MICROSAR Safe

- A vector and TTTech Solution -
Software for Safety ECUs

⇒ Mixed ASIL ECUs
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 software with different integrity levels
Requirement for Coexistence
SafeExecution
Freedom from Interference

Application A
- Task 1 (activate) → Task 2

RAM
CPU

Application B
- Task 3 → ISR 1

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 protected memory partitions

Program Flow Monitoring
- Checks correct execution of safety relevant tasks
SafeExecution
Memory Protection

Software

- **Application A**
  - Task 1
  - Task 2

- **Application B**
  - Task 3

**Operating System**
- Context Switching

**MPU**

**RAM**

- **Task 1**
  - Stack
  - Application Data

- **Task 2**
  - Stack
  - Application Data

- **Task 3**
  - Stack
  - Application Data

© 2013. Vector Informatik GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector.

Slide:
SafeExecution

Memory Protection

Software

- Application A
  - Task1
  - Task2

- Application B
  - Task3

Operating System

- Context Switching

RAM

- Task 1
  - Stack
  - Application Data

- Task 2
  - Stack
  - Application Data

- Task 3
  - Stack
  - Application Data
SafeExecution
Program Flow Monitoring

- Correct timing (Deadline, Frequency)
- Correct sequence
- Safe Watchdog handling

Time

Task A

Task B

Task A

Task C

Watchdog

SafeWatchdog Manager
SafeExecution Architecture

MICROSAR RTE

Safe Context

Safe Watchdog Manager

Wdg Drv

MICROSAR OS (SC3/4)

MICROSAR MEM

MICROSAR CAN

J1939TP

Safety Mechanism

Watchdog

Checkpoint

“Safe” SWC

Safe Context

Checkpoint

“Safe” SWC

MICROSAR DIAG

XCP

Safety Related Function

Non-safety related Function

Checkpoint

Safe Complex Drivers

SWC

Architecture

“rope of pearls”

Watch dog

Hardware
Communication / Data Exchange

Internal

External
Safe Communication

**“Safe” SWC A**
- MICROSAR OS (SC3/4)
- MICROSAR SYS
- MICROSAR DIAG
- MICROSAR MEM
- MICROSAR CAL

**“Safe” SWC B**
- MICROSAR RTE
- MICROSAR COM
- J1939TP

**SWC C**
- MICROSAR EXT
- MICROSOAR IO
- MICROSAR LIN
- MICROSAR IP
- MICROSAR CAL
- MICROSAR EXT

**SWC D**
- Safe Complex Drivers

**Non-safety related Function**
- MICROSAR FR
- MICROSAR MOST
- MICROSAR 1D

**Microcontroller**
SafeRTE – Freedom from Interference

- SafeRTE realizes correct communication
- Freedom from Interference is realized by SafeContext regarding Memory

* Hardware ASIL can be raised by software means
SafeRTE – Tool Based Qualification

Design of safety related communication

Design & Configuration

ECU Extract of System Configuration
ECU Configuration Description
...

RTE Generator

rte.c
tte.h

TCL1

RTE Verify

Report on Integrity

TCL2

Configuration Feedback

© 2013. Vector Informatik GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector.
Slide:
SafeCOM Solution

Application A

E2E Protection Wrapper

RTE
Rte_Write_<A>_<B>

SWC A

MICROSAR RTE

MICROSAR BSW

E2E LIB
increment
message counter

calculate
CRC

E2E LIB
Verify
message counter
verify
CRC

CAN, FlexRay

E2E LIB
verify
message counter

verify
CRC

E2E Protection Wrapper

RTE
Rte_Read_<A>_<B>

Application B

SWC B

MICROSAR RTE

MICROSAR BSW
SafeCOM Solution

All protection profiles are supported

E2E LIB
increment message counter
calculate CRC

E2E LIB
verify message counter
verify CRC

Can, FlexRay

© 2013. Vector Informatik GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector.
Slide: 17
MICROSAR Safe

- is the AUTOSAR basic software of Vector
- combined with safety mechanisms (SafeContext, SafeWatchdog, SafeRTE, SafeCOM) developed by TTTech and Vector

© 2013. Vector Informatik GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector.
Slide: 18
MicrosarSafe is also available for Multi-core Architectures

For further information please contact embedded@de.vector.com
MICROSAR Safe

Integration of SEooC

Your Project

Risk / Hazard Analysis / Safety Requirements

Development

ASIL Software

Vector Products

MICROSAR SAFE

Safety Requirements

Development

- SEooC
  - Microsar Safe
    - OS SafeContext / SafeWatchdog
    - SafeRTE
    - Microsar SafeCOM

- Characteristics
  - Developed according to ASIL-D
  - Certified by TÜV or similar organization

- Integration
  - Safety Case
  - Safety Manual
    - Assumptions on Safety Goals
    - Functional extensions and restrictions
    - Integration requirements, e.g. interrupt handling
    - Process requirements, e.g. reviews

© 2013. Vector Informatik GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector.

Slide: 20
Thank you for your attention.

For detailed information please have a look at:

www.vector.com
www.tttech.com

- We stay online for some more minutes to answer your questions. Please write your questions in the Q&A window.

- Registration to the upcoming Webinars and the list of recorded Webinars:
  http://www.vector.com/vi_webinars_en.html

- Contact data for additional questions, product information or presentation:
  - Helmut.brock@vector.com
  - +49 (0) 711 80670 400
  - embedded@de.vector.com