



Product Service

CERTIFICATE

No. Z10 020132 0306 Rev. 01

Holder of Certificate: Pilz GmbH & Co. KG
Felix-Wankel-Str. 2
73760 Ostfildern
GERMANY

Certification Mark:



Product: Automation Equipment, Safety Related
Programable Safety Systems

Model(s): PSS 4000-G2-Rail

Parameters: Supply voltage: 24 VDC +25%/-30%
Operating temperature: -40°C ... +70°C
IP code: IP 20

The report and the user documentation in the currently valid revision are mandatory part of this certificate. The product complies with the below listed safety requirements only if the specifications documented in the currently valid revision of this report are met.

The certified components are listed in the report PO100914T.

Tested according to:

EN 50126-1:2017 (up to SIL 4)
EN 50129:2018/AC:2019 (up to SIL 4)
EN 50128:2011/A2:2020 (up to SIL 4)
EN 50716:2023 (up to SIL 4)
EN 50159:2010/A1:2020
EN 45545-2:2020 (up to HL3)

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. This certificate is valid until the listed date, unless it is cancelled earlier. All applicable requirements of the Testing, Certification, Validation and Verification Regulations of TÜV SÜD Group have to be complied. For details see: www.tuvsud.com/ps-cert

Test report no.: PO100722C

Valid until: 2030-12-04

Date, 2025-12-08

(Peter Weiß)



Add value.
Inspire trust.

Liste zur Verfolgung der Versionsfreigaben der sicherheitsgerichteten Baugruppen des **Automatisierungssystems:**

List for tracking the version releases of safety related modules
of the automation system:

PSS 4000-G2-Rail

Hersteller / Manufacturer:

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
D-73760 Ostfildern

Bericht-Nr. / Report No.: **PO100914T**

Revision: **1.9**

Datum / Date: **2026-07-03**

Zertifikat / Certificate: **Z10 020132 0306 Rev. 01**

Prüflabor für Sicherheitskomponenten / Testing Laboratory for Safety Components:

TÜV SÜD Rail GmbH - Rail Automation
Westendstraße 199
80686 München

Zertifizierstelle / Certification Body:

TÜV SÜD Product Service GmbH
Ridlerstraße 65
80339 München

Inhalt / content:

1	PAS 4000 (Pilz Automation Suite)	3
2	PSS 4000 - Firmware	4
3	PSS 4000 - Module	4
3.1	PSS 4000 - Kopfmodule - Head modules	4
3.2	PSS 4000 - E/A-Module - I/O Modules	5
3.3	PSS 4000 - Rückwirkungsfreie Module - Interference Free Modules	5
3.4	PSS 4000 - Fail-Safe-Funktionsbausteine / PSS 4000 - Failsafe function blocks	7
3.5	FFR values of example configurations	8
4	Normkonformität / Conformity with Standards	8

Änderung / Changes:

Kapitel / Chapter	Baugruppe / Device	Modifications
1	PAS 4000	Zusätzliche Hinweise Additional hints
3.3	PSS u2 ES 4AI I -R, PSS u2 ES 4AI U -R	Korrigierte Beschreibung Corrected description
allg. / general	-	Editorielle Anpassungen, Korrekturen Editorial alignments, corrections



Rail

1 PAS 4000 (Pilz Automation Suite)

PAS 4000 dient der Programmierung von Steuerungen der Systemfamilie PSS 4000 und des SafetyNET p. Die Verwendung der Softwarebausteine aus den PSS 4000 Software-Paketen wird von **PAS 4000** unterstützt.

PAS 4000 erfüllt die Anforderungen an ein als T3 klassifiziertes Offline-Support-Tool gemäß EN 50129 / EN 50716.

PAS 4000 is used to program control systems of the PSS 4000 system family and SafetyNET p. The use of the software blocks from the PSS 4000 software packages is supported by **PAS 4000**.

PAS 4000 meets the requirements of an offline-support-tool classified as T3 according to EN 50129 / EN 50716

Typ / Type ¹⁾ (Sach-Nr. / Order No.)	Version ³⁾	Interner Prüfbericht Internal Test Report	Beschreibung Description
PAS 4000	1.25.x	PO100722G rev 1.0	<u>Einschränkungen der Sicherheitsfunktion</u>
	1.26.x	PO102362T rev 1.0	Bei PAS-Version 1.25.0 bis 1.27.1 wird es in folgenden seltenen Fällen zur Einschränkung der Sicherheitsfunktion kommen: Bei Einsatz von IL, Ladder oder wenn bei Multi Programmierung die Datentypen FIXED oder LFIXED bei Vergleichsoperationen mit unterschiedlichen Datentypen verwendet werden.
	1.27.x	PO103485T rev 1.0	Daher sind PAS-Versionen 1.25.0 bis 1.27.1 nur dann verwendbar, wenn die zuvor benannte Bedingung nicht zutrifft.
	1.28.x	PO104674T rev 1.1	
	1.29.x	PO105970T rev 1.0	Bei PAS-Versionen 1.25.0 bis 1.29.0 wird es in folgenden seltenen Fällen zur Einschränkung der Sicherheitsfunktionen kommen: Bei Verwendung von nullspannungssicheren Variablen (VAR RETAIN PERSISTENT), die einen strukturierte Datentypen (STRUCT) verwenden. Weitere Details und Fehlerausschlüsse siehe Readme PAS4000 (Änderungen in Version 1.29.2 - 75790) <u>Restriction of the safety function</u> In PAS versions 1.25.0 to 1.27.1 , the safety function will be restricted in the following rare cases: When using IL, ladder, or multi-level programming and the FIXED or LFIXED data types are used in comparison operations with different data types. Therefore, PAS versions 1.25.0 to 1.27.1 can only be used if the previously mentioned condition does not apply. In PAS versions 1.25.0 to 1.29.0 , the safety function will be restricted in the following rare cases: when using non volatile variables (VAR RETAIN PERSISTENT), that use a structured data type (STRUCT). For further details and error exclusions, see the PAS4000 Readme (Changes in Version 1.29.2 - 75790)

Version: "x" = Jede Zahl zwischen 0...9 / Any number between 0...9



Rail

2 PSS 4000 - Firmware

Version ³⁾	Interner Prüfbericht Internal Test Report	Bemerkung Remark
1.25.x	PO100722G rev 1.0	-
1.26.x	PO102362T rev 1.0	-
1.27.x	PO103485T rev 1.0	-
1.28.x	PO104674T rev 1.1	-
1.29.x	PO105970T rev 1.0	-

Version: "x" = Jede Zahl zwischen 0...9 / Any number between 0...9

3 PSS 4000 - Module

3.1 PSS 4000 - Kopfmodule - Head modules

Typ / Type ¹⁾ (Sach-Nr. / Order No.)	Beschreibung Description	Version HW ⁴⁾	Version SW/FW ³⁾	Interner Prüfbericht Internal Test Report	Safety ²⁾ characteristic
PSS u2 P12 F/S -R (329220)	PLC-Kopfmodul für Failsafe und Standard mit SafetyNETp-Anschaltung PLC Head module for fail safe and standard with SafetyNETp interface	1.x	1.28.x 1.29.x	PO104674T rev 1.0 PO105970T rev 1.0	SIL 4
PSS u2 P42 F/S -R (329230)	PLC-Kopfmodul für Failsafe und Standard mit SafetyNETp-Anschaltung PLC Head module for fail safe and standard with SafetyNETp interface	1.x	1.25.x 1.26.x 1.27.x 1.28.x 1.29.x	PO100722G rev 1.0 PO102362T rev 1.0 PO103485T rev 1.0 PO104674T rev 1.1 PO105970T rev 1.0	SIL 4

Version: "x" = Jede Zahl zwischen 0...9 / Any number between 0...9

3.2 PSS 4000 - E/A-Module - I/O Modules

Typ / Type ¹⁾ (Sach-Nr. / Order No.)	Beschreibung Description	Version HW ⁴⁾	Version SW/FW ³⁾	Interner Prüfbericht Internal Test Report	Safety ²⁾ characteristic
PSS u2 EF 8DI -R (327101)	I/O-Modul, 8 digitale Eingänge, 2 Testtaktausgänge I/O Module, 8 digital Inputs, 2 test pulse outputs	1.x	1.2.x	PO100722G rev 1.0	SIL 4
PSS u2 EF 4DO 2A -R (327133)	I/O-Modul, 4 digitale Ausgänge, einpolig, 2A I/O Module, 4 digital Outputs, single pole 2A	1.x	1.2.x	PO100722G rev 1.0	SIL 4
PSS u2 EF 2DO R 8A -R (327150)	I/O-Modul, 2 Relaiskontakte, potentialfrei, 8A I/O Module, 2 Relay contacts, potential free, 8A	1.x	1.2.x	PO100722G rev 1.0	SIL 4

Version: "x" = Jede Zahl zwischen 0...9 / Any number between 0...9

3.3 PSS 4000 - Rückwirkungsfreie Module - Interference Free Modules

Typ / Type ¹⁾ (Sach-Nr. / Order No.)	Beschreibung / Description	Interner Prüfbericht Internal Test Report	Safety ²⁾ characteristic
PSS u2 B 4 -R (327810)	Modulträger mit 4 Steckplätzen Backplane 4 slots	PO100722G rev 1.0	Kein Sicherheitsbauteil No safety device
PSS u2 B 1 -R (327811)	Modulträger mit 1 Steckplatz Backplane 1 slot	PO106374T rev 1.0	Kein Sicherheitsbauteil No safety device
PSS u2 ES 4AI I -R (327520)	I/O-Modul, 4 analoge Differenzstromeingänge: -25,6 mA - +25,6 mA I/O-Electronic Module, 4 analogue differential current inputs: -25,6 mA - +25,6 mA	PO106374T rev 1.0	Kein Sicherheitsbauteil No safety device
PSS u2 ES 4AI U -R (327500)	I/O-Modul, 4 analoge Differenzspannungseingänge: -12,8 V - +12,8 V I/O-Electronic Module, 4 analogue differential voltage inputs: -12,8 V - +12,8 V	PO106374T rev 1.0	Kein Sicherheitsbauteil No safety device
PSS u2 ES 8DID -R (327311)	I/O-Modul, 8 digitale Eingänge, Diagnose, konfigurierbarer Filter, Impulserweiterung I/O-Electronic Module, 8 Digital Inputs, Diagnostic, Configurable Filter, Impulse Expansion	PO106374T rev 1.0	Kein Sicherheitsbauteil No safety device
PSS u2 ES 8DOD 0.5A -R (327401)	I/O-Modul, 8 digitale Ausgänge, 0,5 A, Diagnosefunktion, konfigurierbare Abschaltverzögerung I/O-Electronic Module, 8 Digital Outputs, 0.5 A, Diagnostic, Configurable Switch-Off Delay	PO106374T rev 1.0	Kein Sicherheitsbauteil No safety device
PSS u2 ES CAN -R (327710)	CANopen-Anschaltung CANopen interface	PO103485T rev 1.0	Kein Sicherheitsbauteil No safety device
PSS u2 ES PSP -R (327080)	Spannungsversorgungs-Modul (Periphery Supply 24V) Powersupply module (Periphery Supply)	PO100722G rev 1.0	Kein Sicherheitsbauteil No safety device



Rail

3.3 PSS 4000 - Rückwirkungsfreie Module - Interference Free Modules

Typ / Type ¹⁾ (Sach-Nr. / Order No.)	Beschreibung / Description	Interner Prüfbericht Internal Test Report	Safety ²⁾ characteristic
PSS u2 PS1 -R (329302)	Spannungsversorgungs-Modul (Module- und Periphery Supply 24V) Powersupply module (Module- and Periphery Supply 24V)	PO100722G rev 1.0	Kein Sicherheitsbauteil No safety device

Versionen der HW/SW/FW sind nicht ausschlaggebend für die Rückwirkungsfreiheit / Versions of HW/SW/FW are not relevant for freedom from interference



Rail

3.4 PSS 4000 - Fail-Safe-Funktionsbausteine / PSS 4000 - Failsafe function blocks

Name	Funktion/Function	Vers. ³⁾	CRC	Datum/Date (Last Modif.)	Interner Prüfbericht Internal Test Report	Safety ²⁾ characteristic
FS_EmergencyStop	Not-Halt-Überwachung Emergency stop monitoring	1.1.x	EA57	21.04.2010	PO100722G rev 1.0	SIL 4
FS_EmergencyStop_PLC	Not-Halt-Überwachung Emergency stop monitoring	1.0.x	E73B	01.04.2011	PO100722G rev 1.0	SIL 4
FS_FBL_Monitoring	Rückführkreisüberwachung Feedback loop monitoring	1.0.x	FF2A	03.09.2014	PO100722G rev 1.0	SIL 4
FS_FBL_Monitoring_PLC	Rückführkreisüberwachung (PLC) Feedback loop monitoring (PLC)	1.0.x	4DA2	02.09.2014	PO100722G rev 1.0	SIL 4
FS_SafetyGate	Überwachung Schutztürschalter mit bis zu 3 Kontakten Supervision of safety door switch up to 3 contacts	1.1.x	ADDB	21.04.2010	PO103485T rev 1.0	SIL 4
FS_SafetyGate_PLC	Überwachung Schutztürschalter mit bis zu 3 Kontakten Supervision of safety door switch up to 3 contacts	1.0.x	32EE	04.04.2011	PO103485T rev 1.0	SIL 4

Version: "x" = Jede Zahl zwischen 0...9 / Any number between 0...9

Anmerkung 1: Die Versionsnummer des Bausteins ist von der verwendeten PSS4000-Plattform und/oder PAS-Version abhängig. Die Angaben in den jeweils zugehörigen Benutzerinformationen der Bausteine sind zu beachten. Das System prüft die Kompatibilität der ausgewählten Bausteine zur verwendeten PSS4000-Plattform bzw. PAS-Version. Die Angabe des Sicherheitsmerkmals bezieht sich auf die interne Verarbeitung der sicherheitsgerichteten Signale in der PSS 4000.

Remark 1: The function block version number depends on the used PSS4000-platform and/or PAS version. The application rules in the manual of the respective function block have to be considered. The system checks the compatibility of the selected function blocks and the used PSS-4000-platform and/or PAS version. Indication of the safety feature refers to the internal processing of the safety-related signals in the PSS 4000.

3.5 FFR values of example configurations

Name	FFR [h^{-1}]	Interner Prüfbericht Internal Test Report
SIL 2 de-centralized PSS u2 EF 8DI -R/ PSS u2 EF 4DO 2A -R	1,63E ⁻⁰⁸	PO102362T rev 1.1
SIL 3 de-centralized PSS u2 EF 8DI -R / PSS u2 EF 2DO R 8A -R	6,08E ⁻¹⁰	PO102362T rev 1.1
SIL 4 de-centralized PSS u2 EF 8DI -R / PSS u2 EF 2DO R 8A -R	3,09E ⁻¹⁰	PO102362T rev 1.1
• Proof Test Intervall = none • communication related failure rates are included • Failure rates are based on SN29500 at an ambient temperature of 40°C		

4 Normkonformität / Conformity with Standards

Die gelisteten Baugruppen erfüllen die folgenden Sicherheits-, EMV-, Umwelt- und Brandschutz-Normen:
The listed components also fulfil the following standards of safety, EMC, environment and fire protection:

Norm Standard	Titel der Norm Title of standard
EN 50126-1:2017	Bahnanwendungen - Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) - Teil 1: Generischer RAMS-Prozess Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process
EN 50128:2011 + A2:2020	Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Software für Eisenbahnsteuerungs- und Überwachungssysteme Railway Applications - Communication, Signalling and Processing Systems - Software for Railway Control and Protection Systems
EN 50129:2018 + AC:2019	Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsbezogene elektronische Systeme für Signaltechnik Railway Applications - Communication, Signalling and Processing Systems - Safety Related Electronic Systems for Signalling
EN 50159:2010 + A1:2020	Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante Kommunikation in Übertragungssystemen Railway Applications - Communication, Signalling and Processing Systems - Safety-Related Communication in Transmission Systems
EN 50121-4:2016 + A1:2019	Bahnanwendungen - Elektromagnetische Verträglichkeit - Teil 4: Störaussendungen und Störfestigkeit von Signal- und Telekommunikationseinrichtungen Electromagnetic compatibility - Part 4: Emission and immunity of the signalling and telecommunications apparatus



Rail

4 Normkonformität / Conformity with Standards

Die gelisteten Baugruppen erfüllen die folgenden Sicherheits-, EMV-, Umwelt- und Brandschutz-Normen:
The listed components also fulfil the following standards of safety, EMC, environment and fire protection:

Norm Standard	Titel der Norm Title of standard
EN 50124-1:2017	Bahnanwendungen - Isolationskoordination - Teil 1: Grundlegende Anforderungen - Luft- und Kriechstrecken für alle elektrischen und elektronischen Betriebsmittel Insulation coordination-Part 1: Basic requirements - Clearances and creepage distances for all electrical and electronic equipment
EN 50125-3:2003 + Cor.:2010	Bahnanwendungen - Umweltbedingungen für Betriebsmittel - Teil 3: Umweltbedingungen für Signal- und Telekommunikationseinrichtungen Environmental conditions for equipment - Part 3: Equipment for signalling and telecommunications
EN 50657:2017	Railways Applications - Rolling stock applications - Software on Board Rolling Stock
EN 50716:2023	Railway Applications - Requirements for software development
EN 45545-2:2020	Bahnanwendungen - Brandschutz in Schienenfahrzeugen - Teil 2: Anforderungen an das Brandverhalten von Materialien und Komponenten Railway applications - Fire protection on railway vehicles - Part 2: Requirements for fire behavior of materials and components



Rail

Fußnote / Footnote

1) Typ / Type:

Sach.Nr.: Order No.:	Ergänzar durch Zeichen im Bereich AA...ZZ und 00...99 / Can be added by Character in range AA...ZZ and 00...99.
-T:	Coated Version mit erweitertem Temperaturbereich / Coated Version with extended temperature range

2) Sicherheitsmerkmal / Safety characteristics:

SIL:	Maximal erreichbarer Safety Integrity Level / Maximum achievable Safety Integrity Level Anwendungsbedingungen und Architekturvorgaben siehe Sicherheitshandbuch „Sicherheitsarchitekturen für Bahnanwendungen“ / Application conditions and architectural constraints see safety manual „Safety Architectures for Railway Applications“
-------------	--

3) Version SW:

Last digits „xx“ or „x“ relate to non-safety SW modifications supervised by the Functional Safety Management of Pilz GmbH & Co KG and the related activities of TÜV SÜD Rail GmbH based on its test and certification regulation.

4) Version HW:

Last digits „x“ relate to non-safety HW modifications supervised by the Functional Safety Management of Pilz GmbH & Co KG and the related activities of TÜV SÜD Rail GmbH based on its test and certification regulation.

	Freigabe Prüflabor für Sicherheitskomponenten: Release by Testing Laboratory for Safety Components:	Freigabe Zertifizierstelle: Release by Certification Body:
Datum: Date:		
Unterschrift: Signature:	 Julian Wolf 2026.07.03 10:46:36 +02'00'	 Christian Dirmeier 2026.07.06 17:38:08 +02'00'



Add value.
Inspire trust.

Report

on the

Certificate

Z10 020132 0306 Rev. 01

of the

Generic Logic Device PSS 4000-G2-Rail

Applicant

Pilz GmbH & Co KG
Felix-Wankel-Straße 2
73760 Ostfildern
Germany

Report No.: PO100722C

Version 1.6 of 2025-12-03

Certification Body

TÜV SÜD Product Service GmbH
Ridlerstraße 65
80686 München

(Page 1 of 9)



Table of Contents

page

1	Target of Evaluation (ToE)	4
2	Scope of Testing	4
2.1	Test Specimen	4
2.2	Nomenclature and Identification of PSS 4000-G2-Rail	4
3	Certification Requirements	5
3.1	Certification Documentation	6
4	Standards and Guidelines	7
4.1	Safety Information in the Product Documentation (safety manual, operating instructions, labelling)	7
4.2	Quality Management System	7
5	Safety Parameters	7
5.1	Functional Safety	7
5.2	Development of the application program	8
6	Recommendations	8
7	Conditions of Use	8
8	Certificate Number	9

List of Tables

page

Table 1:	Modification history	3
Table 2:	Technical Report	6
Table 3:	Reports on Modifications	6
Table 4:	Safety information standards	7
Table 5:	Quality Management System	7

Modification History

Rev.	Status	Date	Author	Modification / Description
1.0	replaced	2023-05-16	Guido Neumann	-
1.1	replaced	2023-05-22	Guido Neumann	Enhanced product name
1.2	replaced	2023-08-17	Volker Sperling	Update to 2.2
1.3	replaced	2024-04-03	Guido Neumann	Update to release 26 (PO102362T) Transfer of standards to "List for tracking the version releases of safety related modules" PO100914T

Rev.	Status	Date	Author	Modification / Description
1.4	replaced	2024-09-12	Volker Sperling	Update to release 27 (PO103485T) Formal adaptations to template rev.20 Reference in Rec 1 corrected
1.5	replaced	2025-06-03	Volker Sperling	Update to release 28 (PO104674T) Formal adaptations to template rev.23
1.6	active	2025-12-03	Volker Sperling	Update to release 29 (PO105790T), inclusion of EN 50716 into certification scope, clarification of GPSC in 5.1 and 7. Formal adaptations to template rev.26

Table 1: Modification history

1 Target of Evaluation (ToE)

In 2023 Pilz GmbH & Co KG requested TÜV SÜD Rail GmbH to test and certify the PSS 4000-G2-Rail according to the standard listed in clause 4 of this report. The project number related to this Technical Report is 717529401.

In 2024-06 Pilz GmbH & Co KG requested TÜV SÜD Rail GmbH to test and certify the updated release of PSS 4000-G2-Rail according to the standard listed in clause 4 of this report. The project number related to this Technical Report is 717530440.

The resulting version of this Report on the Certificate is v1.4.

In 2025-03 Pilz GmbH & Co KG requested TÜV SÜD Rail GmbH to test and certify the updated release of PSS 4000-G2-Rail according to the standard listed in clause 4 of this report. The related project number is 71752235.

The resulting version of this Report on the Certificate is v1.5.

In 2025-10 Pilz GmbH & Co KG requested TÜV SÜD Rail GmbH to test and certify the updated release of PSS 4000-G2-Rail according to the standard listed in clause 4 of this report. This includes update of the certificate. The related project number is 717533435.

The resulting version of this Report on the Certificate is v1.6.

The ToE is a safety programmable logic controller used in safety related railway applications. The PSS 4000-G2-Rail is a Generic Logic Device approved for

- Up to SIL 4 according to EN 5012x
- Up to HL 3 according to EN 45545-2
- RAM-Aspects were excluded and are not subject of the assessment report.

2 Scope of Testing

2.1 Test Specimen

The PSS 4000-G2-Rail is a Generic Logic Device used in safety related railway applications.

The safety function of the PSS 4000-G2-Rail is defined by the application.

The mission of the PSS 4000-G2-Rail is to read inputs, calculate a user programmed logic and set outputs accordingly.

The safe state is defined as “de-energized” (logical “0”) for input and output.

2.2 Nomenclature and Identification of PSS 4000-G2-Rail

The PSS 4000-G2-Rail tested is identified by hardware and software as defined in **PO100914T** (List for tracking the version releases of safety related modules of the automation system PSS 4000-G2-Rail).

3 Certification Requirements

The certification of the PSS 4000-G2-Rail is according to the regulations and standards listed in clause 4 of this document. This certifies the successful completion of the following test segments.

- I. Functional Safety including
 - Functional safety management (FSM) and safety lifecycle
 - Applied safety development process
 - Analysis of the product structure / architecture (Block-Diagram-FMEA)
 - Analysis of the hardware (FMEDA on component or block level, quantitative analysis)
 - Analysis of the software
 - Verification and validation procedures/activities
 - Fault simulations and software tests
 - Approval of fault avoidance measures
 - Functional tests
- II. Electrical Safety
- III. Susceptibility to environmental errors including
 - Climate and temperature
 - IP degree of protection
 - Mechanical effects
- IV. Electromagnetic compatibility (EMC)
 - Immunity
 - Emission
- V. Safety information in the product documentation (safety manual, user manual, installation and operating instructions)
- VI. Product-Related Quality Assurance in Manufacture and Product Development

3.1 Certification Documentation

The detailed technical evaluation is documented in the most recent version of the Technical Report:

Document No.	Description	Project No.
PO100722G	Assessment Report	717527108
PO100914T	List for tracking the version releases of safety related modules of the automation system PSS 4000-R generation 2	717529401
PO100906G	Fire Safety Assessment according to EN 45545-2 automation system PSS4000R G2	717527108
Safety related requirements, conditions and restrictions can be found in the following user documentation		
[Sys07]	Safety architectures railway application - Operational Manual 1006614-DE-02	717529401

Table 2: Technical Report

Modifications have been evaluated and tested and are documented in the most recent version of the Technical Report of Modifications (TRM):

Document No.	Modification Description	Project No.
Report on the Certificate v1.4		
PO103485T	Update of to release 27	717530440
Safety related requirements, conditions and restrictions can be found in the following user documentation		
[Sys07]	Safety architectures railway application - Operational Manual 1006614-DE-03	717530440
Report on the Certificate v1.5		
PO104674T	Update to release 28	717532235
Safety related requirements, conditions and restrictions can be found in the following user documentation		
[Sys07]	Safety architectures railway application - Safety Manual 1006614-DE-04	717532235
Report on the Certificate v1.6		
PO104674T	Update to release 28, aligned accreditation scope	717532235
PO105970T	Update to release 29	717533435
Safety related requirements, conditions and restrictions can be found in the following user documentation		
[Sys07]	Safety architectures railway application - Safety Manual 1006614-DE-05	717533435

Table 3: Reports on Modifications

Based on the specified purpose of use of the PSS 4000-G2-Rail in safety critical process applications, the certification is based on the set of standards listed in clause 4 of this document. The issuance of the certificate states compliance with these references unless specifically noted otherwise.

4 Standards and Guidelines

The regulations and guidelines which form the basis of the type testing are listed in the “List for tracking the version releases of safety related modules of the automation system PSS 4000-R generation 2” PO100914T.

4.1 Safety Information in the Product Documentation (safety manual, operating instructions, labelling)

No.	Reference	Description
/N1/	EN 50129:2018 / AC:2019	Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling

Table 4: Safety information standards

4.2 Quality Management System

No.	Reference	Description
[M1]	QMS	Quality Management System TÜV SÜD Rail GmbH

Table 5: Quality Management System

5 Safety Parameters

5.1 Functional Safety

Pilz GmbH & Co KG provided user documents including Safety-Related Application Conditions (SRAC) and covering the required contents of a generic product safety case (GPSC) in accordance with EN 50129.

The tests performed and quality assurance measures implemented by the Pilz GmbH & Co KG have shown that the PSS 4000-G2-Rail complies with the safety parameters specified in clause 4 subject to the conditions defined in clause 6 and is suitable for safety-related use in applications up to

- SIL 4 in accordance with EN 50126-1 / EN 50129 / EN 50128 / EN 50159.

A separate manual is available to support application developers in the area of IT-/ Cyber Security.

5.2 Development of the application program

Application programs have to be developed according to the specifications in the safety manual using the tool PAS.

The development environment and the PSS 4000-G2-Rail devices provide basic mechanisms for protection against unauthorized access.

6 Recommendations

- Rec 1. Safety Qualification Tests according to EN 50129:2018 Chapter 5.3.12 (TSR Section 6) are not part of this assessment report. A safety qualification with independent safety supervision units may be conducted based on the existing safety acceptance tests documented hereby. It has to be assured that the functionality of the PSS 4000-G2-Rail can be monitored and logged to evaluate the target achievement.
- Rec 2. For every first-time acceptance of a generic and/or specific application the completeness of the application test must be proven by the application manufacturer.
For modifications the necessary verification and validation testing must be determined based on a modification impact analysis.
- Rec 3. In case a generic or specific application needs details on the used standards beyond the statements in manuals and SRACs Pilz GmbH & Co KG should provide an export of the related chapters of the document [RailReq].

7 Conditions of Use

- CoU 1. The guidelines and requirements specified by the Safety-Related Application Conditions (SRAC) shall be followed.
- CoU 2. Only modules certified for safety-related operation shall be used for safety-critical functions.
- CoU 3. The application manufacturer shall consider the railway manuals which include the safety related application conditions at their latest valid release.



8 Certificate Number

This report specifies technical details and implementation conditions required for the application of PSS 4000-G2-Rail to the certificate:

Z10 020132 0306 Rev. 01

Technical Certifier

A handwritten signature in blue ink, appearing to read 'Peter G. Weiß'.

Peter Weiß
2025.12.08
10:01:24 +01'00'

Assessment Report

for the testing of the

Generic Product - Safety PLC PSS 4000-G2-Rail

Applicant

Pilz GmbH & Co KG

Felix-Wankel-Straße 2
73760 Ostfildern
Germany

Report No.: PO100722G

Version 1.1 of 2023-08-17

Testing Laboratory for Safety Components

TÜV SÜD Rail GmbH

Barthstraße 16
D-80339 München

(Page 1 of 55)

This report may be represented only in complete wording. The use for promotion needs written permission. This report contains the result of a unique investigation of the product being tested and places no generally valid judgment about characteristics out of the running fabrication. Official translations of this technical report are to be authorized by the test and certification body.

Template: TR_RA_F_04.41_v2

Table of Contents	page
1 Target of Evaluation (ToE)	9
1.1 Client and Purpose	9
1.2 Evaluation and constraints	9
2 Scope of Testing	10
2.1 Test Specimen	10
2.1.1 Safety Function	10
2.1.2 Safe State	10
2.1.3 System Architecture	10
2.2 Nomenclature and Identification of PSS 4000-G2-Rail	14
2.3 Assessment	16
2.3.1 Assessment Method.....	16
2.3.2 Assessors.....	17
2.3.3 Test Areas.....	17
3 Standards and Guidelines	18
3.1 Guidelines.....	18
3.2 Product Standards	18
3.3 Functional Safety Standards	18
3.4 Application Standards	19
3.5 Susceptibility to Environmental Errors	19
3.5.1 Electrical Safety	19
3.5.2 Environmental Conditions	20
3.5.3 Mechanical Compatibility and IP Code testing	20
3.5.4 Electromagnetic Compatibility	20
3.6 Safety Information in the Product Documentation (safety manual, operating instructions, labelling)	20
3.7 Quality Management System	21
4 Documentation and Results	22

4.1	General	22
4.2	General information related to system safety and the safety goal	22
4.2.1	Requirements	22
4.2.2	Examination Result	22
4.2.3	Assessor evaluation result	23
4.3	Hazard Control.....	24
4.3.1	Requirements	24
4.3.2	Examination Result	24
4.3.3	Assessor evaluation result	24
4.4	General Information related to the Safety Case	25
4.4.1	Requirements	25
4.4.2	Examination Result	25
4.4.3	Assessor evaluation result	27
4.5	Quantitative Safety Requirements / Probabilistic Data.....	27
4.5.1	Requirements	27
4.5.2	Examination Result	27
4.5.3	Assessor evaluation result	29
4.6	Quality Management.....	29
4.6.1	Requirements	29
4.6.2	Examination Result	30
4.6.3	Assessor evaluation result	30
4.7	Safety Management.....	31
4.7.1	Requirements	31
4.7.2	Examination Result	31
4.7.3	Assessor evaluation result	31
4.8	Technical Safety – Introduction of Design and Safety Principles	32
4.8.1	Requirements	32
4.8.2	Examination Result	32

4.8.3	Assessor evaluation result	33
4.9	Safety Related Communication.....	34
4.9.1	Requirements	34
4.9.2	Examination Result	34
4.9.3	Assessor evaluation result	35
4.10	Technical Safety - Assurance of correct functional operation	36
4.10.1	Requirements	36
4.10.2	Examination Result	36
4.10.3	Assessor evaluation result	39
4.11	Technical Safety - Effects of Faults.....	39
4.11.1	Requirements	39
4.11.2	Examination Result	39
4.11.3	Assessor evaluation result	43
4.12	Technical Safety – Operation under external influences.....	44
4.12.1	Requirements	44
4.12.2	Examination Result	44
4.12.3	Assessor evaluation result	45
4.13	Technical Safety – Safety Relevant Application Conditions.....	46
4.13.1	Requirements	46
4.13.2	Examination Result	46
4.13.3	Assessor evaluation result	47
4.14	Technical Safety – Safety Qualification Testing.....	47
4.14.1	Requirements	47
4.14.2	Examination Result	47
4.14.3	Assessor evaluation result	47
4.15	Dependencies between Safety Cases	48
4.15.1	Requirements	48
4.15.2	Examination Result	48

4.15.3	Assessor evaluation result	48
4.16	Assurance of correct software functionality	48
4.16.1	Requirements	48
4.16.2	Examination Result	49
4.16.3	Assessor evaluation result	50
4.17	Modifications	51
4.17.1	Requirements	51
4.17.2	Examination Result	51
4.17.3	Assessor evaluation result	52
5	Testing Body	53
6	Results and Recommendations	54
6.1	Result	54
6.2	Recommendations	54
6.3	Conditions of Use	54
7	Summary	55

List of Tables	page
Table 1: Modification history	7
Table 2: Abbreviations	8
Table 3: Identification of PSS 4000-G2-Rail safety modules	15
Table 4: Identification of PSS 4000-G2-Rail non-safety modules	15
Table 5: Identification of PSS 4000-G2-Rail Functional Blocks (safety)	15
Table 6 Assessors	17
Table 7: Guidelines and directives	18
Table 8: Product standards	18
Table 9: Functional safety standards	19
Table 10: Application standards	19

Table 11:	Electrical Safety standards	19
Table 12:	Environmental condition standards.....	20
Table 13:	IP Code testing standards	20
Table 14:	Electromagnetic compatibility standards	20
Table 15:	Safety information standards	20
Table 16:	Quality Management System.....	21
Table 17:	System Safety and Safety Goal data	23
Table 18:	System Safety and Safety Goal results	23
Table 19:	Hazard Control data	24
Table 20:	Hazard Control results	24
Table 21:	Safety Case data	25
Table 22:	Safety Case results	27
Table 23:	Probabilistic data	28
Table 24:	Safety Characteristic Data	29
Table 25:	Probabilistic data result	29
Table 26:	Quality Management data	30
Table 27:	Quality Management result.....	30
Table 28:	FSM documentation data	31
Table 29:	FSM results	31
Table 30:	Design and Safety Principles data	33
Table 31:	Design and Safety Principles result	33
Table 32:	Safety related communication documentation data	35
Table 33:	Safety related communication results	35
Table 34:	Functional and Technical Safety - Function.....	38
Table 35:	Functional and Technical Safety - Function result.....	39
Table 36:	Functional and Technical Safety - Effects of Faults data	42
Table 37:	Functional and Technical Safety - Effect of Faults result.....	43
Table 38:	Operation under external influences	45

Table 39:	Operation under external influences result	45
Table 40:	SRACs / Manual	46
Table 41:	SRACs / Manual result	47
Table 42:	Software Data	50
Table 43:	Software result	50
Table 44:	Modification procedure documents	52
Table 45:	Modification results	52
Table 48:	Test Reports issued from other laboratories	53

List of Figures

page

Figure 1:	Overview of PSS 4000-G2-Rail System – example setup	11
Figure 2:	Overview of PSS 4000-G2-Rail SIL4 Architecture – composite fail-safe 12	
Figure 3:	Overview of PSS 4000-G2-Rail SIL3 Architecture – composite fail-safe 12	
Figure 4:	Overview of PSS 4000-G2-Rail SIL1/2 Architecture – reactive fail-safe 13	
Figure 5:	Overview of PSS 4000-G2-Rail SW-Architecture	14
Figure 6	PSS 4000R communication structure	34

Modification History

Rev.	Status	Date	Author	Modification / Description
1.0	replaced	2023-05-16	Guido Neumann	-
1.1	active	2023-08-17	Guido Neumann	Enhanced product name Update for corrected SINA1 (and DOKREF) Formal corrections on references.

Table 1: Modification history

List of Abbreviations

Abbreviation	Description
COTS	commercial off-the-shelf
DC	Diagnostic Coverage
E/E/PE	electrical/electronic/programmable electronic systems
(T)FFR	(Tolerable) Functional Failure Rate
FMEDA	Failure Mode, Effects and Diagnosis Analysis
FSM	Functional Safety Management
FW	Firmware
(T)HR	(Tolerable) Hazard Rate
HW	Hardware
OS	Operating System
PFD	Probability of Dangerous Failure on Demand
PFH	Average Frequency of Dangerous Failure (h^{-1})
PLC	Programmable Logic Controller
QMS	Quality Management System
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
SRAC	Safety-Related Application Condition
SW	Software
ToE	Target of Evaluation

Table 2: Abbreviations

1 Target of Evaluation (ToE)

1.1 Client and Purpose

In February 2023 Pilz GmbH & Co KG requested TÜV SÜD Rail GmbH to test and certify the PSS 4000-G2-Rail according to the standard listed in clause 3 of this report.

The project number related to this Technical Report is 717527108.

This assessment report can be used for the provision of independent assessment results towards railway authorities.

1.2 Evaluation and constraints

The assessor evaluated the conformity of the product identified in chapter 2.2 with respect to the standards and regulations given in chapter 3 and the given Safety Integrity Level 4 according to EN 50126, EN 50129, EN 50128 and EN 50657.

RAM-Aspects were excluded and are not subject of the assessment report.

The product assessment was performed between February 2023 and 2023-08-17.

The assessor considered:

- PSS 4000-G2-Rail is based on PSS 4000-r first generation, assessment report PO84128G revision 1.15 dated March 16., 2021 and TÜV SÜD certificate Z10 020132 0289 Rev. 01
- As well as PSS 4000-R generation 1 the PSS 4000-G2-Rail makes use of pre-certified safety PLC components based on IEC 61508, ISO 13849-1 and other safety standards of automation industry areas.
- PSS 4000-G2-Rail head module has been modified to achieve a channel separation, thus leading to an optimized Common Cause analysis result and a simpler to-be-used SIL 4 architecture.

2 Scope of Testing

2.1 Test Specimen

2.1.1 Safety Function

The PSS 4000-G2-Rail is a Safety PLC used in safety related railway applications.

The safety function of the Generic Product is defined by the application.

The mission of the PSS 4000-G2-Rail is to read inputs, calculate a user programmed logic and set outputs accordingly.

2.1.2 Safe State

The safe state is defined as “de-energized” (logical “0”) for input and output.

2.1.3 System Architecture

The Safety PLC executes the specific application defined and programmed by the user. It evaluates the connected inputs, executes the application logic and sets the corresponding output values.

The system operates in a cyclic way. One cycle is defined as “read inputs – execute logic – set outputs”. The cycle time depends on configuration of the cycle times of the PLC. It is limited by required execution time of application program, module bus setup and network load.

The overview of the PSS 4000-G2-Rail series is depicted in the figures below.

It can be seen in the figures that the product consists of multiple separate modules that can be combined individually to realize a generic or specific application:

- head module – performed the execution of the user programmed logic
- input modules – read the input data and provide the result to the head module
- output module – receives the output status from the head module and sets the output accordingly.
- power supply

The devices are connected by a serial data bus in the backplane (local safety architecture) or an ethernet based network (de-centralized architecture). All safety connections are protected by safety layers.

Different safety architectures for combining modules can be used to achieve different safety levels and/or Functional Failure Rates.

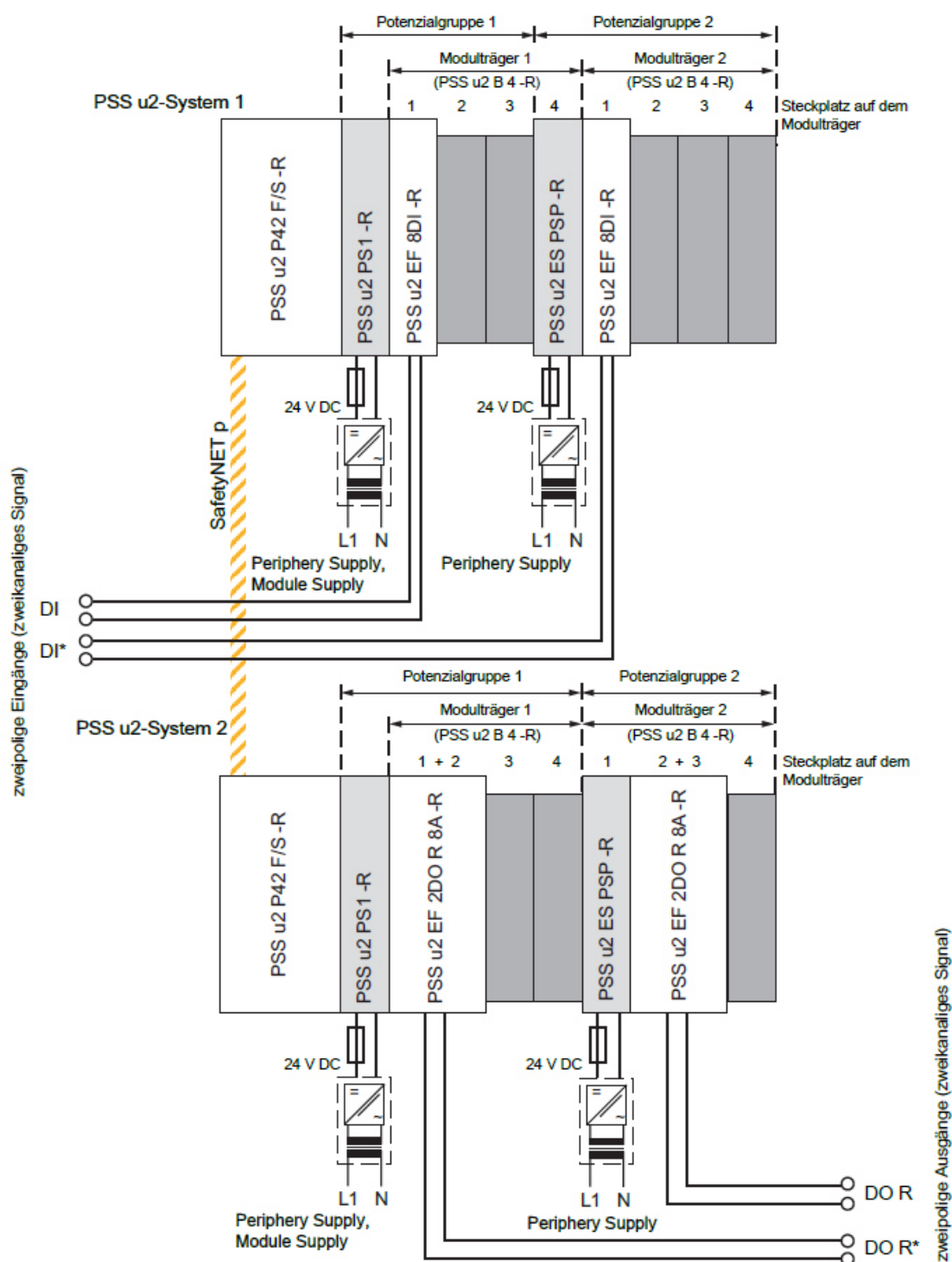


Figure 1: Overview of PSS 4000-G2-Rail System – example setup

The following basic HW architecture principles are used:

- Head module: composite fail safe (dual channel structure with strict channel separation, cross-comparison and diagnosis)
- I/O-module: reactive fail safe (dual channel structure with cross-comparison and diagnosis)
- Architectural patterns: I/O-modules can be combined to achieve either a composite fail-safe or a reactive fail-safe system architecture on application level

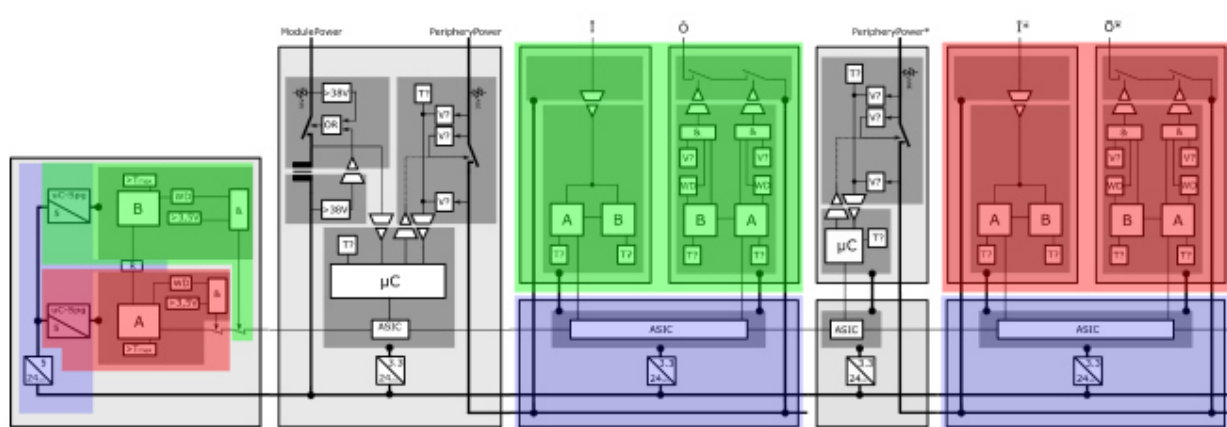


Figure 2: Overview of PSS 4000-G2-Rail SIL4 Architecture – composite fail-safe

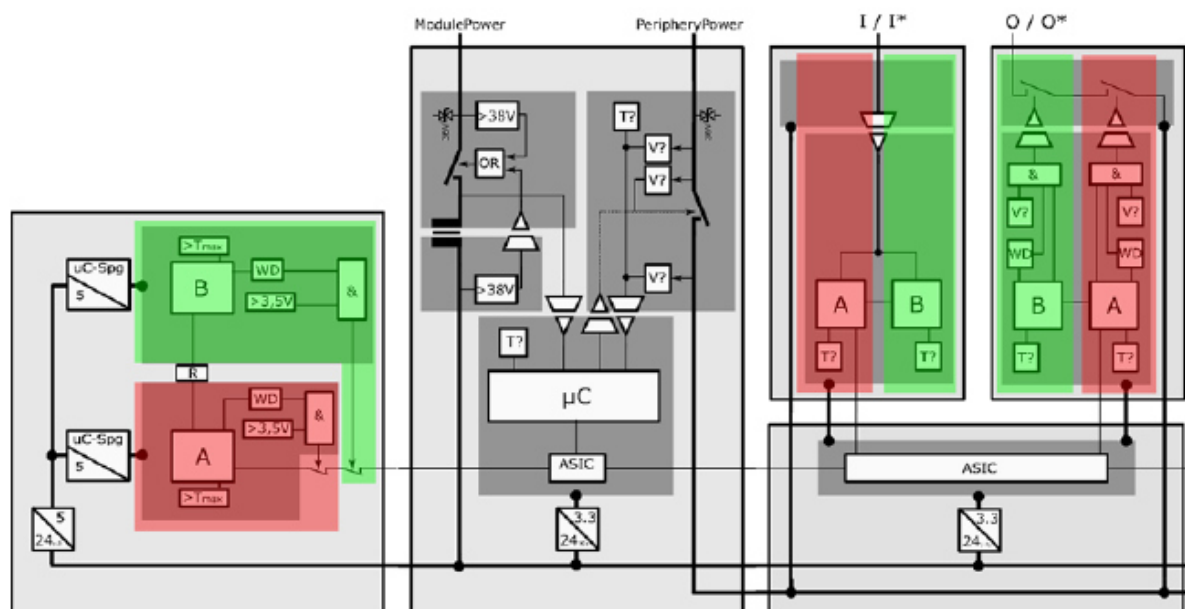


Figure 3: Overview of PSS 4000-G2-Rail SIL3 Architecture – composite fail-safe

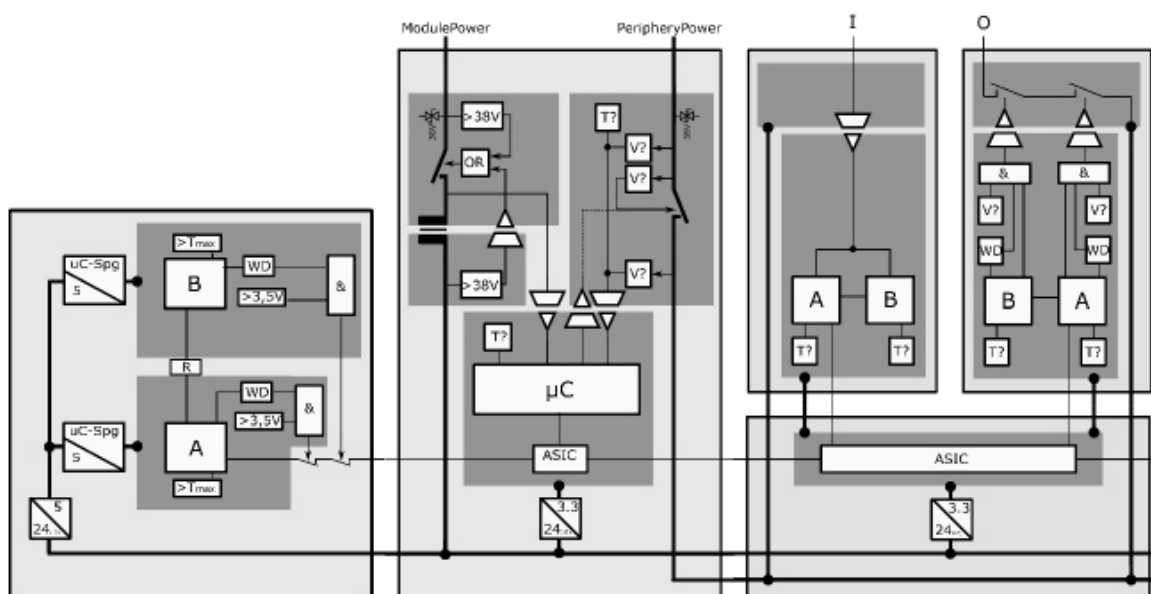


Figure 4: Overview of PSS 4000-G2-Rail SIL 1/2 Architecture – reactive fail-safe¹

The following basic SW architecture principles are used:

- System Platform incl. firmware of head modules
 - Runtime
 - Engineering Software PAS4000 (T3 classified) programming and configuration Tool, diagnosis support
 - Safety Communication Protocols (“SafetyNET p” and “Module bus PSS u2”)
- Firmware of the I/O modules
 - Firmware on power supplies
 - Firmware on Input modules
 - Firmware of Output modules
- Libraries for Functional Block on application level

¹ Head module remains composite fail-safe

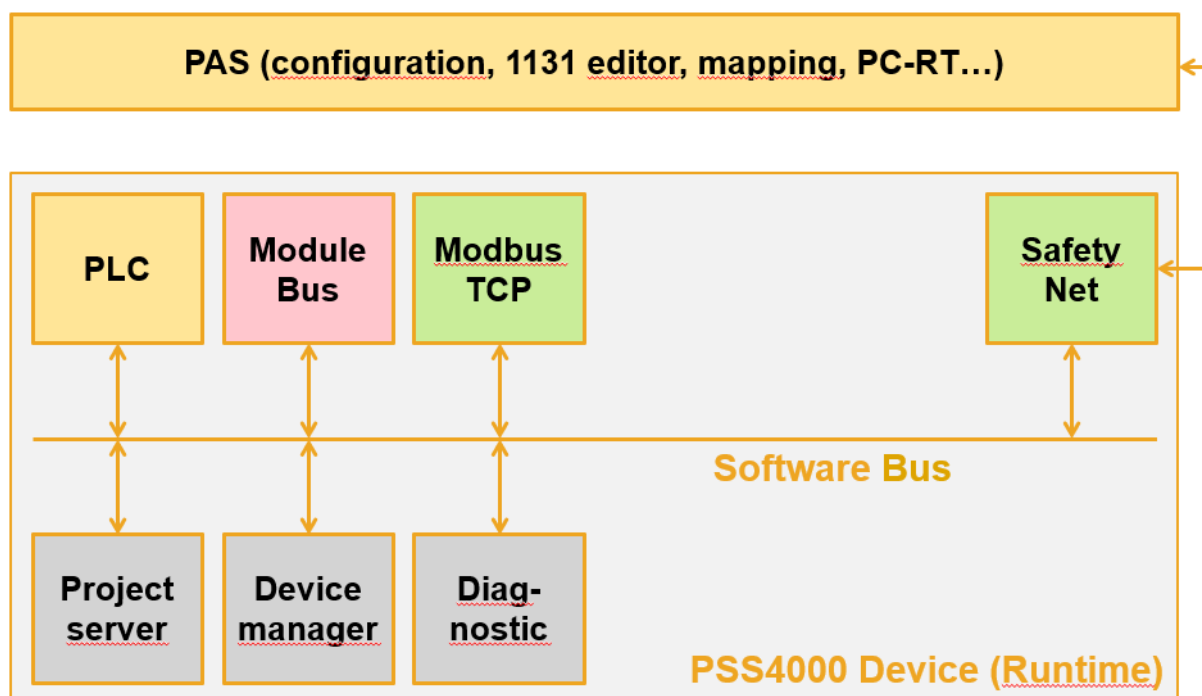


Figure 5: Overview of PSS 4000-G2-Rail SW-Architecture

2.2 Nomenclature and Identification of PSS 4000-G2-Rail

This assessment report covers the product identified by hardware and software version as follows:

Name	ID	SW	HW	Remarks
PAS4000	-	01.25.xx ²	n/a	Programming tool
PSS u2 P42 F/S -R	329230	01.25.xx ²	01.x ³	Head module
PSS u2 EF 8DI -R	327101	01.02.x ²	01.x ³	Digital input module
PSS u2 EF 4DO 2A -R	327133	01.02.x ²	01.x ³	Digital output module

² Last digits „xx“ relate to non-safety SW modifications supervised by the Functional Safety Management of Pilz GmbH & Co KG and the related activities of TÜV SÜD Rail GmbH based on its test and certification regulation.

³ Last digit „x“ relates to non-safety HW modifications supervised by the Functional Safety Management of Pilz GmbH & Co KG and the related activities of TÜV SÜD Rail GmbH based on its test and certification regulation.

Name	ID	SW	HW	Remarks
PSS u2 EF 2DO R 8A -R	327150	01.02.x ²	01.x ³	Relay output module
Runtime Firmware (head module)	-	R25.0s.RTSB63.170047	n/a	SW major Release 1.25.0

Table 3: Identification of PSS 4000-G2-Rail safety modules

Interference free non-safety modules:

Name	ID	SW	HW	Remarks
PSS u2 PS1 -R	329302	01.03.x ²	01.x ³	-
PSS u2 ES PSP -R	327080	01.01.x ²	01.x ³	-
PSS u2 B 4 -R	327810	n/a	01.x ³	-

Table 4: Identification of PSS 4000-G2-Rail non-safety modules

Name	SW	CRC	Remarks
FS_EmergencyStop	V 1.1.x	EA57	Function block emergency stop
FS_EmergencyStop_PLC	V 1.0.x	E73B	
FS_FBL_Monitoring	V 1.0.x	FF2A	Function block electromechanical contactors
FS_FBL_Monitoring_PLC	V 1.0.x	4DA2	

Table 5: Identification of PSS 4000-G2-Rail Functional Blocks (safety)

2.3 Assessment

2.3.1 Assessment Method

The assessment was conducted using the following methods:

Analysis of the documentation, evaluation of completeness, comprehensibility, and traceability

- Clarifications of findings together with Pilz GmbH & Co KG
- Review of the methods and results to calculate the Functional Failure Rate

The completeness of the results is documented by the list of open points (LOP), review reports and checklists.

PSS 4000R gen 1 is already assessed by TÜV SÜD Rail GmbH ([R4]). PSS 4000-G2-Rail partly re-used unchanged artefacts from generation 1. Pilz GmbH & Co KG provided a Safety Plan [SPLAN] (/D1/) detailing re-used, modified or newly added artefacts including resulting development activities. TÜV SÜD Rail GmbH reviewed and accepted the Safety Plan and assessed the projects according to the derived project structure:

- PSS 4000-G2-Rail umbrella project incl. new HW and SW for P42-module
project number concept phase: 717522574
project number detailed phase: 717527108
This comprises or refers to
 - Referred PSS 4000-R generation 1 project
TÜV SÜD Rail GmbH certificate Z10 020132 0289 Rev. 01.pdf
 - Updated Firmware and Tool
project number: 717527554
 - Updated I/O modules
project number: 717524894
 - Modulbus 2
project number: 717525487

2.3.2 Assessors

The following persons contributed to the assessment result:

Name	Tasks	Company
Guido Neumann	Assessor	TÜV SÜD Rail GmbH
Volker Sperling	Reviewer SW and Safety Case	TÜV SÜD Rail GmbH
Khaled Essahli	Reviewer HW	TÜV SÜD Rail GmbH
Julian Wolf	Review SW / system level I/O modules	TÜV SÜD Rail GmbH
Jiayi Dong	Reviewer Safety Plan and Safety Case	TÜV SÜD Rail GmbH
Walter Schlögl	Review Modulbus 2	TÜV SÜD Rail GmbH

Table 6 Assessors

2.3.3 Test Areas

Base of the assessment procedure is the safety case in accordance with EN 50129 as provided by the manufacturer.

The PSS 4000-G2-Rail was examined with respect to the following testing operations:

- I. Functional Safety including
 - Functional safety management (FSM) and safety lifecycle
 - Applied safety development process
 - Analysis of the product structure / architecture (Block-Diagram-FMEA)
 - Analysis of the hardware (FMEDA on component or block level, quantitative analysis)
 - Analysis of the software
 - Verification and validation procedures/activities
 - Fault simulations and software tests
 - Approval of fault avoidance measures
 - Functional tests
- II. Electrical Safety
- III. Susceptibility to environmental errors including
 - Climate and temperature

- IP degree of protection
 - Mechanical effects
- IV. Electromagnetic compatibility (EMC)
- Immunity
 - Emission
- V. Safety information in the product documentation (safety manual, user manual, SRACs).
- VI. Product-Related Quality Assurance in Manufacture and Product Development

3 Standards and Guidelines

The regulations and guidelines which form the basis of the type testing are listed below.

3.1 Guidelines

No.	Reference	Description
/N1/	-	-

Table 7: Guidelines and directives

3.2 Product Standards

No.	Reference	Description
/N2/	-	-

Table 8: Product standards

3.3 Functional Safety Standards

No.	Reference	Description
/N3/	EN 50126-1:2017 (SIL 4)	Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process
/N4/	EN 50129:2018 / AC:2019	Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling

No.	Reference	Description
/N5/	EN 50128:2011/ A2:2020	Railway applications -- Communication, signalling and processing systems -- Software for railway control and protection systems
/N6/	EN 50657:2017	Railways Applications - Rolling stock applications - Software on Board Rolling Stock
/N7/	EN 50159:2010 / A1:2020	Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

Table 9: Functional safety standards

3.4 Application Standards

Because of the expected applications of the system the following additional standards and regulations were considered. These standards require a final approval of the specific application. The assessment of the PSS 4000-G2-Rail has been performed against the parts of the standard applicable.

No.	Reference	Description
Railway		
/N8/	EN 45545-2:2020	Railway applications – Fire protection on railway vehicles – Part 2: Requirements for fire behavior of materials and components

Table 10: Application standards

3.5 Susceptibility to Environmental Errors

Remark: The following standards were approved by other testing services.

3.5.1 Electrical Safety

No.	Reference	Description
/N9/	EN 50124-1:2017	Railway applications – Insulation coordination Part 1: Basic requirements – Clearances and creepage distances for all electrical and electronic equipment

Table 11: Electrical Safety standards

3.5.2 Environmental Conditions

No.	Reference	Description
/N10/	EN 50125-3:2003/AC 2010	applications – Environmental conditions for equipment – Part 3: Equipment for signalling and telecommunications

Table 12: Environmental condition standards

3.5.3 Mechanical Compatibility and IP Code testing

No.	Reference	Description
/N11/	IEC 60529:1989/ A2:2013/ COR2:2015	Degrees of protection provided by enclosures (IP Code)

Table 13: IP Code testing standards

3.5.4 Electromagnetic Compatibility

No.	Reference	Description
/N12/	EN 50121-4:2016 / A1:2019	Railway applications – Electromagnetic compatibility – Part 4: Emission and immunity of the signalling and telecommunications apparatus

Table 14: Electromagnetic compatibility standards

3.6 Safety Information in the Product Documentation (safety manual, operating instructions, labelling)

No.	Reference	Description
/N13/	EN 50129:2018 / AC:2019	Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling

Table 15: Safety information standards

3.7 Quality Management System

No.	Reference	Description
[M1]	QMS	Quality Management System TÜV SÜD Rail GmbH
	TR_RA_P_04.50	Test Program Functional Safety
	TR_RA_P_04.51	Definition Scope of testing
	TR_RA_P_04.07	Product Modification
	TR_RA_P_04.52	Concept Phase & Safety Lifecycle
	TR_RA_P_04.53	Detail Phase Hardware
	TR_RA_P_04.54	Detail Phase Software
	TR_RA_P_04.55	Safety Manual
	TR_RA_P_04.56	Result of Testing
[M3]	D-PL-11190-08-00	DAkkS accreditation according to DIN EN ISO 17025:2018 / EN ISO/IEC 17025:2017

Table 16: Quality Management System

4 Documentation and Results

4.1 General

The structure in each case follows the following systematic approach:

1. Designation of the examined life cycle phase and/or the related section of the testing basis within the heading.
2. Designation of the requirements
3. Description of examination result
4. Assessor evaluation result

4.2 General information related to system safety and the safety goal

4.2.1 Requirements

The to-be-met Safety Integrity Level (SIL) and the Functional Failure Rate (FFR) of the overall system must be defined.

4.2.2 Examination Result

For the generic product a Tolerable Functional Failure Rate (TFFR) based on a risk analysis is not defined. It must be determined by the application.

Pilz GmbH & Co KG defined the generic SIL and FFR to met SIL2, SIL 3 or SIL 4 based on different configuration patterns / architectures

The goals and approach used for the determination of the FFR are defined in the safety plan /D1/. It includes

- System description
- Restrictions and assumptions
- Strategy for re-used components from IEC 61508 developments
- Life cycle issues
- Safety goals incl. to-be-applied measures and techniques
- Safety organization
- Auditplan
- Documentation
- Configuration management
- Requirement Management

The following documents were provided to evaluate the system safety and safety goal:

No.	Title	Document number / ID	Rev.	Date
The following documents were issued by the customer:				
/D1/	Safety Plan Sicherheitsplan PSS 4000 Gen. 2 (Bahn) Rail Certification PSS 4000-R G2	[SPLAN]	64881	07.03.2023
/D2/	Matrix for roles during development of the library blocks	[ROMATRIX]_Rollenmatrix_Bahnnormen_G2_CS_Bausteine	informational	

Table 17: System Safety and Safety Goal data

4.2.3 Assessor evaluation result

No.	Title	Document number / ID	Rev.	Date
The following test reports were issued by TÜV SÜD Rail GmbH:				
[R1]	Review Protocol concept and planning documents	717522574_Review Protocol_PSS4000Rgen2_1.14	1.14	2023-07-31
[R2]	Assessment report for PSS 4000-R generation 1 (TÜV SÜD Rail GmbH)	PO84128G rev1_15_signed.pdf	1.15	16.03.2021
	Certificate for PSS 4000-R generation 1 (TÜV SÜD Product Service GmbH)	Z10 020132 0289	01	16.03.2021
	Report on certificate for PSS 4000-R generation 1 (TÜV SÜD Product Service GmbH)	PO84268C_rev_1_6.pdf PO84268C_rev_1_6_en.pdf	1.6	16.03.2021

Table 18: System Safety and Safety Goal results

The results of the TÜV SÜD Rail assessment are documented in [R1]. The basic approach is the same as used in PSS 4000-R generation 1 ([R2]). During the concept phase special attention has been drawn on the influences of modifications of the head module that influence the SIL architecture and FFR calculation.

The customer documents showed that the to-be-met SIL and FFR of the generic product have been defined.

The results reported in the above listed documents show that the requirements are fulfilled.

4.3 Hazard Control

4.3.1 Requirements

The management for the implementation of a system, which meets with the demanded hazard rates as well as the associated safety functions, must be performed in accordance with the normative requirements (EN 50129 A.4.3). For a generic product this can only be performed in a limited way based on e.g. use cases. Special attention should be given to the identification and treatment of new hazards arising from design (EN 50129 A.4.4).

4.3.2 Examination Result

Since the development of the first generation of PSS 4000-R Pilz GmbH & Co KG uses a Functional Safety Management process established to meet the requirements to develop the generic product in accordance with the requirements of the EN 5012x standards. This process is based on the existing processes in accordance with IEC 61508 and enhanced with railway specific requirements in a project specific safety plan. Technical and organizational measures and techniques are defined accordingly.

For PSS 4000-G2-Rail the safety plan has been established, see /D1/. A hazard log is used to control new hazards arising from design.

The safety case is established to demonstrate that the product complies with the requirements for quality management, safety management, functional and technical safety.

The following documents were provided to evaluate the process of the hazard control:

No.	Title	Document number / ID	Rev.	Date
The following documents were issued by the customer:				
/D3/	Safety Plan	see /D1/		
/D4/	Safety Case	see /D6/ - /D11/		
/D5/	Hazard Log	Database within Pilz Quality Center		

Table 19: Hazard Control data

4.3.3 Assessor evaluation result

No.	Title	Document number / ID	Rev.	Date
The following test reports were issued by TÜV SÜD Rail GmbH:				
[R3]	Review Protocol PSS4000Rgen2	see [R1]		

Table 20: Hazard Control results

The results of the TÜV SÜD Rail assessment showed that all safety related objections haven been closed for the referenced document versions.

The customer documents showed that the management for the implementation of the system has been performed and PSS 4000-G2-Rail meets the demanded hazard rates as well as the associated safety functions.

The results reported in the above listed documents show that the requirements are fulfilled.

4.4 General Information related to the Safety Case

4.4.1 Requirements

A safety Case has to be provided. The formal structure and content is defined by EN 50129 Chapter 7.

4.4.2 Examination Result

The following documents were provided by Pilz GmbH & Co KG as a safety case:

No.	Title	Document number / ID	Rev.	Date
The following documents were issued by the customer:				
/D6/	Safety Case part 1 Definition of System	[SINA1]_Sicherheitsnachweis_Teil_1_-_Definition_des_Systems.pdf	66160	26.05.2023
/D7/	Safety Case part 2 Quality Management Report	[SINA2]_Sicherheitsnachweis_Teil_2_-_Qualitätsmanagement_Bericht.pdf	65798	08.05.2023
/D8/	Safety Case part 3 Safety Management Report	[SINA3]_Sicherheitsnachweis_Teil_3_-_Sicherheitsmanagement_Bericht.pdf	65792	08.05.2023
/D9/	Safety Case part 4 Technical Safety Report	[SINA4]_Sicherheitsnachweis_Teil_4_-_Technischer_Sicherheitsbericht.pdf	65838	08.05.2023
/D10/	Safety Case part 5 Related Safety Case	not applicable		
/D11/	Safety Case part 6 Conclusion	not provided		
/D12/	Reference to all relevant documents of the project	[DOKREF]_DokumentenreferenzBahnzulassung_PSS_4000-R_G2.pdf	65955	10.05.2023
			66162	26.05.2023

Table 21: Safety Case data

A Safety Case Part 5 has not been established, as no other related Safety Case is referenced. As well as the previous safety case for generation 1 (see [R2]) the safety case for generation 2 lists all relevant documentation directly, hence being consistent.

A Safety Case part 6 “Conclusion” has not been provided. Pilz GmbH & Co KG deems a summary to be not needed for the generic product and a claim of being “adequately safe”

as requested in EN 50129 chapter 7.1 for part 6 is only possible with knowledge of an application.

4.4.3 Assessor evaluation result

No.	Title	Document number / ID	Rev.	Date
The following test reports were issued by TÜV SÜD Rail GmbH:				
[R4]	Assessment Report PSS 4000-R generation 1	see [R2]		
[R5]	Review Protocol PSS4000Rgen2	see [R1]		

Table 22: Safety Case results

The results of the TÜV SÜD Rail assessment showed that the provided Safety Case fulfils the normative requirements.

The results reported in the above listed documents show that the requirements are fulfilled.

4.5 Quantitative Safety Requirements / Probabilistic Data

4.5.1 Requirements

The safety requirements defined for the overall system are to be fulfilled by a combination of functions, subsystems, or installations.

The classification for the use of PSS 4000-G2-Rail was commissioned by the client to have to attain EN 50129 safety integrity level up to SIL 4 with a "tolerable functional failure rate" of:

$$10^{-9} \leq \text{TFFR} < 10^{-8}$$

The THR does not only apply to the PSS 4000-G2-Rail but rather refers to the overall function. The apportioned TFFR of the PSS 4000-G2-Rail therefore may only lay claim to a part of the THR for SIL 4.

4.5.2 Examination Result

PSS 4000-G2-Rail is a modular system that is to be configured by the user in accordance with his needs, e.g. based on required types and number of inputs and outputs, local setup or needs to cover long distance connections by data communication (called "de-centralized").

In addition, Pilz GmbH & Co KG defined different architectural setups to allow coverage of different SIL requirements with an efficient number of modules.

Thus, a single TFFR value cannot be given in a reasonable way for the generic product itself.

Pilz GmbH & Co KG calculated the TFFR for each module and gives the needed information in the manual and data sheet. This includes calculation rules and application notes.

The calculation method of the FFR for each module uses the methodology of FMEDAs. Related documents for each module are named [HW02]_FMEA_* (see /D14/ - /D16/).

The used failure modes are based on the standards IEC 61508, ISO 13849-1 and EN 50129 annex C. A common cause analysis in accordance with EN 50129 is performed in addition to avoid normative differences regarding the handling of such failures by the different standards.

A Fault-Tree based calculation of the given architecture patterns is provided to give evidence of the principal capabilities of the PSS 4000-G2-Rail to achieve the required FFRs.

No.	Title	Document number / ID	Rev.	Date
The following documents were issued by the customer:				
/D13/	Safety Case	see /D6/ - /D11/		
/D14/	FMEDA PSS u2 P42 F/S -R	FMEA Bauteile HW P4x – HW02.pdf	3.1	06 Februar 2023
/D15/	FMEDA [HW02] [HW02V] Bauteile-FMEA FDI (-R)	_00102_-_Controller_00102_-_Products_00209_-_PSS_u2_7088_-_PSS_u2_IO_PSS_u2_FDI_FDO_PSP_HW_FDI_PSS_u2_EF_DI_-_HW02.htm	54688	11.04.2023
/D16/	FMEDA [HW02] [HW02V] Bauteile-FMEA FDO (-R)	_00102_-_Controller_00102_-_Products_00209_-_PSS_u2_7088_-_PSS_u2_IO_PSS_u2_FDI_FDO_PSP_HW_FDO_PSS_u2_EF_DO_-_HW02.htm	54688	11.04.2023
/D17/	[FTREE] [Berechnung der Gefährdungsrate Functional Failure Rate PSS 4000 G2	[FTREE]_Berechnung_Gefährdungsrate_PSS_4000-R_G2.pdf	65843	02.05.2023
/D18/	[FTREE] - Ratenberechnung PSS 4000-R G2	[FTREE]_Ratenberechnung_PSS_4000-R_G2.pdf	63487	20.12.2022
/D19/	[CCFA] Auswirkungsanalyse von Common-Cause-Ausfällen im Steuerungssystem PSS 4000-R G2	[CCFA]_CommonCauseFehlerAnalyse_PSS_u2.pdf	65843	2.05.2023

Table 23: Probabilistic data

The probabilistic data for the E/E/PE System for example configurations is given in the table below:

	Product Values	Remark
SIL 2 de-centralized DI / DOR		- communication related failure rates are included - Failure rates are based on SN29500 at an ambient temperature of 40°C
FFR [h ⁻¹]	7,94E ⁻⁰⁹	
SIL 3 de-centralized DI / DOR		
FFR [h ⁻¹]	1,84E ⁻⁰⁹	
SIL 4 de-centralized DI / DOR		
FFR [h ⁻¹]	1,60E ⁻⁰⁹	
Proof Test Interval	-	
Lifetime [years]	20	

Table 24: Safety Characteristic Data

4.5.3 Assessor evaluation result

No.	Title	Document number / ID	Rev.	Date
The following test reports were issued by TÜV SÜD Rail GmbH:				
[R6]	see Table 37: Functional and Technical Safety - Effect of Faults result			

Table 25: Probabilistic data result

The detailed hardware design analysis and verification of the PSS 4000-G2-Rail complies with required limits of the safety standards, for the specified safety classifications, see related documents above.

4.6 Quality Management

4.6.1 Requirements

The quality of the system, subsystem or the installation should be ensured by an appropriate quality management system. The quality management system should be applicable over the entire life cycle. The proof of quality management is to be recorded in part of 2 of the safety case (quality management report).

4.6.2 Examination Result

Pilz GmbH & Co KG maintains a quality management system in accordance to ISO 9001.

No.	Title	Document number / ID	Rev.	Date
The following documents were issued by the customer:				
/D20/	QM-certificate ISO 9001:2015	002462 QM15 (DQS GmbH)	-	17.07.2021
/D21/	Occupational Health and Safety Management System ISO 45001:2018	002462 OHS18	-	17.02.2023
/D22/	Quality plan	part of safety plan, see /D1/ chapter 7.2.1 / 12.2.2		
/D23/	Quality Management Report	See Safety Case part 2, /D7/		

Table 26: Quality Management data

4.6.3 Assessor evaluation result

The customer documents and the audits performed on site showed that the requested Quality Management has been established, maintained, and supervised for the applicable lifecycle phases. Completeness of lifecycle activities has been approved during the development of the PSS 4000-G2-Rail, via document reviews, audits and spot checks.

No.	Title	Document number / ID	Rev.	Date
The following test reports were issued by TÜV SÜD Rail GmbH:				
[R7]	Review Protocol PSS4000Rgen2	see [R1]		

Table 27: Quality Management result

The results reported in the above listed documents show that the requirements are fulfilled.

4.7 Safety Management

4.7.1 Requirements

The development of the PSS 4000-G2-Rail has to be assessed at appropriate stages of the safety lifecycle by TÜV SÜD Rail GmbH or other independent organisations as requested by the safety standards. The independence of involved parties should be defined in the safety plan.

4.7.2 Examination Result

The following documents were provided to evaluate the Functional Safety Management, technical and assessment 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 PSS 4000-G2-Rail:

No.	Title	Document number / ID	Rev.	Date
The following documents were issued by the customer:				
/D24/	Safety Plan Sicherheitsplan PSS 4000 Gen. 2 (Bahn) Rail Certification PSS 4000-R G2	see /D1/		
/D25/	Functional Safety Management IEC 61508:2010	Q4B 020132 0221	01	10.02.2020
/D26/	V&V Plan	part of safety plan, see /D1/ chapter 14.x		
/D27/	Safety Management Report	see safety case part 3 /D8/		

Table 28: FSM documentation data

4.7.3 Assessor evaluation result

No.	Title	Document number / ID	Rev.	Date
The following test reports were issued by TÜV SÜD Rail GmbH:				
[R8]	Review according to EN 50126-1	Unchanged processes to [R2]		
[R9]	Review Protocol PSS4000Rgen2	see [R1]		
[R10]	FSM Audit Report	Meeting Minutes see project folder 717527108_Pilz_PSS4000R_gen\Ergebnisse\Besprechungen		

Table 29: FSM results

The customer documents and the audits performed on site showed that the requested Functional Safety Management has been established, maintained and supervised for the applicable safety lifecycle phases. Completeness of safety lifecycle activities has

been approved during the development of the PSS 4000-G2-Rail, via document reviews, audits (via web conferences) and spot checks.

The results reported in the above listed documents show that the requirements are fulfilled.

4.8 Technical Safety – Introduction of Design and Safety Principles

4.8.1 Requirements

The following characteristics of the system/subsystem/installations are to be described at top level:

- the design
- a summary of the technical safety principles, on which safety is based.

The description of characteristics has to be covered in section 1: Introduction, and in more detail in the section 2.1: Description of the system architecture, together with section 2.2: Definition of the interfaces of the Technical Safety Report.

4.8.2 Examination Result

Pilz GmbH & Co KG provided the Technical Safety Report as part 4 the safety case.

The architecture consists of two hierarchical levels:

- Architecture of the used HW: composite fail safe (dual channel architecture) for each module
- Architectural configuration pattern for SIL 3 and SIL 4 applications: additional separation requirements to avoid common causes

Main change to the already existing PSS 4000-R generation 1 are modifications on the head module leading to an improved channel separation (see chapter 4.11). These improvements allow a reduction of the initial SIL 4 configuration pattern comprising two separate head modules to one head module.

The safety relevant communication protocol SafetyNET p remains unchanged to the PSS 4000R generation1 ([R2]).

For the internal communication Modulbus 2 see chapter 4.9.

The PC-based tool PAS 4000 is used for configuration and application programming.

Interfaces are described in detail splitted into internal and externa interfaces.

All documents have undergone the needed reviews and release procedures according to the quality and safety management process.

The following documents were provided by Pilz GmbH & Co KG to evaluate the overall product architecture of the PSS 4000-G2-Rail.

No.	Title	Document number / ID	Rev.	Date
The following documents were issued by the customer:				
/D28/	Technical Safety Report	see /D9/		
/D29/	Product SRS (exported from DOORS)	[RailReq]_Railway_Railway_Standards_and_Safety_Requirements.htm	65856	02.05.2023
/D30/	Sicherheitsarchitekturen für Bahnanwendungen	[Sys07]_INSTBAHN	65885	04.05.2023

Table 30: Design and Safety Principles data

4.8.3 Assessor evaluation result

On the basis of the existing documentation, reviews and discussions were held with the responsible persons and staff.

No.	Title	Document number / ID	Rev.	Date
The following test reports were issued by TÜV SÜD Rail GmbH:				
[R11]	Basic concept accepted in release 1, see [R2]			
[R12]	Review Protocol concept and planning documents generation 2	see [R1]		
[R13]	HW Architecture	see chapter 4.11		

Table 31: Design and Safety Principles result

The Technical Safety Report does not directly name the used standards in the introduction section, it refers to the Requirement specification /D29/. The assessor gives the following recommendation Rec 3: "In case a generic or specific application needs details on the used standards beyond the statements in manuals and SRACs Pilz GmbH & Co KG should provide an export of the related chapters of the document [RailReq]."

The PSS 4000-G2-Rail from Pilz GmbH & Co KG is able to fulfil the requirements in accordance to the standards mentioned in clause 3. Forward and backward traceability between the specifications, architecture and testing documents has been planned to avoid systematic failures. The results reported in the above listed documents show that the requirements are fulfilled.

4.9 Safety Related Communication

4.9.1 Requirements

The used safety-related communication in transmission systems has to be classified based on its technical properties, the consistency of the performance of the potential access to the system. Safety services for message authenticity, message integrity, message timeliness and message sequence have to be provided by the system. Contribution to the overall failure rate of the system has to be addressed.

4.9.2 Examination Result

The system uses a communication network of the category 2 based on the protocol SafetyNET p. SafetyNET p is pre-certified in accordance to IEC 61508-3:2010 and unchanged with respect to PSS 40000-R generation 1.

The analysis for compliance contribution to the overall Functional failure rate with EN 50159 is shown in /D31/.

The internal communication protocol Modulbus2 has been changed with respect to the previously used PSS 4000-R generation 1. It has been specified by Pilz GmbH & Co KG (see /D32/, /D33/) in accordance to EN 61784-3:2021, IEC 61508-1/-3:2010 and EN 50159:2010.

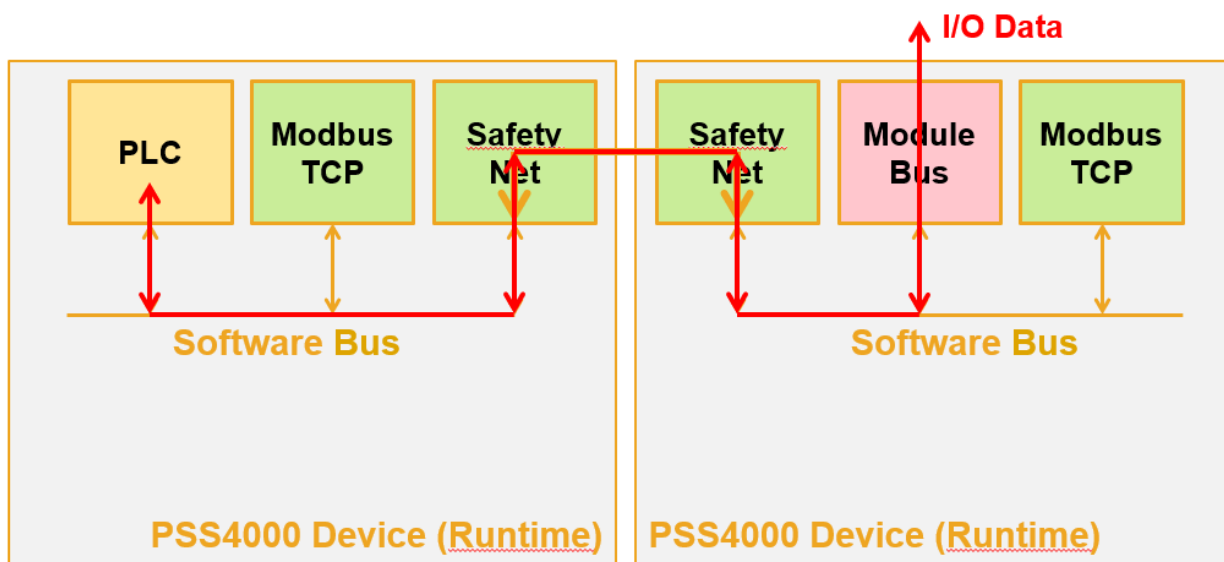


Figure 6 PSS 4000R communication structure

The following documents were reviewed to evaluate the design details of safety communication to fulfil the requirements of the standards referenced in clause 3 for the targeted risk reduction level:

No.	Title	Document number / ID	Rev.	Date
The following documents were issued by the customer:				
/D31/	SafetyNET p compliance to EN 50159	SIKON_SNET	11832	30.03.2022
/D32/	Modulbus 2 FS Specification	[PrMdSp]	3.0	2015-11-16
/D33/	Modulbus 2 FS Measurements (export)	/PSSuGeneration2/Modulbus/Modulbus 2 FS Maßnahmen	3.0	2015-11-16

Table 32: Safety related communication documentation data

4.9.3 Assessor evaluation result

According to the safety standards the fault models in combination with the required integrity measures for communication via black channel have been analysed and evaluated. The calculated resulting failure rate for the communication is very low compared to the safety characteristic data.

The implemented safety layer detects the defined transmission errors; like repetitions, deletion, insertion, resequencing, corruption, delay and masquerade.

No.	Title	Document number / ID	Rev.	Date
The following test reports were issued by TÜV SÜD Rail GmbH:				
[R14]	Certificate of compliance SafetyNET p to IEC 61508	Z10 020132 0275	00	29.11.2018
[R15]	Technical Report Modulbus 2	PO88230T	1.1	30.03.2023

Table 33: Safety related communication results

EN 50159:2010/A1:2020 has no technical impact. The requirements of /N7/ (EN 50159) are fulfilled.

4.10 Technical Safety - Assurance of correct functional operation

4.10.1 Requirements

The system, in its fault-free normal state, is to implement the function correctly, in agreement with the specified operational requirements and the safety requirements.

The proof is to be recorded within section 2 of the of the Technical Safety Report.

4.10.2 Examination Result

The safety case document /D34/ contains the technical safety report.

System railway specific architecture description including the definition of interfaces is depicted in the safety case part 1 (/D6/). It is based on the IEC 61508 and IEC 13849-1 conformant modules and the PSS 4000-R generation 1. Specific additional requirements have been defined and traced throughout the development process in DOORS.

Changes to the modules were analysed by impact analysis, the safety plan /D1/ has been to justify applicability of existing evidence as well as filling potential gaps between different standards. It contains the measures and techniques to be applied in accordance with EN 50129 and EN 50128.

Fulfilment of the system and safety requirements specification is shown by used design principles, calculations, test specifications and results of the validation.

Assurance of correct hardware functionality is shown by the fulfilment of the module specific Project Safety Plans [PSP]_* (/D56//D57//D58/).

For assurance of correct software functionality please refer to chapter 4.16.

Verification and validation have been performed accordingly and is documented or referenced in the safety case and the document reference list /D12/ respectively.

No.	Title	Document number / ID	Rev.	Date
The following documents were issued by the customer:				
/D34/	Technical Safety Case	/D9/		
/D35/	System architecture description	Part of SRS /D4/ and Safety case part 1 /D6/		
/D36/	Hardware_Aenderungsmeldung	Hardware_Aenderungsmeldung_TÜV-Süd_PSSu_E-Module_V1.0.pdf	54275	14.02.2023
/D37/	[HW01] [HW05V] HW-Spezifikation Base (-R)	_00102_-Controller_00102_-Products_00209_-PSS_u2_7088_-PSS_u2_IO_PSS_u2_Base_HW_PSS_u2_B_-HW010309.htm	BI Set 0.2 (Release 4.0)	11.04.2023

No.	Title	Document number / ID	Rev.	Date
/D38/	[HW01] [HW05V] HW-Spezifikation FDI (-R)	_00102_-_Controller_00102_-_Products_00209_-_PSS_u2_7088_-_PSS_u2_IO_PSS_u2_FDI_FDO_PSP_HW_FDI_PSS_u2_EF_DI_-_HW010309.htm	BI Set 0.2 (Release 4.0)	11.04.2023
/D39/	[HW01] [HW05V] HW-Spezifikation FDO (-R)	_00102_-_Controller_00102_-_Products_00209_-_PSS_u2_7088_-_PSS_u2_IO_PSS_u2_FDI_FDO_PSP_HW_FDO_PSS_u2_EF_DO_-_HW010309.htm	BI Set 0.2 (Release 4.0)	11.04.2023
/D40/	[HW01] [HW05V] HW-Spezifikation FDOR (-R)	_00102_-_Controller_00102_-_Products_00209_-_PSS_u2_7088_-_PSS_u2_IO_PSS_u2_FDI_FDO_PSP_HW_FDO_PSS_u2_EF_DO_-_HW010309.htm	BI Set 0.2 (Release 4.0)	11.04.2023
/D41/	[HW01] [HW05V] HW-Spezifikation PSP (-R)	_00102_-_Controller_00102_-_Products_00209_-_PSS_u2_7088_-_PSS_u2_IO_PSS_u2_FDI_FDO_PSP_HW_PSP_PSS_u2_ES_PSP_-_HW010309.htm	BI Set 0.2 (Release 4.0)	11.04.2023
/D42/	[HW07] [HW05V] Schaltplan-Beiblatt Base (-R)	2990-06_00-Spez.pdf	54129	26.01.2023
/D43/	[HW07] [HW05V] Schaltplan-Beiblatt FDI (-R)	5241-03_03-spez.pdf	54129	26.01.2023
/D44/	[HW07] [HW05V] Schaltplan-Beiblatt FDO (-R)	5246-03_01-spez.pdf	54129	26.01.2023
/D45/	[HW07] [HW05V] Schaltplan-Beiblatt FDOR (-R)	5249-05_00-spez.pdf	54129	26.01.2023
/D46/	[HW07] [HW05V] Schaltplan-Beiblatt PSP (-R)	5236-03_00-spez.pdf	54129	26.01.2023
/D47/	[HW05] [HW05V] Schaltplan Base (-R)	32X810_PSS_u2_B_4_(-R)_2990-06_00_106036-06_schpl.pdf	54044	17.01.2023
/D48/	[HW05] [HW05V] Schaltplan FDI	328101_PSS_u2_EF_8DI_5241-03_04_103298-01_schpl.pdf	54454	16.03.2023
/D49/	[HW05] [HW05V] Schaltplan FDI -R	327101_PSS_u2_EF_8DI_-R_5241-03_03_101407-07_schpl.pdf	54044	17.01.2023
/D50/	[HW05] [HW05V] Schaltplan FDO (-R)	32X133_PSS_u2_EF_4DO_2A_(-R)_5246-03_01_101411-04_schpl.pdf	54044	17.01.2023
/D51/	[HW05] [HW05V] Schaltplan FDOR (-R)	32X150_PSS_u2_EF_2DO_R_8A_(-R)_5249-05_00_101413-05_schpl.pdf	54044	17.01.2023
/D52/	[HW05] [HW05V] Schaltplan PSP (-R)	328101_PSS_u2_EF_8DI_5241-03_04_103298-01_schpl.pdf	54044	17.01.2023

No.	Title	Document number / ID	Rev.	Date
/D53/	[HW05] [HW05V] Schaltplan P42 Head Module	\Schaltpläne\PSS u2 P42 FS -R\0729-01_02_105079-04_schpl.pdf \Schaltpläne\PSS u2 P42 FS -R\0729-01_02_assembly.pdf \Schaltpläne\PSS u2 P42 FS -R\1102-04_02_101455-07_schpl.pdf \Schaltpläne\PSS u2 P42 FS -R\1102-04_02_assembly.pdf \Schaltpläne\PSS u2 P42 FS -R\7433-03_00_103219-03_schpl.pdf \Schaltpläne\PSS u2 P42 FS -R\7433-03_00_assembly.pdf \Schaltpläne\PSS u2 PS1 -R\1354-03_00_101457-03_schpl.pdf \Schaltpläne\PSS u2 PS1 -R\1354-03_00_assembly.pdf \Schaltpläne\PSS u2 PS1 -R\1355-03_01_101456-06_schpl.pdf \Schaltpläne\PSS u2 PS1 -R\1355-03_01_assembly.pdf	54897	2023-04-21
/D54/	[HW03] HW-Integrationstest-Spezifikation xxx	see /D12/ and detailed reviewreports Table 35: Functional and Technical Safety - Function result		
/D55/	[HW09] [HW09V] HW-Integrationstest-Protokoll xxx			
/D56/	Projektsicherheitsplan der P4x Kopfmodule	[PSP]_HEADMODULE		
/D57/	Projektsicherheitsplan der Elektronikmodule PSS u2	[PSP]_EMODULE-DIG		
/D58/	Projektsicherheitsplan der Elektronikmodule PSS u2	[PSP]_EMODULE-DIG		

Table 34: Functional and Technical Safety - Function

4.10.3 Assessor evaluation result

The examination took place on basis of the submitted documentation, the existing certification and via discussions with the responsible staff.

No.	Title	Document number / ID	Rev.	Date
The following test reports were issued by TÜV SÜD Rail GmbH:				
[R16]	Review Report I/O modules system level	Review Protocol - System - V3.0.pdf	3.0	11.05.2023
[R17]	Review Report I/O modules HW level	Review Protocol - HW - V1.0.pdf	1.0	05.05.2023
[R18]	Review Report I/O head module	717522574_Review Protocol_PSS4000Rgen2_FMEDA_2023 0411_1.2.pdf	1.2	11.05.2023
[R19]	Reports SW release 1.25	see chapter 4.16 Assurance of correct software functionality		

Table 35: Functional and Technical Safety - Function result

The hardware architecture and design has been realized according to the specified requirements as requested by the referenced standards. Fault avoidance measures and fault detection measures for the specified risk reduction level have been implemented and maintained.

The proof of the correct functional behaviour corresponds to the rail-specific requirements.

4.11 Technical Safety - Effects of Faults

4.11.1 Requirements

The system has to fulfil the specified safety requirements including the quantified safety goal, if random hardware failures occur.

The risk connected with possibly existing systematic errors must be reduced to an acceptable level through technical measures. The technical measures for the control of the remaining systematic errors are to be stated.

Parts of the system, whose safety integrity levels are smaller than those of the system, are not to interfere with the safety of the system.

The proof is to be led in the Technical Safety Report Section 3.

4.11.2 Examination Result

The technical safety case, including the normative demanded chapters related to failure effects and detection, is contained in the safety case.

Main change to the already existing PSS 4000-R generation 1 are modifications on the head module leading to an improved channel separation.

The safety case includes explanations of

Section 3.1 Effects of single faults

The dual channel architecture (composite fail safe) assures that single component failures do not lead to violations of the safety goals. On dissent of the two channels the system will enter the safe state. FMEDAs have been performed for each HW item/module. Fault insertion tests have been performed to give evidence for the claimed behaviour.

Section 3.2 Independence of items

Independency of items is assured by design requirements and architectural patterns for the system configuration on different Safety Integrity Levels. A Common Cause Failure Analysis (CCFA) in accordance to EN 50129 has been performed.

Section 3.3 Detection of single faults

Diagnosis running in the background reveals failures per channel within a suitable detection time.

The two channels exchange and compare the result of input/logic/output calculations within each operation cycle.

In case internal diagnosis mechanisms reveal a failure or discrepancy of the two channels the safe state will be entered.

FMEDAs have been performed for each HW item/module. Fault insertion tests have been performed to give evidence for the claimed behaviour.

Section 3.4 Action following detection (including retention of safe state)

Action following detection of a failure varies from the type of module and is described in the safety manuals. In any case a safe state will be activated, and outputs turned off (de-energized, logical "0").

retention of the safe state is guaranteed by using multiple switch-off elements and dynamic principles for the outputs, leaving the safe state requires successful passing of all self-tests / diagnosis by a system restart.

Section 3.5 Effects of multiple faults

The CCFA assures that multiple faults can only occur as independent single component failures.

Background tests per channel would even detect single failures not leading to a discrepancy of the two channels within a suitably short detection time.

For each given railway architecture, a Fault Tree Analysis was performed to show that the probabilistic safety goals are not violated in case of multiple failures.

Section 3.6 Defence against systematic faults

The applied safety process including the verification and validation measures assures sufficiently the defence against systematic faults.

Technically the system comprises additional measures to avoid safety issues due to undetected remaining systematic failures:

- Partly diverse components, e.g., the processors of each channel module are diverse.
- Dynamic principles, e.g., charge pumps for digital outputs are used.
- De-energized-to-trip principles are used.

No.	Title	Document number / ID	Rev.	Date
The following documents were issued by the customer:				
/D59/	[HW02] [HW02V] Bauteile-FMEA FDI (-R)	_00102_-_Controller_00102_-_Products_00209_-_PSS_u2_7088_-_PSS_u2_IO_PSS_u2_FDI_FDO_PSP_HW_FDI_PSS_u2_EF_DI_-_HW02.htm	54688	11.04.2023
/D60/	[HW02] [HW02V] Bauteile-FMEA FDO (-R)	_00102_-_Controller_00102_-_Products_00209_-_PSS_u2_7088_-_PSS_u2_IO_PSS_u2_FDI_FDO_PSP_HW_FDO_PSS_u2_EF_DO_-_HW02.htm	54688	11.04.2023
/D61/	[HW02] [HW02V] Bauteile-FMEA FDOR (-R)	_00102_-_Controller_00102_-_Products_00209_-_PSS_u2_7088_-_PSS_u2_IO_PSS_u2_FDI_FDO_PSP_HW_FDO_PSS_u2_EF_DOR_-_HW02.htm	54688	11.04.2023
/D62/	[HW12] [HW02V] Praktische Bauteile-FMEA FDI (-R)	_00102_-_Controller_00102_-_Products_00209_-_PSS_u2_7088_-_PSS_u2_IO_PSS_u2_FDI_FDO_PSP_HW_FDI_PSS_u2_EF_DI_-_HW12.htm	BI Set 0.2 (Release 4.0)	11.04.2023
/D63/	[HW12] [HW02V] Praktische Bauteile-FMEA FDO (-R)	_00102_-_Controller_00102_-_Products_00209_-_PSS_u2_7088_-_PSS_u2_IO_PSS_u2_FDI_FDO_PSP_HW_FDO_PSS_u2_EF_DO_-_HW12.htm	BI Set 0.2 (Release 4.0)	11.04.2023
/D64/	[HW12] [HW02V] Praktische Bauteile-FMEA FDOR (-R)	_00102_-_Controller_00102_-_Products_00209_-_PSS_u2_7088_-_PSS_u2_IO_PSS_u2_FDI_FDO_PSP_HW_FDO_PSS_u2_EF_DOR_-_HW12.htm	BI Set 0.2 (Release 4.0)	11.04.2023
/D65/	[HW08] [HW08V] Sicherheitskennwerte FDI	[HW08] Sicherheitskennwerte PSS u2 EF 8DI.pdf	34050	14.04.2023
/D66/	[HW08] [HW08V] Sicherheitskennwerte FDO	[HW08] Sicherheitskennwerte PSS u2 EF 8DO 0.5A.pdf	34050	14.04.2023
/D67/	[HW08] [HW08V] Sicherheitskennwerte FDOR	[HW08] Sicherheitskennwerte PSS u2 EF 2DO R 8A.pdf	34050	14.04.2023

No.	Title	Document number / ID	Rev.	Date
/D68/	[SoftErr] [SoftErrV] Berechnung der Softerror-Rate	[-] Sicherheitsbetrachtung für Soft-Errors.pdf	54783	17.04.2023
/D69/	[HW08] Sicherheitskennwerte PSS u2 P42_Draft.pdf	[HW08] Dokumentation Sicherheitskennwerte PSS 4000 G2 – CPU 2.1	54002	09.01.2023
/D70/	Fehlerbilder FMEDA vs. EN50129:2019	Bauteile-FMEA – Epedia.htm	-	05. 08 2022
/D71/	[SoISp] [SoISpV] Zielsystemspezifikation	CID1921_#1_SoiSp.PSS4000_final.pdf	64504	2023-02-16
/D72/	[SoiFMEA] [SoiFMEAV] Zielsystem-FMEA	CID1921_FMEA_Review_SoiFMEA.PSS 4000_final.pdf	64504	2023-02-16
/D73/	[SoiM] [SoiFMEAV] Katalog Maßnahmen auf Zielsystemebene	CID1921_FMEA_Review_SoiM.PSS4000_final.pdf	64504	2023-02-16
/D74/	[PrMdSp] [PrMdSpV] Produkt-/Modulspezifikation	CID1921_CID1968_PrMdSp_final.pdf	64504	2023-02-16
/D75/	[PrMdFMEA] [PrMdFMEAV] Produkt-/ Modul-FMEA	CID1921_PrMdFMEA.P4x_final.pdf	64504	2023-02-16
/D76/	[PrMdM] [PrMdFMEAV] Katalog Maßnahmen auf Produkt-/Modulebene	CID1921_FMEA_Review_SoiM.PSS4000_final.pdf	64504	2023-02-16
/D77/	[MD01] [MD01V] Mechanische Spezifikation	MeSpPSSu2P4x_final.pdf	54320	2023-02-27
/D78/	[HW08] [HW08V] Sicherheitskennwerte	[HW08] Sicherheitskennwerte.pdf	54772	2023-04-17
/D79/	[Bau01] [Bau01V] Fertigungs- und Fertigungstestkonzept	Fertigung: \\Fertigung\04_Fertigungs- und_Fertigungstestkonzept_329302.xlsx \\Fertigung\04_Fertigungs- und_Fertigungstestkonzept_P42-R.xlsx	54875	2023-04-21
/D80/	Common Cause Fehler Analyse	[CCFA]_CommonCauseFehlerAnalyse_PSS_u2.pdf	64866	06.03.2023
/D81/	Berechnung der Gefährdungsrate Functional Failure Rate PSS 4000 G2 Rail Certification PSS 4000 G2	[FTREE]_Berechnung_Gefährdungsrate_PSS_4000-R_G2.pdf	63382	13.12.2022
/D82/	Ratenberechnung PSS 4000-R G2	[FTREE]_Ratenberechnung_PSS_4000-R_G2.pdf	65843	02.05.2023

Table 36: Functional and Technical Safety - Effects of Faults data

4.11.3 Assessor evaluation result

The assessor reviewed the documentation of the implemented measures. Explanations were provided by the involved staff.

The measures for adherence to the quantified safety goal were also reviewed. See chapter 4.5: Quantitative Safety Requirements / Probabilistic Data of this report for details.

By review of the submitted FMEDA the assessor has convinced himself of the correctness of the facts related to failure effects and the implemented failure detection.

Due to the nature of the project understanding the CCFA requires knowledge of multiple documents to gather completeness, consistency and understanding:

- CCFA document
- Safety case part 4
- [HW02]_FMEA_xx for each module
- FTREE-document

The normative areas of interest (type A/B/C1/C2/C3/D) are not handled sequentially per module. They are distributed to different chapters of the CCFA, the safety case and the FMEDAs.

Test documentations and measurement logs were provided and reviewed.

No.	Title	Document number / ID	Rev.	Date
The following test reports were issued by TÜV SÜD Rail GmbH				
[R20]	Review HW P42 head module	717522574_Review Protocol PSS4000Rgen2_FMEDA_2023 0411_1.2.pdf	1.2	11.05.2023
[R21]	Review HW I/O modules	Review Protocol - HW - V1.0.pdf	1.0	11.05.2023
[R22]	Technical Report of Modifications Safety-Related Programmable System PSS u2	PO100927T	1.0	12.05.2023
[R23]	Review CCFA, FTREE, Systemlevel argumentation	see [R1]		

Table 37: Functional and Technical Safety - Effect of Faults result

The analysis results for effects of multiple failures and protection against systematic errors fulfil the requirements.

4.12 Technical Safety – Operation under external influences

4.12.1 Requirements

The system should, if it is exposed to the external influences as specified in the system requirement specification:

- Continue to fulfil the specified operational requirements
- Continue to fulfil the specific safety requirements (inclusive of the failure conditions)

The proof is to be led, in accordance in the Technical Safety Report Section 4.

4.12.2 Examination Result

Pilz GmbH & Co KG provided a Technical Safety Report, including the normative demanded chapters in relation to operation with external requirements.

All requirements are specified in the Requirement Specification and subject to the requirement tracing processes.

Pilz GmbH & Co KG executed the tests in its own independently accredited test laboratory.

It covers climatic conditions, mechanical conditions, altitude, electrical conditions, protection against unauthorized access.

More severe conditions were not applied.

No.	Title	Document number / ID	Rev.	Date
The following documents were issued by accredited laboratories:				
/D83/	[HW10] Prüfberichte zu Umwelteinflüssen P42	\TestBay\C-329230-220609-01.pdf \TestBay\E-329230-220808-01.pdf \TestBay\M-329230-220609-01.pdf	54843	2023-04-20
/D84/	[HW10] Prüfberichte zu Umwelteinflüssen Bahn Klima EN61131	C-329230-220609-01.pdf	53873	12.12.2022
/D85/	[HW10] Prüfberichte zu Umwelteinflüssen Bahn Klima EN50155	C-329230-220609-02.pdf	53873	12.12.2022
/D86/	[HW10] Prüfberichte zu Umwelteinflüssen Bahn Klima EN50125	C-329230-220609-04.pdf	53873	12.12.2022
/D87/	[HW10] Prüfberichte zu Umwelteinflüssen Industrie EMV EN61131	E-328062-220907-01.pdf	53876	12.12.2022

No.	Title	Document number / ID	Rev.	Date
/D88/	[HW10] Prüfberichte zu Umwelteinflüssen Industrie EMV Feuerungst.	E-328062-220907-02.pdf	53878	12.12.2022
/D89/	[HW10] Prüfberichte zu Umwelteinflüssen Bahn EMV EN61131	E-329230-220808-01.pdf	53873	12.12.2022
/D90/	[HW10] Prüfberichte zu Umwelteinflüssen Bahn EMV EN50121	E-329230-220808-03.pdf	53873	12.12.2022
/D91/	[HW10] Prüfberichte zu Umwelteinflüssen Bahn Mechanik EN61131	M-329230-220609-01.pdf	53873	12.12.2022
/D92/	[HW10] Prüfberichte zu Umwelteinflüssen Bahn Mechanik EN50125	M-329230-220609-03.pdf	53873	12.12.2022
/D93/	More severe conditions	Not applicable		
/D94/	EN 45545-2 test report	see [R34]		

Table 38: Operation under external influences

4.12.3 Assessor evaluation result

No.	Title	Document number / ID	Rev.	Date
The following test reports were issued by TÜV SÜD Rail GmbH:				
[R24]	see Table 35: Functional and Technical Safety - Function result			

Table 39: Operation under external influences result

Type testing has been performed by accredited test laboratories providing the evidence that the PSS 4000-G2-Rail has withstand the specified environmental conditions as defined in the test basis. The results reported in the above listed documents show that the requirements are fulfilled.

4.13 Technical Safety – Safety Relevant Application Conditions

4.13.1 Requirements

The system is to observe specified rules, conditions, and constraints to allow safe employment.

The safety related application conditions (SRAC) are to be recorded in section 5 of the Technical Safety Report, a separate document for the SRACs needs to be provided.

4.13.2 Examination Result

Pilz GmbH & Co KG extracted the information in the manual and SRACs from the requirement specification to the railway specific Operation and Maintenance Manuals, in a traceable way. It refers underlying manuals like e.g., separate HW modules.

A railway specific user manual has been provided by the manufacturer, see /D95/. It contains recommendations as well as the safety related application conditions. It describes the instructions related to the installation, commissioning, and operation for the product under evaluation.

/D97/ describes the security measures that were applied throughout the development at Pilz GmbH & Co KG.

Though security threads cannot be handled by a generic product itself Pilz GmbH & Co KG provides a Manual describing all network interfaces to facilitate correct application of related features in the PSS 4000-G2-Rail by users, see /D98/.

No.	Title	Document number / ID	Rev.	Date
The following documents were issued by the customer:				
/D95/	Manual	[Sys07]_INSTBAHN	65885	04.05.2023
/D96/	SRAC document	see /D95/		
/D97/	Security Management Plan	[Sec01]_Security_Management_Plan.doc	64935	09.03.2023
/D98/	Network Data Sheet	NWDS]_Network_Data_Sheet_PSS_4000_(0102_-_Controller)	Release 25.0	17.02.2023

Table 40: SRACs / Manual

4.13.3 Assessor evaluation result

No.	Title	Document number / ID	Rev.	Date
The following test reports were issued by TÜV SÜD Rail GmbH:				
[R25]	Review Protocol on User Manual / SRACs	see [R1]		

Table 41: SRACs / Manual result

The amount of SRACs is kept very low. This complies with the intention of EN 50129 chapter 5.3.13 Note 4: “the Safety Case does not need to repeat SRACs that are general legal/normative rules to be followed by the users. Additionally, the generic product has no ability to refer Hazards derived from an application level. It should be noted that the principles of handling a (safety) PLC are presumed to be known by an applicant and related normative rules from e.g., IEC 61131-series are contained in the manuals and data sheets, thus not being repeated as SRACs.

The user documentation includes all safety relevant data as requested by the standards. This has been reported in the above listed documents.

4.14 Technical Safety – Safety Qualification Testing

4.14.1 Requirements

The system is to fulfil the operational requirements under operating conditions. The system is to reach the specified reliability and safety goals under operating conditions. The proof is to be led within section 6 of the safety evaluation of the Technical Safety Report.

4.14.2 Examination Result

For the generic product no safety qualification tests have been performed.

4.14.3 Assessor evaluation result

Responsibility for safety qualification tests is within the generic and/or specific application.

4.15 Dependencies between Safety Cases

4.15.1 Requirements

The relations with all safety cases of which the main safety case of the system under assessment / subsystem and/or the dependant equipment, should be indicated. The safety relevant application conditions of the safety cases should be fulfilled.

The proof is to be recorded according to chapter 7.5 of EN 50129 within the safety case.

4.15.2 Examination Result

The safety case of the PSS 4000-G2-Rail does not depend on other safety cases. Wherever re-use of existing evidence of the generation 1 has been done, it has been referenced independently within the generation 2 product, thus making the safety case consistent.

4.15.3 Assessor evaluation result

Not applicable. With regard to EN 50129, no relations with other safety cases exist for this generic product.

4.16 Assurance of correct software functionality

4.16.1 Requirements

For safety-related systems which include software, the requirements of EN 50128 shall be complied with.

For SIL 1-4 EN 50657 is covered by these EN 50128 requirements.

For programmable components see EN 50129 Annex F. The results of software validation report (see EN 50128) shall be included or referenced in this section.

In addition, the interaction between hardware and software shall be explained.

These requirements imply the evaluation of:

- software requirements specification and software architecture
- designing, developing, and testing the software according to the software quality assurance plan
- software SIL and software lifecycle
- software / hardware integration
- software validation

The generic products is intended as a user programmable system and a base for the development of application data or algorithms by means of EN 50128 chapter 8. As such it requires to provide suitable procedures and tools to develop such data and/or algorithm.

4.16.2 Examination Result

The used SW is based on the existing generation 1 product.

Changes and modifications have been analysed and the needed activities of the lifecycle performed accordingly. This applies mainly to the runtime system 1.25.x including the new P42 head module, the new Modulbus 2 stack and updated to the I/O modules.

SW quality assurance for the avoidance of systematic errors by identification, supervising and controlling of all relevant technical and management activities is performed by Pilz GmbH & Co KG based on its ISO 9001-accredited/conform quality management system.

Pilz GmbH & Co KG selected a SW development lifecycle in accordance to EN 50128, see safety plan /D1/.

In the context of the provided safety case the company Pilz GmbH & Co KG has defined the SW SIL as up to “4”.

The personnel that have responsibility for the software is sufficiently qualified. It continuously practices the necessary training, experience, and qualification according to the phases of the software lifecycle. An independent assessor has been assigned.

The requirements of the software are completely covered in a central database (DOORS) and from this a related test specifications are derived.

The architecture for the software has been created. It specifies the requirements imposed on software development.

The reciprocal effects between hardware and software are evaluated and the design procedure is selected.

The design and implementation the software requirements are based on the architectural requirements.

The qualification and classification of the tools has been performed according to the classification of the standards referenced in clause 3. The support tools used for the development are controlled by the implemented configuration and change management.

Testing and evaluating of the SW was performed within the individual phases of the life cycle. The results of the verification activities were recorded within the verification reports.

The software/ hardware integration is not a separated step in the development life cycle, but an integral component of software development. SW-HW-integration was performed and shows correct software-hardware cooperation of the intended functions.

Conformance with the software requirement specification was shown by the SW validation.

The system PSS 4000-G2-Rail provides means for the first-time development of a user specific configuration and logic and the subsequent development of the general installation specific data set. The support tool PAS 4000 for setting up an application specific configuration is depicted in /D102/. This includes application rules and parameters.

No.	Title	Document number / ID	Rev.	Date
The following documents were issued by the customer:				
/D99/	Impact Analysis Runtime	[AEM] Aenderungsmeldung PSS 4000 Runtime Plattform V1.25.0	65675	20.04.2023
/D100/	List of Documents ⁴	[LOD] ListOfDocuments, PAS / RT Major Release, Version 1.25.0	65704	21.04.2023
/D101/	[SW18] [SW18V] ToolQualification	[SW18] ToolQualification.pdf	54753	14.04.2023
/D102/	PAS4000 Manual	PAS4000_Help_DE_V1.25.0.chm	65132	21.03.2023

Table 42: Software Data

4.16.3 Assessor evaluation result

No.	Title	Document number / ID	Rev.	Date
The following test reports were issued by TÜV SÜD Rail GmbH:				
[R26]	Review report SW runtime release 1.25	Review Protocol PSS4000 RT R25_V1.2.pdf	1.2	28.04.2023
[R27]	Review report SW I/O modules	Review Protocol - Software - V3.0.pdf	3.0	11.05.2023
[R28]	Review Report Tool Qualification	included in [R26][R27]		
[R29]	Review Report Programming Tool release 1.25	Review Protocol PSS4000 PAS R25_V1.2.pdf	1.2	28.04.2023
[R30]	Technical Report of Modifications PSS 4000 – Firmware / PAS 4000 R1.25	PO100913T	1.0	15.05.2023

Table 43: Software result

⁴ References in total >150 documents incl all internal document release revies and detailed test result logs in the sections for System Documents (PAS+RT); PAS Tool; 1131 Compiler and XML2Bin; Runtime generic; Runtime system framework and PAS; runtime OS; Runtime - FS+ST PLC; Runtime - Modulbus 2; Runtime - Network Manager; manuals

With respect to generic products and the related software the organizational arrangement of Pilz GmbH & Co KG for the PSS 4000-G2-Rail is in accordance to the requirements of SIL 4 of EN 50128.

The submitted documentation confirms the adherence to planning of the SW development lifecycle.

The SW requirements have been defined in an appropriate way.

Within the safety case the selected approach is described whereby the selection of the architectural characteristics of the system are based on the already existing generation 1 architecture, they are described and become comprehensible.

Design and development of the SW follow the defined procedures.

Verification and validation have been performed successfully.

The applied procedures and provided results fulfil the normative requirements of the inspection basis.

The necessary process steps to produce a safe application are suitably described. The interfaces to, and the requirements imposed on the designer of the application, are clearly represented.

The validation activities and the related results have been assessed at appropriate stages of the development as documented in the related reports. The product safety validation has confirmed that the safety functions are implemented as specified.

4.17 Modifications

4.17.1 Requirements

Modifications after product release shall be authorised, analysed, and finally realised according to the applicable phases of the safety lifecycle. The relevant steps shall be defined by a procedure or work instruction involving all relevant parties.

4.17.2 Examination Result

Revision 1.0 of this assessment report handles the first release of PSS 4000-G2-Rail, thus no modifications have been assessed so far.

Pilz GmbH & Co KG maintains a Functional Safety Management Process that includes rules on handling modifications.

With respect to the PSS 4000-G2-Rail the safety plan /D1/ contains the railway specific enhancements in chapter 15.

The following documents describe the modification procedure applied to the product under evaluation:

No.	Title	Document number / ID	Rev.	Date
The following documents were issued by the customer:				
/D103/	Safety Plan Sicherheitsplan PSS 4000 Gen. 2 (Bahn) Rail Certification PSS 4000-R G2	see /D1/		

Table 44: Modification procedure documents

4.17.3 Assessor evaluation result

No.	Title	Document number / ID	Rev.	Date
The following test reports were issued by TÜV SÜD Rail GmbH:				
[R31]	QM-certificate ISO 9001:2015	002462 QM15 (DQS GmbH)	-	17.07.2021
[R32]	Occupational Health and Safety Management System ISO 45001:2018	002462 OHS18	-	17.02.2023

Table 45: Modification results

The procedure defines the required steps for analysing, verifying, and validating those safety lifecycle phases, which need to be repeated for a re-assessment of the product modifications.

5 Testing Body

This report is based on the accreditation of the testing laboratory for safety components; see table “Quality Management System”.

The following test reports were issued from other accredited laboratories (in addition to the environmental testing in chapter 4.12 Technical Safety – Operation under external influences), as integrated part of the test result:

No.	Issued by and Title	Document number / ID	Rev.	Date
[R34]	EN 45545-2:2020 Laboratory TÜV SÜD Rail GmbH: department TR-RS21-BER for rolling stock	PO100906G	1.0	16.05.2023

Table 48: Test Reports issued from other laboratories

6 Results and Recommendations

6.1 Result

Pilz GmbH & Co KG successfully finished the necessary verification and validation activities for the generic product. Pilz GmbH & Co KG provided a generic product safety case (GPSC) in accordance to EN 50129. The GPSC refers to the measures applied according to IEC 61508 and other relevant standards. It gives the rationale for the compliance of these measures to the railway specific CENELEC standards given in chapter 3.

6.2 Recommendations

- Rec 1. Safety Qualification Tests according to EN 50129 Chapter B.6 (TSR Section 6) are not part of this assessment report. A safety qualification with independent safety supervision units may be conducted based on the existing safety acceptance tests documented hereby. It has to be assured that the functionality of the PSS 4000-G2-Rail can be monitored and logged to evaluate the target achievement.
- Rec 2. For every first-time acceptance of a generic and/or specific application the completeness of the application test must be proven by the application manufacturer.
For modifications the necessary verification and validation testing must be determined based on a modification impact analysis.
- Rec 3. In case a generic or specific application needs details on the used standards beyond the statements in manuals and SRACs Pilz GmbH & Co KG should provide an export of the related chapters of the document [RailReq]. (origin: chapter 4.8.3)

6.3 Conditions of Use

- CoU 1. The Generic Product Safety Case in the current version has to be considered.
- CoU 2. The guidelines and requirements specified by the Safety-Related Application Conditions (SRAC) shall be followed.
- CoU 3. Only modules certified for safety-related operation shall be used for safety-critical functions.
- CoU 4. The application manufacturer shall consider the railway manuals which include the safety related application conditions at their latest valid release.

7 Summary

The test results of clause 4 showed that the ToE, as specified in clause 2.1, fulfils the requirements of the standards and guidelines referenced in clause 3, if the constraints and conditions defined in chapter 6 and the safety manuals are met.

Department Manager Embedded Systems

Project Manager



Guido Neumann
2023.08.17
16:54:33 +02'00'



Digital
unterschieden von
Volker Sperling
Datum: 2023.08.17
15:43:29 +02'00'