Results of the IEC 61508 Functional Safety Assessment

Project:
Series 9000 devices

Customer:
PR electronics A/S
Rønde,
Denmark

Contract No.: Q23/12-098
Report No.: PR 23/12-098 R035
Version V1, Revision R0, August 01, 2024
Jürgen Hochhaus

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.

Management Summary

The Functional Safety Assessment of the PR electronics

Series 9000 devices

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

- *exida* assessed the development process used by PR electronics through an audit and review of a detailed safety case against the *exida* certification scheme which includes the relevant requirements of IEC 61508. The assessment was executed using subsets of the IEC 61508 requirements tailored to the work scope of the development team.
- *exida* reviewed and assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.
- *exida* reviewed field failure data to verify the accuracy of the FMEDA analysis.

The functional safety assessment was performed to the SIL 2 (Type B) / SIL 3 (Type A) requirements of IEC 61508:2010. 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 Series 9000 devices development project, complies with the relevant safety management requirements of IEC 61508:2010 SIL 2 (Type B) / SIL 3 (Type A).

The assessment of the FMEDA, done to the requirements of IEC 61508, has shown that the Series 9000 devices can be used in a high or low demand safety related system in a manner where the PFH/ PFD_{avg} meets the requirements of table 2 or table 3 of IEC 61508-1.

The assessment of the FMEDA also shows that the Series 9000 devices meet the requirements for architectural constraints of an element such that it can be used to implement a SIL 2 / SIL3[1] safety function.

This means that the Series 9000 devices is capable for use in SIL 2 / SIL3 applications in Low demand mode or high demand mode when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual and when using the versions specified in section 3.7 of this document.

[1] See **Table** 1 to identify which of the Series 9000 devices can be used for up to SIL2 and which for SIL3.

Device	Architectural Constraints Route	Hardware Fault Tolerance	Capable for
9106 (single channel use)	1H, Type A	0	SIL2
9106 (dual channel use)	1H, Type A	0	SIL3
9107	1H, Type A	0	SIL2
9113, 9116	2H, Type B	0	SIL2 (Low Demand)[2]
		1	SIL2 (High Demand)[2]
9202, 9203	2H, Type B	0	SIL2 (Low Demand)[2]
		1	SIL2 (High Demand)[2]

Table 1: Fulfilment of requirements for SIL for the Series 9000

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFH/PFD_{avg} considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each element must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

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

[2] For the dependence of the safety integrity level on the hardware fault tolerance when following route 2_H see IEC 61508-2:2010, 7.4.4.3.1.

Table of Contents

1 Purpose and Scope

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

- Series 9000

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 Series 9000 devices with the technical IEC 61508-2 and -3 requirements for SIL2 / SIL 3 and the derived product safety property requirements

and

- the Series 9000 devices development processes, procedures and techniques as implemented for the safety-related deliveries with the managerial IEC 61508-1, -2 and -3 requirements for SIL 2 (Type B) / SIL 3 (Type A).

and

- the Series 9000 devices 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.

1.1 Tools and Methods used for the assessment

The assessment is based on earlier assessments according to IEC 61508:2000. Assessment reports for these assessments are listed in the document section (chapter 2.4.2).

Based on the assessment results as shown in the earlier reports, a delta assessment considering the changes in the standard was carried out. An *exida* checklist listing these changes was used to do a gap analysis to identify needed additional activities to be carried out to ensure the compliance with the IEC 61508:2010. The delta assessment was carried out based on this gap analysis. The evidences for the fulfillment of the changed objectives and requirements of the standard were assessed.

The hardware assessment in terms of an FMEDA was updated for all devices of the Series 9000 devices in the scope of this report. For details please refer to chapter 5.4.6 FMEDA Update.

The results of the earlier assessment against IEC 61508:2000 were taken over into this report. Chapter 5 contains the results of the delta assessment.

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

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, availability and cybersecurity with over 500 person-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 350 billion hours of field failure data.

2.2 Roles of the parties involved

PR electronics A/S	Manufacturer of the Series 9000
exida	Performed the hardware assessment [R8] - [R12]
exida	Performed a gap analysis of the PR electronics development process against IEC 61508:2010
exida	Performed the Functional Safety Assessment [R7] per the accredited *exida* scheme.

PR electronics 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 61508:2010 (Parts 1 – 3)	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – Normative Parts
[N2]	IEC 61508:2010 (Parts 4 – 7)	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – Informative Parts

2.4 Reference documents

2.4.1 Documentation provided by PR electronics

For the documentation provided by PR electronics for the earlier assessment (see chapter 1.1), please refer to the related assessment reports [R1] - [R6].

For the documentation provided by PR electronics for the delta assessment and the surveillance audit, please refer to chapter 5.1.

2.4.2 Documentation generated by *exida*

[R1]	*exida* report number 0709-02C R016	Assessment Report 9106 HART transparent repeater V1R1
[R2]	*exida* report number 0709-02C R017	Assessment Report 9107 HART transparent driver V1R2
[R3]	*exida* report number 0709-02C R012	Assessment Report 9113 Temperature / mA Converter V1R5
[R4]	*exida* report number 0709-02C R014	Assessment Report 9116 Universal Converter V1R1
[R5]	*exida* report number 0709-02C R003	Assessment Report 9202 Pulse Isolator V1R5
[R6]	*exida* report number 0709-02C R007	Assessment Report 9203 Solenoid / Alarm Driver V1R2
[R7]	PR 2312-098-C R032 assessment and review comments V0R5 Series 9000 2ed 61508.docx	Documentation of the delta assessment and the surveillance audit 2024.
[R8]	PR 9106-9107 06-03-19 R025 V2R1.pdf	FMEDA report 9106 and 9107 (Based on IEC 61508:2010), V2R1 dated July 11, 2016
[R9]	PR 06-03-19 R022 FMEDA 9113_V3R2.pdf	FMEDA report 9113 (Based on IEC61508:2010), V3R2 dated February 1, 2024
[R10]	PR 06-03-19 R024 FMEDA 9116_V3R3.pdf	FMEDA report 9116 (Based on IEC 61508:2010), V3R3 dated April 09, 2024
[R11]	PR 06-03-19 R018 FMEDA 9202_V3R3.pdf	FMEDA report 9202 (Based on IEC 61508:2010), V3R3 dated April 09, 2024
[R12]	PR 06-03-19 R023 FMEDA 9203_V3R3.pdf	FMEDA report 9203 (Based on IEC 61508:2010), V3R3 dated April 09, 2024
[R13]	PR electronics GAP analysis 61508 2010 V0R8.docx	Gap analysis of the PR electronics development process against IEC 61508:2010 showing gaps between the original safety case based on IEC 61508:2000 and the IEC 61508:2010.
[R14]	9000_series_PR_FFA_Overview.xlsx	Overview on failure rate calculation based on the field history
[R15]	9106 FFA Spreadsheet_V0R1.xlsx	Failure rate calculation based on field history

[R16]	9107 FFA Spreadsheet_V0R1.xlsx	Failure rate calculation based on field history
[R17]	9113 FFA Spreadsheet_V0R1.xlsx	Failure rate calculation based on field history
[R18]	9116 FFA Spreadsheet_V0R1.xlsx	Failure rate calculation based on field history
[R19]	9202 FFA Spreadsheet_V0R1.xlsx	Failure rate calculation based on field history
[R20]	9203 FFA Spreadsheet_V0R1.xlsx	Failure rate calculation based on field history
[R21]	PR 23-12-098 R035	IEC 61508 Functional Safety Assessment for Series 9000 (this document)
[R22]	PR 23-12-098 R035 V0R2	Recommendations Report. Recommendations given based on the surveillance audit and certification update assessment activities.

2.5 Assessment Approach

The assessment audit was driven by the differences between edition1 (2000) and edition 2 of the standard (2010) as documented in the gap analysis [R13]. A surveillance audit according to the exida assessment scheme was carried out in addition.

3 Product Description

The Series 9000 consist of the following devices:

- 9106 HART transparent repeater
- 9107 HART transparent driver
- 9113 Temperature / mA Converter
- 9116 Universal Converter
- 9202 Pulse Isolator
- 9203 Solenoid / Alarm Driver

The following device descriptions are taken over from the earlier assessment reports [R1] to [R6].

3.1 9106 HART transparent repeater

The 9106 HART transparent repeater shall provide the following Type-A safety functions:

> The 9106 HART transparent repeater isolates 4-20 mA process signals and realizes a ground loop elimination.

The following figure shows the principle product architecture of the 9106 HART transparent repeater.

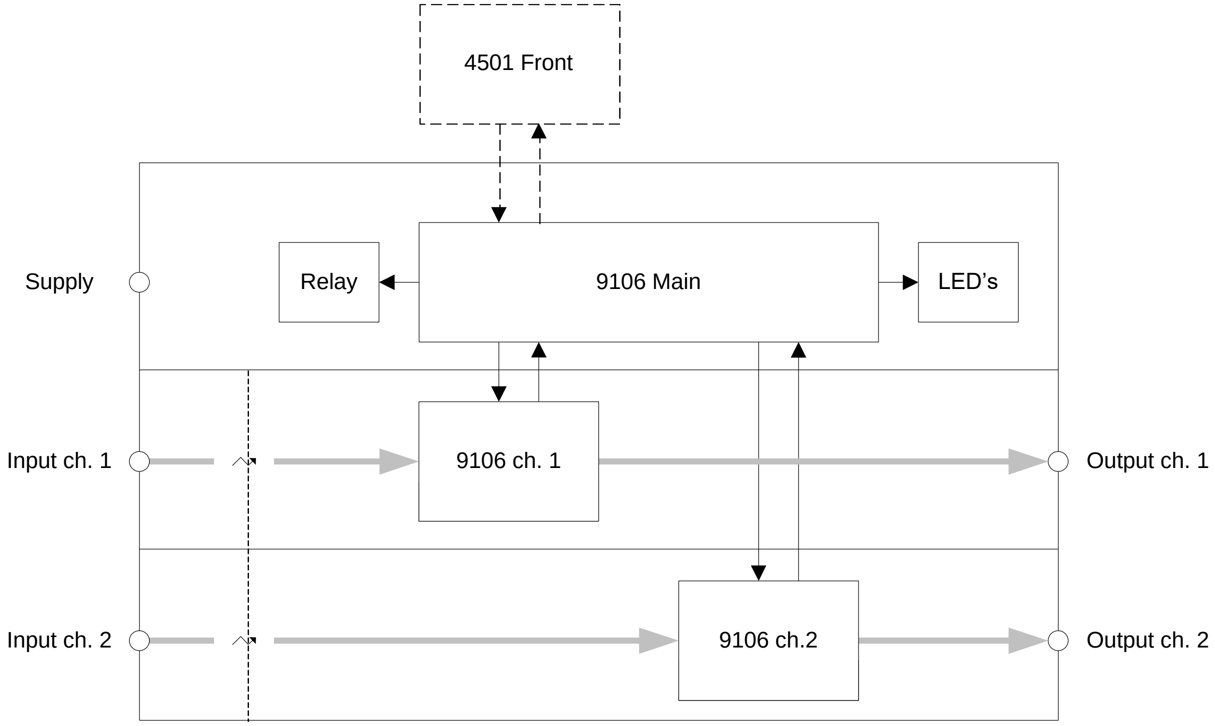

Figure 1 Product architecture of the 9106 HART transparent repeater

The safety architecture of the device makes no use of any microprocessor. A separate HW supervision circuitry ensures the independence of the safety function and the microprocessors accuracy adjustments.

For use in SIL 3 applications the inputs and the outputs have to be connected in series.

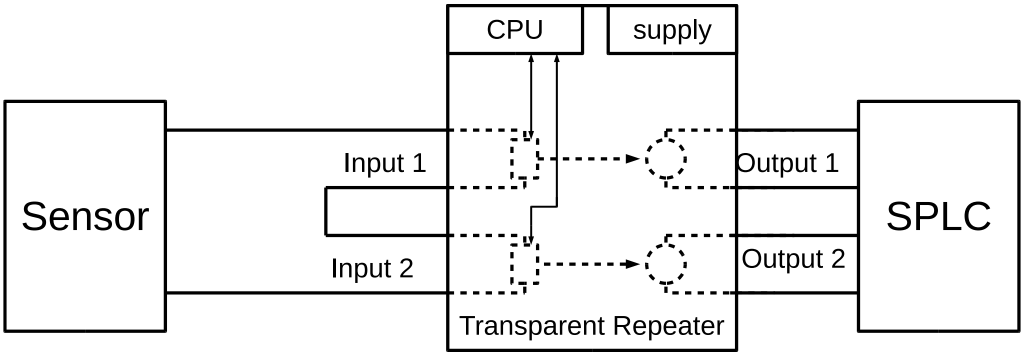

Figure 2: Dual channel Connection of one Sensor

As shown in Figure 2, a sensor is connected to both inputs. Only one input may supply the sensor. Only a passive input can supply a sensor. Active inputs are driven by external sensors or other devices. In this configuration it is required that the Safety PLC (SPLC) compares the two output signals with an accuracy of +/- 2% of full span. A discrepancy of more than +/- 2% shall lead to a fault detection. This configuration is recommended for SIL3 application.

The status relay is not part of the safety function.

Dangerous detected (DD) failures can only be detected by an external logic solver, which is assumed to be connected to the 9106 Transparent Repeater.
Internally the 9106 Transparent Repeater doesn’t have any diagnostic function.
For the dual channel configuration, an internal dangerous detected failure is assumed if the difference between both output signals is more than 2% full span. This difference must be detected by the external logic solver.

3.2 9107 HART transparent driver

The 9107 HART transparent driver shall provide the following Type-A safety functions:

> The 9107 HART transparent driver isolates 4-20 mA process signals and realizes a ground loop elimination.

The following figure shows the principle product architecture of the 9107 HART transparent driver.

The figure shows the principle product architecture of the 9106. The principle in 9107 is the same except EX protection applies to the outputs.

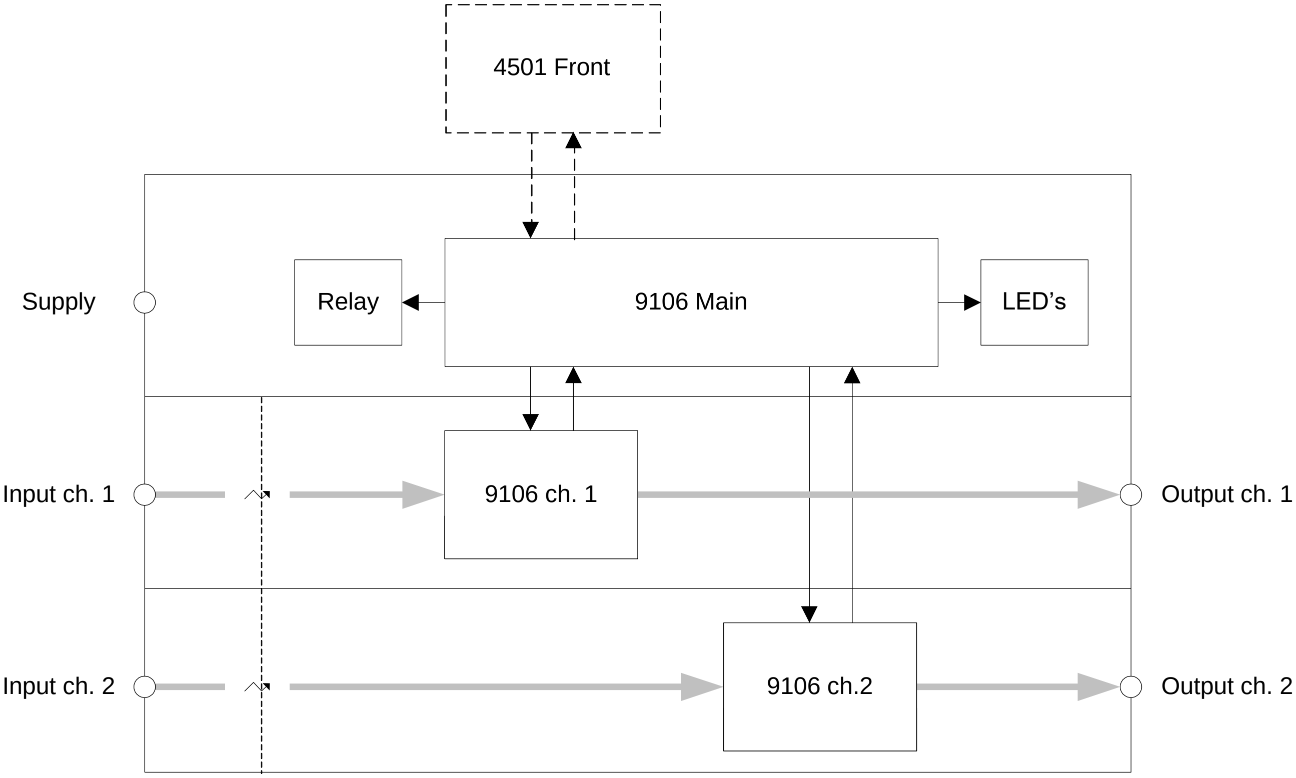

Figure 3 Product architecture of the 9106 / 9107 HART transparent driver

The safety architecture of the device makes no use of any microprocessor. A separate HW supervision circuitry ensures the independence of the safety function and the microprocessors accuracy adjustments.

The status relay is not part of the safety function.

Dangerous detected (DD) failures can only be detected by an external logic solver, which is assumed to be connected to the 9107 Transparent Driver.
Internally the 9107 Transparent Driver doesn't have any diagnostic function.

3.3 9113 Temperature / mA Converter

The 9113 Temperature / mA Converter shall provide the following Type-B safety functions:

> The 9113 Temperature / mA Converter shall convert various sensor input signals from hazardous areas to a 4..20 mA current output signal.
>
> The 9113 Temperature / mA Converter shall be available in a single and a dual channel[3] version.

The following figure shows the principle product architecture of the 9113 Temperature / mA Converter.

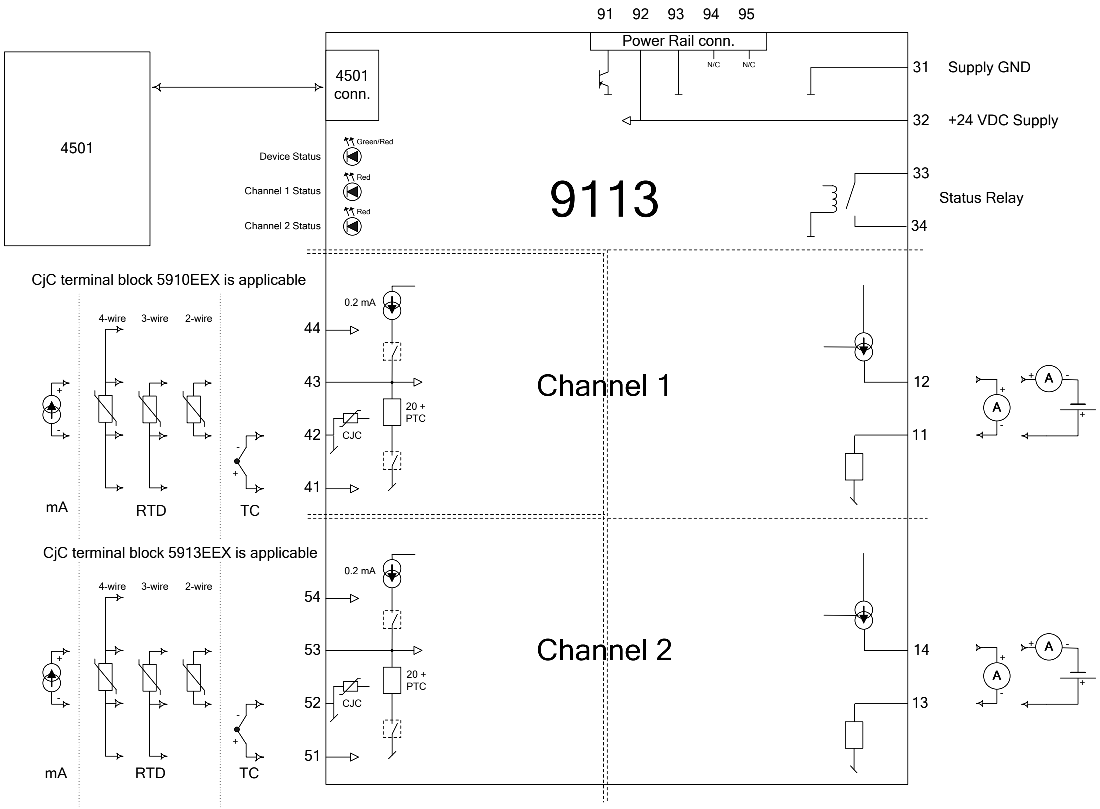

Figure 4 Product architecture of the 9113 Temperature / mA Converter

The safety architecture of the device makes - per channel - use of two microprocessors and a separate HW supervision circuitry that realizes a second independent shutdown path, which is not shown in this diagram.

The status relay is not part of the safety function.

The two channels on the device shall not be used in the same safety function, e.g. to increase the hardware fault tolerance of the device (to achieve a higher SIL), as they contain common components. The two channels may be used in separate safety instrumented functions if due regard is given to common cause failures.

[3] The dual channel version is not intended to be used in a single safety function, e.g. to increase the hardware fault tolerance. The two channels can be used in two separate safety instrumented functions.

3.4 9116 Universal Converter

The 9116 Universal Converter shall provide the following Type-B safety functions:

> The 9116 Universal Converter shall convert various sensor input signals from hazardous areas to a 4..20 mA current output signal. An additional safety related output relay shall be available.

The following figure shows the principle product architecture of the 9116 Universal Converter.

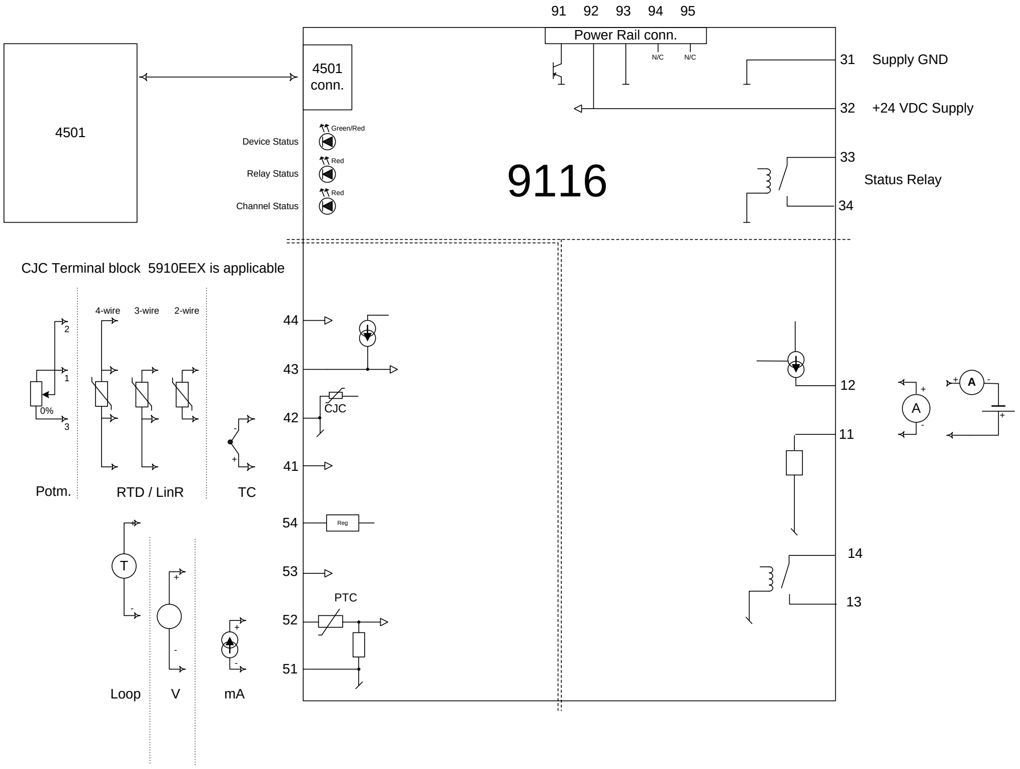

Figure 5 Product architecture of the 9116 Universal Converter

The safety architecture of the device makes use of two microprocessors and a separate HW supervision circuitry that realizes a second independent shutdown path, which is not shown in this diagram.

The possibility to use the device with a single Relay output, where the Relay has been subject to endurance testing and external over current protection is required by the Safety Manual, is seen to be compliant to IEC 61508.

The status relay is not part of the safety function.

3.5 9202 Pulse Isolator

The 9202 Pulse Isolator shall provide the following Type-A safety functions:

> The 9202 Pulse Isolator shall convert NAMUR sensor input signals from hazardous areas to a digital output signal in safe area.
>
> Additionally, the 9202 Pulse Isolator provide a Type-B safety function operating on the Type-A safety functions which results in the consideration of the 9202 Pulse Isolator as Type-B systems:
>
> The 9202 Pulse Isolator shall provide a menu-configured possibility for inverting the output via the Output CPU

The following figure shows the principle product architecture of the 9202 - Pulse Isolator:

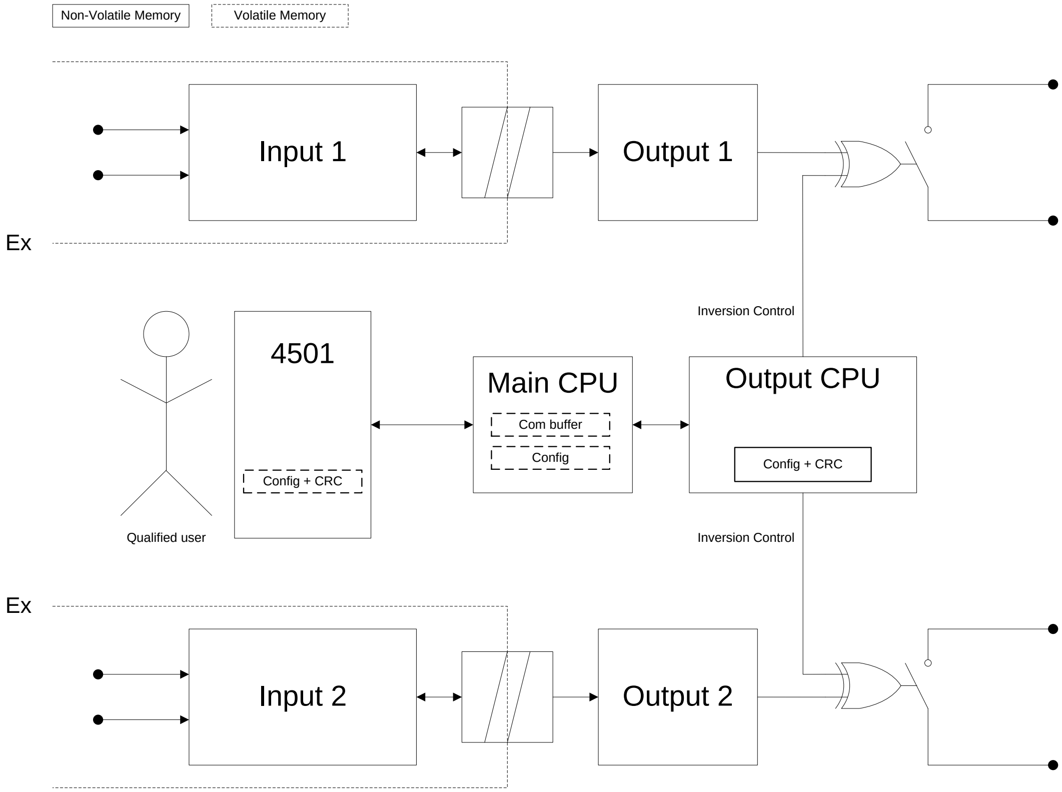

Figure 6 Product architecture of the 9202 Pulse Isolator

It can be seen that the complex electronics (Type B) are only used to control the direct / invert setting of the output. The read back of the Output CPU's control signal by the Main CPU for diagnostic purposes and the possible second independent shutdown path are available, but not shown in this diagram.

The possibility to use the device with a single Relay output, where the Relay has been subject to endurance testing and external over current protection is required by the Safety Manual, is seen to be compliant to IEC 61508.

3.6 9203 Solenoid / Alarm Driver

The 9203 Solenoid / Alarm Driver shall provide the following Type-A safety function:

> The 9203 Solenoid / Alarm Driver shall convert NPN/contact/PNP signals from safe area into digital drive signals in hazardous area.

Additionally, the 9203 Solenoid / Alarm Driver provide a Type-B safety function operating on the Type-A safety function which results in the consideration of the 9203 Solenoid / Alarm Driver as Type-B system:

> The 9203 Solenoid / Alarm Driver shall provide a menu-configured possibility for inverting the output via the Output CPU

The following figure shows the principle product architecture of the 9203 Solenoid / Alarm Driver:

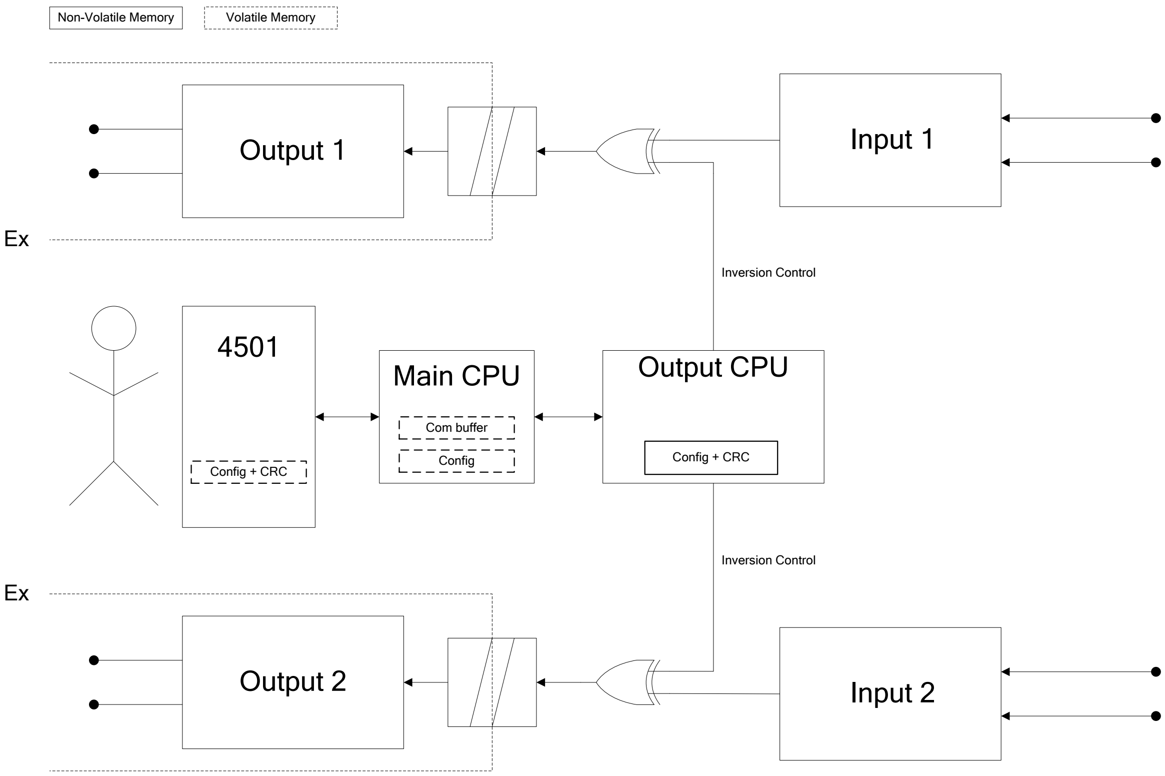

Figure 7 Product architecture of the 9203 Solenoid / Alarm Driver

It can be seen, that the complex electronics (Type B) are only used to control the direct / invert setting of the output. The read back of the Output CPU's control signal by the Main CPU for diagnostic purposes and the possible second independent shutdown path are available, but not shown in this diagram.

In the high current version there is only one channel available.

The two channels on the device shall not be used in the same safety function, e.g. to increase the hardware fault tolerance of the device (to achieve a higher SIL), as they contain common components. The two channels may be used in separate safety instrumented functions if due regard is given to common cause failures.

3.7 Hardware and Software Version Numbers

This assessment is applicable to the following hardware and software versions of Series 9000:

Device	Software Version	Software Version	Hardware Version	Device Version
9106	Not relevant	Not relevant	9106-1 V8AR0	9106-002
9107	Not relevant	Not relevant	9107-1-V2R0	9107-002
9113	V16R0 (FW 911362xx)	V10R0 (FW 911363xx)	9113-1 V6AR0	9113-004
9116	V16R0 (FW 911362xx)	V10R0 (FW 911363xx)	9116-1-04A	9116-004
9202	V13R0 (FW 920260xx)	V10R0 (FW 920262xx)	9202-1-06A	9202-003
9203	V13R0 (FW 920260xx)	V10R0 (FW 920262xx)	9203-1 V8AR0	9202-003

4 IEC 61508 Functional Safety Assessment Scheme

exida assessed the development process used by PR electronics for this development project against the objectives of the *exida* certification scheme. The results of the assessment are documented in [R1] - [R6]. All objectives have been successfully considered in the PR electronics development processes for the development.

exida assessed the set of documents against the functional safety management requirements of IEC 61508:2000. 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 61508:2000-1 to 3.

The detailed development audit (see [R1] - [R6]) evaluated the compliance of the processes, procedures and techniques, as implemented for the PR electronics Series 9000, with IEC 61508:2000.

The assessment was executed using the exida certification scheme which includes subsets of the IEC 61508:2000 requirements tailored to the work scope of the development team.

exida assessed the activities that were carried out by PR electronics to meet the modified objectives in IEC 61508:2010 (see chapter 5).

The result of the both assessment activities shows that the Series 9000 is capable for use in SIL2 / SIL 3 applications, when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual. For the detailed information of type and safety capability of the different devices and configurations see **Table 1**.

4.1 Product Modifications

The modification process has been successfully assessed and audited, so PR electronics 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 Surveillance audit and delta assessment 2024

5.1 Reference documents

Ref.	Name	Description	Revision, Date
[D1]	9202SCR24	Impact Analysis	V0R4 dated 2012-04-24
[D2]	PR electronics GAP Analysis 61508 2010 V0R8.docx	Gap Analysis Report	V0R9
[D3]	RE: PR 2312-098-C R032 assessment and review comments series 9000 2ed 61508.msg	Email dated 13.02.2024 from Flemming Sørensen listing the firmware change requests after the initial assessment	
[D4]	9000 Product History.xlsx	Overview on changes since last assessment for all units in scope	V1R0
[D5]	9202 - Diode Assembly Failure - Official Statement_Evidence pack 2024-06-11.pdf	Summary report about the activities related to the fault / field failures including a failure description	
[D6]	I10.4 Return types and Failure types (used in AX).pdf	The purpose of this instruction is to provide clarity on how to categorize products being returned to PR electronics and provide them with a correct failure type for statistical purposes.	Revision 2024-05-17
[D7]	I25.2 IMS Databases & Registrations.pdf	Contains a description of a claim handling, included handling of safety related claims.	Revision 2024-06-07
[D8]	I3.82 Product Quality Surveillance Group.pdf	Description of monitoring product quality, including monitor of failure rates (considering the safety related failure classification)	Revision 2024-06-07
[D9]	I30.14 SIL products and FMEDA calculations.pdf	Investigation on field returns of all products (frequently updated). This includes a description of described failure classifications	Revision 2024-06-04
[D10]	RE_ Series 9000 surveillance audit _ Field returns .msg	Questions and PR reactions regarding numerous dangerous faults (shown in the Field History of 9202 and 9106)	

[D11]	RE_ 9202 _ Zener Diode statement_Discussion .msg	Agreement on evidence documentation related to the systematic fault in 9202 – (provided documentation see [D6] to [D9])
[D12]	PCO201	Change request with Impact Analysis
[D13]	SCR 20	Change request with Impact Analysis
[D14]	SCR 21	Change request with Impact Analysis
[D15]	SCR 24	Change request with Impact Analysis
[D16]	SCR 51/52	Change request with Impact Analysis
[D17]	SCR 53	Change request with Impact Analysis

Note: The documents as shown above are those audited during the surveillance audit / delta assessment.

For the documentation provided by PR electronics for the earlier assessment (see chapter 1.1), please refer to the related assessment reports [R1] - [R6].

5.2 Roles of the parties involved

PR electronics	Manufacturer of the Series 9000
exida	Performed the hardware assessment update
exida	Performed the IEC 61508:2010 Functional Safety Surveillance Audit per the accredited *exida* scheme.

PR electronics contracted *exida* in December 2023 to perform the surveillance audit for the above Series 9000. The surveillance audit was conducted January to April 2024.

5.3 Surveillance Methodology

As part of the IEC 61508 functional safety surveillance audit the following aspects have been reviewed:

- Procedure Changes – Changes to relevant procedures since the last audit are reviewed to determine that the modified procedures meet the requirements of the *exida* certification scheme.
- Engineering Changes – The engineering change list is reviewed to determine if any of the changes could affect the safety function of the Series 9000.
- Impact Analysis – If changes were made to the product design, the impact analysis associated with the change will be reviewed to see that the functional safety requirements for an impact analysis have been met.
- Field History – Shipping and field returns during the certification period will be reviewed to determine if any systematic failures have occurred. If systematic failures have occurred during the certification period, the corrective action that was taken to eliminate the systematic failure(s) will be reviewed to determine that said action followed the approved processes and was effective.
- Safety Manual – The latest version of the safety manual will be reviewed to determine that it meets the IEC 61508 requirements for a safety manual.
- FMEDA Update – If required or requested the FMEDA will be updated. This is typically done if there are changes to the IEC 61508 standard and/or changes to the *exida* failure rate database.
- Evaluate use of the certificate and/or certification mark - Conduct a search of the applicant's web site and document any misuse of the certificate and/or certification mark. Report any misuse of the certificate and/or certification mark to the exida Managing Director.
- Recommendations from Previous Audits – If there are recommendations from the previous audit, these are reviewed to see if the recommendations have been implemented properly.

5.4 Surveillance Results

5.4.1 Procedure Changes

There were no changes to the procedures during the previous certification period. But the procedures applied during the initial development were compared to the changes in IEC 61508:2010 compared to IEC 61508:2000.

This was done in a Gap Analysis [R13]. The basis of the analysis is a compare between the two editions of IEC 61508. The processes and procedures used for the initial development of the Series 9000 devices were compared to the relevant changed requirements of IEC 61508:2010. Based on this comparison it was analyzed wether the modified objectives and requirements of the standard are fulfilled. Argumentations for the fulfillment are given. Were needed, actions to close identified gaps were defined and carried out. The Gap Analysis resulted in no remaining gaps.

Based on the result of the Field History, the field return handling was improved.

[D6] to [D9] is the documentation of the improved field return handling. The areas of improvement were identified based on the summary report regarding the systematic fault ([D5]). The improvements cover categorization of products and the returned devices, claim handling with improved consideration of functional safety. It also describes the enhanced reporting of field returns in [D9].

5.4.2 Engineering Changes

There were no significant design changes to these products during the previous certification period.

The minor changes were processed with change requests based on the change management procedure that was audited in the initial assessment.

5.4.3 Impact Analyses

The impact of each change since the initial assessment was analyzed. [D4] shows the overview an of all changes, referencing the impact analyses that were carried out (included in the listed change requests). A description of each change and the verifications carried out are shown as well as documentation updates and version number changes.

The major part of the changes were done more than ten years ago.

The impact analyses documents resulted in having no impact on the safety capability of the devices.

5.4.4 Field History

The review of the field data for the 9202 showed that there were field failures due to a systematic fault. The systematic fault was no design, but a hardware component fault. The hardware component was changed to one without fault.

Similarly, the review of the field data for the 9106 showed that there were field failures due to a minor design fault. The design was changed by using a more robust hardware component.

The root causes for systematic faults were investigated, improvements to the processes steps of the related activities were introduced.

When excluding the systematic faults, the failures rates resulting from field histories of the Series 9000 products were analyzed and found to be consistent with the failure rates predicted by the FMEDA.

5.4.5 Safety Manual

One of the actions defined in the Gap Analysis was updating the safety manuals.

This addresses one of the differences that were identified in the comparison of the 2000 and the 2010 version of the standard: in IEC 61508:2010 Annex D was added.

The updated safety manuals were reviewed and found to be compliant with IEC 61508:2010.

5.4.6 FMEDA Update

The FMEDA were updated. For 9106 and 9107 devices the update was done in 2016 already. These FMEDA were done to fulfill the IEC61508:2010 requirements on the failure rate estimation and the architectural constraints for Route 1_H.

The FMEDA for the 9113, 9116, 9202, 9203 were updated in 2024 to fulfill the IEC61508:2010 requirements on the failure rate estimation and the architectural constraints for Route 2_H.

The FMEDA were reviewed. Related FMEDA reports are available ([R8] to [R12]). For the failure rate results please refer to the reports [R8] to [R12].

5.4.7 Evaluate use of certificate and/or certification mark

The PR electronics website was searched and no misleading or misuse of the certification or certification marks was found.

5.4.8 Previous Recommendations

Previous recommendations for improvement were reviewed. The recommendations are addressing activities that are carried out for a new development. There were no recommendations identified that need to be considered as having a major input on the scope of the activities audited in the surveillance audit.

5.5 Surveillance Audit Conclusion

The result of the Surveillance Audit Assessment can be summarized by the following observations:

The PR electronics Series 9000 devices meet the relevant requirements of IEC 61508:2010 based on the initial assessment and considering:

- field failure history

- permitted modifications completed on the product

- FMEDA updates and changes

This conclusion is supported by the updated assessment certification documentation.

exida assessed the development process used by PR electronics during the product development against the objectives of the *exida* certification scheme which includes IEC 61508:2000 parts 1, 2, & 3. The development of the Series 9000 was done per this IEC 61508:2000 SIL 2 (Type B) / SIL 3 (Type A) compliant development process. The impact of the changes in IEC 61508:2010 was analyzed. Identified gaps that might have impact on the safety capability of the devices were closed. The Safety Case was updated with project specific design documents.

6 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
PVST	Partial Valve Stroke Test
	It is assumed that the Partial Stroke Testing, when performed, is automatically performed at least an order of magnitude more frequent than the proof test, therefore the test can be assumed an automatic diagnostic. ; therefore, the test can be assumed an automatic diagnostic. Because of the automatic diagnostic assumption, the Partial Valve Stroke Testing also has an impact on the Safe Failure Fraction.
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 A element	“Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2
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

7 Status of the document

7.1 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.

7.2 Version History

Contract Number	Report Number	Revision Notes
Q23/12-098	23/12-098 R035 V0R1	First version for internal review 11 July 2024
Q23/12-098	23/12-098 R035 V1R0	Revised after review, updated with new versions of gap analysis report and assessment and review comments, added recommendations report, 01 Aug 2024

Review: V0R1:

Stephan Aschenbrenner, *exida*, July 15, 2024

Flemming Svanholm Sørensen PR electronics, July 25, 2024

Status: Released Aug 01, 2024:

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

J. Hochhaus

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

Dipl.-Ing. (Univ.) Stephan Aschenbrenner

END OF DOCUMENT