MICROSAR

Document Information

History

Author	Date	Version	Remarks
	- -		
	- -		
	- -		
	- -		
	- -		
	- -		
	- -		
	- -		
	- -		
	- -		
	- -		
	- -		-

Reference Documents

No.	Source	Title	Version
[1]			
[2]			
[3]			
[4]			
[5]			
[6]		-	
[7]		-	
[8]		-	
[9]		-	
[10]		-	
[11]		-	
[12]		- - - -	
[13]		- - - -	
[14]		- - - -	

Contents

Illustrations

Tables

1 Introduction

1.1 Purpose

-

-

1.2 Scope

-

1.3 Definitions

No.	Term	Description
		-

-

1.4 Overview

-

-

2 Functional safety on system level

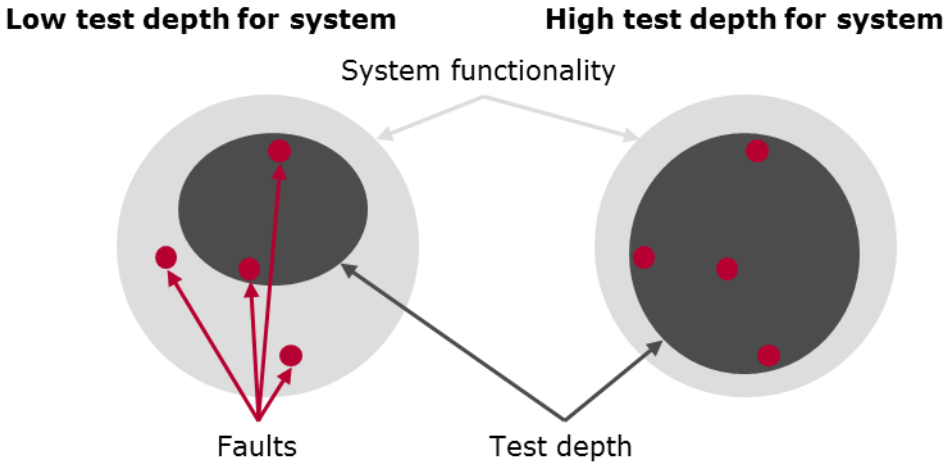
-

functional safety *absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems*

Malfunctioning behavior *failure or unintended behavior of an item with respect to its design intent*

Thus, a functionally safe system has to mitigate the risk associated with a failure and prevent unintended behavior.

2.1 Prevention of unintended behavior



-

>

>

>

Thus, the system should be as simple as possible to keep it testable.

-

Thus, the system should be as deterministic as possible to ease verification.

2.2 Mitigation of risk associated with a failure

failure
fault Faults *random hardware faults*
technical safety requirements
fault **detect** *random hardware faults* **act**
safe state
Random hardware faults *permanent faults* *transient faults*

random hardware faults

permanent faults
hardware components
transient faults

- -

-
- -

Thus, we recommend the consideration of transient faults starting from ASIL B. For ASIL C systems transient faults must be handled appropriately.

fault *hardware component*

>

>

>

>

>

>

2.3 Fail-safe and fail-operational systems

- *random hardware fault* *safe state* *random hardware faults*

safe state *failure*

Thus, only fail-safe systems are considered in this guide.

faults *fail-operational*

- -

-

-

3 Recommendations on safety mechanisms

3.1 Integrity of the microcontroller

>
>
>

3.1.1 Operation in lock-step mode

enabling lock-step as early as possible in the boot process

diagnostic coverage

latent fault

3.1.2 Monitoring the temperature of the microcontrollers

3.1.3 Self-test of the microcontroller components

Thus, the requirements on self-tests are defined by the required ASIL.

- - -

3.2 Integrity of volatile data

>

>

3.2.1 Static tests of volatile memory

-

latent fault

3.2.1.1 Initial test of volatile memory

-

-

-

- -

Caution

-

3.2.1.2 Periodic tests of volatile memory

-

-

3.2.2 Protection of volatile memory through error correcting codes (ECC)

-

-

enabling the use of ECC-mechanisms as early as possible in the boot process

-

3.2.2.1 Redundant storage of data

-

-

-

-

Redundant storage of data is not supported by the Vector MICROSAR stack.

3.3 Integrity of non-volatile data

-

diagnostic coverage

-

-

diagnostic coverage

-

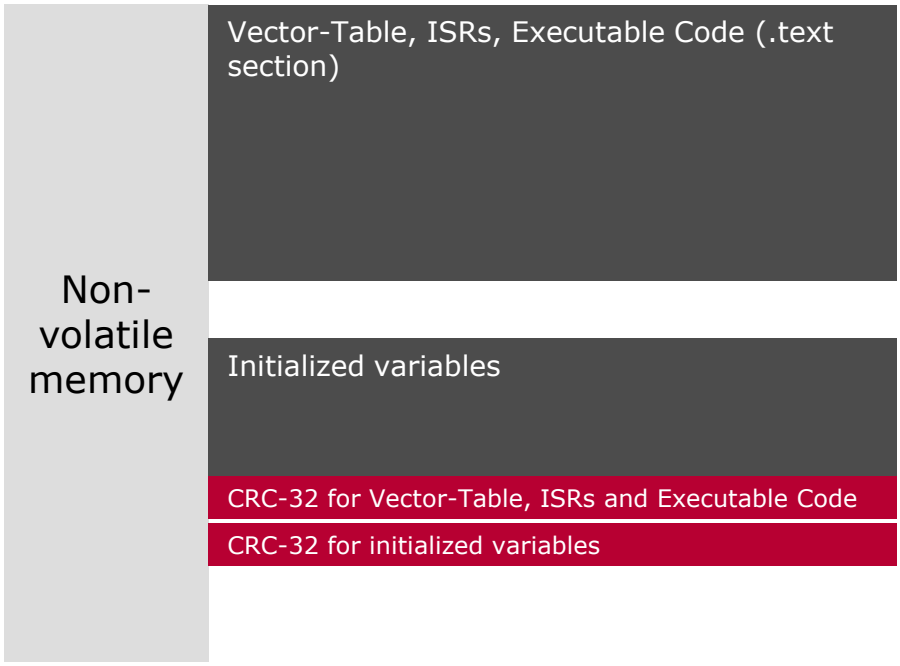
-

-

-

-

-



- -

3.3.1 Consistency of configuration and calibration data

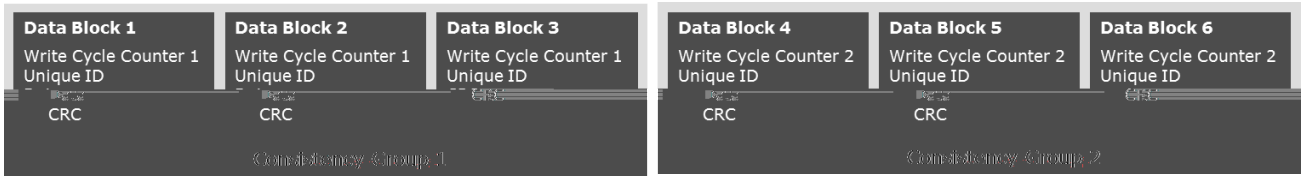
-

3.3.2 Securing non-volatile data with use of NVRAM Manager

-

-

-



-

-

-

3.4 Initialization of the microcontroller

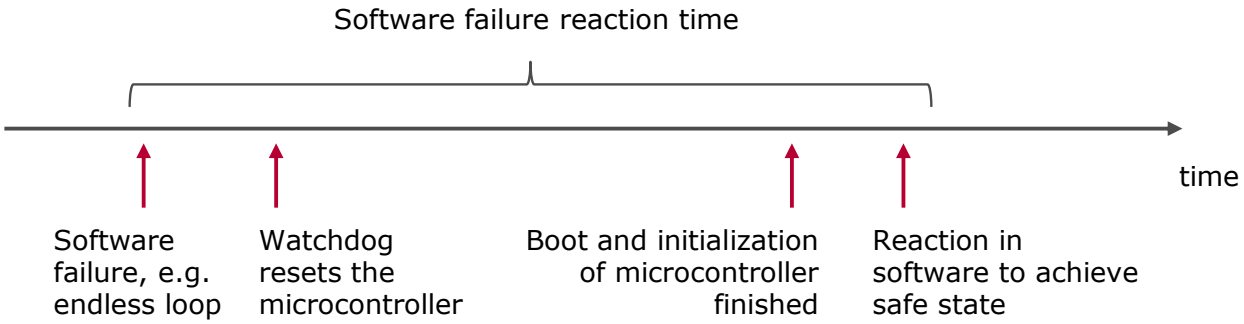
-

`StartOS()`

fault reaction

time

-



-

3.5 Separation in memory

-

freedom from interference

-

- -

-

freedom from interference

3.6 Separation in time

-

-

-

3.7 Scheduling

-

3.8 Communication

- -

-

- -

-

3.9 Input and output

- -

-

4 Example use-cases

-

4.1 ECU with direct I/O

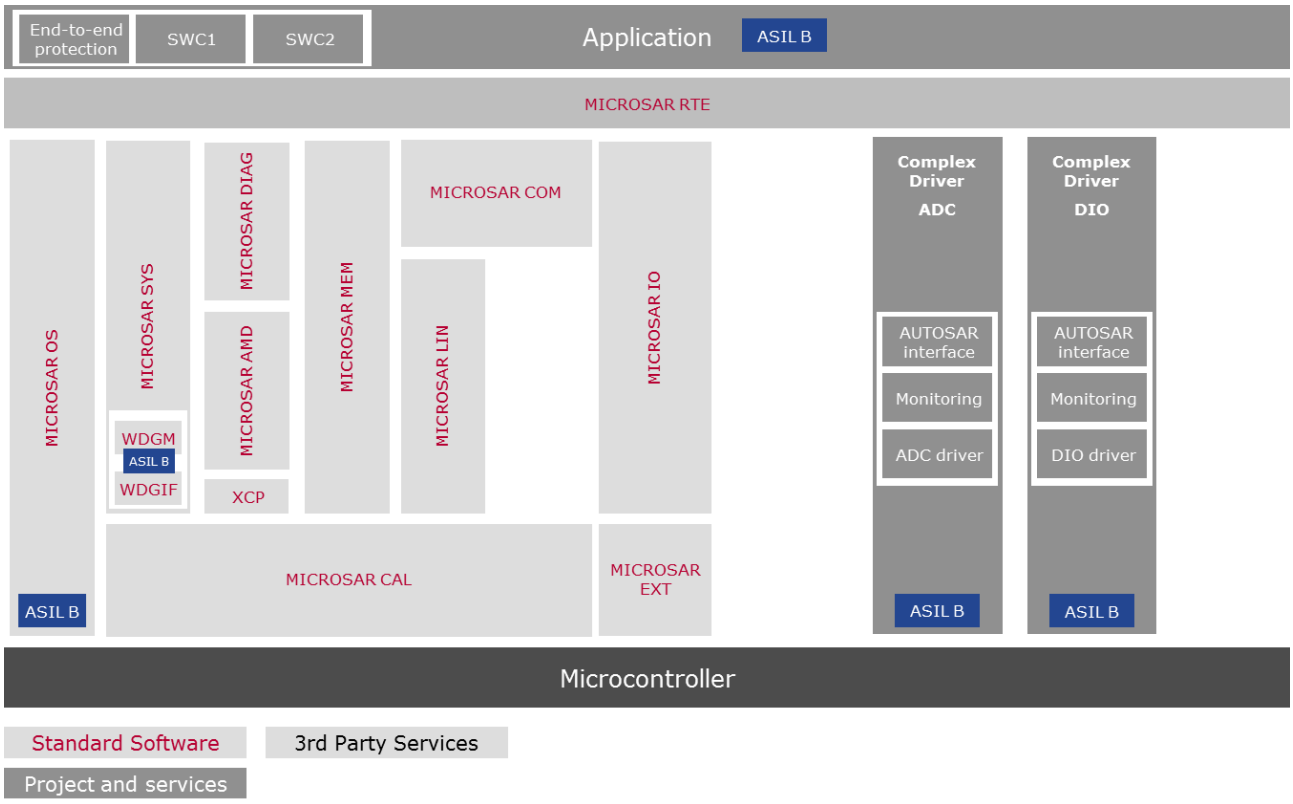
- -

-

-

- -

-

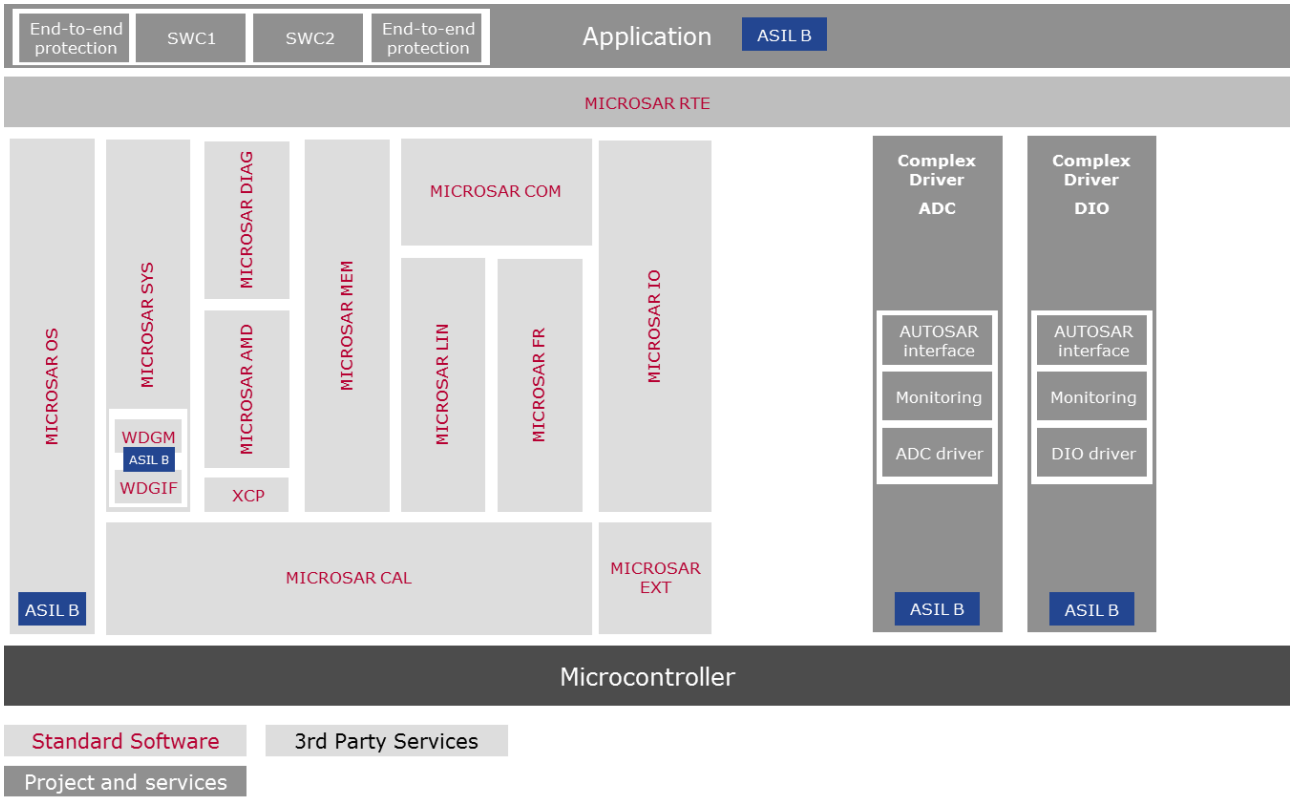


-

Property	Value
-	
-	
	-
	> >

- -

4.2 ECU with direct I/O and safety-related bus communication



Property	Value
-	
-	
	-
	>

> |
| | |

- - -

4.3 Mixed ASIL SWCs with safety-related bus communication

- -

-

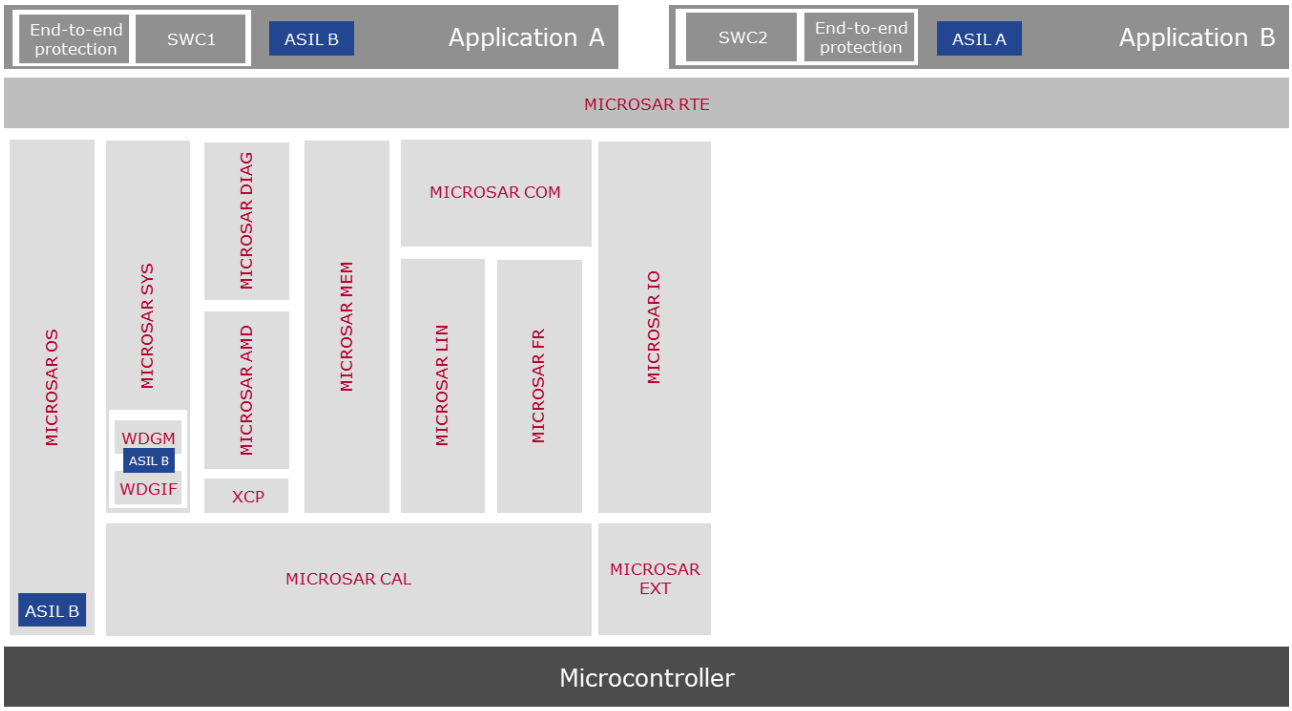
-

-

-

-

-



-

-

Property	Value
-	
-	
	-
	> - - > - - >

-

-

-

5 Recommendations for the MICROSAR stack

5.1 Initialization

-

1. -
2.
3. -

5.2 ECU State Manager (EcuM)

>

> -

>

5.3 Basic Software Mode Manager (BswM)

5.4 Development Error Tracer (Det)

-

5.5 Diagnostic Event Manager (Dem)

5.6 NVRAM Manager

5.7 Run-Time Environment (RTE)

5.8 End-to-End Protection (E2E)

5.9 Operating System (OS)

diagnostic coverage

5.10 Interrupt service routines (ISRs)

5.11 Microcontroller Abstraction Layer (MCAL)

-

6 Procedural requirements

>

>

>

7 Assumptions of Vector's safety solution

7.1 Assumptions of RTE

Assumption	Description	Can be shown by
	>	
	>	
	>	
	>	
	>	

Assumption	Description	Can be shown by
	> > > >	
	-	
	> > > > > > > > > > > > > >	

Assumption	Description	Can be shown by
	- -	

-

7.2 Assumptions of SafeWatchdog

Assumption	Description	Can be shown by
	> > > - - >	
	-	
	> >	
	-	
	-	
	-	

Assumption	Description	Can be shown by
	> - > 	

-

8 Glossary and Abbreviations

8.1 Glossary

8.2 Abbreviations

Abbreviation	Description
	- -

-

9 Contact

>
>
>
>
>
>