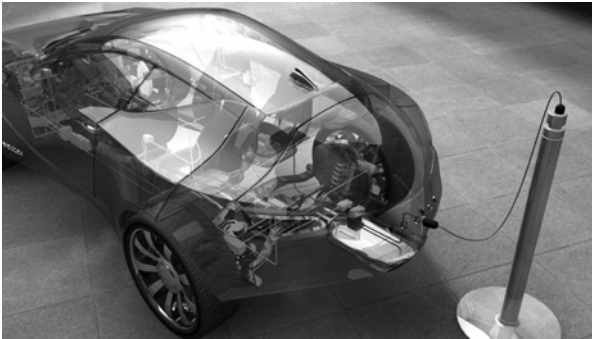
### AUTOSAR Basic Software for Safety Related Applications

Martin Fassl  
Dr. Günther Heling



## 1. Driver Assistance

→ **Autonomous Driving**



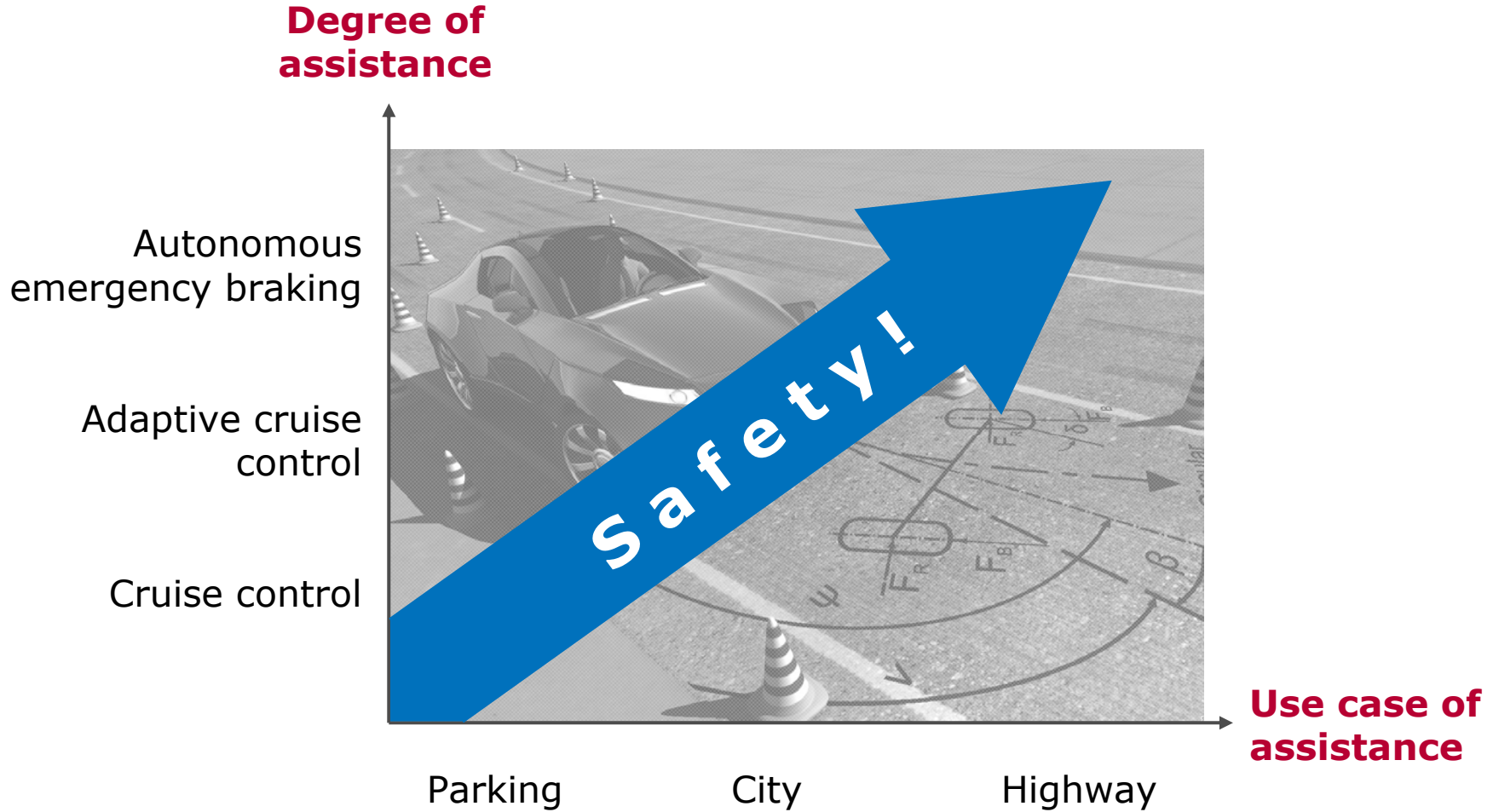
## 2. Electrification

→ **Zero Emission (locally)**



## 3. Connectivity

→ **Always On**



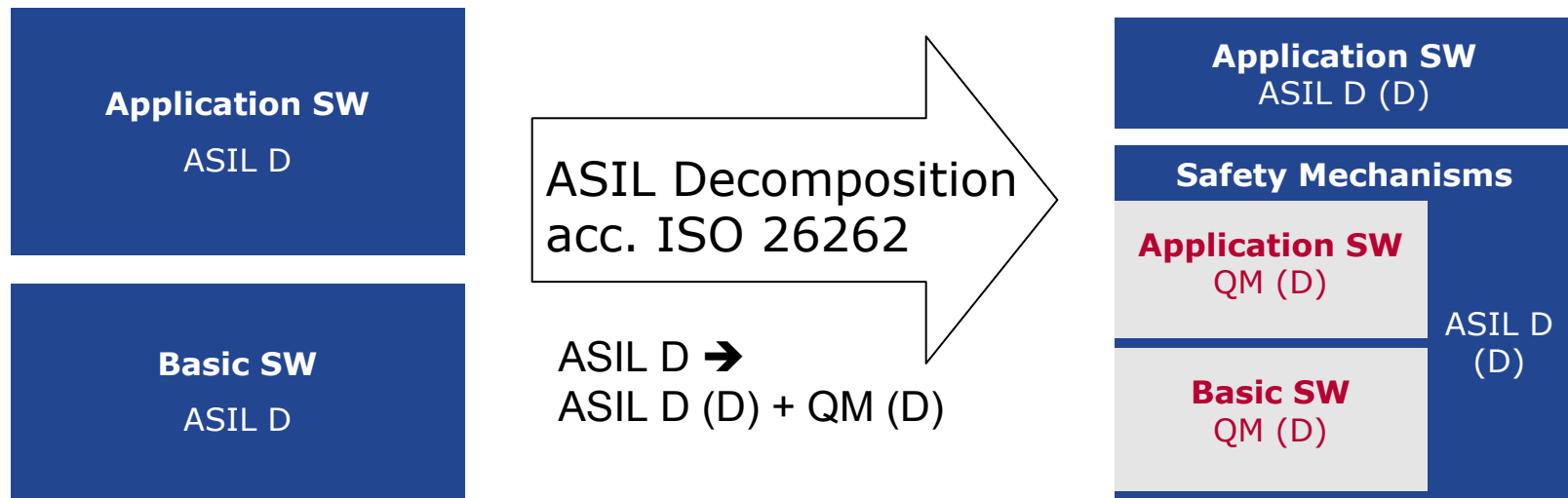


**1 ECUs with safety goals acc. ISO 26262  
are no longer an exception**

2

3

4



## The **safety mechanisms**

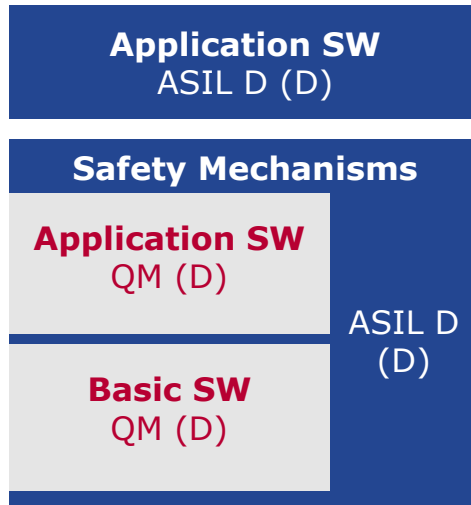
- ▶ detect and handle faults
  - > in the basic SW
  - > in the application SW
  - > in the hardware
- ▶ and thus allow the coexistence of SW with different integrity levels

**1 ECUs with safety goals acc. ISO 26262  
are no longer an exception**

**2 Fulfillment of safety goals does not require  
100% software conform to target ASIL**

3

4



## Protection:

### 1. Memory encapsulation

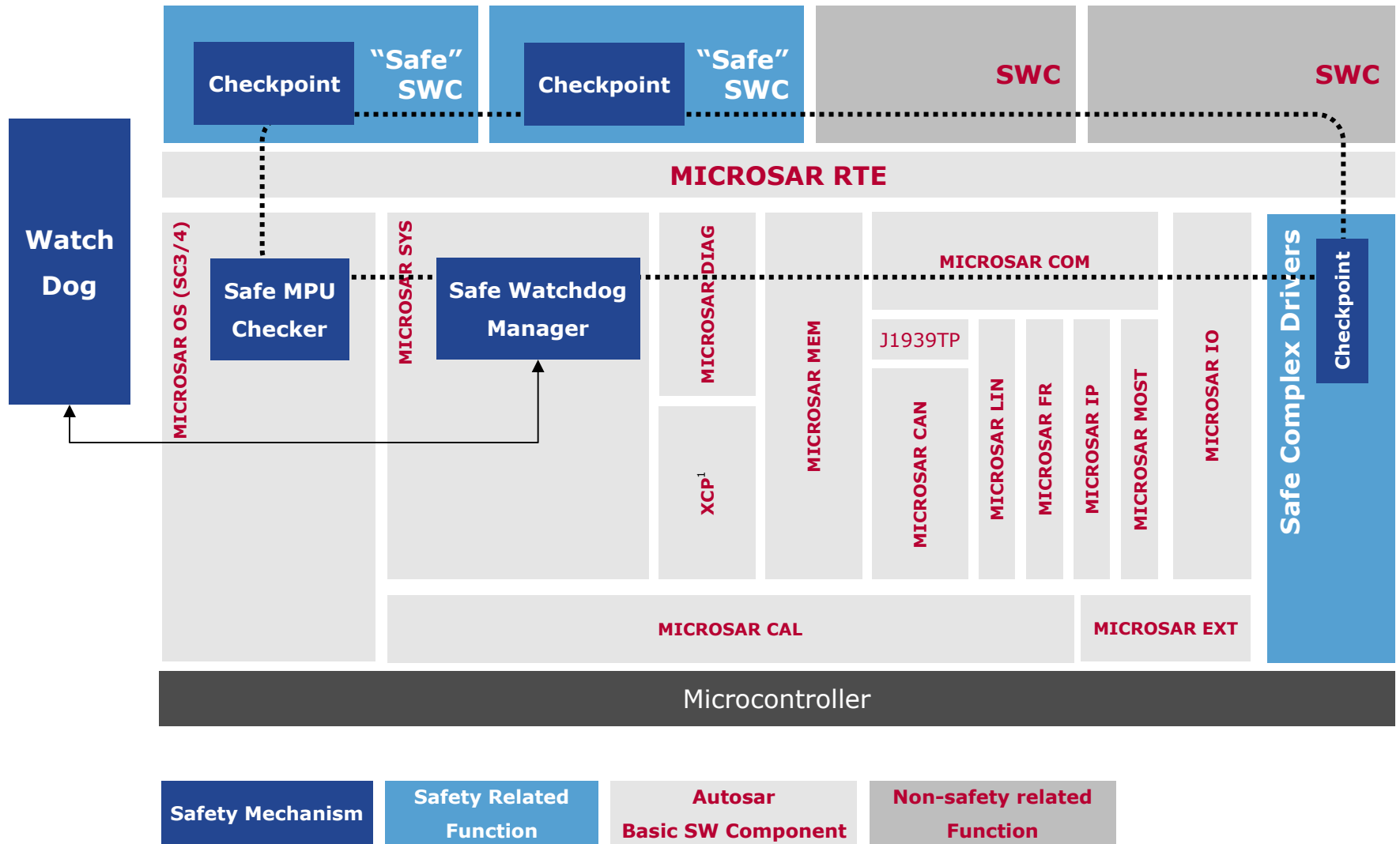
- ▶ Tasks in different memory segments
- ▶ Memory Protection Unit (MPU)
- OS SC3 (QM)+ MPU Checker (ASIL D)

### 2. Program Flow Monitoring

- ▶ Checks correct execution of safety tasks
- ▶ Supervision by independent HW-Watchdog
- According to AUTOSAR 4.0

provided by **SafeExecution**

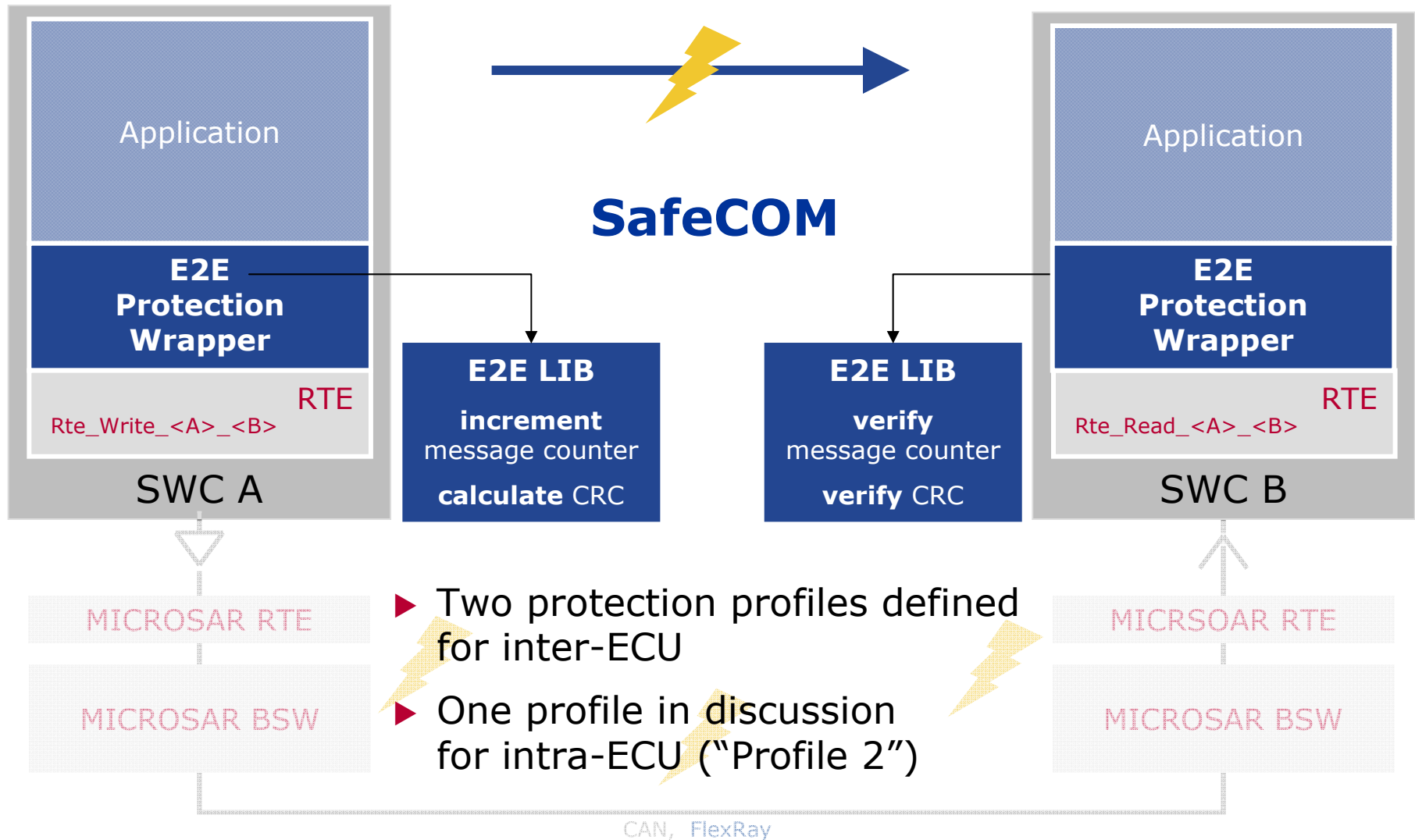
- ensuring "Freedom from Interference" and
- reaction within max. error reaction time



1. HW-support for memory protection needed (MPU)
2. Independent element for watchdog functionality needed
3. SafeExecution has to be started correctly (safe startup code)
4. Proper selection of checkpoints to cover safety related sequence of the program flow
5. Watchdog Manager has to be configured according to checkpoints and error reaction time
- 6. Watchdog Manager has to be scheduled by OS**
7. Proper configuration of memory protection to define the safety related memory partitions

Additional remark:

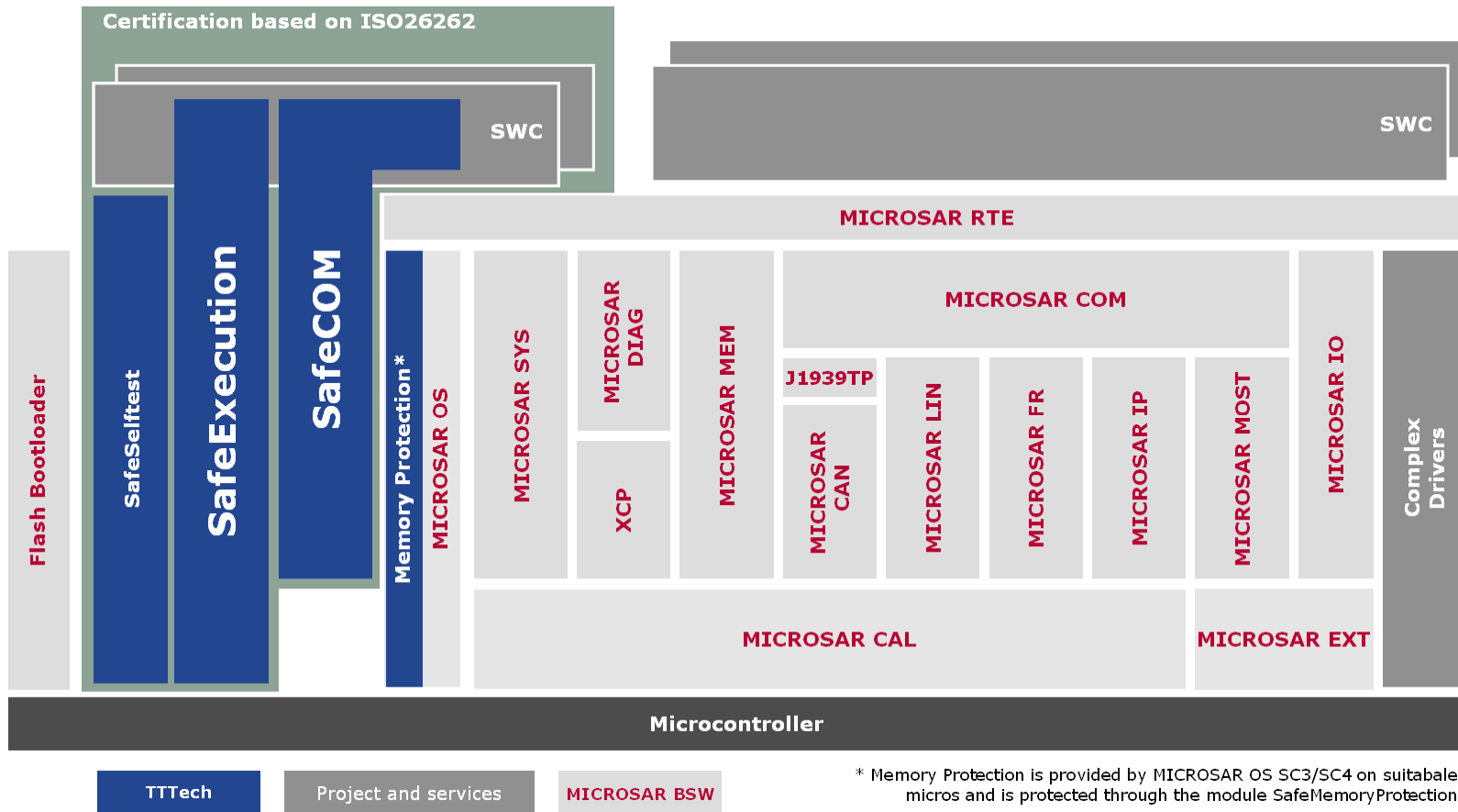
- ▶ **HW has to comply with the required ASIL**



- ▶ Two protection profiles defined for inter-ECU
- ▶ One profile in discussion for intra-ECU ("Profile 2")

E2E: End-to-End

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



## SafeExecution:

- |                      |                    |         |
|----------------------|--------------------|---------|
| ▶ Beta release       | Infineon TriCore   | Q4/2010 |
|                      | TI TMS570 (t.b.c.) | Q1/2011 |
| ▶ Production Release | 1st platform       | Q2/2011 |
| ▶ Qualified Release  | 1st platform       | Q4/2011 |

## SafeCOM:

- |                      |           |
|----------------------|-----------|
| ▶ Beta Release       | available |
| ▶ Production Release | Q1/2011   |
| ▶ Qualified Release  | Q2/2011   |

- ▶ as part of AUTOSAR-BSW 3.x; planned for 4.0
- ▶ and CANbedded

- 1 **ECUs with safety goals acc. ISO 26262 are no longer an exception**
- 2 **Fulfillment of safety goals does not require 100% software conform to target ASIL**
- 3 **“MICROSAR Safe” is the basic software for ECUs with safety goals up to ASIL-D**

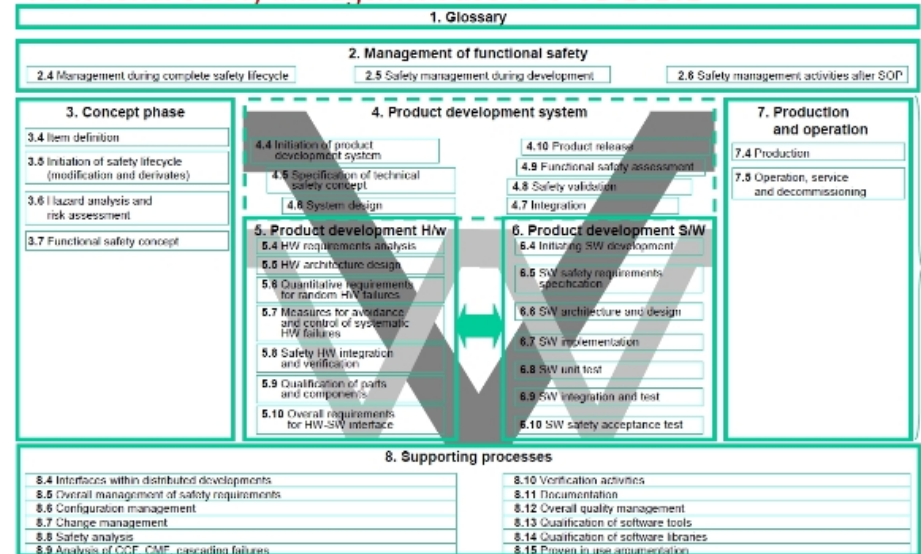
4

- ▶ “Safety elements out of context” based on safety assumptions
  - ➔ to be integrated according to Safety Manual
  - ➔ to be confirmed:
    - > Do assumptions comply with safety requirements ?

## ➔ Additional 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. ...

Functional Safety Management acc. ISO CD 26262



- 1 ECUs with safety goals acc. ISO 26262 are no longer an exception**
- 2 Fulfillment of safety goals does not require 100% software conform to target ASIL**
- 3 MICROSAR Safe is the basic software for ECUs with safety goals up to ASIL D**
- 4 TTTech and Vector provide overall support for ISO 26262 projects**

- 1 ECUs with safety goals acc. ISO 26262 are no longer an exception**
- 2 Fulfillment of safety goals does not require 100% software conform to target ASIL**
- 3 MICROSAR Safe is the basic software for ECUs with safety goals up to ASIL D**
- 4 TTTech and Vector provide overall support for ISO 26262 projects**

Thank you for your attention.

For detailed information please have a look at:

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

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

Authors:

Martin Fassl  
TTTech Automotive GmbH  
Schönbrunner Straße 7  
A-1040 Wien

Dr. Günther Heling  
Vector Informatik GmbH  
Ingersheimer Str. 24  
D-70499 Stuttgart