Results of the IEC 61508 Functional Safety Assessment

Project:
Temperature Transmitter PR5435 / PR5437 / PR6437

Customer:
PR electronics A/S
Rønde,
Denmark

Contract No.: Q18/10-076-C
Report No.: Q1603-107-C R019
Version 2, Revision 0, August 10, 2020
Peter Müller, Jürgen Hochhaus

Management Summary

The Functional Safety Assessment of the PR electronics A/S

Temperature Transmitter PR5435 / PR5437 / PR6437

development project, performed by *exida* consisted of the following activities:

- *exida* assessed the development process used by PR electronics A/S and MESCO Engineering GmbH through an audit and review of a detailed safety case against the *exida* certification scheme which includes the relevant requirements of IEC 61508:2010, hereafter called IEC 61508. The assessment was executed using subsets of the IEC 61508 requirements tailored to the work scope of the development teams.
- *exida* reviewed and assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.

The functional safety assessment was performed to the SIL 3 requirements of IEC 61508:2010 for systematic capability in redundant configuration and to SIL 2 requirements for the single device configuration. A full IEC 61508 Safety Case was created using the *exida* Safety Case tool, which also was used as the primary audit tool. Hardware and software process requirements and all associated documentation were reviewed. Environmental test reports were reviewed. The user documentation and safety manual also were reviewed.

The results of the Functional Safety Assessment can be summarized by the following statements:

The audited development process, as tailored and implemented by the PR electronics A/S Temperature Transmitter PR5435 / PR5437 / PR6437 development project, complies with the relevant safety management requirements of IEC 61508 SIL 3.

The assessment of the FMEDA, done to the requirements of IEC 61508, has shown that the Temperature Transmitter PR5435 / PR5437 / PR6437 can be used in a high demand mode (demand rate is less than once per 100 minutes) safety related system in a manner where the PFH is within the allowed range for SIL 2 (HFT = 0) according to table 3 of IEC 61508-1.

The assessment of the FMEDA also shows that the Temperature Transmitter PR5435 / PR5437 / PR6437 meets the requirements for architectural constraints of an element such that it can be used to implement a SIL 2 safety function (with HFT = 0) or a SIL 3 safety function (with HFT = 1).

This means that the Temperature Transmitter PR5435 / PR5437 / PR6437 is capable for use in SIL 2 / SIL 3 applications in high demand / continuous mode when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual and when using the versions specified in section 3.1 of this document.

The manufacturer will be entitled to use the Functional Safety Logo.

Table of Contents

1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the:

- Temperature Transmitter PR5435 / 5437 / 6437

by *exida* according to the accredited *exida* certification scheme which includes the requirements of IEC 61508: 2010.

The purpose of the assessment was to evaluate the compliance of:

- the Temperature Transmitter PR5435 / 5437 / 6437 with the technical IEC 61508-2 and -3 requirements for SIL 2 and the derived product safety property requirements

and

- the Temperature Transmitter PR5435 / 5437 / 6437 development processes, procedures and techniques as implemented for the safety-related deliveries with the managerial IEC 61508-1, -2 and -3 requirements for SIL 3.

and

- the Temperature Transmitter PR5435 / PR5437 / PR6437 hardware analysis represented by the Failure Mode, Effects and Diagnostic Analysis with the relevant requirements of IEC 61508-2.

The assessment has been carried out based on the quality procedures and scope definitions of *exida*.

The results of this assessment provide the safety instrumentation engineer with the required failure data per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

It was not the purpose to assess the fulfillment of the statement of conformance from PR electronics A/S for the following European Directives;

- EMC Directive
- Pressure Directive
- Low Voltage Directive
- ATEX Directive

The correct execution of all activities that lead to the statement of Conformance to these European Directives is in the responsibility of PR electronics A/S and builds a basis for the certification.

It was not the purpose of the assessment / audits to investigate PR electronics A/S's quality management system versus ISO 9000 series respectively.

1.1 Tools and Methods used for the assessment

This assessment was carried by using the *exida* Safety Case tool. The Safety Case tool contains the *exida* scheme which includes all the relevant requirements of IEC 61508.

For the fulfillment of the objectives, expectations are defined which builds the acceptance level for the assessment. The expectations are reviewed to verify that each single requirement is covered. Because of this methodology, comparable assessments in multiple projects with different assessors are achieved. The arguments for the positive judgment of the assessor are documented within this tool and summarized within this report.

The assessment was planned by *exida* agreed with PR electronics A/S (see [R2]).

All assessment steps were continuously documented by *exida* (see [R1] and [R3])

2 Project Management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies, specializing in automation system safety and availability with over 500 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment based on 250 billion hours of field failure data.

2.2 Roles of the parties involved

PR electronics A/S	Manufacturer of the Temperature Transmitter PR5435 / 5437 / 6437.
MESCO Engineering GmbH	Sub supplier of the software for the devices.
exida	Performed the hardware assessment [R4].
exida	Performed the Functional Safety Assessment [R1] per the accredited *exida* scheme.

PR electronics A/S contracted *exida* with the IEC 61508 Functional Safety Assessment of the above mentioned devices.

2.3 Standards / Literature used

The services delivered by *exida* were performed based on the following standards / literature.

[N1]	IEC 61508 (Parts 1 – 7): 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

2.4 Reference documents

2.4.1 Documentation provided by PR electronics A/S and MESCO

[D1]	08710 Functional Safety Management Plan FSMP	Version 1.1
[D2]	08710 Qualification and Validation Plan QVP	Version 1.4
[D3]	5300NP Requirements Specification	Version 1.11
[D4]	08710 System Design Requirement Specification	Version 1.5
[D5]	SDRS Review	Version 1.0
[D6]	08710 Software Requirement Specification SWRS	Version 1.6
[D7]	SWRS Review Version	Version 1.0
[D8]	08710 Software Design Specification SWDS OCPU	Version 1.29
[D9]	SWDS_OCPU Review	Version 1.22
[D10]	08710 Software Design Specification SWDS ICPU	Version 1.17
[D11]	SWDS ICPU Review	dated 2017.05.18
[D12]	08710 Review 20161128 (SWDS)	
[D13]	08710 Technical Safety Concept TSC	Version 1.6
[D14]	TSC Review Record	
[D15]	08710 Software Safety Concept	Version 1.6
[D16]	08710 Review 2017-08-09 (review of TR_SWRS_SWDS)	
[D17]	Traceability_SDRS1v1_TSC1v2_SWC1v1	
[D18]	TR_SDRS_TSC_SWC_V1.3TOV1.3V1.4	V1.3TOV1.3V1.4
[D19]	Review_TR_SDRS_TSC_SWC	V1.4TOV1.4V1.6
[D20]	Traceability Report: SDRS, HWDS -> HWTS	V1.4V1R4TOV1.2 2017-10
[D21]	Traceability Table SDRS to Software Requirements and Hardware Design	V1.4TOV1.5V1R4
[D22]	Traceability SDRS to Test (TR_SDRS_TO_Test)	V1.4TOV1.8V1.5V1.2V0.3
[D23]	Traceability Table SDRS to Safety Concepts	V1.4TOV1.4V1.6
[D24]	Traceability Table SWRS to SWDS	V1.5TOV1R25V1R17
[D25]	Traceability Report SWRS and SWDS to SWTS	V1.5V1R25V1R17TOV1.2V1.0V1.8
[D26]	08710_Review_2017-08-09 (SW architecture)	
[D27]	08710 Hardware Design Specification HWDS	Version 1.4

[D28]	08710 Safety Interface Protocol Specification	Version 1.9
[D29]	Firmware Style guide for C and Assesmbler	
[D30]	Firmware Style guide for C++	
[D31]	Software Design Standard MES-SDS-010	Revision 1.0
[D32]	IAR Safety Guide	
[D33]	PR543x Team Meeting Minutes	
[D34]	“Change Requests” in Polarion	
[D35]	08710 Software Criticality Analysis SWCA	Version 0.11
[D36]	08710 System Concept FMEA	Version 1.3
[D37]	08710 Review 2016-12-09 (Concept FMEA)	
[D38]	5300NP sensitivity analysis	Version 0.2
[D39]	Doxygen documentation of “DIAG Monitor”	
[D40]	543761xx 08710_DoxyGenSwds	dated 2017-08-07
[D41]	5300NP63xx Code Review Checklist	
[D42]	5300NP61xx Code Review V0R79.doc, 26-7-2017	
[D43]	5300NP61xx Code Review V0R76 Safe InputCompute, 07.07.2017	
[D44]	08710 Safety Guide adv check	
[D45]	Enterprise Architect file: 31_08710 SWDS	
[D46]	SafeOutputCtrl.cpp	
[D47]	SafeInputdrv.cpp	
[D48]	Sst3F3F.asm	
[D49]	Printout FMEDA 5300NP Dual RTD (.xls)	
[D50]	5300NP Derating Analysis	Version 1.1
[D51]	5437SMD2__2028 (BOM)	29. Nov 17
[D52]	5437_5435 Safety Manual	Version 3.0
[D53]	CodeReviewPlan	
[D54]	08710 Testplan TP	Version 1.7
[D55]	Testplan PR543X Temperature Transmitter	Version 1.3
[D56]	Test Specification Integration Test (OutputCPU)	Version 0.3
[D57]	08710_Review_SWTS_OCPU_1V0.xlsx	
[D58]	08710 Fault Insertion Test Specification FITS	Version 1.5
[D59]	08710 FITR	Version 1.0
[D60]	08710 Software Testspecification SWTS ICPU	Version 1.2

[D61]	08710 Software Testreport SWTR ICPU	Version 1.14
[D62]	08710 Software Testspecification SWTS OCPU	Version 1.1
[D63]	08710 Software Testreport SWTR OCPU	Version 1.3
[D64]	08710_Review_SWTR_OCPU_1V0.xlsx	
[D65]	Review_MESCO_PR_Test_Report	Version 1.1
[D66]	08710_Ch_Rq (Change Request list)	
[D67]	5300NP63xx FW Module Test Report	Version 1.11
[D68]	FW Modul Test Report Review	dated 23 May 2017
[D69]	TÜV Süd Report to the certificate Z10 140678930002 for Tessy	
[D70]	TÜV Süd Certificate Z10 141284282 003 IAR Workbench	
[D71]	54xx Confidence from use of SW tools Assembler for Microchip	
[D72]	54xx Confidence from use of SW tools Assembler for PC-Lint	
[D73]	Impact Analysis Summary	Version 1.0
[D74]	08710 RegressionTest Impact	Version 1.3
[D75]	08710 SWC	Version 1.5
[D76]	MESCO PR Integration Specification	Version 1.2
[D77]	MESCO PR Integration Report	Version 1.2
[D78]	MESCO PR Test Report	Version 1.2
[D79]	TESSY OverviewReport	Version 0.96
[D80]	08710 Hardware Testspecification	Version 1.2
[D81]	08710 Hardware Testreport HWTR	Version 0.6
[D82]	08710 Hardware Software integration Test Specification ITS	Version 1.2
[D83]	08710 Hardware Software integration Test report ITR	Version 0.7
[D84]	08710 Acceptance Test Specification ATS	Version 1.0
[D85]	5300NP Acceptance Test Specification - Extension Port	Version 0.12
[D86]	5300NP Acceptance Test Specification – Firmware	Version 0.55
[D87]	5300NP Acceptance Test Specification Part1	Version 2.0
[D88]	5300NP Acceptance Test Specification Part2	Version 2.0
[D89]	5300NP Acceptance Test Specification Part3	Version 2.0

[D90]	5300NP Acceptance Test Specification Part4	Version 2.0
[D91]	5300NP Acceptance Test Specification Part5	Version 2.0
[D92]	5300NP61xx Main Firmware Version History	
[D93]	5300NP63xx Input Firmware Version History	
[D94]	5300NP61xx Firmware History	
[D95]	5300NP63xx Firmware History	

2.4.2 Documentation provided by PR electronics A/S and MESCO May 2018

[D96]	Impact Analysis Summary 0V97	Version 1.1
[D97]	Impact Analysis Summary 0V100	Version 1.0
[D98]	08710 Regression Test planning overview V0R97	Version 1.1
[D99]	08710 Regression Test planning overview V0R100	Version 1.0
[D100]	08710 Software Design Specification SWDS OutputCPU	Version 1.31
[D101]	Test report 5300NP63xx (tecmata)	Version 1.2
[D102]	Tessy Overview Report 20180507T174318+200	Dated 2018-05-07
[D103]	08710 Software Testreport SWTR OCPU	Version 1.5
[D104]	08710 Acceptance Test Specification ATS	Version 1.1
[D105]	5300NP Product Version Log	(00.00.xx – 01.03.xx)
[D106]	Impact Analysis Summary 0V100	Version 1.0
[D107]	08710 Regression Test planning overview V0R100	Version 1.0
[D108]	08710 Software Design Specification SWDS OutputCPU	Version 1.31
[D109]	08710 Software Testspecification SWTS ICPU	Version 1.3
[D110]	5300NP63xx FW Module Test Report	V1R15
[D111]	5300NP63xx FW Module Test Report Review	V1R15
[D112]	08710 Acceptance Test Specification ATS	Version 1.1
[D113]	5300NP Product Version Numbering V0R3.docx	Version 0.3

2.4.3 Documentation provided by PR electronics A/S and MESCO 2019/2020

The documentation was provided as a basis for the extension of the certificate regarding the PR6437 variant. At the same time, the documentation was provided to show the impact and evidence of safety compliance of the changes applied to PR543x variants.

[D114]	DeliveryNote_2019-11-20_Change6347Part1	
[D115]	PCR40 - 6437 Draft Impact Analysis - Int CJC	V0R0
[D116]	PCR41 - 5437 Draft Impact Analysis - Sensor Offset	V0R0
[D117]	PCR42 - 5437 Draft Impact Analysis - Input Limits	V0R0
[D118]	PCR43 - 5437 Draft Impact Analysis - Broken sense wire detection	V0R0
[D119]	PCR44 - 5437 Draft Impact Analysis - Readout unlinearized value	V0R0
[D120]	PCR50 - 5437 Draft Impact Analysis - Customized Potmeter Input Limits	V0R0
[D121]	PCR54 - 5437 Draft Impact Analysis - HART EMC improvement	V0R0
[D122]	PCR56 - 5437 Draft Impact Analysis - Improvement of noise filters in FW	V0R0
[D123]	PCR58 - 5437 Draft Impact Analysis - Source code cleanup	V0R0
[D124]	PCRxx -5437 Draft Impact Analysis - LINT parser	V0R0
[D125]	PCR61 - 5437 Draft Impact Analysis - GOST Nickel sensor limits	V0R0
[D126]	PCR62 - 5437 Draft Impact Analysis - FLASH CRC calculation in production	V0R0
[D127]	PCR63 - 5437 Draft Impact Analysis - Using Kelvin for Configuration	V0R0
[D128]	08710_SWDS_OCPU_V1R45	V1R45
[D129]	TESSY_OverviewReport_20190517T141959+0200	Dated 2019-05-17
[D130]	08710_SWRS_V1.7	V1.7
[D131]	08710_SDRS_V1.6	V1.6
[D132]	08710_TSC V 1.8	V1.8
[D133]	08710_RegressionTest_Impact	V1.4
[D134]	08710_HWDS	V1.8

[D135]	5300NP Derating analysis	V1R4
[D136]	Acceptance Test Specification (08710_ATS)	V1.5
[D137]	5300NP Acceptance Test Specification Part4	V3R0
[D138]	5300NP Acceptance Test Specification Part2 V4R0	V4R0
[D139]	5300NP - 6437 CJC Test	V2R0
[D140]	08710_FITS_V1.8	V1.8
[D141]	5300NP Acceptance Test Specification – Firmware	V4R0
[D142]	08710_SWCA V.013 Software Criticality Analysis (SWCA)	V0.13
[D143]	08710_FITR Fault Insertion Test Report (FITR) V1.1	V1.1
[D144]	5435_5437_6437 Safety Manual Manual of PR543X	V4R0
[D145]	08710_PR543X V16R0	Set of Source code files V16R0
[D146]	Impact Analysis Summary-6437 V1.4	V1.4
[D147]	08710_SWTR_OCPU V1.7	V1.7
[D148]	5300NP Acceptance Test FW versions V1R0.pdf	V1R0
[D149]	MESCO_PR_Test_Report	V1.4
[D150]	5300NP - 6437 EMC test	V1R0
[D151]	08710_RegressionTest_Impact-6437.xlsx	V1.4
[D152]	TESSY_DetailsReport_diagnostic.mcuTemp.Execute().pdf	Dated 2019-05-17
[D153]	08710-SafetyImpact5437	V1.0
[D154]	I11.54 Product Version Numbering 2020-08-07 12.20.pdf	Version 2020-08-07 12.20
[D155]	DocList-6437.xlsx	List of evidence documents V0R5

Documentation generated by *exida*

[R1]	Safety Case WB-61508 v1.7.3b PR5435_37	Safety Case Workbook
[R2]	Q1603-107-C	Quotation for assessment
[R3]	Q1603-107-C R018 V1R13	Assessment and Review comments
[R4]	PR electronics 16-03-107-C R028 V1R5	FMEDA report PR543x
[R5]	Q18-10-076-C	Quotation for the assessment update (PR6437)

[R6]	PR 1810-076-C R021 V1R8	assessment and review comments 6347 update
[R7]	PRelectronics 18-10-076-C R030 V1R0	FMEDA report PR6437

2.5 Assessment Approach

The certification audit was closely driven by requirements of the *exida* scheme which includes subsets filtered from IEC 61508.

The assessment was planned by *exida* and agreed with PR electronics A/S.

The following IEC 61508 objectives were subject to detailed auditing at PR electronics A/S:

- FSM planning, including
  - Safety Life Cycle definition
  - Scope of the FSM activities
  - Documentation
  - Activities and Responsibilities (Training and competence)
  - Configuration management
  - Tools and languages
- Safety Requirement Specification
- Change and modification management
- Software architecture design process, techniques and documentation
- Hardware architecture design - process, techniques and documentation
- Hardware design / probabilistic modeling
- Hardware and system related V&V activities including documentation, verification
  - Integration and fault insertion test strategy
- Software and system related V&V activities including documentation, verification
- System Validation including hardware and software validation
- Hardware-related operation, installation and maintenance requirements

The project teams, not individuals were audited.

The certification audit was done in Rønde 21 – 22 June 2016, Lörrach (at MESCO) 30 November - 2 December 2016 and Lörrach (MESCO) 31 May - 1 June 2017. Additional internet based meetings were held to complete the assessment.

For the extension of the certificate to include the new variant PR6437, additional audits were committed. The audits were internet based and took place between Nov 2019 and July 2020.

3 Product Description

The device builds a 2-wire HART temperature transmitter for temperature measurement with TC and RTD sensors as well as linear input signals (voltage, resistance and potentiometer).

True dual input with high density seven terminal design allows measurement of two 4-wire RTDs.

Sensor redundancy allows automatic switch to secondary sensor in the event of primary sensor failure and sensor drift detection issues an alert when sensor differential exceeds predefined limits.

The transmitter is intended for use in high demand / continuous mode applications with a process safety time > 120sec.
The single transmitter is realized in a 1oo1D structure with internal diagnostics and a second shutdown path. The Safe state is defined for the output signal as ≤ 3,6mA / ≥ 21mA.

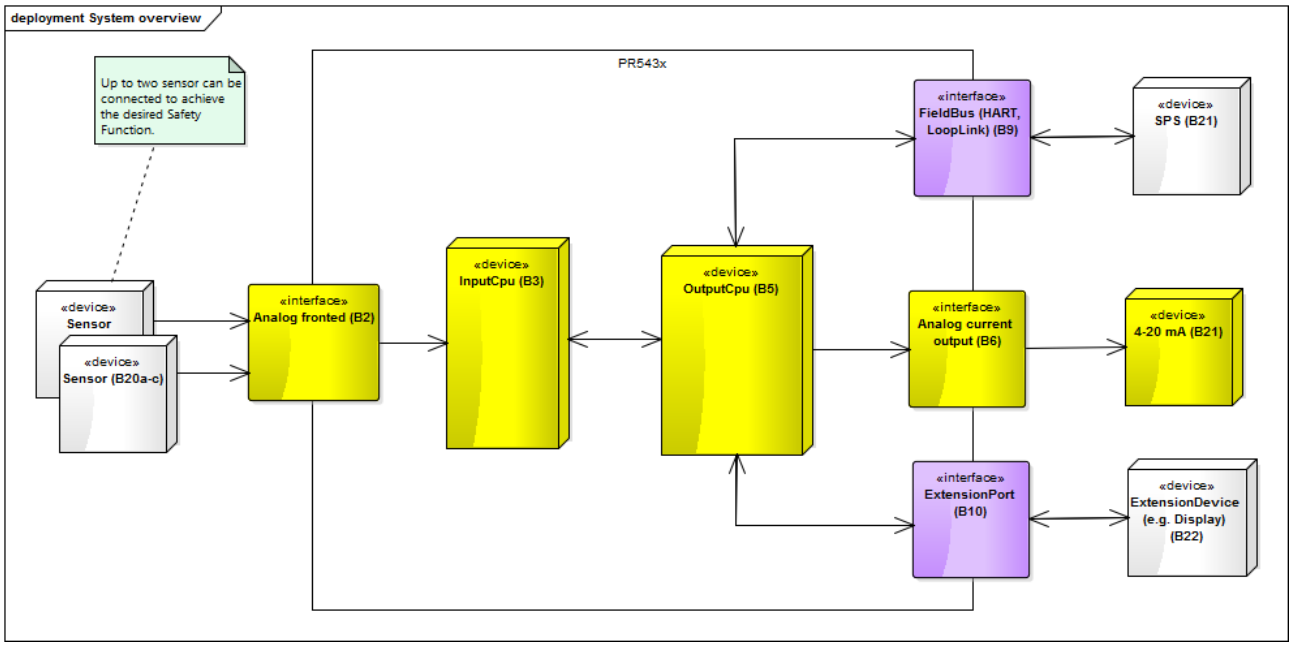

Figure 1: principle internal 1oo1D structure

The internal diagnostic principles are based on dynamic active testing, protection of data, monitoring of safety limits, partial redundancies, separation of safety and non-safety functions and output monitoring.
A safe parameterization concept is defined for the configuration of the device.

The software provides a mixture of diversity, diagnostic measures and plausibility checks and a low complex architecture to fulfill the requirements.

Both safe and non-safe code is implemented, safe and non-safe code executes in separate time and spatial domains in the “output CPU”.

3.1 Hardware and Software Version Numbers

This assessment is applicable to the following hardware and software versions of the Temperature Transmitter PR5435 / 5437 / 6437:

Product Version	Main FW version (output CPU) 5300NP61xx	Input FW version (input CPU) 5300NP63xx	Hardware Version (PCB)
V01.xx.xx	V1.2R0	V1.3R0	V10R0
V01.xx.xx	V1.6R0	V1.3R0	V11R0

3.2 Device variants overview

	Description	Suffix	HART
[V1]	Head mounted 2w programmable temperature transmitters	5435x1Sx Note1	5
		5437x1Sx Note1	5 and 7
		5437x2Sx Note1	5 and 7
[V2]	DIN rail mounted 2w programmable temperature transmitters	5435DINL-1S	5
		5437DINL-1S	5 and 7
		5437DINL-2S	5 and 7
[V3]	DIN rail mounted 2w programmable temperature transmitters	6437x1Sx Note1	5 and 7
		6437x2Sx Note1	5 and 7
		6437x3Sx Note1	5 and 7

Note 1: The “x” on first and fourth position after the main product name, indicates various approvals that does not have any impact on the safety aspects of the device.

4 IEC 61508 Functional Safety Assessment Scheme

exida assessed the development process used by PR electronics A/S and MESCO Engineering GmbH for this development project against the objectives of the *exida* certification scheme. The results of the assessment are documented in [R1].
All objectives have been successfully considered in the PR electronics A/S and MESCO Engineering GmbH development processes for the development.

exida assessed the set of documents against the functional safety management requirements of IEC 61508. This was done by a pre-review of the completeness of the related requirements and then a spot inspection of certain requirements, before the development audit.
The safety case demonstrated the fulfillment of the functional safety management requirements of IEC 61508-1 to 3.

The detailed development audit (see [R1]) evaluated the compliance of the processes, procedures and techniques, as implemented for the PR electronics A/S Temperature Transmitter PR5435 / 5437 / 6437, with IEC 61508.

The assessment was executed using the *exida* certification scheme which includes subsets of the IEC 61508 requirements tailored to the work scope of the development team.

The result of the assessment shows that the Temperature Transmitter PR5435 / 5437 / 6437 is capable for use in SIL 2 and SIL 3 (redundant configuration) applications, when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual.

4.1 Product Modifications

The modification process has been successfully assessed and audited, so PR electronics A/S may make modifications to this product as needed.

As part of the *exida* scheme a surveillance audit is conducted prior to renewal of the certificate. The modification documentation listed below is submitted as part of the surveillance audit. *exida* will review the decisions made by the competent person in respect to the modifications made.

- List of all anomalies reported
- List of all modifications completed
- Safety impact analysis which shall indicate with respect to the modification:
  - The initiating problem (e.g. results of root cause analysis)
  - The effect on the product / system
  - The elements/components that are subject to the modification
  - The extent of any re-testing
- List of modified documentation
- Regression test plans

5 Results of the IEC 61508 Functional Safety Assessment

exida assessed the development process used by PR electronics A/S during the product development against the objectives of the *exida* certification scheme which includes IEC 61508 parts 1, 2, & 3 [N1]. The development of the Temperature Transmitter PR5435 / 5437 / 6437 was done per this IEC 61508 SIL 3 compliant development process. The Safety Case was updated with project specific design documents.

5.1 Lifecycle Activities and Fault Avoidance Measures

PR electronics A/S has an IEC 61508 compliant development process as assessed during the IEC 61508 certification. This compliant development process is documented in [D1].

This functional safety assessment evaluated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the product development. The assessment was executed using the *exida* certification scheme which includes subsets of IEC 61508 requirements tailored to the SIL 3 work scope of the development team. The result of the assessment can be summarized by the following observations:

The audited development process complies with the relevant managerial requirements of IEC 61508 SIL 3.

5.1.1 Functional Safety Management

Objectives

- Structure, in a systematic manner, the phases in the E/E/PES safety lifecycle that shall be considered in order to achieve the required functional safety of the E/E/PE safety-related systems.
- Specify the management and technical activities during the overall, E/E/PES and software safety lifecycle phases which are necessary for the achievement of the required functional safety of the E/E/PE safety-related systems.
- Specify the responsibilities of the persons, departments and organizations responsible for each overall, E/E/PES and software safety lifecycle phase or for activities within each phase.
- Specify the necessary information to be documented in order that the management of functional safety, verification and the functional safety assessment activities can be effectively performed.
- Document all information relevant to the functional safety of the E/E/PE safety-related systems throughout the E/E/PES safety lifecycle.
- Document key information relevant to the functional safety of the E/E/PE safety-related systems throughout the overall safety lifecycle.
- Specify the necessary information to be documented in order that all phases of the overall, E/E/PES and software safety lifecycles can be effectively performed.
- Select a suitable set of tools, for the required safety integrity level, over the whole safety lifecycle which assists verification, validation, assessment and modification.

5.1.2 Safety Lifecycle and FSM Planning

Assessment

Functional Safety Lifecycle

The functional safety management plan defines the safety lifecycle for this project. Chapter 4.1 contains a definition of the safety activities and documents to be created for this project. This information is communicated via these documents to the entire development team so that everyone understands the safety plan.

The software development procedure described in chapter 4.1.4 identifies the phases of the software development lifecycle and the inputs/outputs associated with each phase.

All phases of the safety lifecycle have verification steps described in the FSM plan or the verification plan for one or more phases. This plan includes criteria, techniques and tools used in the activities. The verification is carried out against this plan.

Quality Management

The FSM plan refers to the PR internal web portal for access to the ISO 9000 certificate

- PR electronics: DNV 154273-2014-AQ-DEN-DANAK valid until 15 September 2018
- MESCO: TÜV Süd 12 100 43812 TMS valid until 30 July 2018
  The FSMP refers to the quality management system description of PR electronics.

Conclusion:

The objectives of the standard are fulfilled by the PR electronics A/S functional safety management system and new product development processes.

5.1.3 Documentation

Assessment

The “08710_Worksheet”, sheet “DocList” contains the documents which are planned for the product including version control information. The worksheet plans for the reviews and approvals. The FSM plan plans the persons relevant for the verification of each document.

Documents are mainly based on templates. The version control is done by “visual source safe”.

The Configuration Management Plan describes the generic handling of documents.

All safety related documents are required to meet the following requirements:

-Have titles or names indicating scope of the contents

-Contain a table of contents

-Have a revision index which lists versions of the document along with a description of what changed in that version

-Documents must be searchable electronically

Conclusion

The objectives of the standard are fulfilled by the PR electronics A/S functional safety management system.

5.1.4 Training and competence recording

Assessment

The FSM Plan lists the key people working on the project along with their roles in chapter 3.1.

The FSM Plan describes the competency requirements on organizational level (chapter 3.3.3) and on personal level (chapter 3.3.x).

In chapter 3.3.1 the needed experience, competency is defined and compared with the actual state. In case of discrepancies the mitigation measure is listed in chapter 3.3.2.

Conclusion

The objectives of the standard are fulfilled by the PR electronics A/S functional safety management system and internal organizational procedures.

5.1.5 Configuration Management

Assessment

The configuration of the product to be certified is documented including all hardware and software versions that make up the product.
This is covered by a baseline (covering the complete project documentation and firmware) when the product is released.

Formal configuration control is defined and implemented for Change Authorization, Version Control, and Configuration Identification. A documented procedure exists to ensure that only approved items are delivered to customers. Master copies of the software and all associated documentation are kept during the operational lifetime of the released software.

Conclusion

The objectives of the standard are fulfilled by the PR electronics A/S organizational release procedures, functional safety management system and new product development processes.

5.1.6 Tools (and languages)

Assessment

The QVP gives an overview about all tools used within the project covering the classification.

The Tools are listed with their version number, manufacturer, the intended purpose and the criticality level (T1…T3). Hardware tools are listed but not classified for criticalities.

For all listed tools, the manuals are available.

For the IAR Embedded Workbench ARM a TÜV report is available. The report shows that the assessment was done with the target to show the suitability for use in safety related developments for T3 tools.

For the Assembler Microchip MPASMX proven in use is claimed. The report refers to the PR electronics series 9000 (9113/16 and 9106/07). The newer version of the assembler was used to assemble the sources of the 9000 series. The diff of the hex files showed only one differences of two bits (no problem in the 9000 series).

In addition, the test on the input CPU are based on test harnesses and the tests are executed on the target hardware. For showing code coverage, the test will also be performed in a simulator.

The result is not a statement that the assembler is always working correctly, but that the application of the transmitter contains no fault.

The tests are executed in the simulation environment and on target hardware. The tests have successfully passed in both environments.

For PC-Lint proven in use is claimed and the code reviews are referenced. The report argues with the in house use of PC-Lint at PR electronics. But the C++ version is used for one previous project only.

The tool QA-C is used to verify the correctness of PC-Lint. The code is prepared for the PC-Lint static code analysis. Before the code reviews are performed the QA-C analysis is executed. This will show where PC-Lint exceptions / code correction should be made. Additionally, QA-C checks rules which are required by PR electronics but are not supported by PC-Lint.

For Tessy, a TÜV Süd report is available. The report shows that the assessment was done with the target hardware to show the suitability for use in safety related developments for T2 tools.

Conclusion

The objectives of the standard are fulfilled by the PR electronics A/S functional safety management system.

5.2 Safety Requirement Specification

Objectives

The main objectives of the related IEC 61508 requirements are to:

- Specify the requirements for each E/E/PE safety-related system, in terms of the required safety functions and the required safety integrity, in order to achieve the required functional safety.

Assessment

Safety Functions

In chapter 4.1.2 of the SDRS the safety function of the transmitter is required. In chapter 4.1.5 of the SDRS document the safe state is defined as drawing a current outside the valid analog output range; related requirements are provided (WI-373, WI-258). WI-287 defines the safety accuracy with 2%, the standard accuracy is defined by PR electronics with 0,5%.

The entering and maintenance of the safe state is further detailed in the safety concept.

Software Safety Requirements

The traceability from the SRS to the SW requirements is provided in the Polarion Tool. The Software Requirements are mapped to the System Requirements (SRS). The mapping table can be used bidirectional. Reports can be exported from the Tool. The report shows the Header of the requirement and the short description.

The review record show that adaptions to the content of the requirements were performed. The reviews themselves are done on baselined versions of documents (here the SDRS). The review findings were imported to Polarion as change requests. The handling of requests is based on a pre-defined workflow. The requirements were reviewed by software developers, hardware developers and the functional safety manager. The review was based on a checklist. Findings were fully closed; Review of Version 1 resulted consequently in no findings.

The SWRS is divided in two sections: Input CPU and Output CPU.

The traceability report (requirements traceability in the Polarion tool) was reviewed and the findings were corrected.

Details of Safety Integrity Requirements

The SRS was reviewed by MESCO and by PR electronics.

The review report from PR electronics shows a checklist based inspection addressing different topics (functionality, Performance, safety integrity, Constraints and assumptions, Standard compliance, Design HW & SW (including interfaces, operating modes, architecture, communication etc.)) with written comments. A role assignment of two reviewers is made.

The review comments were imported to the Polarion Tool as open items and led to related corrections. The Version 1 was reviewed with no further findings.

Startup requirements

WI-252 requires that the device starts up in the safe state in order to carry out start up tests. This is also valid for the restart (WI-362).

System and Operator Interfaces

Requirements for the sensor input, the communication interfaces, the 4..20mA output and the configuration data interface are defined.

Hardware software requirements

Figure 2 in the SWRS shows the existing hardware software interfaces. The Hardware Software Interface is detailed in the software design.

Conclusion

The objectives of the standard are fulfilled by the PR electronics A/S functional safety management system and use of requirements management tools.

5.3 Change and modification management

Objectives

The main objectives of the related IEC 61508 requirements are to:

- Ensure that the required safety integrity is maintained after corrections, enhancements or adaptations to the E/E/PE safety-related systems.

Assessment

A modification procedure exists for the safety products of PR electronics, which was introduced during the series 9000 development that identifies how a modification request is initiated and processed in order to authorize a product modification request (including hardware and software modifications). A product modification request system exists to support this process.

The modification procedure requires that an Impact Analysis shall be performed to assess the impact of the modification, including the impact of changes to the software design (which modules are impacted) and on the functional safety of the system. The results of an Impact Analysis are documented within the change request.

The modification procedure requires to return to an appropriate earlier phase of development based on an impact analysis, depending on the modification. All subsequent activities in the lifecycle are performed in accordance with approved development lifecycle procedures.

The impact analysis documents which tests must be run to validate the change and which tests must be re-run to validate that the change did not affect other functionality.

The software modification procedure requires that the changed software module is reverified after the change has been made.

The software modification procedure requires that all affected software modules are reverified after modification.

The software modification procedure allows regression validation for certain modifications.

The Impact Analysis indicates the plan for software verification and validation of the modification. The plan is a tailored version of the plan expected for a full verification, based on the SIL.

Modifications are initiated with an Engineering Design Change procedure. All changes are first reviewed and analyzed for impact before being approved. Measures to verify and validate the change are developed following the normal design process.

The modification process has been successfully assessed and audited, so PR electronics A/S may make modifications to this product as needed. An impact analysis is performed for any change related to functional safety.

Conclusion

The objectives of the standard are fulfilled by the PR electronics A/S functional safety management system, change management procedures, and sustaining product procedures.

5.4 System Design

Objectives

The objective of the related IEC 61508 requirements of this subclause are to specify the design requirements for each E/E/PE safety-related system, in terms of the subsystems and elements.

Assessment

Architecture partitioning and SIL allocation

The system is subdivided to subsystems. The notation B.x.y is used to name the sub systems. The subsystems are described in the technical safety concept. The interfaces between the sub systems are described (e.g. chapter 3.6.2 Interfaces).

The non-safety related parts of the system are identified in chapter 3.3.2 “Overview diagram”. The other sub systems are all SIL 2 classified (software SIL 3 for the systematic capability). Requirements to reach independence are defined in the SDRS.

Fault reaction

The technical safety concept describes the safe state. The safe state is to bring the current output to the fail low or fail high state. Chapter 3.8.2 describes the sequence of the shutdown procedure.

Critical interfaces

The HART signal is for non safety use only. The HART signal is de-coupled by hardware and may not be used for safety critical communication. The software requirements define that the safe domain is executed in the highest prior ISR in order to reach interference freeness from the HART communication.

The communication between the input and the output CPU is protected by 16bit CRC, timeout supervision and the sequence of expected data as described in the technical safety concept.

Maintainability

Maintenance during the field operation is not required. The proof test cycle is assumed to be set to the lifetime. The device shall be replaced after the lifetime (refer to IEC 61508-2:2010 section 7.4.9.5 note 3). If lower PFD_{avg} values are required, a proof test is defined in the safety manual. This can be used with a proof test cycle that must be calculated by the user.

Software design

All software components or subsystems listed in the software architecture design have corresponding Software Designs which further partition the design into software modules. The design has a focus on simplicity.

The software detailed design and the architectural design are made in the same documents for the input and the output CPU.

Diagnostics design

The Software Design describes the design of all diagnostics required to detect faults in software control flow and data flow. The resulting behavior of the device due to a detected fault is specified.

The diagnostics to detect control flow faults and faults of the Hardware are described for the input and output CPU in the related “FailSafe Module”. Failures related to safety related data are covered by the redundant input reading, the read back of the output control and the double storage.

Design reviews

Formal design reviews are held and the results recorded; action items are identified, assigned, and resolved.

The detailed design was reviewed together with the architectural design. This can be accepted because of the simplicity of the architecture in which the input CPU acts mainly as a part of the ADC converter and the Output CPU SW is structured in a safety and non safety domain.

Modification protection

The safe parameterization concept describes the use of the tools. The Software Safety Concept details the parameterization concept. HART (loop link is a variant of HART) and the extension port (for Siemens) are the defined interfaces for the parametrization. Loop link is only possible by aborting the safe operation mode.

Systematic fault avoidance

The hardware design is based on previously designed devices (e.g. the input – output CPU concept, the WD concept, the HART interface, output current monitoring). Hardware inspections are used to verify the hardware design. Some parts are verified by simulations. Worst Case Analysis are performed.

There was no ASIC design carried out within this project.

Conclusion

The objectives of the standard are fulfilled by the PR electronics A/S functional safety management system and new product development processes.

5.5 Hardware Design and Verification

Objectives

The main objectives of the related IEC 61508 requirements are to:

- Create E/E/PE safety-related systems conforming to the specification for the E/E/PES safety requirements (comprising the specification for the E/E/PES safety functions requirements and the specification for the E/E/PES safety integrity requirements).
- Ensure that the design and implementation of the E/E/PE safety-related systems meets the specified safety functions and safety integrity requirements.
- Demonstrate, for each phase of the overall, E/E/PES and software safety lifecycles (by review, analysis and/or tests), that the outputs meet in all respects the objectives and requirements specified for the phase.
- Test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase.
- Integrate and test the E/E/PE safety-related systems.

5.5.1 Hardware architecture design

Assessment

The system is subdivided to subsystems. The notation B.x.y is used to name the sub systems. The subsystems are described in the technical safety concept. The interfaces between the sub systems are described (e.g. chapter 3.6.2 Interfaces).

PR electronics maintains a component database where only PR electronics qualified components may be used. The production system can only use components from the existing database.

EMC and Intrinsic safety is addressed by the design. The device is moulded.

Hardware architecture design has been partitioned into subsystems, and interfaces between subsystems are defined and documented. Design reviews are used to discover weak design areas and make them more robust. Measures against environmental stress and over-voltage are incorporated into the design.

The FSM Plan and development process and guidelines define the required verification activities related to hardware including documentation, verification planning, test strategy and requirements tracking to validation test.

Conclusion

The objectives of the standard are fulfilled by the PR electronics A/S functional safety management system and new product development processes.

5.5.2 Hardware Design / Probabilistic properties

Assessment

To evaluate the hardware design of the Temperature Transmitter PR5435 / PR5437, a Failure Modes, Effects, and Diagnostic Analysis was performed by *exida* for each component in the system. This is documented in [R4] and [R7]. The FMEDA was verified using Fault Injection Testing as part of the development, see [D58] and [D59], and as part of the IEC 61508 assessment.

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration. An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design.

From the FMEDA failure rates are derived for each important failure category.

These results must be considered in combination with PFD_{AVG} of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL). The Safety Manual states that the application engineer should calculate the PFD_{AVG} for each defined safety instrumented function (SIF) to verify the design of that SIF.

Conclusion

The objectives of the standard are fulfilled by the PR electronics A/S functional safety management system, FMEDA quantitative analysis, and hardware development guidelines and practices.

5.6 Software Design

Objectives

The main objectives of the related IEC 61508 requirements are to:

- Create a software architecture that fulfils the specified requirements for software safety with respect to the required safety integrity level.
- Review and evaluate the requirements placed on the software by the hardware architecture of the E/E/PE safety-related system, including the significance of E/E/PE hardware/software interactions for safety of the equipment under control.
- Design and implement software that fulfils the specified requirements for software safety with respect to the required safety integrity level, which is analyzable and verifiable, and which is capable of being safely modified.

Assessment

Architecture partitioning to modules

The SW architecture shows a hierarchical design, which is refined to software components. All components are newly developed.

Input CPU:

The input CPU has only restricted resources and is mainly used to control the sensor measurement. (including the part of the CPU). A static view (block diagram) shows the SW elements. Timing is based on one single timer, to assure the correct sequence which is necessary for the A/D converter functionality. Timing diagrams show the sequence of the endless main loop.

Output CPU

The output CPU SW follows a layered approach. Each layer contains safe domain and non-safety domain parts. The safe parts run in an own context (own interrupt with the highest priority). Package diagrams show the layer concept on both the overall SW architecture and the safety domain architecture.

In normal operation the safety domain is triggered by the communication driven from the Input CPU. The communication is done with a DMA channel that rises an interrupt at the end of each communication block. In case of a missing communication, a timer interrupt triggers the safe domain that then handles the exception.

SIL classification

A software criticality analysis was performed.

For the input CPU all components are classified as SIL 3 software.

The output CPU's static architecture shows that for all layers whether they are safety related or non safety-related parts. The safety parts are collected in one package, the so called "safe domain". This covers the software parts related to the safety function and parts related to the diagnostics. The "safe Domain" itself has a layered architecture. The safe domain is executed in an own interrupt service routine (with the highest priority in the system). The measures against interference are related to the use of the highest priority of the ISRs and the CRC protection of (or optional normal / inverse storage) of the Safe Domain's data.

The Safe Domain is classified as SIL3.

Semi-formal methods

The Software Architecture Design uses the following diagram types:

- Logic/Function Block Diagrams
- Package Diagrams
- State Charts / State Transition Diagrams
- Sequence Diagrams
- Data Flow Diagrams
- Timing diagrams

The deployment diagram for the input CPU shows the software design elements. The timing diagrams of the input CPU shows the details of the interrupt usage. A control flow diagram shows the main function of the input CPU. Details of sequence of the ADC readings are shown in figure 12 (SWDS ICPU).

The Output CPU's architecture shows that the software system is based on an operating system. The "Safe Domain" is split into two ISR. The safe domain interrupt RX ISR is triggered by the DMA access (communication to the input CPU). The diagram shows that in case of a missing DMA interrupt the timer interrupt takes place which triggers the Timer ISR.

The static view of the safe domain shows the software components and their dependencies.

The dynamic views of the two ISRs are modelled in sequence diagrams.

Fault detection measures

For the input CPU the safe state is to disable the interrupts and to remain in an endless loop. The diagnostics of the input CPU are located in the FAILSAFE component. For the input CPU there are RAM checks, flow CRC check, Init check, jitter table check, setup data checks, flash CRC checks and the handshake check.

The sequence diagram of the RX ISR and the timer ISR shows that the execution of the diagnostics is scheduled first. The timer ISR controls the PWM output stage to the safe state. As this is only executed when the communication to the input CPU fails the WD has already brought the system to safe state.

The diagnostics of the output CPU are related to RAM protection, RAM check, program flow, stack test, supervision of supply voltages and output monitoring. Within the non safe domain the CPU test, ROM test, configuration CRC check are executed. The diagnostics from the non safe domain are supervised by the safe domain.

For the input CPU the integrity of the static data is verified by the fail safe handler

For the output CPU the Configuration data is protected by CRC, the RAM data is protected by normal/inverted storage (chapter 8.9.2 SWDS Output CPU).

The software design describes the design of all diagnostics required to detect faults in software control flow and data flow. The resulting behavior of the device due to a detected fault is specified.

The diagnostics to detect control flow faults and faults of the hardware are described for the input and output CPU in the related “FailSafe Module”. Failures related to safety related data are covered by the redundant input reading, the read back of the output control and the double storage.

Degradation

The Software Architecture Design specifies re-try fault recovery mechanisms to recover from faults.

Input CPU:

If the internal diagnosis detects a failure, the input CPU terminates the program execution by entering an endless loop.

The input CPU requires a power down / power up cycle to leave the endless loop. The only way to return from the safe state is to restart.

Output CPU:

A state diagram shows the different output CPU failure states:

- Failure state
- Fatal Failure state
- Sensor Error

The output CPU also requires a power down / power up cycle to recover from the “failure state”.

In the “Fatal Failure State” the device enters an endless loop doing nothing at all anymore.

The “Sensor Error State” indicates a problem with the sensor itself. A pre-configured value will be used as output value, which is checked to be outside the defined range if the device is in SIL mode.

Memory allocation

The Software Design describes an acceptable memory allocation strategy.

Input CPU: The memory mapping from ROM and RAM is shown in chapter 5 of the SDWS ICPU document.

OutputCPU: The memory allocation is shown in chapter 7 of the SWDS OCPU document.

Software Analysis / Design verification

The Software Analysis has been carried out. Design changes were identified and incorporated.

Conclusion

The objectives of the standard are fulfilled by the PR electronics A/S functional safety management system.

5.7 Software Verification

Objectives

The main objectives of the related IEC 61508 requirements are to:

- To the extent required by the safety integrity level, test and evaluate the outputs from a given software safety lifecycle phase to ensure correctness and consistency with respect to the outputs and standards provided as input to that phase.
- Verify that the requirements for software safety (in terms of the required software safety functions and the software safety integrity) have been achieved.
- Integrate the software onto the target programmable electronic hardware. Combine the software and hardware in the safety-related programmable electronics to ensure their compatibility and to meet the requirements of the intended safety integrity level.

Assessment results

Architecture design review

Both documents (architecture for Input- and Output CPU) were reviewed based on a checklist and by SW responsible, HW developer (Hardware software interface part) and a SW developer from PR electronics. The review comments address topics of functionality, understandability and correctness.

The checklist asks if the design documents cover the architectural requirements and if the software requirements are addressed. The checklist asks also for functional description, module descriptions, hardware interface descriptions. There are functionality related and interface related review targets.

The review of the requirements traceability (output CPU) was performed as a focused review for the traceability.

The findings for the output CPU are tracked in the Polarion tool. At PR electronics the findings are resolved and marked in the review report as solved. The findings are followed up and closed. To formally document that the activity is closed, the review report is signed.

Modular approach

A modular approach has been used in the software design.

Output CPU: The modules are modelled in the detailed design, that is well structured.

Input CPU: The SWDS shows the public and the private functions.

Partly, the SW elements in detailed design are directly allocated to one source code file. Sometimes an element is allocated to more source code files. The allocation can be seen in the UML model in enterprise architect. For the output CPU a Doxygen documentation can be extracted from the code for the private functions.

Structural test coverage

Evidence for the Branch Coverage for the input CPU is given in the module test report for the input CPU. Arguments for “not executed” lines are given (e.g. the look up tables for the CRC signs). The tests are executed on a simulator (input CPU). The measurement is reported by the simulator. The result is manually transferred to the test report.

All tests are also executed on target. The test report shows that all module tests of the input CPU are passed.

The test report shows the input values used for the specific tests.

The test report shows the results for each function. Where required equivalence classes and boundary values are defined. It is required that at least one invalid value is tested (e.g. chapter 6.3.1.2.3).

The report for the output CPU shows the C1 (branch) coverage of the Output CPU SW (on different levels). The code coverage measurement is listed. Where 100% code coverage is not reached, arguments are provided.

The test specifications for the output CPU are done in Tessy. In a word document the traceability to the requirements is documented.

The test specification is based on the parameter values of the function under test. Also global variables are seen as input values. The equivalence classes are defined mainly as minimum and maximum value of the data related datatype. The expected result is defined. The test cases contain a brief description of the test.

Code inspections and static code analysis

The Code reviews for the input CPUs are completed. The Code review status in the code review plan, all code reviews are completed.

The MISRA-C++:2008 rules are checked with PC Lint. The guideline contains the definition which rules are applied. Additionally QA-C checks rules which are required by PR electronics but are not supported by PC-Lint.

For each MISRA violation an argument is provided. Having an argument the code is instrumented to allow the related MISRA violation. At the end of the code files the Lint exceptions are explained. The Code review asks for the correctness of the exceptions.

Integration testing and Block box testing

The QVP describes the analytic verification methods like review and analysis (e.g. Concept FMEA). The “V&V” Plan sheet in the QVP shows in a RACI style all document based reviews

The test environments (e.g. Tessy) are the QVP (“Tooling”).

The testplan covers the tests on product level (during the development), during production and covers the safety validation plan (integration into a machine).

The product development level covers the module test, integration test and validation test.

The validation covers the fault insertion test.

The SW / HW integration plans test related to HW aspects, SW aspects and functional tests / proof of design.

The “HW aspects” related tests cover functional testing.

The “SW aspects” related tests cover for each CPU the testing of the integrated software against the software requirements (SWRS), the integration of the software on board and system integration.

So-called acceptance test are covering the black box / functionality and performance. These tests are carried out at PR electronics.

For each test, the integration test results record identifies the test case, its version, the version of the product being tested, the tools; and the equipment used, along with their calibration data. In addition, the Integration test results record references the integration test plan including version number.

Test management and automation tools

The tools to be used are planned in the QVP. HW/SW integration is done manually. As testing tools e.g. Tessy is planned. For static analysis PC-Lint is planned. No dedicated test management tool is used. The test specifications are done in Polarion and to a certain extent, test management facilities of Tessy is used.

Results are documented in Word documents.

Offline numerical analysis

The sensitivity analysis was performed which contains the verification of the floating-point calculation. The floating-point calculation in the output CPU software is compared with an offline calculation in a PC-SW tool.

Fully defined interface

The Interfaces (public functions) are defined in Enterprise Architect and exported to the Software Design Specification. The modules are documented in Doxygen. Types and names of the interfaces are defined.

The safety related analog dataflow is not protected by variables with limited ranges as the software is configurable with user parameters. Therefore, the full range of the variables is judged to be a valid range. There are to two limit supervisions implemented to supervise the safety related dataflow. Other variables are mainly handled with the datatype “enum”.

The testing takes as equivalence classes the full range of the datatypes into account.

Test plan review

The integration test plan was reviewed and found to be adequate with regard to its coverage of the software safety requirements, the software architecture design, the software system design, the types of tests to be performed and the procedures to be followed. All action items have been resolved or deferred.

Conclusion:

The objectives of the standard are fulfilled by the PR electronics A/S functional safety management system, software development process, and new product development processes.

5.8 Safety Validation

Objectives

- Ensure that the design and implementation of the E/E/PE safety-related systems meets the specified safety functions and safety integrity requirements.
- Plan the validation of the safety of the E/E/PE safety-related systems.

- Validate that the E/E/PE safety-related systems meet, in all respects, the requirements for safety in terms of the required safety functions and the safety integrity.
- Ensure that the integrated system complies with the specified requirements for software safety at the intended safety integrity level.

Assessment

Validation planning and fault insertion testing

Acceptance Tests are planned (Acceptance Test Specification ATS). These tests are functional tests on device level. The target is to cover the requirements of the SDRS. (IEC 61508 Validation)

Product Validation Tests are planned (Type Approval test specification TATS). These tests cover the environmental tests, EMC tests and ATEX related tests.

The Validation tests covers the fault insertion tests. The fault insertion test specification (FITS) is planned. The fault insertion testing is based on the FMEDA and the diagnostic definitions of the TSC.

Validation report

Test results are documented including reference to the test case and test plan version being executed.

The following information is documented in the test results:

a) a record of validation activities, permitting validation results to be reproduced and/or retraced.

b) The safety function associated with each test case.

d) The tools and equipment with ID used as trace to the calibration data.

e) The configuration identification of the item under test.

Performance modelling

The product is not complex enough to warrant performance modeling. There is only one performance parameter in the system (Safety Function Response Time) and this parameter is sufficiently tested by validation tests.

Process simulation

The validation testing requires simulation of process inputs and timing between input changes (process simulation). This is done by testing the software in the product hardware and simulating the input signal(s) and other process conditions using a test fixture or test equipment.

Conclusion

The objectives of the standard are fulfilled by the PR electronics A/S functional safety management system, software development process, and new product development processes.

5.9 Safety Manual

Objectives

- Develop procedures to ensure that the required functional safety of the E/E/PE safety-related systems is maintained during operation and maintenance.

Assessment

The manufacturer responsibility is limited to providing the end-user with all the necessary product

information for the proper engineering of the product in a safety function in addition to enabling the required verification analysis steps of the complete safety function. The Safety Manual shall describe or shall refer the required information.

Additionally, the Safety Manual should be used during validation for justification of correctness to the extent applicable.

The safety manual describes the purpose of the product (chapter 4). In terms of the interfaces it describes the extension port, the output and the input including the connection of sensors to the input. The (safe) configuration is also described.

The Safety Manual describes the "functional test procedure" in chapter 13.

The Safety Manual states that no maintenance is required.

Maintenance is not applicable. Field returns are handled by the functional safety management process.

Conclusion

The objectives of the standard are fulfilled by the PR electronics A/S functional safety management system and the safety manual.

6 Results of the assessment covering additions for DIN rail housing variant PR6437

6.1 Summary of modifications

Main purpose of the product modifications was to derive DIN rail housing variants (PR6437)[1].

At the same time, known issues were analysed and the design was improved where applicable.

The design of the devices is common to all variants, the PCB and the electronic circuits are also common to all devices. In PR6437 devices, the PCB is mounted to an additional “mainboard”. The only difference in the circuitry is the mounting of a temperature sensor on the mainboard instead of the common PCB. The temperature sensor is used to determine the terminal temperature for the so-called cold junction compensation. This compensation is part of the known measurement principles for thermocouples.

The firmware (both input and output CPU) is also common to all variants. The small differences in hardware related to the cold junction compensation is reflected in the firmware by configuration data.

6.2 Safety impact on the PR543x devices

The firmware changes applied to the output CPU firmware include safety relevant parts of the firmware.

[1] The DIN rail variants as shown as [V2] in chapter 3.2 are used for OEM customers, that create DIN rail housing products using these variants. The PR6437 are variants that are fully assembled in DIN rail housings and sold to end users.

The changes were analysed for their impact on the safety properties, safety integrity and safety capability of the PR543x devices.

A description [D153] shows that the changed safety relevant parts have no impact on the PR543x devices. The parts are inactivated for these devices by setting configuration data accordingly.

The product version numbering [D154] specifies that safety relevant changes affecting the compatibility related to the safety properties are indicated by incrementing the first two digits of the version number.

According to the above mentioned description, the output CPU firmware changes from V1.2R0 to V1.6R0 are not considered to be safety relevant for the PR543x variants. As a consequence, the product version remains 01.xx.xx.

6.3 Safety activities carried out to process the modifications

All modifications are initiated by a product change request. Every change is analysed for its impact on the product functionality and on functional safety. Impacts are judged for their safety relevance.

The analysis is based on a template with a pre-defined checklist.

The elements of the system that are subject of modifications are identified. Also, realization phase steps that need to be repeated and the affected documentation are identified. The steps include verification. Additionally, regression tests are planned and carried out. Tests are documented and are passed.

Conclusion:

The modifications were carried out in accordance with the results of the basis assessment as documented in chapter 5.3.

7 Terms and Definitions

Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3)
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode where the demand interval for operation made on a safety-related system is greater than twice the proof test interval.
High demand mode	Mode where the demand interval for operation made on a safety-related system is less than 100x the diagnostic detection/reaction interval, or where the safe state is part of normal operation.
PFD_{AVG}	Average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
SFF	Safe Failure Fraction - Summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
HART	Highway Addressable Remote Transducer
AI	Analog Input
AO	Analog Output
DI	Digital Input
DO	Digital Output
Type B element	“Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

8 Status of the document

8.1 Liability

exida prepares reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

8.2 Version History

Contract Number	Report Number	Revision Notes
Q16/03-107-C	PRE 16/03-107-C R019 V0, R1	Initial draft document.
Q16/03-107-C	PRE 16/03-107-C R019 V0, R2	Updated based on review comments, Document list added.
Q16/03-107-C	PRE 16/03-107-C R019 V0, R3	Updated with review comments from customer and certifying assessor
Q16/03-107-C	PRE 16/03-107-C R019 V0, R4	Chapter 3 filled in, continuous mode added in Management Summary Chapter 7.2 updated
Q16/03-107-C	PRE 16/03-107-C R019 V1, R0	Product version in chapter 3.1 added, document released
Q16/03-107-C	PRE 16/03-107-C R019 V1, R1	Version Number of input and output CPU changed, Impact analysis and related documents added to the list of documents
Q16/03-107-C	PRE 16/03-107-C R019 V1, R2	Safety Manual Version changed from 2.0 to 3.0
Q18-10-076-C	PRE 16/03-107-C R019 V2, R0	Update with the result of the assessment activities to include the PR6437 variant in the scope of the certificate.

Review: Jürgen Hochhaus, exida, 2nd March 2018

Review V2R0: Peter Müller, exida, Aug 3, 2020

Peter Söderblom, exida, Aug 7, 2020

Status: Released, Aug 10, 2020

8.3 Future Enhancements

At request of client.

8.4 Release Signatures

Peter Müller, Dipl. Ing. (FH), Senior Safety Engineer

Jürgen Hochhaus, Dipl. Ing. (FH), Senior Safety Engineer

Peter Söderblom, Senior Safety Engineer