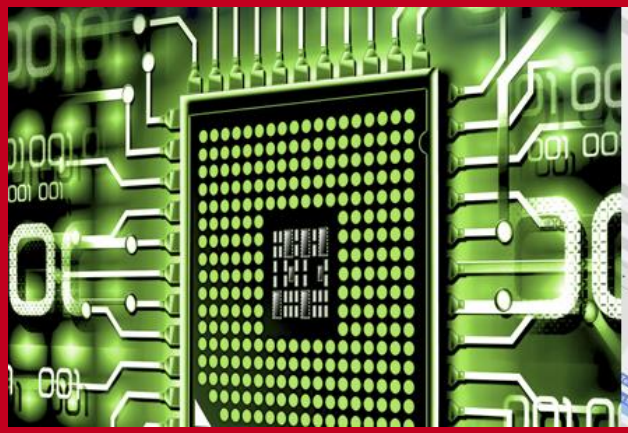
Functional Safety with XMC™

Dr. Kurt Boehringer, Head of Engineering, Hitex GmbH

April 16, 2015



High-Tech with History

- Hitex was founded in 1976 in Karlsruhe, Germany as a software company
- 39 years of experience in microcontroller technology
- Part of the Infineon Group since 2003
- Global setup with subsidiaries and partners in all regions
- Leading provider of development and software quality tools
- Security and power optimization solutions
- Extensive track record of services and project work

Agenda

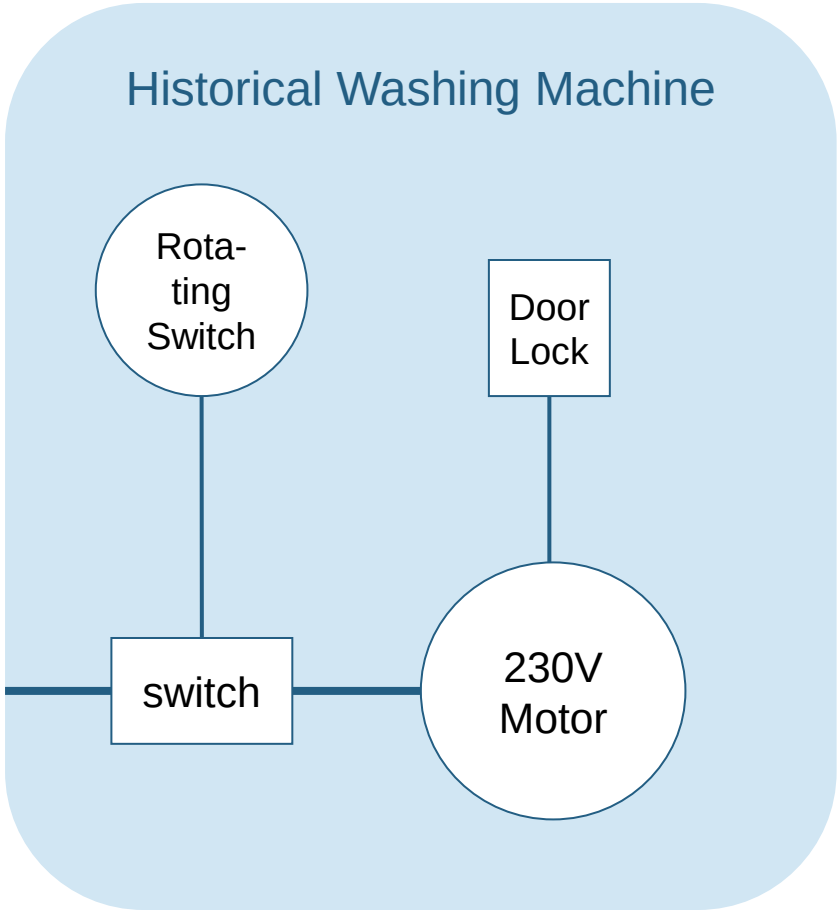
- Introduction into Functional Safety
- Functional Safety demands
- Class B Solution
- SIL/ASIL Solution
- Summary

Agenda

- **Introduction into Functional Safety**
- Functional Safety demands
- Class B Solution
- SIL/ASIL Solution
- Summary

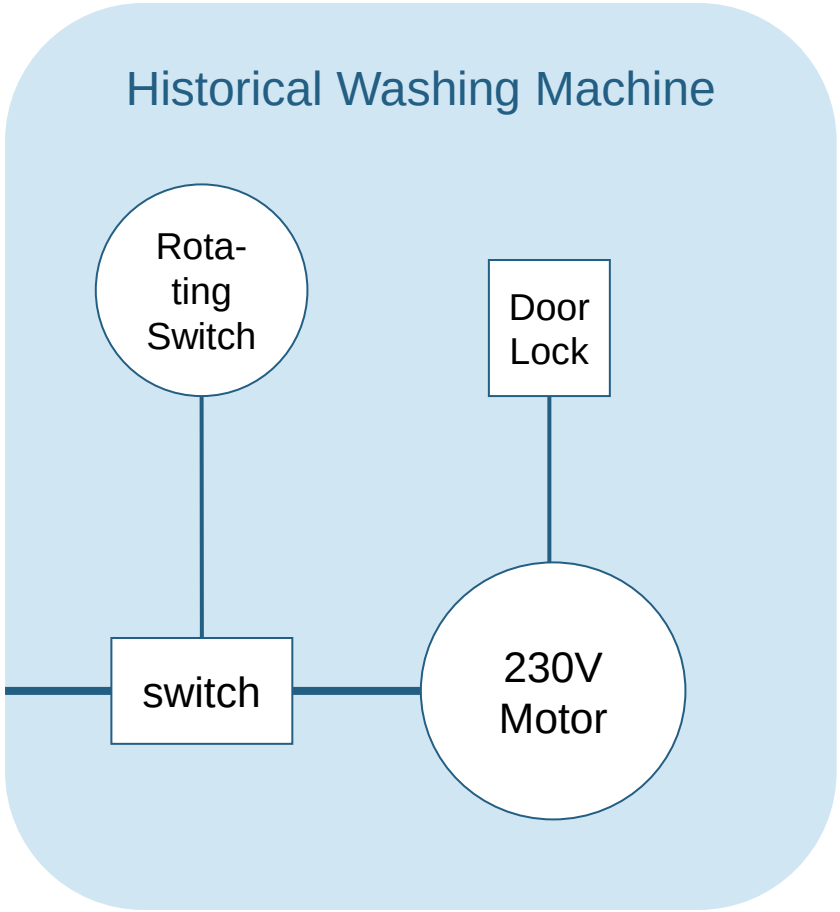
The world is changing

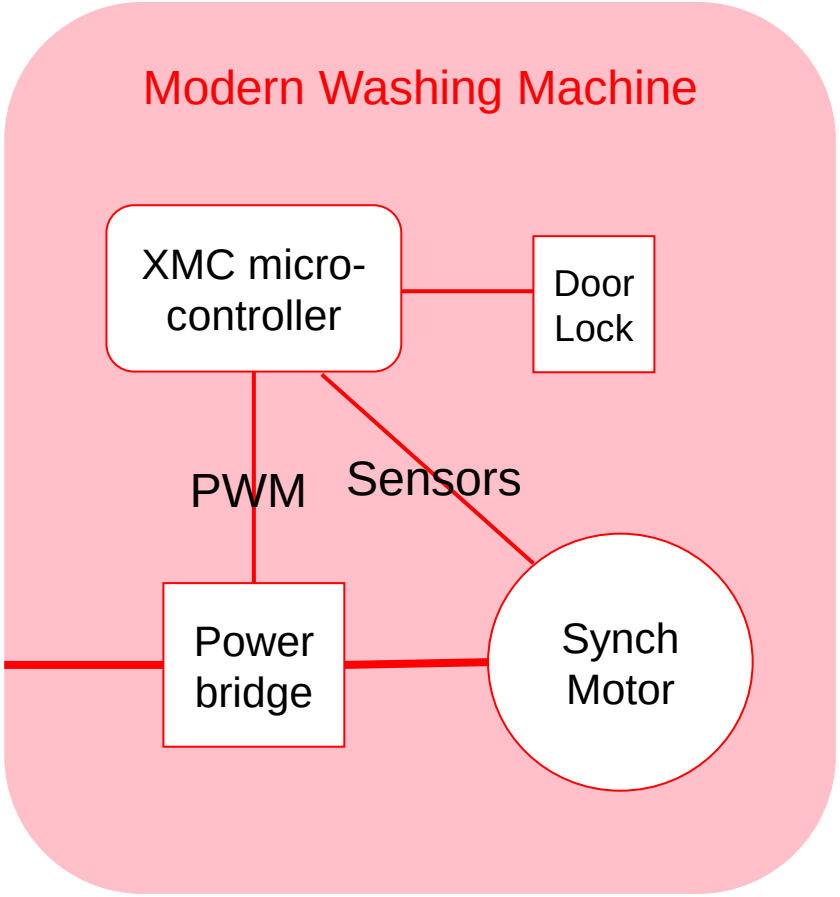
- Example: Washing Machine



The world is changing

- Example: Washing Machine

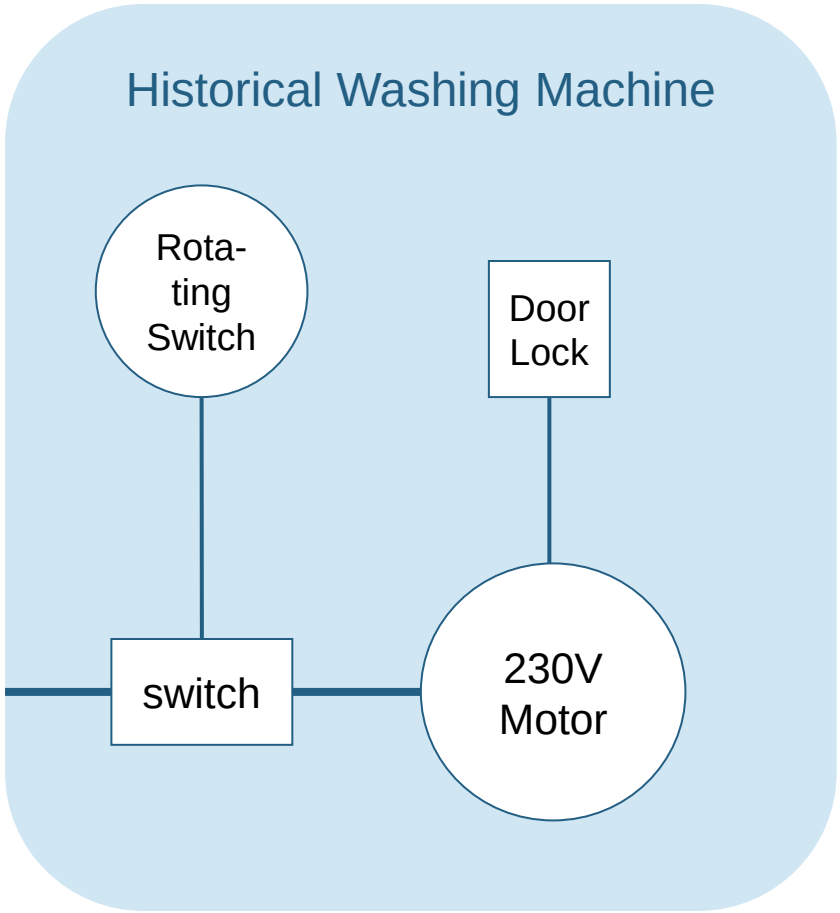


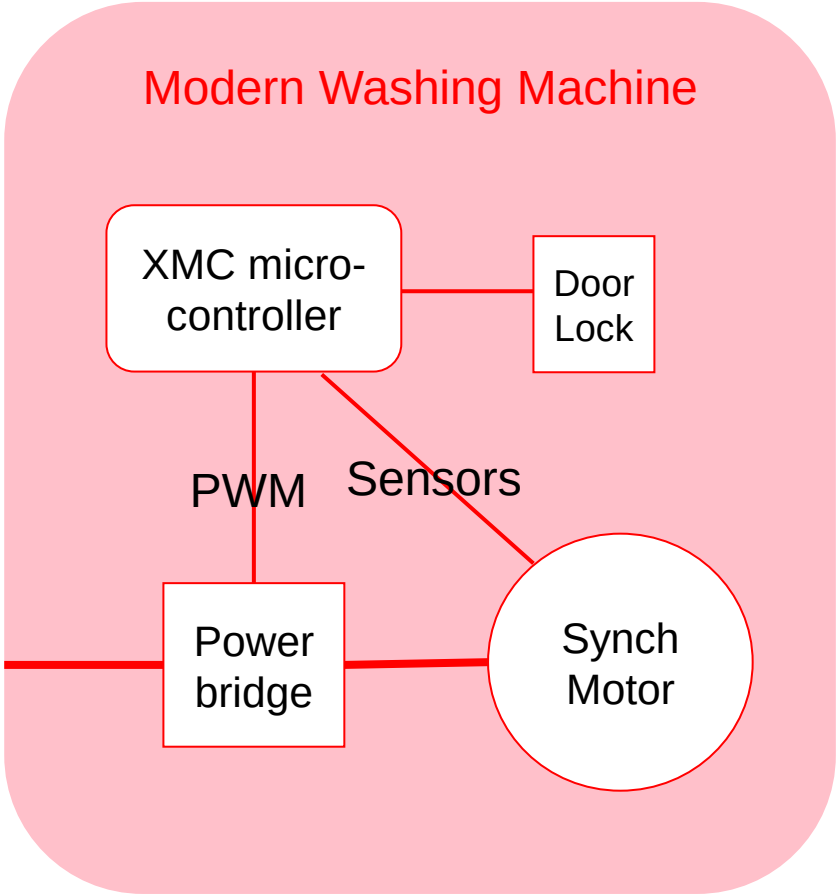


The world is changing

- Example: Washing Machine

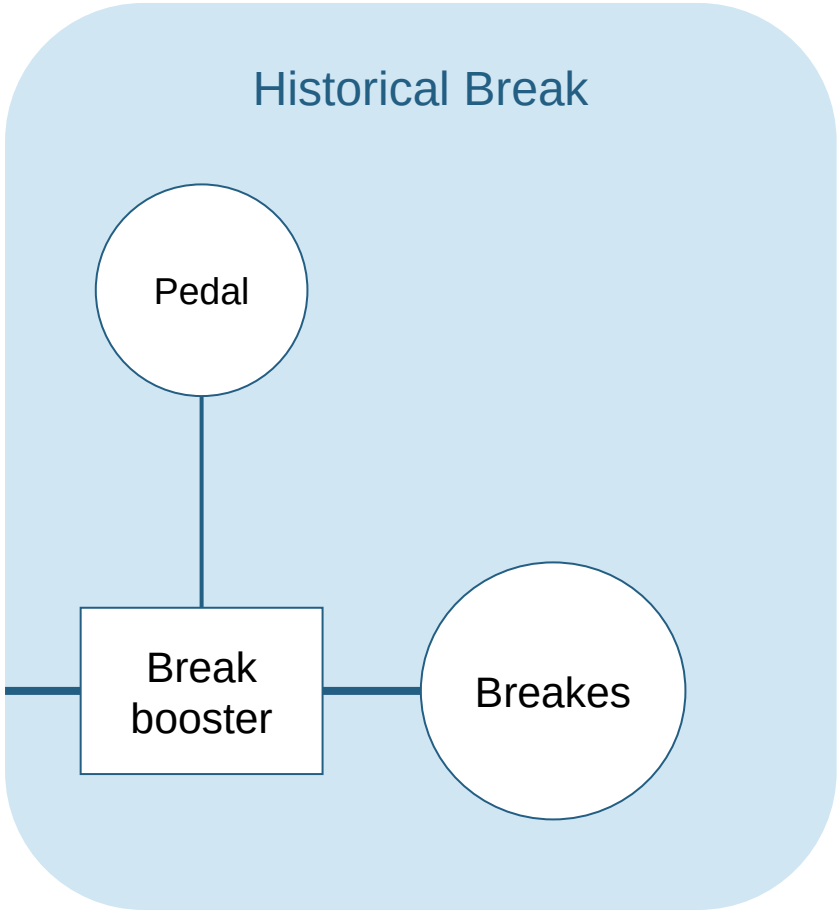
Microcontroller failure may lead to damage or even injury !





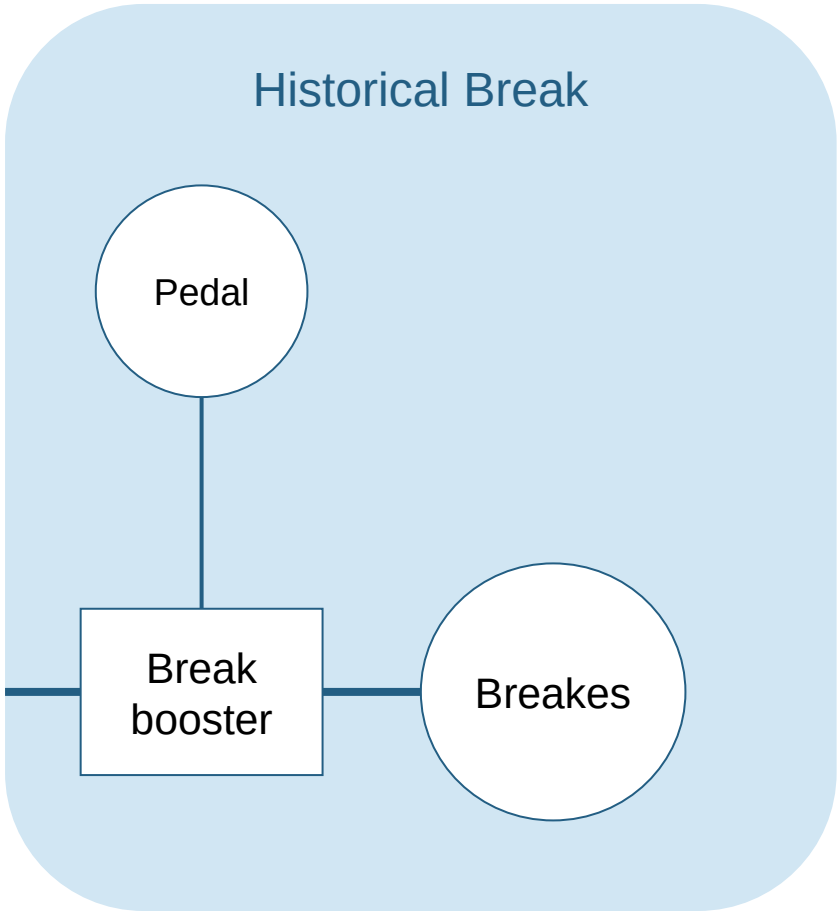
The world is changing

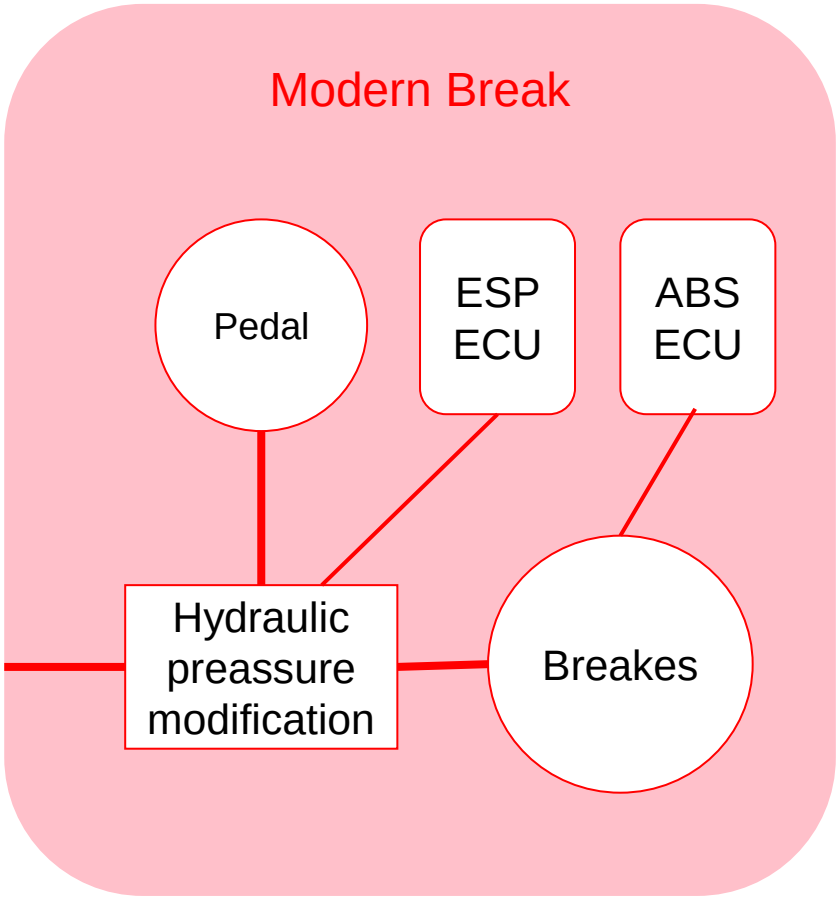
- Example: Car Break



The world is changing

- Example: Car Break

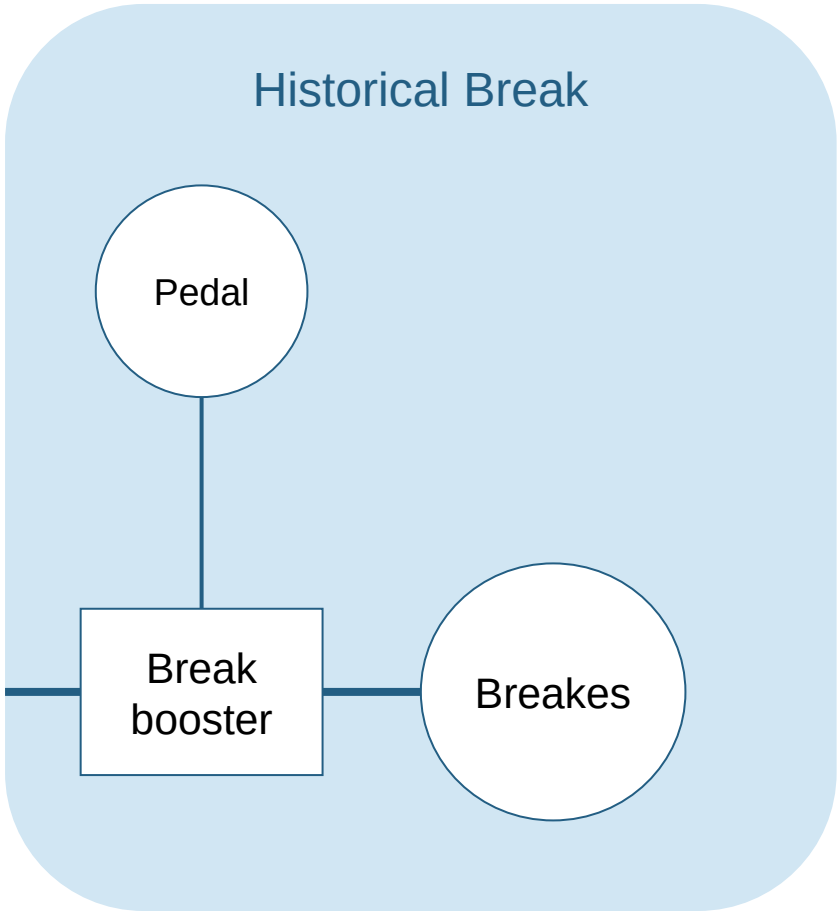


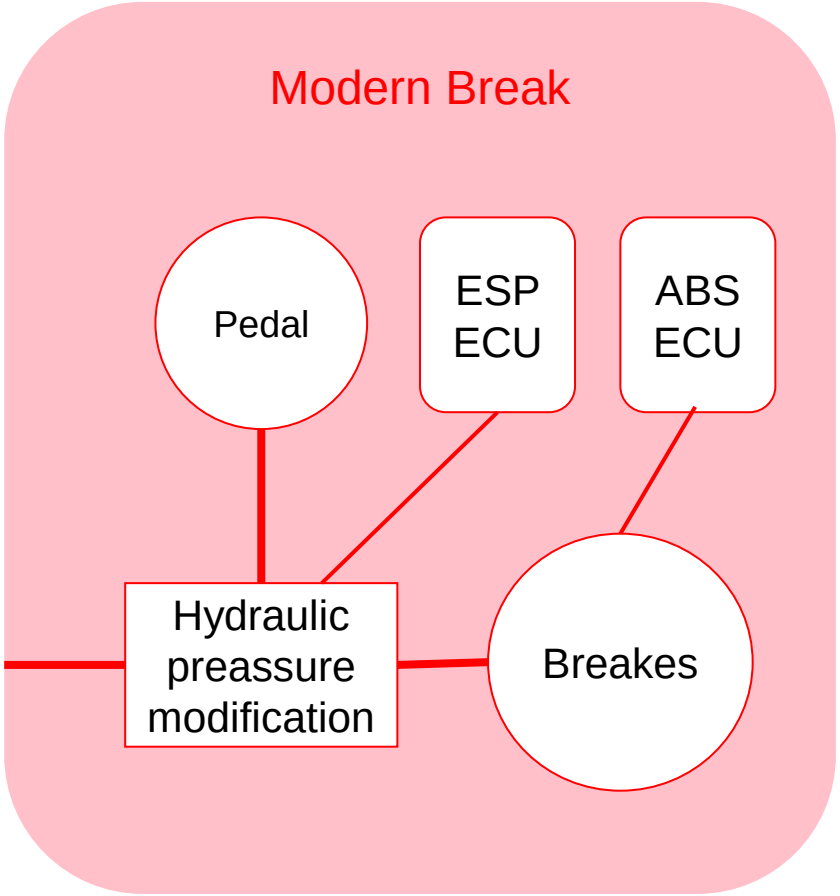


The world is changing

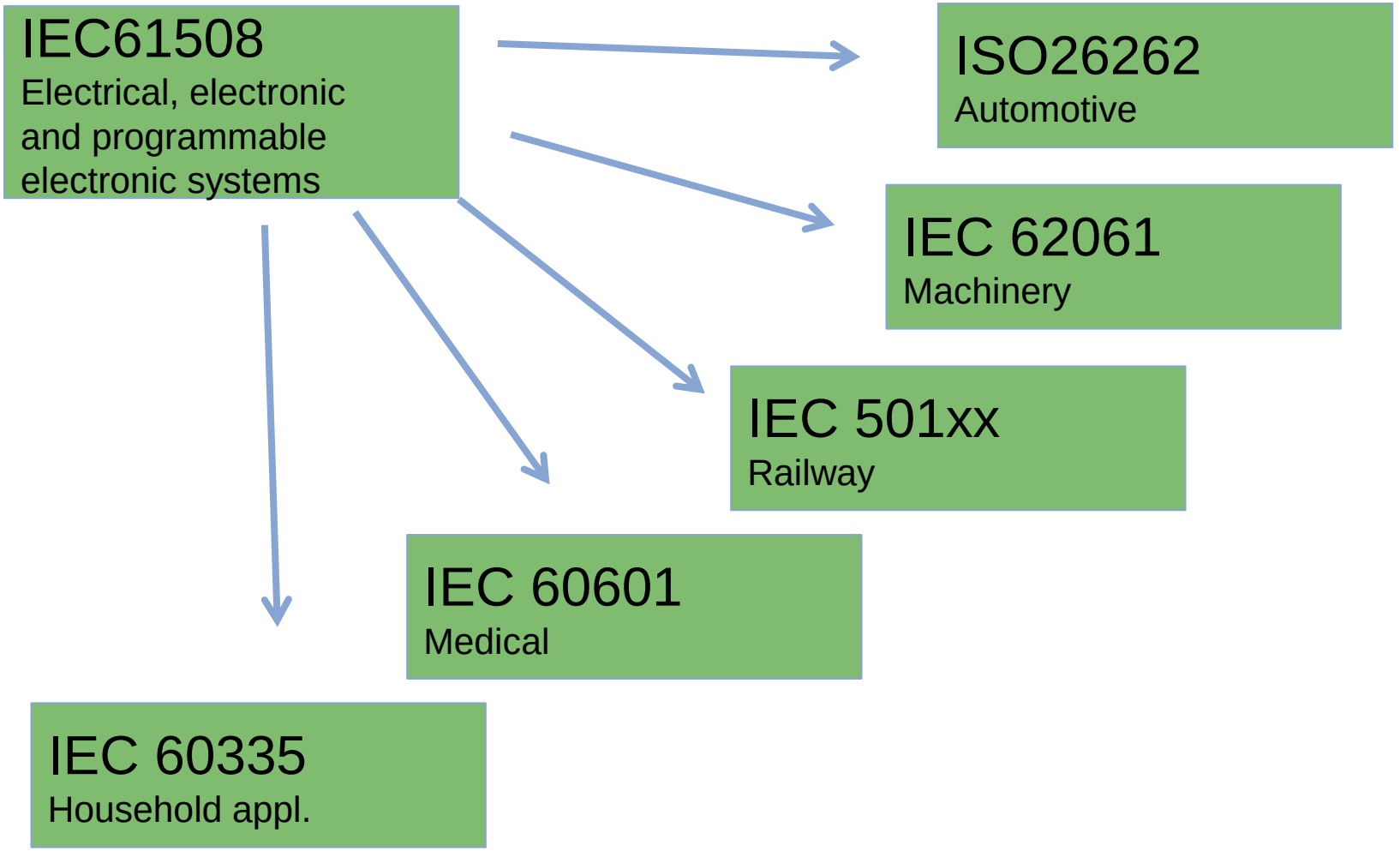
- Example: Car Break

Microcontroller failure may lead to damage or even injury !



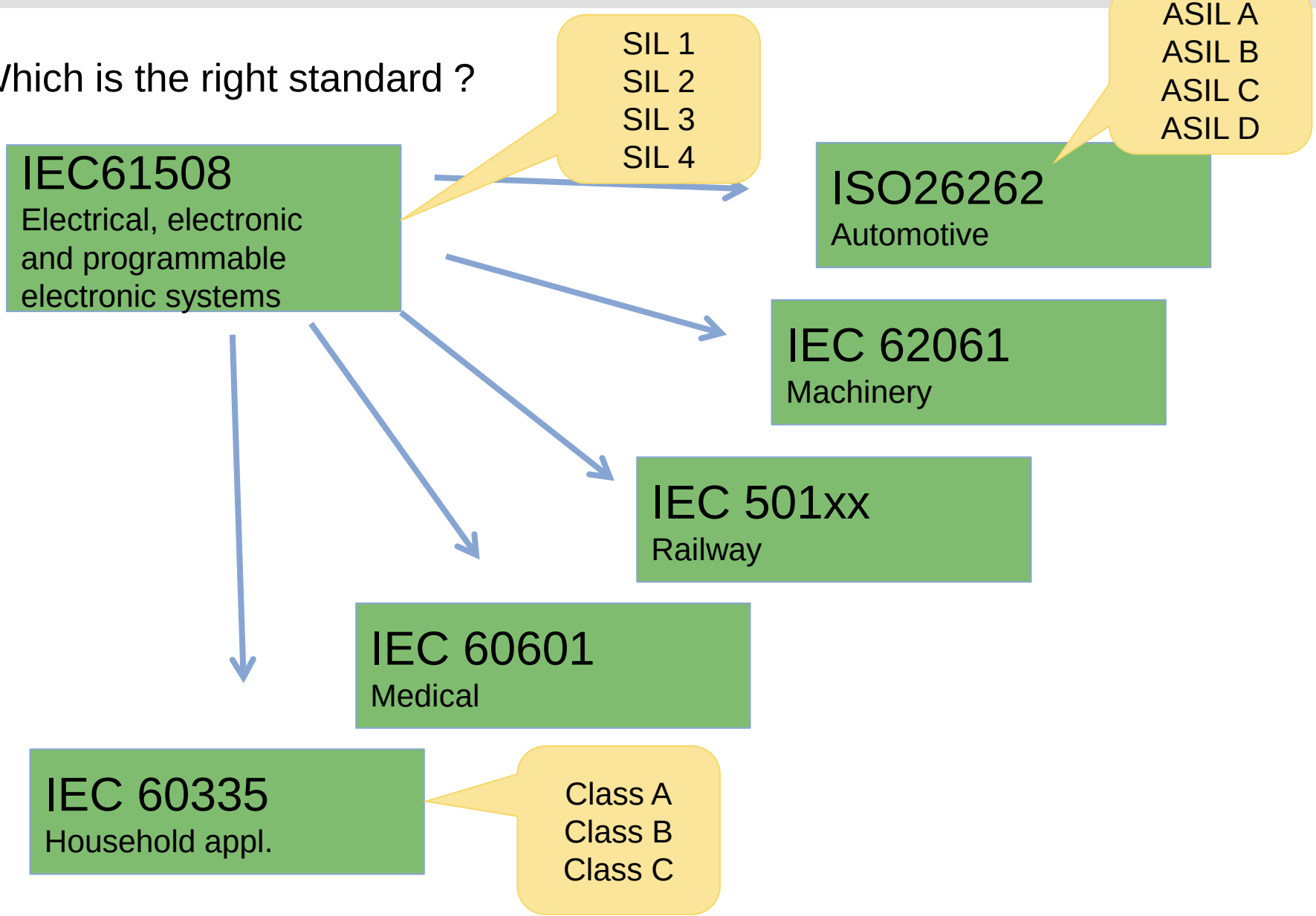


Which is the right standard ?



Introduction into Functional Safety

Which is the right standard ?



Agenda

- Introduction into Functional Safety
- **Functional Safety demands**
- Class B Solution
- SIL/ASIL Solution
- Summary

Functional Safety Demands

- Aim of the standards is to reduce the risks of a system to a tolerable amount

Safety-Integrity Level	Dangerous failures / h	Dangerous failures / a
SIL 4	max 10^{-8}	~ 10^{-4}
SIL 3	max 10^{-7}	~ 10^{-3}
SIL 2	max 10^{-6}	~ 10^{-2}
SIL 1	max 10^{-5}	~ 10^{-1}

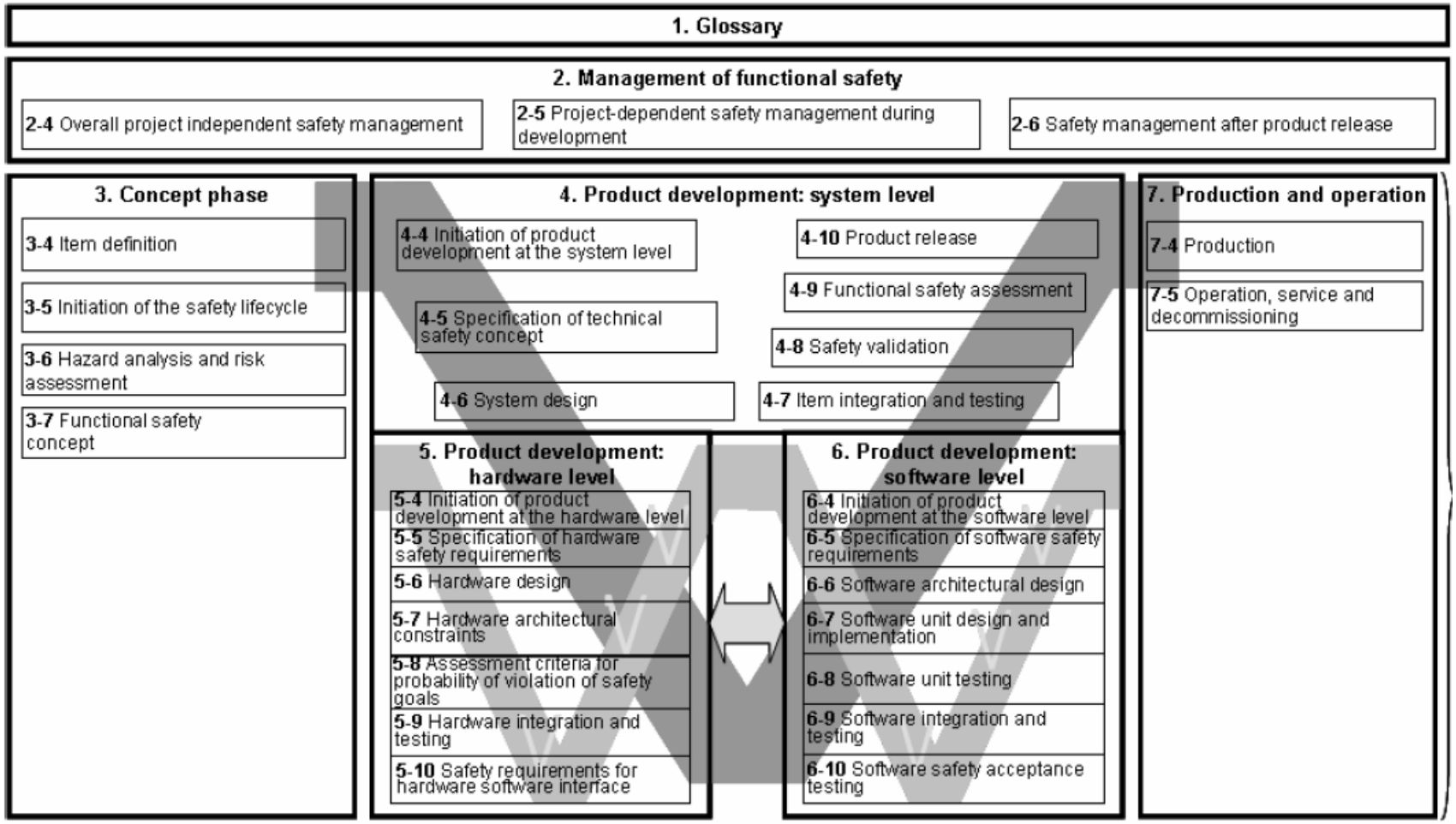
Functional Safety Demands

Systematical Failures
- **Software**
- **Hardware**

Statistical Failures
- Software
- **Hardware**

Functional Safety Demands

- **How to reduce systematical failures:**



Functional Safety Demands

- How to reduce systematical failures

- Development process and roles
- Specification Documents
- Change Management
  - E.g. SVN
- Development Documentation
  - E.g. Doxigen
- Review of source code
  - Static analysis, MISRA etc.
- Test specification and Unit Tests
  - E.g. CTE and Tessy
- Usage of qualified tools

Functional Safety Demands

- **ARM** and **IAR** provide compiler tools for functional safety applications
  - IAR Embedded workbench certified for functional safety: Validated according to EN 50128, IEC 61508 & ISO 26262
  - ARM certified Compiler meets the toolchain requirements of ISO 26262 (through ASIL D) and IEC 61508 (through SIL 3)
- Certification refers usually to a fixed or frozen branch (version) of the compiler
- To support the validation of the user application a qualification package or validated package is provided
  - Safety documentation
  - Quality, defect, test reports
  - …

Functional Safety Demands

- Tessy and CTE are prepared for functional safety relevant tests
  - Certified from TÜV SÜD
  - Tool Qualification Package available

ZERTIFIKAT ◆ CERTIFICATE ◆ 認証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Product Service

CERTIFICATE

No. Z10 14 06 78930 002

Holder of Certificate: Razorcat Development GmbH
Witzlebenplatz 4
14057 Berlin
GERMANY

Factory(ies): 78930

Certification Mark:

Product: Software Tool for Safety Related Development

Model(s): TESSY

Parameters: Tool Classification: T2 (acc. to IEC 61508)
TCL3 (acc. to ISO 26262)

The verification tool fulfills the requirements for support tools according to IEC 61508-3.
The tool is qualified to be used in safety-related software development according to IEC 61508 and ISO 26262.
The test report is a mandatory part of this certificate.

Tested according to: IEC 61508-3:2010
ISO 26262-8:2011

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: RB84018C

Date, 2014-06-17

Page 1 of 1

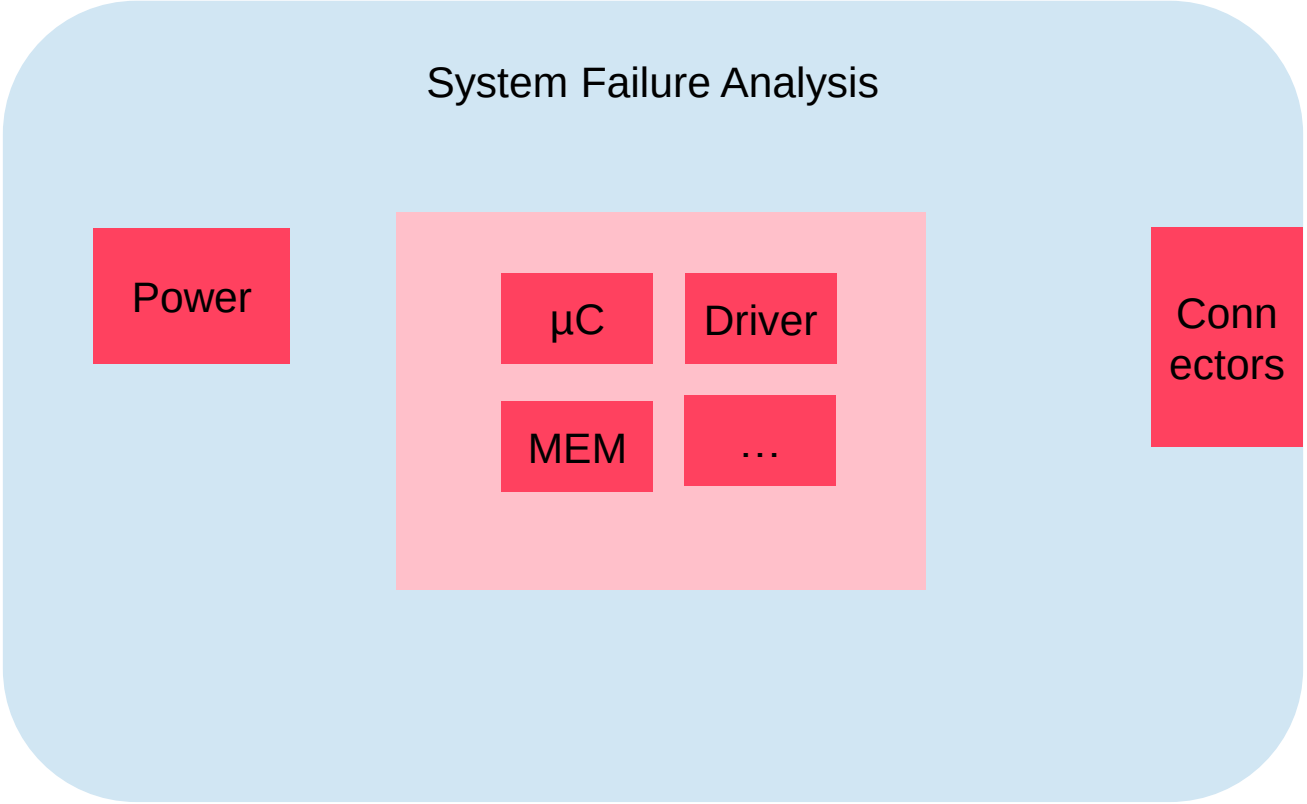
584193

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80339 München · Germany

TÜV®

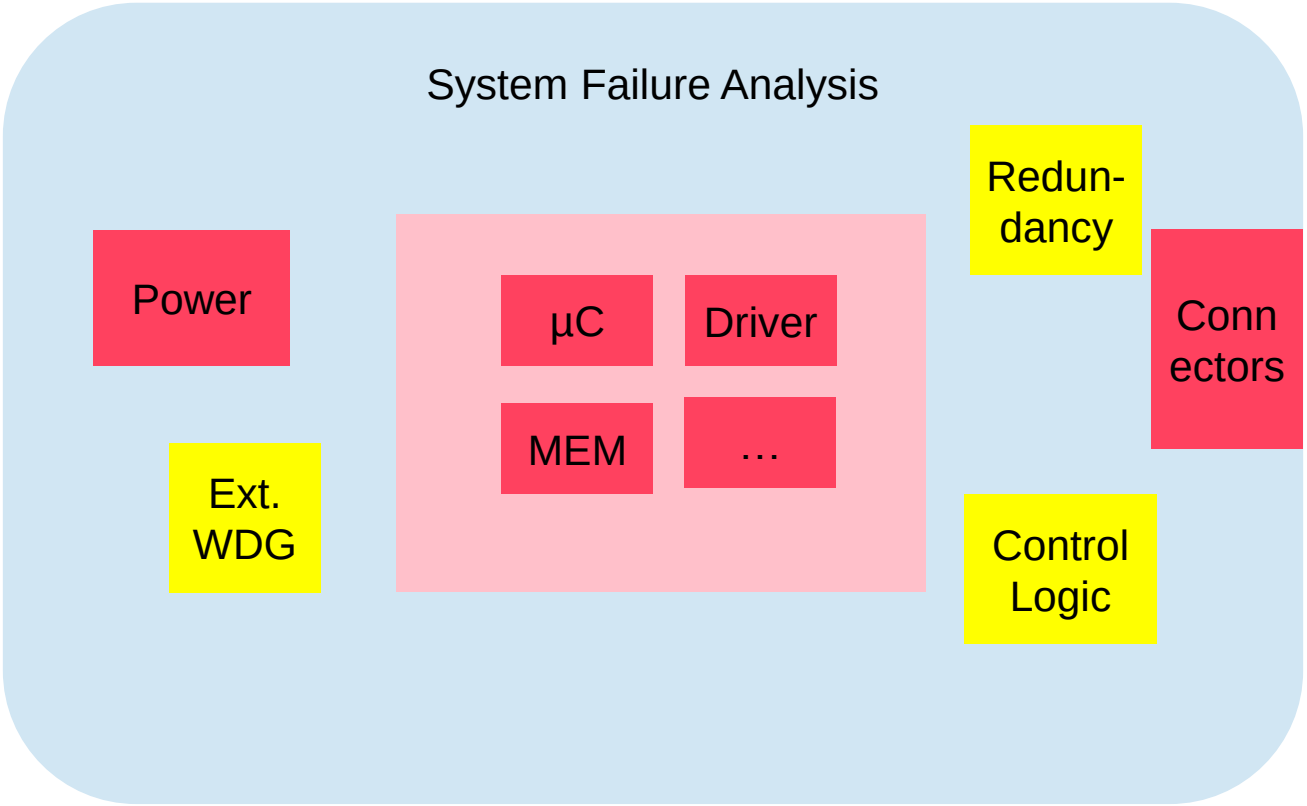
Functional Safety Demands

- How to reduce statistical failures:



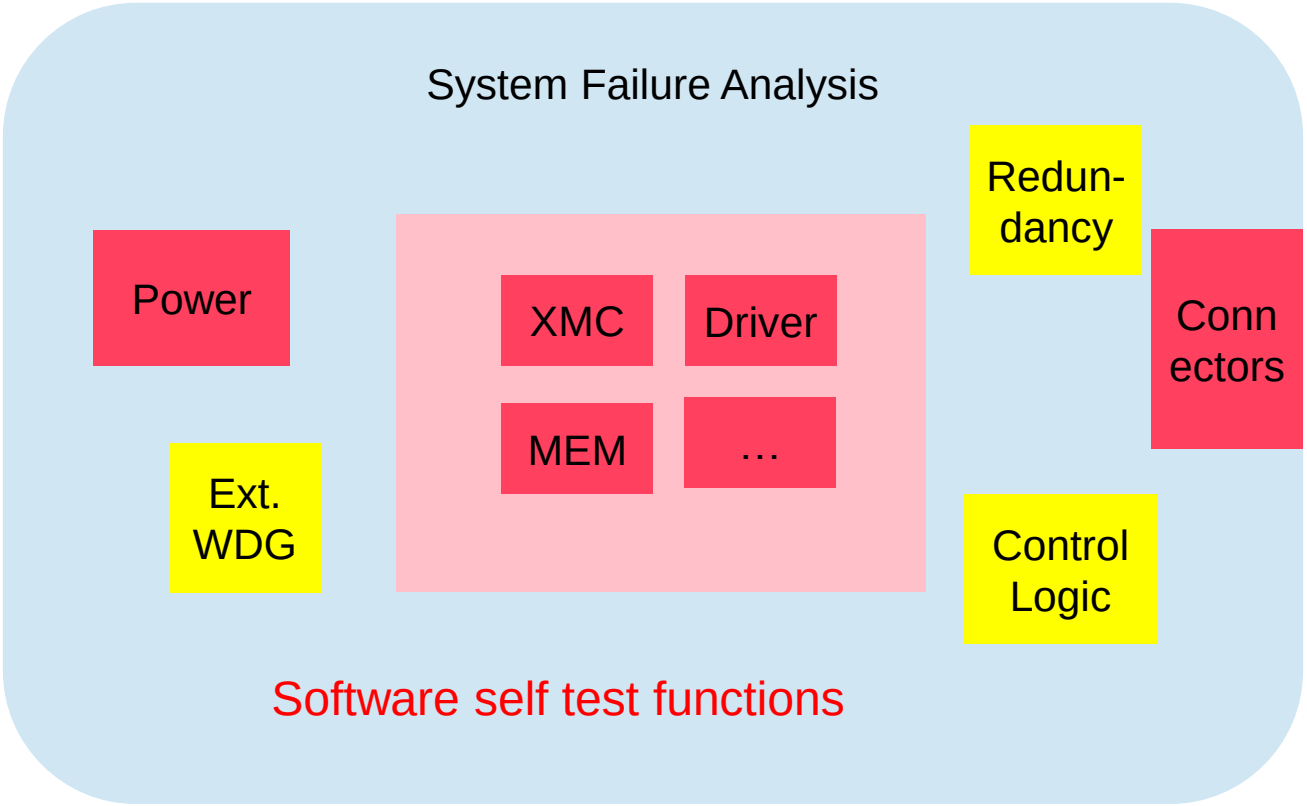
Functional Safety Demands

- How to reduce statistical failures:



Functional Safety Demands

- How to reduce statistical failures:



Agenda

- Introduction into Functional Safety
- Functional Safety demands
- **Class B Solution**
- SIL/ASIL Solution
- Summary

Class B Solution for XMC

- Demands from IEC 60335 -> IEC 60730 -> Table H1

- Register Test
- PC Test
- ROM Test
- RAM Test
- Clock Test
- Interrupt Test
- Flow Control
- ….

Tabelle H.1 (H.11.12.7 der vorherigen Ausgabe) [6)]

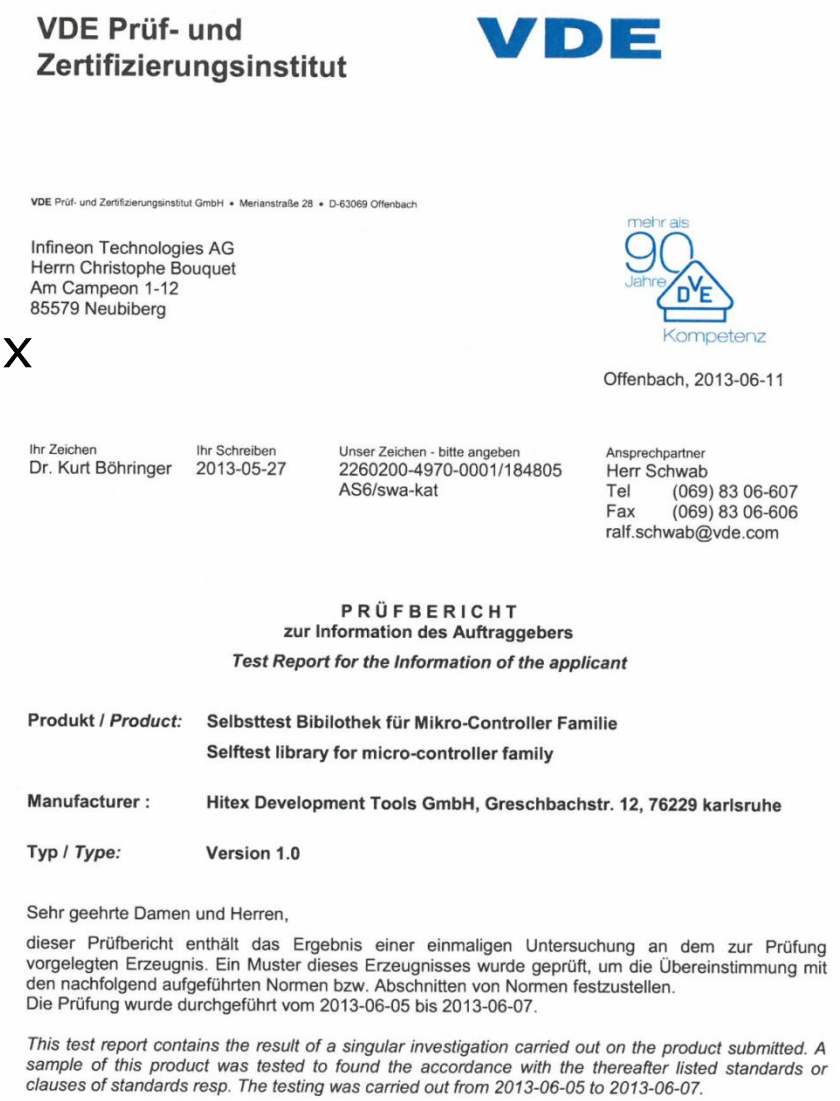
Bauteil [1)]	Fehler	Soft-ware-Klasse		Annehmbare Maßnahmen [2) 3) 4)]	Begriffe
		B	C		
1. CPU					
1.1 Register	Stuck-at	rq		Funktionsprüfung oder	H.2.16.5
				periodische Selbstprüfung entweder durch:	H.2.16.6
				– statische Speicherprüfung oder	H.2.19.6
				– Wortschutz mit Einzelbit-Redundanz	H.2.19.8.2
	Kopplungsfehler		rq	Vergleich redundanter CPUs durch entweder:	
				– reziproken Vergleich,	H.2.18.15
				– unabhängigen Hardware-Komparator oder	H.2.18.3
				inneren Fehlernachweis oder	H.2.18.9
				redundanter Speicher mit Vergleich oder	H.2.19.5
				periodische Selbstprüfungen durch entweder	
				– Walkpat-Speicherprüfung,	H.2.19.7
				– Abraham-Prüfung,	H.2.19.1
				– transparente GALPAT-Prüfung oder	H.2.19.2.1
				Wortschutz mit Mehrbit-Redundanz oder	H.2.19.8.1
				statischer Speicherprüfung und Wortschutz mit	H.2.19.6
				Einzelbit-Redundanz	H.2.19.8.2

Class B Solution for XMC

- Class B Library is ready to use **free of charge**:
  - www.hitex.com/classb
  - Supporting XMC 1xxx and MC4xxx
- Developed and Supported by Hitex
- Pre Certified by VDE

Deliverables:

- User Manual
- Source Code
- Example projects for KEIL and IAR
- Certificate



VDE Prüf- und Zertifizierungsinstitut

VDE

VDE Prüf- und Zertifizierungsinstitut GmbH • Merianstraße 28 • D-63069 Offenbach

Infineon Technologies AG
Herrn Christophe Bouquet
Am Campeon 1-12
85579 Neubiberg

mehr als 90 Jahre VDE Kompetenz

Offenbach, 2013-06-11

Ihr Zeichen	Ihr Schreiben	Unser Zeichen - bitte angeben	Ansprechpartner
Dr. Kurt Böhringer	2013-05-27	2260200-4970-0001/184805 AS6/swa-kat	Herr Schwab Tel (069) 83 06-607 Fax (069) 83 06-606 ralf.schwab@vde.com

PRÜFBERICHT
zur Information des Auftraggebers
Test Report for the Information of the applicant

Produkt / *Product:*	**Selbsttest Bibilothek für Mikro-Controller Familie** **Selftest library for micro-controller family**
Manufacturer :	**Hitex Development Tools GmbH, Greschbachstr. 12, 76229 karlsruhe**
Typ / *Type:*	**Version 1.0**

Sehr geehrte Damen und Herren,

dieser Prüfbericht enthält das Ergebnis einer einmaligen Untersuchung an dem zur Prüfung vorgelegten Erzeugnis. Ein Muster dieses Erzeugnisses wurde geprüft, um die Übereinstimmung mit den nachfolgend aufgeführten Normen bzw. Abschnitten von Normen festzustellen.
Die Prüfung wurde durchgeführt vom 2013-06-05 bis 2013-06-07.

This test report contains the result of a singular investigation carried out on the product submitted. A sample of this product was tested to found the accordance with the thereafter listed standards or clauses of standards resp. The testing was carried out from 2013-06-05 to 2013-06-07.

Class B Solution for XMC

How to reach a certification of your product?

Case 1: Make by your own

- Implement a development process and roles according to IEC60335
- Make a safety concept for your system
- Specify the system, the SW and HW architecture, the modules
- Include the Class B library
- Implement the modules
- Verify/Test the modules, the integration and the complete system
- Document all correctly
- Present this at the certifier

Class B Solution for XMC

How to reach a certification of your product?

Case 2: Concentrate to the application and buy the safety part from Hitex

- System concept with divided unsafe application and safe add on
- Application developed by yourself
  - Can be maintained with low impact to certification
  - Can be developed without the need of process and roles
- Safe part developed by Hitex
  - Safety know-how, Class B library know-how and process is available

Agenda

- Introduction into Functional Safety
- Functional Safety demands
- Class B Solution
- **SIL/ASIL Solution**
- Summary

SIL/ASIL Solution for XMC

- SIL/ASIL is harder to reach than Class B

- E.g. OpCode test with detection coverage of 90% for SIL2 or 99% for SIL3
- Demands to reach the needed FIT rates
- …

SIL/ASIL Solution for XMC

- Self Test Library for XMC Core available (Cortex M0 and M4)

XMC1xxx	fRSTL-armCM0
XMC4xxx	fRSTL-armCM4

- Developed by Yogitech SPA
- Developed according to IEC61508
- Deliverables.
  - Source Code
  - Example
  - Safety Documentation

SIL/ASIL Solution for XMC

- Self Test Library for XMC Core available (Cortex M0 and M4)

XMC1xxx	fRSTL-armCM0
XMC4xxx	fRSTL-armCM4

- Developed by Yogitech SPA
- Developed according to IEC61508
- Deliverables.
  - Source Code
  - Example
  - Safety Documentation

- SIL2 reachable with 1 channel system
- SIL3 reachable with 2 channel system

Agenda

- Introduction into Functional Safety
- Functional Safety demands
- Class B Solution
- SIL/ASIL Solution
- **Summary**

Summary

- Functional Safety is hard for beginners
- Development effort is higher than for normal development
- There are components available to proof the microcontroller’s functional behavior
- XMC microcontrollers have a lot of build in safety features

Summary

Confucius:

There are three was to reach the target:

1. To imitate, that is the easiest
2. To think about, that is the most precious
3. By own experience, that is the hardest

I would not recommend the 3rd way ☺

(by own experience) ☹

Thank you for your attention.

kurt.boehringer@hitex.de
www.hitex.com

Hitex Development Tools GmbH
Greschbachstr. 12
76229 Karlsruhe

Phone: +49 721 9628-0
Fax: +49 721 9628-149
E-Mail: info(at)hitex.de