Session 3A:
Functional safety

Jorgo Beenen
Project manager/engineer
DEKRA Certification B.V.

Pieter Verstraelen
Technical project leader

Agenda

- Functional Safety Overview (Jorgo Beenen, Dekra)
- Implementation example @ E.D.&A. (Pieter Verstraelen, E.D.&A.)
- Questions

No Doubt.

Functional safety and software assessment

DEKRA Certification Group

Jorgo Beenen (Jorgo.Beenen@dekra.com)

Introduction

Contents

What is functional safety?

Safety is “Freedom from unacceptable risk“

Risk analysis:

Harm	
To People	or
To Property	or
To Environment	or

→

Severity
Catastrophic
…..
Negligible

Harm	
To People	or
To Property	or
To Environment	or

→

Likelihood
Frequent
…..
Incredible

And

Risk
Acceptable?
yes/no
→
safe/unsafe

What is functional safety?

What is basic safety?

Freedom from unacceptable risk caused by physical hazards (e.g. electric shock, fire, skin burn or economic, environmental damage), achieved by physical construction, design, instructions or training.

-Proven by evaluation of construction & safety tests.

Functional safety

Freedom from unacceptable risk that depends on an (electronic) function.

Loss of the function would lead to an unacceptable risk (hazardous situation).

-Proven by evaluation of function design, supported by physical tests to prove reliability of the function (more later).

Development of functional safety

Traditional situation

Safety is provided by basic safety. Protection against hazards realized by electromechanical components (fuses, TCO's, etc), reliable due to physical properties, proven over time and by compliance with safety standards. Electronic systems were mainly used to perform NSR (Non Safety Relevant) functions, improving comfort and efficiency.

Rise of electronics providing FS

Nowadays, and still increasing, electronics are also used to perform SR (Safety Relevant) functions. Electronics includes heavy computing power, reads multiple sensors and drives various actuators to manage increasingly complex functionality. Typical washing machine uses several µP, electronic controls, thousands of lines of software code. Latest trend is connectivity to other internal/external devices or internet.

Functional safety applications

Electronics & software providing safety found in:

- Door locks (ovens, washing machines)
- Thermal cut-outs, motor protectors
- Machinery & power tools
- Smoke / CO detectors
- Anti-intruder systems
- Medical devices
- Gas appliances
- Airplanes
- Self driving cars
- …

Functional safety - standards

- IEC 61508
  Functional safety for E/E/PE safety related systems
  - ISO 26262
    Functional safety in Automotive Electronics
  - IEC 60730
    Electric controls in domestic environment
  - IEC 60335
    Appliances for household and similar use
  - IEC 62304
    Medical Devices
  - IEC 62841
    Power tools, lawn & garden equipment
- ISO 13849
  Safety related parts of control systems

Various product safety standards address FS as an essential part of the technical requirements for the safety of products.

IEC 60730; IEC 60335; IEC 62841; IEC 62733, etc.

Functional safety - standards

Requirements in FS standards address several aspects

As SR functions generally use combination of technologies

- Overall system integrity

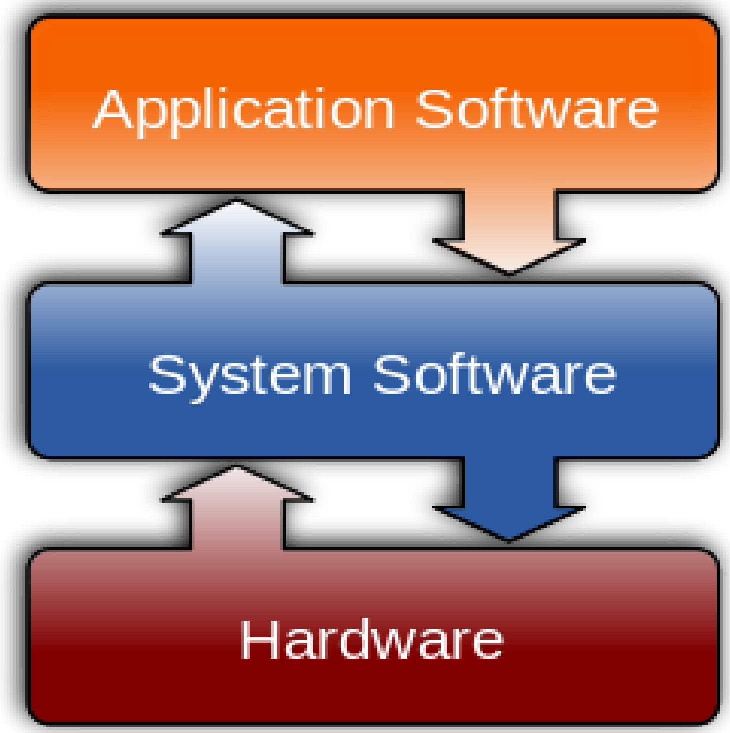
- Hardware integrity

- System software integrity (faulty hardware or unexpected application software/sensor behavior)

- Application software integrity (user input, sensors, communication, etc)

- Design process

- Compatibility with environment (EMC)



No. of aspects further discussed

Functional safety - hardware integrity

Approach 1: Assumption of random hardware failures

Individual components are considered to fail (one or two faults), independent of reliability or complexity of component. Fault may be open/short but also ‘all possible output signals’.

Random faults are generally due to physical causes (e.g. thermal stress, ageing, corrosion, etc) or productions flaws.

Redundancy (hardware), fault detection (self tests, hardware/software)

Approach 2: Calculation of probability of hardware failures

Statistical information resulting from testing and historical data about a type of fault for each individual component. This data is used to calculate the average probability of a failure of the system hardware, and hence the risk, associated with the occurrence of a fault.

High MTTF rated components, redundancy, fault detection (self tests)

Only components involved in SR functions are considered.

Functional safety - Software integrity

Can software do harm?

Nest Labs Suspends Sale of Smoke and Carbon Monoxide Detector until Software Fixed

Miscalculated Radiation Doses

Bug can cause deadly failures when anesthesia device is connected to cell phones

To keep a Boeing Dreamliner flying, reboot once every 248 days

LOST IN SPACE

One of the subcontractors NASA used when building its Mars climate orbiter had used English units instead of the intended metric system, which caused the orbiter's thrusters to work incorrectly. Due to this bug, the orbiter crashed almost immediately when it arrived at Mars in 1999. The cost of the project was $327 million, not to mention the lost time (it took almost a year for the orbiter to reach Mars).

Functional safety – software classification

Software classification

Used throughout several product standards.

Originally from IEC 60730-1 (automatic electrical controls in domestic and public environment).

Based on function and severity of hazard the related software is classified.

Depending on classification, certain CPU faults are to be considered and measures to avoid systematic software errors are to be taken.

Functional safety – software classification

Software class A

Control functions which are not intended to be relied upon for the safety of the application

Failure will not lead to hazardous situation. Software not involved in safety.

Software class B

Control functions which are intended to prevent an unsafe state of the application

Failure of the control function will not lead directly to a hazardous situation or the hazard is limited.

Software class C

Control functions which are intended to prevent special hazards such as an explosion or whose failure could directly cause a hazard in the application.

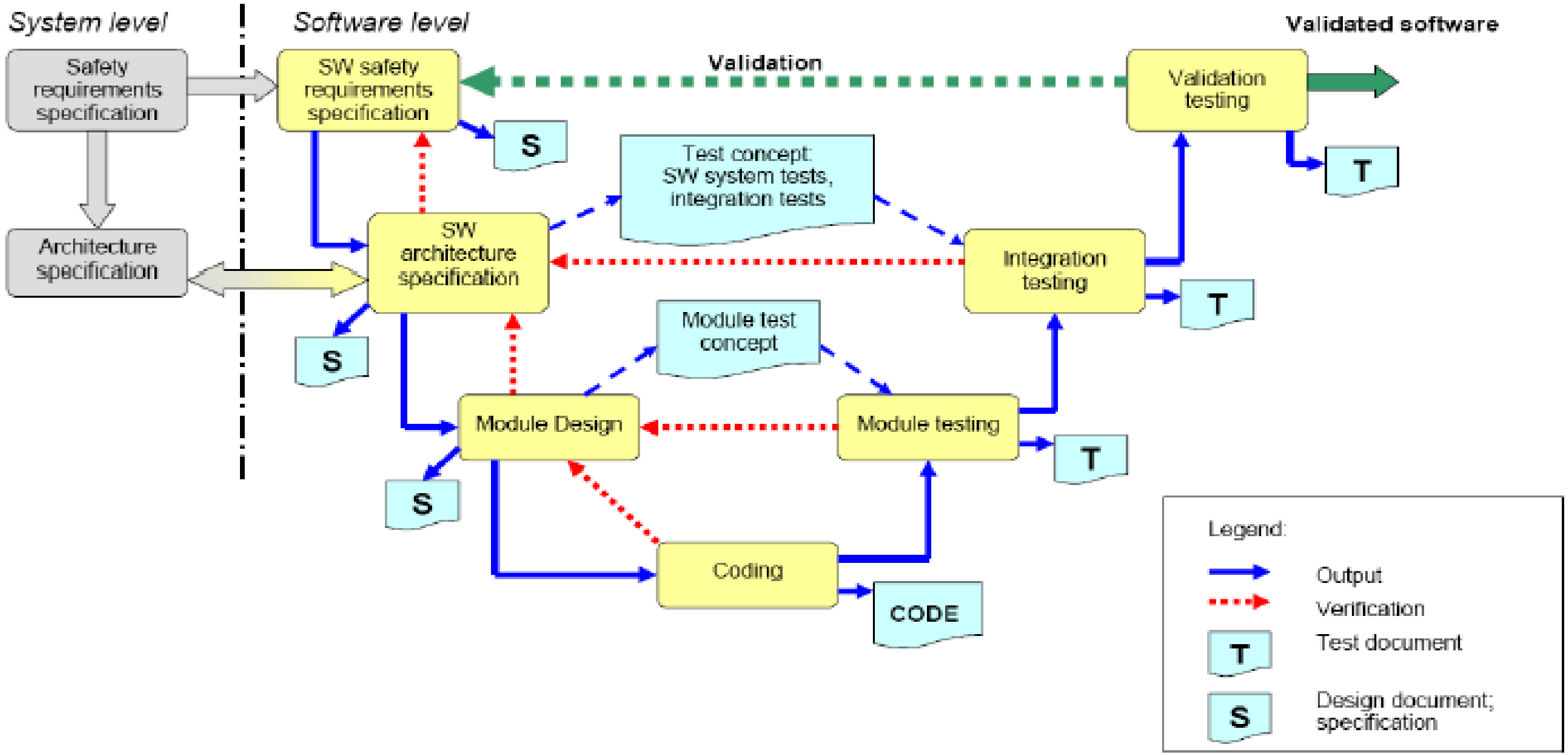
Functional safety – software measures

Example: Software class B, CPU faults

Test	Fault
CPU register	Stuck at
CPU program counter	Stuck at
Interrupt handling	No interrupt or too frequent interrupt
Clock	Wrong frequency
Invariable memory	Single bit faults
Variable memory	DC fault
Addressing (memory)	Stuck at
Internal data path	Stuck at
Addressing	Wrong address
External communication	Hamming distance
Timing	Wrong point in time
Input / output	Open / short , misuse , unexpected,
A/D and D/A converter	Open / short , misuse , unexpected,
Analog multiplexer	Wrong addressing

Functional safety – software design process

Software development requirements, V-model



Session 3A:
Functional safety example

Pieter Verstraelen
Technical project leader

Project description

The power to control

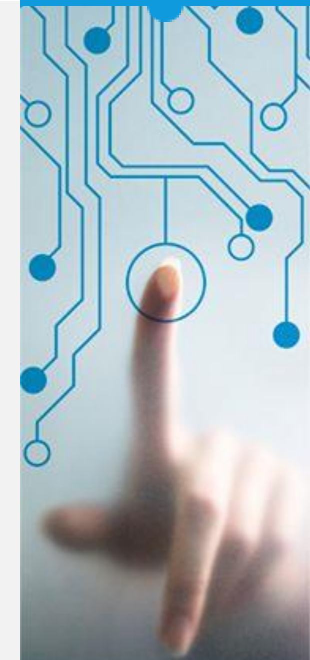
The challenge:

- Development of a controller board for an industrial washing machine.
- Comply with European and US standards.
- Ready for all product variants of the machine.

Phases in a design with functional safety

The
power to
control

- Risk assessment (Customer)
- Risk reduction (Customer, E.D.&A. and Dekra)
- Establish safety function requirements (Customer, E.D.&A. and Dekra)
- Implement functional safety (E.D.&A.)
- Verify functional safety (E.D.&A. and Dekra)
- Document functional safety (E.D.&A.)
- Prove compliance (E.D.&A. and Dekra)



ed&a

Risk assessment

Customer

The power to control

- Extensive document with all risks involved in a washing machine (FMEA).
- We did not assist in this assessment, our customer is best placed to make a list of the risks and an estimation of the severity.

Process Step	Potential Failure Mode	Potential Failure Effect	SEV[1]	Potential Causes	OCC[2]	Current Process Controls	DET[3]	RPN[4]	Action Recommended
What is the step?	In what ways can the step go wrong?	What is the impact on the customer if the failure mode is not prevented or corrected?	How severe is the effect on the customer?	What causes the step to go wrong (i.e., how could the failure mode occur)?	How frequently is the cause likely to occur?	What are the existing controls that either prevent the failure mode from occurring or detect it should it occur?	How probable is detection of the failure mode or its cause?	Risk priority number calculated as SEV x OCC x DET	What are the actions for reducing the occurrence of the cause or for improving its detection? Provide actions on all high RPNs and on severity ratings of 9 or 10.
ATM Pin Authentication	Unauthorized access	• Unauthorized cash withdrawal • Very dissatisfied customer	8	Lost or stolen ATM card	3	Block ATM card after three failed authentication attempts	3	72	
	Authentication failure	Annoyed customer	3	Network failure	5	Install load balancer to distribute work-load across network links	5	75	
Dispense Cash	Cash not disbursed	Dissatisfied customer	7	ATM out of cash	7	Internal alert of low cash in ATM	4	196	Increase minimum cash threshold limit of heavily used ATMs to prevent out-of-cash instances
	Account debited but no cash disbursed	Very dissatisfied customer	8	• Transaction failure • Network issue	3	Install load balancer to distribute work-load across network links	4	96	
	Extra cash dispensed	Bank loses money	8	• Bills stuck to each other • Bills stacked incorrectly	2	Verification while loading cash in ATM	3	48	

1. **Severity**: Severity of impact of failure event. It is scored on a scale of 1 to 10. A high score is assigned to high-impact events while a low score is assigned to low-impact events.
2. **Occurrence**: Frequency of occurrence of failure event. It is scored on a scale of 1 to 10. A high score is assigned to frequently occurring events while events with low occurrence are assigned a low score.
3. **Detection**: Ability of process control to detect the occurrence of failure events. It is scored on a scale of 1 to 10. A failure event that can be easily detected by the process control is assigned a low score while a high score is assigned to an inconspicuous event.
4. **Risk priority number**: The overall risk score of an event. It is calculated by multiplying the scores for severity, occurrence and detection. An event with a high RPN demands immediate attention while events with lower RPNs are less risky.

ed&a

Risk reduction and safety functions

Customer, E.D.&A. and Dekra

The
power to
control

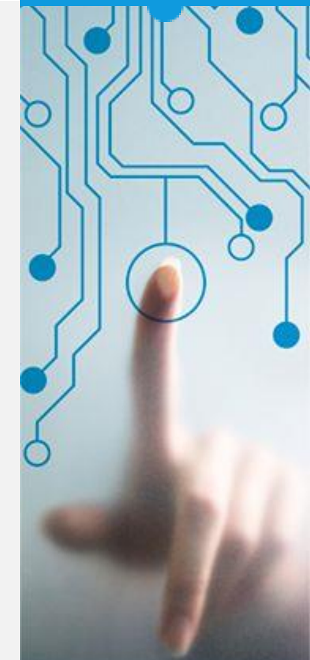
- Meeting with all of the stakeholders at the start of the project. Targets:
  - Agreement between all parties on how to read the standard.
  - Define the main principles of the safety solutions.
  - High level of certainty that selected solutions will result in successful certification.
- The exercise is “risk reduction”, not “go to zero risk”.
  - We select a solution and check if this is sufficient.

ed&a

Risk reduction and safety functions

Customer, E.D.&A. and Dekra

The
power to
control



- Important design decisions have to be made. How will we reduce the risks?
  - Hardware without electronics involved (switches, mechanical interlocks, …)
  - An electronic circuit
  - Electronic circuit and software (Class B software)
- All decisions that are taken now have a huge impact later on in the project and are hard to change!

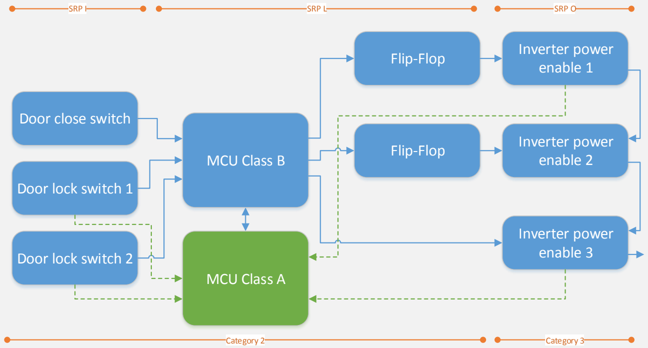
ed&a

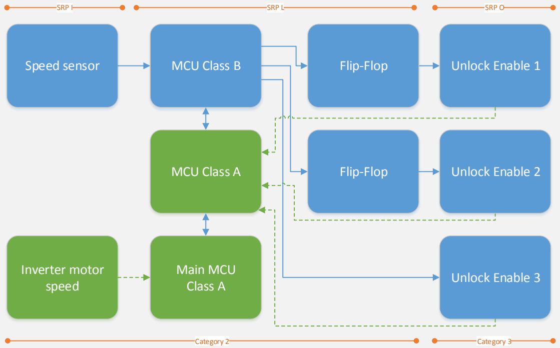
Establish safety function requirements

Customer, E.D.&A. and Dekra

- The safety functions are driven by the requirements from the standards:
  - Define action that safety function has to execute to go to safe state.
  - Determine required safety performance level required for this risk.

- Result: a set of safety functions



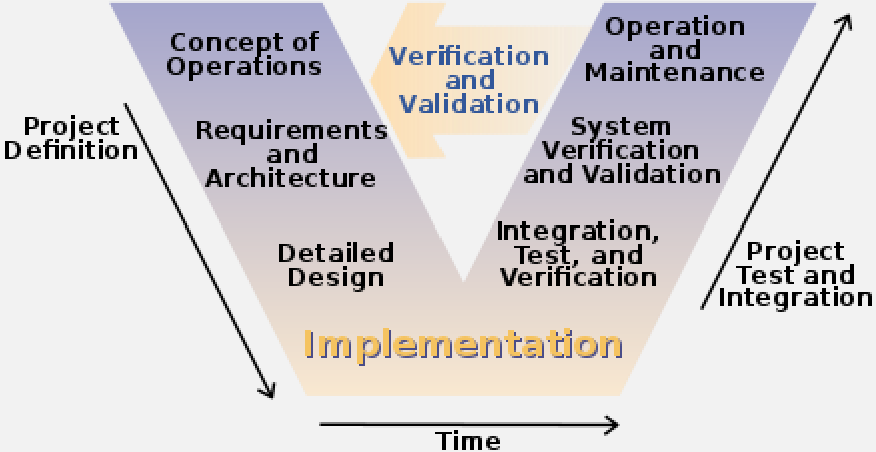


The power to control

Implement functional safety

E.D.&A.

- Work with the V-model



Implement functional safety

E.D.&A.

- Hardware and software development start in parallel to reduce development time.
- Software development:
  - Documentation of the high level functions.
  - Implement the safety functions.
  - Add code to execute the tests required by the standards.
- Hardware development:
  - Finalize hardware specification documents.
  - Start hardware design. Clearance and creepage distances need to be obeyed!
  - Component level FMEA to be sure that the design complies with the requirements.

Tests required by the standards

The
power to
control

Table H.1 (H.11.12.7 of edition 3) – Acceptable measures to address fault/errors [a] *(1 of 6)*

Component [b]	Fault/error	Software class B	Software class C	Example of acceptable measures [c d e]	Definitions
1. CPU 1.1 Registers	Stuck at	rq		Functional test, or	H.2.16.5
				periodic self-test using either:	H.2.16.6
				– **static memory test**, or	H.2.19.6
				– **word protection with single bit redundancy**	H.2.19.8.2
	DC **fault**		rq	Comparison of redundant CPUs by either:	
				– **reciprocal comparison**	H.2.18.15
				– **independent** hardware **comparator**, or	H.2.18.3
				internal error detection, or	H.2.18.9
				redundant memory with comparison, or	H.2.19.5
				periodic self-tests using either	
				– **walkpat memory test**	H.2.19.7
				– **Abraham test**	H.2.19.1
				– **transparent GALPAT test**; or	H.2.19.2.1
				word protection with multi-bit redundancy, or	H.2.19.8.1
				static memory test and word protection	H.2.19.6
				with single bit redundancy	H.2.19.8.2
1.2 Instruction decoding and execution	Wrong decoding and execution		rq	Comparison of redundant CPUs by either:	
				– **reciprocal comparison**	H.2.18.15
				– **independent** hardware **comparator**, or	H.2.18.3
				internal error detection, or	H.2.18.9
				periodic self-test using **equivalence class test**	H.2.18.5
1.3 Programme counter	Stuck at	rq		Functional test, or	H.2.16.5
				periodic self-test, or	H.2.16.6
				independent time-slot monitoring of the program sequence, or	H.2.18.10.4
				logical monitoring of the programme sequence	H.2.18.10.2
	DC **fault**		rq	Periodic self-test and monitoring using either:	H.2.16.7
				– **independent time-slot and logical monitoring**	H.2.18.10.3
				– **internal error detection**, or	H.2.18.9
				comparison of redundant functional channels by either:	
				– **reciprocal comparison**	H.2.18.15
				– **independent** hardware **comparator**	H.2.18.3

FMEA on component level

The
power to
control

	FMEA_REQUIREMENT	DESCRIPTION
	Required fault tolerance count	2
	Safe state conditions	No unlock action MCU control signal all LOW except DREG_CLK HIGH

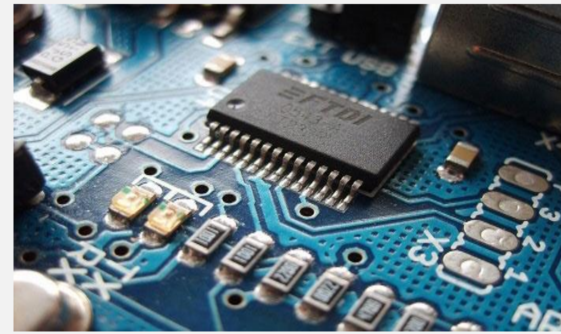
RefDES	Failure	Failure Analysis	Effect	Detection	Severit	Safety mechanisn	Risk	TestID
	(REL14_UNLOCK) UNLOCK control							
	U8							
R38	Open	Clock signal is still controlled by CPU U27. No effect.	0					
R38	Short	No status change of outputs U8 possible. Detected by Class B software.	1	1	0	Diagnostic SW		
R41	Open	Input of U8 will become low because of R37. Clock pulses would put that low signal on safety output. Safe state and detected by Class B software.	1	1	0	Diagnostic SW		
R41	Short	No effect.	0					
R167	open	Input on U8 floating. State of REL_UNLOCK3 unknown. Class B software can verify correct state at signal REL_UNLOCK_FB	1	1	1	Diagnostic SW	1	fmea_ft_0001
R167	short	No effect.	0					
U8 pin 1	Short 1-2	1. U8-2 dominant - 0: system reset: safe - 1: no status change: safe 2. U27-1 dominant - 0: system is in reset: safe. - 1: One of the 3 control signals for REL_UNLOCK is enabled, the others stay unchanged. Detected by Class B software before next CLK pulse.	1	1	1	Diagnostic SW triple IO control	1	fmea_ft_0002
U8 pin 1	to GND	all outputs set to low :safe	1	1	0	Diagnostic SW		

Verify functional safety

E.D.&A. and Dekra

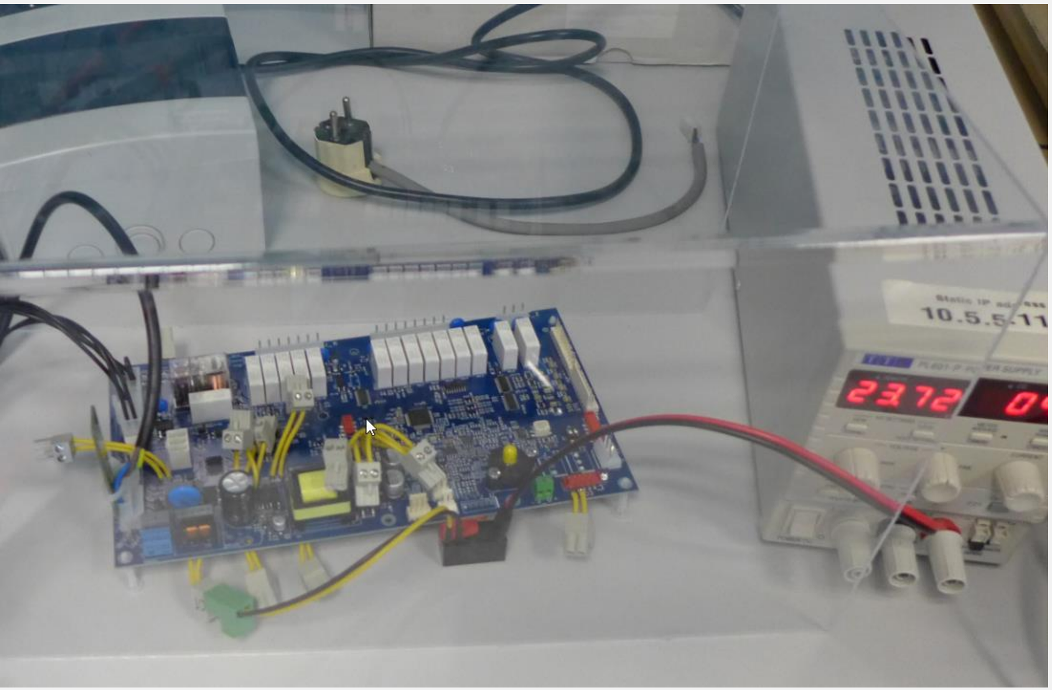
The power to control

Hardware



- Standard product testing.
- Test the effect of a component failure on the real hardware (based on FMEA findings).
  - We created a board with wires and switches attached, to simulate faults.
  - Each of the faults was simulated, the effects were documented.
- 3th party review of the printed circuit board layout (in this case: Dekra).
  - Are clearance and creepage rules obeyed?

Component failure test



Version	Date	Author	Comment
1	10/03/2017	PeterDP	fmea_fire_0002: D30 short 2-3

PCB serial number: 1057 7489

PCB rev.: 1

Test number: 0002

Used equipment:

Description	MAX ID	Serial Number	Comment
Fluke 177 multimeter	20610	7A-20610-000001	
Oscilloscope TDS5104	20562	7A-20562-000001	
Current probe			

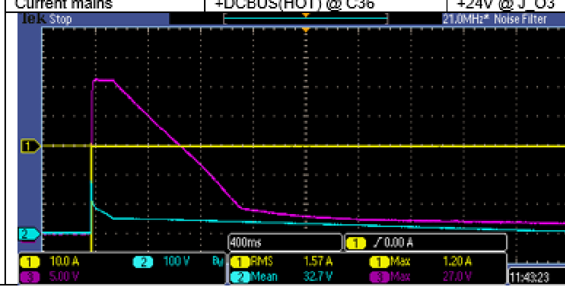
Description:

D30 short pins 2 and 3
Test setup: mains to 6A switchable fuse and then to power cable which has a (2AT, 20x5mm) glass fuse in series with the N. A relay was used to introduce the short (Omron G5RL-1A-E-HR).
2017/02/27: crowbar circuit changed, see crowbar change.

Result:

Tested both with the fault present when the mains of the board was not powered yet and the fault introduced when the board was already powered. The result was the same:

	Oscilloscope channel1	Oscilloscope channel2	Oscilloscope channel3
TEK000201	Current mains	+DCBUS(HOT) @ C36	+24V @ J_O3



TEK000201: the fault is introduced before the mains power is switched on. The measurement of the current is incorrect because it gave an overload error (the maximum current is 30A).
When the fault is introduced and the mains power is turned on, the glass fuse flashes and the 6A fuse switches off. The doorlock is not unlocked.
D30 is broken; internal short.
After removing the fault and replacing D30 and the glass fuse everything works normal again.

Verify functional safety

E.D.&A. and Dekra

The
power to
control

Software

- Static code analysis (MISRA rules, E.D.&A. coding guidelines)
- Internal code reviews
- System and integration test (automatic testing with python scripts)

Internal code review report

The power to control

Revision #2442

Developer	Geert VC
Reviewer	Michael H
Review date	2017-02-15

Review

	Remark	Applies to	Risk
1	Fix TABs (use 4 spaces instead) on lines 293, 306, 354-364, 396-397	DigIoL1.c	Low
2	Move GPIO ports & pin macros to source file?	DigIoL1.h, DigIoL1.c	Low
3	DigIoL1_DoWork is empty, was placeholder, not required => remove	DigIoL1.c	Med
4	Inconsistency in DigIoL1_GetInput & DigIoL1_GetInputs: different approach, one uses ST peripheral library, other uses registers directly	DigIoL1.c	High
5	Doxygen comments on enumeration values (are kind of self-explanatory though)	DigIoL1.h	Low
6	Doxygen comments on structure member fields	DigIoL1.c	Med
7	Doxygen comments on static variables	DigIoL1.c	Med
8	Isn't it the task of the Rpm module to set its required GPIO correctly? Thought behind question: "Don't count on default pin values, either defined by MCU or by another module"	DigIoL1.c, line 116	Low
9	Isn't it the task of the Inverter module to set its outputs correctly during "Init"?	DigIoL1.c, lines 137-138	Low
10	Doxygen comments, DigIoL1_GetInput "index" parameter description: refer to enumeration in DigIoL1.h, can use doxygen \ref tag	DigIoL1.c, line 189	Low

Document functional safety

E.D.&A.

- Work with the V-mode: document on each level (specification, architecture, module)
- Hardware
  - Design specifications
  - FMEA document
  - Reports of the simulated component failures
  - Certificates of components used in the design
- Software
  - Software documentation
  - Static code analysis reports
  - Internal code review reports

The power to control

ed&a

Prove compliance

E.D.&A. and Dekra

The power to control

Self certification or certification by 3th party is possible. In this case, Dekra took care of the review:

- Assessment of all documentation
- Re-assessment of some of the component failure tests.
- Endurance testing of the hardware and the class B software.

Final result:

- CB report
  - Report containing all information in the standard CB format.
- CSA approval of the design

Prove compliance

Test Report issued under the responsibility of:

DEKRA

TEST REPORT
IEC 60730-1
Automatic electrical controls for household and similar use

Report Number ....:	**2197980.50A**
Date of issue ....:	04-10-2017
Total number of pages....................:	81
Applicant's name.........................:	[redacted]
Address...:	[redacted]
Test specification:	
Standard ....:	IEC 60730-1:2013 (Fifth Edition)
Test procedure ....:	CB scheme
Non-standard test method ....:	N/A
Test Report Form No................. :	IEC60730_1H
Test Report Form(s) Originator......:	UL(US)
Master TRF ....:	2014-04

If this Test Report Form is used by non-IECEE members, the IECEE/IEC logo and the reference to the CB Scheme procedure shall be removed.

This report is not valid as a CB Test Report unless signed by an approved CB Testing Laboratory and appended to a CB Test Certificate issued by an NCB in accordance with IECEE 02.

General disclaimer:

The test results presented in this report relate only to the object tested.
This report shall not be reproduced, except in full, without the written approval of the Issuing CB Testing Laboratory. The authenticity of this Test Report and its contents can be verified by contacting the NCB, responsible for this Test Report.

Test Report issued under the responsibility of:

DEKRA

TEST REPORT
IEC 60730-1
Automatic electrical controls for household and similar use
Controls using software

Report Number............................ :	**2197980.50B**
Date of issue.................................. :	04-10-2017
Total number of pages .... :	24
Applicant's name .... :	[redacted]
Address .... :	[redacted]
Test specification:	
Standard.. :	IEC 60730-1:2013 (Fifth Edition)
Test procedure.............................. :	CB Scheme
Non-standard test method............. :	N/A
Test Report Form No. .... :	IEC60730_1H_SOFTWARE
Test Report Form(s) Originator...... :	UL(US)
Master TRF..................................... :	2014-05

If this Test Report Form is used by non-IECEE members, the IECEE/IEC logo and the reference to the CB Scheme procedure shall be removed.

This report is not valid as a CB Test Report unless signed by an approved CB Testing Laboratory and appended to a CB Test Certificate issued by an NCB in accordance with IECEE 02.

General disclaimer:

The test results presented in this report relate only to the object tested.
This report shall not be reproduced, except in full, without the written approval of the Issuing CB Testing Laboratory. The authenticity of this Test Report and its contents can be verified by contacting the NCB, responsible for this Test Report.

Conclusions

The power to control

- Functional safety is only a part of the safety solution for a machine.
- Strong collaboration is needed at the beginning of the project to start in the right direction.
- Functional safety is not 1 or 0. It's about reducing the risk to acceptable levels.

Questions?
Evaluation