Choose certainty.
Add value.

Technical report

of the

Type testing

Programmable Logic Controller TREI 5B-04

Applicant

JSC TREI

1G Germana Titova Street
440028 Penza
Russia

Manufacturer

JSC TREI

1G Germana Titova Street
440028 Penza
Russia

Report No.: TP91300T
Version 1.0 of 2017-07-26

Test Body

TÜV SÜD Rail GmbH
Rail Automation
Barthstraße 16
D-80339 München

Table of Contents

page

TÜV SÜD Rail GmbH
Barthstraße 16
80339 München
phone: +49 89 5791-2050, fax: -2933
e-mail: franz.seika@tuev-sued.de

List of tables

page

List of figures

page

Revision history

Revision	Status	Date	Author	Modification / Description
1.0	Final	2017-07-26	Franz Seika	

Table 1: Revision history

List of abbreviations

Abbreviation	Description
MM	master module/ мастер-модуль
MIO	I/O module / модуль ввода/вывода
ST-BUS	serial I/O interface / последовательный интерфейс ввода/вывода
TP PWR	Terminal panel power /терминальная панель питания
MCU	Microcontroller device/микроконтроллер
DO	Digital output/цифровой выход

Table 2: Abbreviations

1 Target of Evaluation (ToE)

On 2016-06-28 JSC TREI requested TÜV SÜD Rail GmbH to test and certify the TREI 5B-04 according to the standard listed in clause 3 of this report. The project number related to this technical report is 717513117.

The ToE is a Programmable Logic Controller (in the following named PLC) according to EN 61131-2, SIL 3 according to IEC 61508, SILCL 3 according to IEC 62061 and Category 4 / PL e according to EN ISO 13849-1.

The mission of the TREI 5B-04 is to control local and distributed systems, automated process control and management in the critical systems in industrial plants with normal and hazardous areas, as well as for the construction of emergency locks and protection systems.

2 Scope of Testing

2.1 Test specimen

The TREI 5B-04 consists of the following modules:

- M401E master module
- M452D digital input module (for up to 32 channels)
- M445A analogue input module (for up to 16 channels)
- M451O digital output module (for up to 32 channels)
- ST-BUS communication between the modules

The overview of the TREI 5B-04 series is depicted in the figures below.

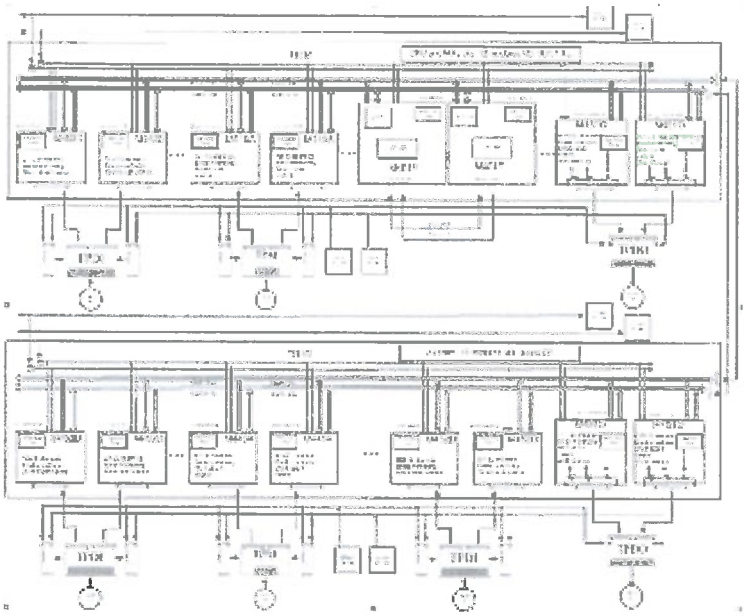

Figure 1: System overview of TREI 5B-04

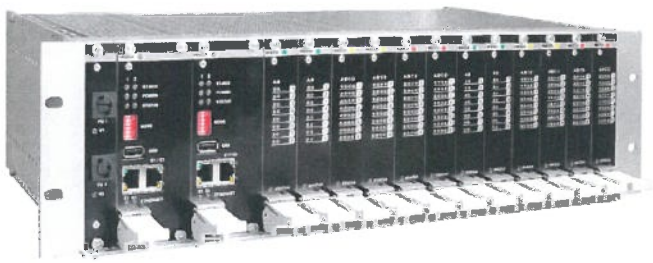

Figure 2: TREI 5B-04 Programmable Logic Controller

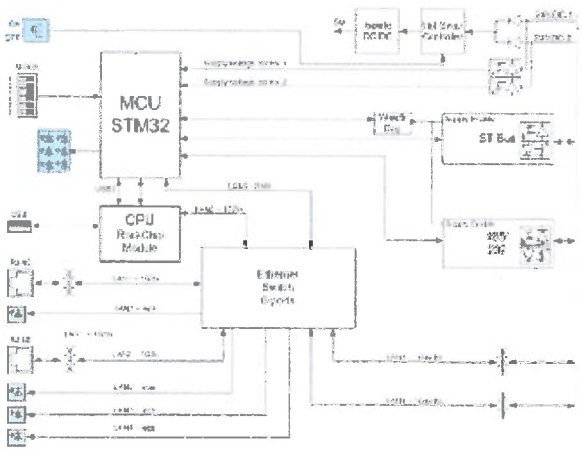

Figure 3: Block scheme of M401E Master Module

TÜV SÜD Rail GmbH
Barthstraße 16
80339 München
phone: +49 89 5791-2050, fax: -2933
e-mail: franz.seika@tuev-sued.de

2.2 Nomenclature of TREI 5B-04

The system tested is identified by hardware and software version as follows:

Name	Design	Serial number	SW	HW	Quantity
PLC central rack CR M	TREI.421457.533	00535	-	Back Panel M 1.3	1
PLC I/O rack CR IO	TREI.421457.533	00536	-	Back Panel IO 1.3	1
Master module M401E	TREI.421457.517	G4M0008 G4M0009	Executive system: 2.11 Operating system: 1.0 Communication controller: 1.0	PAZ-Master 1.2 CPU Board 3288 1.1	2
Discrete input module M452D	TREI.421457.522	4D00008 4D00012	1.0	PAZ32DI 1.2	2
Discrete output module M451O	TREI.421457.521	4O00012 4O00009	MCU1: 1.0 MCU2: 1.0	PAZ32DO 1.2	2
Analog input module M445A	TREI.421457.520	4A00009 4A00008	1.0	PAZ16AI 1.2	2
TPDI discrete input terminal panel	TREI.421457.526	TI00008	-	TPDI 1.2	1
TPDO discrete output terminal panel	TREI.421457.525	TO00008	-	TPDO 1.2	1
TPAI analog input terminal panel	TREI.421457.527	TA00009	-	TPAI 1.2	1
TPPWR power supply terminal panel	TREI.421457.528	TPW0012 TPW0011 TPW0009 TPW0010	-	TPPWR 1.1	4

Table 3: Identification of TREI 5B-04

2.3 Tests

The TREI 5B-04 was examined with regard to the following testing operations:

I. Functional Safety including
- Functional safety management (FSM) und safety lifecycle
- Analysis of the system structure (System-FMEA)
- Analysis of the hardware (FMEDA[1] on component or block level, quantitative analysis)
- Analysis of the software
- Error simulations and software tests
- Test of the error prevention 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

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

[1] Failure Mode, Effects and Diagnosis Analysis

3 Standards and guidelines

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

3.1 Guidelines and directives

No.	Reference	Description
/N1/	2006/42/EC	DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 May 2006 on machinery

Table 4: Directives

3.2 Product standards

No.	Reference	Description
/N2/	EN 61131-2:2007	Programmable controllers – Part 2: Equipment requirements and tests

Table 5: Product standards

3.3 Functional safety

No.	Reference	Description
/N3/	IEC 61508-1:2010 (SIL 3)	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements
/N4/	IEC 61508-2:2010 (SIL 3)	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/ programmable electronic safety-related systems
/N5/	IEC 61508-3:2010 (SIL 3)	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements
/N6/	IEC 61508-4:2010 (SIL 3)	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations
/N7/	IEC 62061:2005/A2:2015 (SIL CL 3)	Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems
/N8/	EN ISO 13849-1:2015 (Cat. 4, PL e,)	Safety of machinery - Safety-related parts of control systems Part 1: General principles for design

Table 6: Functional safety

3.4 Susceptibility to environmental errors

3.4.1 IP Code testing

No.	Reference	Description
/N9/	EN 60529:1991/A1:2000/ A2:2013	Degrees of protection provided by enclosures (IP Code)

Table 7: IP Code testing

3.4.2 Electromagnetic compatibility

No.	Reference	Description
/N10/	IEC 61000-6-7: 2015	Electromagnetic compatibility (EMC) – Part 6-7: Generic standards – Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations

Table 8: Electromagnetic compatibility

3.5 Safety information in the product documentation (safety manual, operating instructions)

No.	Reference	Description
/N11/	IEC 62061:2005/A2:2015 (SIL CL 3)	Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
/N12/	EN ISO 13849-1:2015 (PL e, Cat. 4)	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design
/N13/	IEC 61508-2: 2010	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

Table 9: Safety information

4 Documents provided for testing of TREI 5B-04

4.1 System level

No.	Title	Document number / ID	Rev.	Date
/D1/	Safety Plan and V&V Plan	PSP 30_06_16.pdf	1.2	30.06.2016
/D2/	Safety Requirements Specification (SRS)	SRS.doc	3.1	14.09.2016
/D3/	Requirement Specification	R1.doc	8.1	12.09.2016
/D4/	Design PLC TREI-5B-04	Design 18_04_2017 eng.doc	8.1	18.04.2017
/D5/	System-FMEA - M401E	SystemFMEA__M401E 29_06_16.pdf	1.1	29.06.2016
/D6/	System-FMEA - M445A	SystemFMEA_M445A 29_06_16.pdf	1.1	29.06.2016
/D7/	System-FMEA - M451O	SystemFMEA_M451O 29_06_16.pdf	1.1	29.06.2016
/D8/	System-FMEA - M452D	SystemFMEA__M452D 29_06_16.pdf	1.1	29.06.2016
/D9/	Qualification of development tools	SWDevelopmentTools_ eng 14_03_2017.docx	1.1	14.03.2017
/D10/	System Validation report	PROTOCOL on testing for compliance with the requirements R1.PDF	1.0	30.03.2017

Table 10: Documentation system level

4.2 HW level

No.	Title	Document number / ID	Rev.	Date
/D11/	Architecture Description	ArhitectureHW.pdf	3.1	18.09.2016
/D12/	Design M401E	FBD.vsd	2.0	27.03.2017
/D13/	Circuit diagram M401E	FBD M401E.pdf	2.0	27.03.2017
/D14/	Component List M401E	PAZ-MASTER history.xls	2.0	06.07.2017
/D15/	Layout M401E	PAZ-MASTER.PDF	2.0	06.07.2017
/D16/	Design M445A	FBD AI 12_04_17.vsd	6.0	12.04.2017
/D17/	Circuit diagram M445A	FBD AI.PDF	6.0	12.04.2017
/D18/	Component List M445A	PAZAI16 history.xls	6.0	12.04.2017
/D19/	Layout M445A	PAZ16AI.PDF	6.0	12.04.2017
/D20/	Design M451O	FBD DO.vsd	5.0	12.04.2017
/D21/	Circuit diagram M451O	PAZ32DO.PDF	5.0	12.04.2017

No.	Title	Document number / ID	Rev.	Date
/D22/	Component List M451O	PAZ32DO history.xls	5.0	12.04.2017
/D23/	Layout M451O	PAZ32DO.PDF	5.0	12.04.2017
/D24/	Design M452D	FBD DI 12_04_17.vsd	3.0	12.04.2017
/D25/	Circuit diagram M452D	FBD DI.pdf	3.1	20.10.2016
/D26/	Component List M452D	PAZ32DI history.xls	3.1	20.10.2016
/D27/	Layout M452D	PAZ32DI.PDF	3.1	24.06.2016
/D28/	Block FMEDA	block_fmeda_TREI-5B-04_Modul_20170716.xlsx	1.1	16.07.2017

Table 11: Documentation HW level

4.3 SW level

No.	Title	Document number / ID	Rev.	Date
/D29/	Architecture M401E	Algorithm M401E Com-Controller eng.vsd	1.1	05.06.2017
/D30/	Architecture M445A	Algorithm M445A.vsd	4.0	05.06.2017
/D31/	Architecture M451O	Algorithm M451O.vsd	3.0	16.03.2017
/D32/	Architecture M452D	Algorithm M452D.vsd	2.0	07.03.2017
/D33/	SW Design M401E	Software design M401E eng.docx	1.1	23.06.2017
/D34/	SW Design M445A	Software design M445a eng.docx	1.1	08.06.2017
/D35/	SW Design M452D	Software design M452D eng.docx	1.1	08.06.2017
/D36/	Source Code Listing M401E	Listing M401E ComCon-troller eng.docx	1.1	27.06.2017
/D37/	Source Code Listing M445A	Listing_M445A eng.docx	1.1	08.06.2017
/D38/	Source Code Listing M452D	Listing M452D eng.docx	1.1	08.06.2017
/D39/	Design- and coding guidelines for SW	SWCodingGuidelines eng 16_03_2017.doc	2.1	16.03.2017

Table 12: Documentation SW level

4.4 Tests and Manual

No.	Title	Document number / ID	Rev.	Date
/D40/	Test Protocol	Protocol 29 06 17 eng.doc	1.0	29.06.2017

No.	Title	Document number / ID	Rev.	Date
/D41/	SW Test	Protocol of testing SW (Eng).doc	1.0	01.06.2017
/D42/	Tested Modules	PLC TREI.doc	1.0	11.07.2017
/D43/	User manual with respective safety references	TREI-5B-04_M400_User_ Manual_v1.5_en.pdf	1.5	20.07.2017
/D44/	Functional Safety Manual TREI-5B-04	Functional Safety Manual PLC TREI-5B-04.docx	1.1	06.07.2017
/D45/	Unimod Pro Engineering System	Unimod PRO User Manual english.PDF	1.1	05.07.2017
/D46/	Requirements tracking	PROTOCOL on testing for compliance with the requirements R1.PDF	1.0	30.03.2017

Table 13: Documentation Tests and Manual

5 Performance and result of tests

5.1 Test reports

The following test reports were issued by TÜV SÜD Rail GmbH or other accredited test laboratories.

No.	Title	Document number / ID	Rev.	Date
[R1]	Minutes of Meeting	Meeting TREI 2016 May V1 0.pdf	1.0	11.05.2016
[R2]	Minutes of Meeting	Meeting TREI 2017 July V1 0.pdf	1.0	12.07.2017
[R3]	Review protocol on System	Review_System_V1_3.pdf	1.3	14.07.2017
[R4]	Review protocol on HW	Review_HW_V1_1.pdf	1.1	14.07.2017
[R5]	Review protocol on SW	Review_SW_V1_1.pdf	1.1	14.07.2017
[R6]	Review protocol on Test and User Manual	Review_Test_and_Manual_V1_0.pdf	1.0	20.07.2017
[R7]	Report on HW and SW FIT[2]	HW_and_SW_FIT_Report.pdf	1.0	11.07.2017
[R8]	Checklist according to IEC 61508, part 1 (FSM)	Checklist IEC 61508-1 FSM.pdf	1.0	12.07.2017
[R9]	Checklist according to IEC 61508, part 2 (Hardware)	Checklist IEC 61508-2 Hardware.pdf	1.0	12.07.2017
[R10]	Checklist according to IEC 61508, part 3 (Software)	Checklist IEC 61508-3 Software.pdf	1.0	12.07.2017
[R11]	Checklist according to EN ISO 13849-1	Checklist EN ISO 13849-1.pdf	1.0	13.07.2017
[R12]	Checklist according to IEC 62061	Checklist IEC 62061.pdf	1.0	13.07.2017
[R13]	Checklist according to IEC 61010-1	ES_717513117.pdf	1.0	21.07.2017
[R14]	Checklist IEC 61508 Manual	Checklist IEC 61508 Manual.pdf	1.0	21.07.2017
[R15]	Checklist ISO 13849-1 Manual	Checklist ISO 13849-1 Manual.pdf	1.0	21.07.2017
[R16]	Checklist according to EN 61131-2	Checklist IEC 61131-2.docx	1.0	25.07.2017

Table 14: Test reports

[2] Fault Insertion Test

6 Functional Safety Management and Lifecycle Audit

A functional safety management and lifecycle audit was executed to evaluate the management and technical activities during the overall, E/E/PES and software safety lifecycle phases which are necessary for the achievement of the required functional safety of the E/E/PES safety-related systems. The involved parties and activities are described in /D1/.

Result:

The analysis of the organization and procedures of JSC TREI has shown that the requirements specified in checklists [R8] for SIL 3 according to IEC 61508 (see /N3/ to /N6/) are covered.

7 Lifecycle activities

7.1 Common

Relevant activities to ensure a compliant development of functional safety shall be in place. The phases relevant for E/E/PE Systems are focused on the realization phase of hardware and software development, in particular specification, planning of validation, design and development, hardware & software integration, operation & user instruction as well as validation activities.

The activities to fulfill these requirements are described in clause 4.1, /D1/ to /D10/.

Result:

The generated specification, implementation and validation activities have been assessed during a lifecycle audit, see [R8].

7.2 System requirement specification

The system is specified based on the required risk reduction level. A risk analysis has not been conducted as the required risk reduction level is derived from customer's needs. Requirements to safety functions, environmental conditions, EMC and application specific needs have been addressed, see /D2/, /D11/ and /D29/.

Result:

The system requirement specification has been assessed to comply to the requirements according to target risk reduction level. The details are given in the protocol [R3].

7.3 Validation planning of the safety of the TREI 5B-04

All relevant validation activities have to be planned prior to the start of development to assure that all requirements can be tested against their specification. The V&V planning is documented in /D1/.

Result:

The review of the V&V planning activities is documented in [R3], all specified requirements are addressed to be validated.

7.3.1 Hardware design

The HW architecture fulfils the requirements to the addressed risk reduction level, the E/E/PE System incorporates a dual channel architecture, see /D11/.

The reliability of the E/E/PE System is analyzed on component level, see /D28/.

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

Module	PFH [h^{-1}]	SFF	$MTTF_D$ [years]	DC [%]	CAT	PL
M401E (1oo2-A)	1,3728E-08	99%	High	High	4	e
TPPWR (1oo2-A)	5,7214E-09	99%	High	High	4	e
M445A (1oo2-A)	7,2993E-09	99%	High	High	4	e
TPAI (1oo2)	2,3694E-09	99%	High	High	4	e
M452D (1oo2-A)	7,9841E-09	99%	High	High	4	e
TPDI (1oo1)	1,3960E-09	99%	High	High	3	d
M451O (1oo2-A)	7,6332E-09	99%	High	High	4	e
TPDO (1oo1)	0,00	100%	High	High	3	d
CR IO (1oo1)	1,1191E-08	99%	High	High	3	d
CR M (1oo1)	1,0702E-08	99%	High	High	3	d

Table 15: Probabilistic data

Result:

The review of the probabilistic calculation as well as fault insertion testing showed that the system fulfils the targeted risk reduction level, see protocols [R4] and FIT report [R7]

7.3.2 Software design

The architecture of the firmware fulfils the requirements addressed by the specification, see clause 4.3, /D29/ to /D39/.

Result:

The firmware architecture is diverse. The results of each channel are exchanged between the processors at certain stages of the execution. Failures in execution of the code are revealed by the implemented safety measures; see [R5].

7.3.3 Support tool chain

The support tools used shall be judged to have an impact on the safety of the E/E/PE System. The qualification and classification of the tools is according to the classes T1, T2 and T3, impact of failures caused by the tools used is judged in the tool qualification report /D9/.

Result:

The support tools used for the development are controlled by the implemented configuration management. The review of the tool qualification report is documented in [R3].

7.3.4 Engineering System development

The Engineering system Unimod Pro is one essential part of the overall system to develop, simulate, download and maintain the application software SRASW of the machine. Unimod Pro provides measures as CRC checking, read-back of download and independent confirmation routines to safely download the correct application to the safety controller system, see /D45/ for details.

Result:

The engineering system provides measures to safely download the engineered application to the safety controller. Measures have been met to safely download the correct application to the designated safety controller, see [R5].

7.4 System integration

System integration test shall proof that the internal interfaces between single modules as well as external interfaces to the overall system interact as specified. The hardware and software integration planning is documented in /D1/.

Result:

Based on module test concept and system integration testing the system complies to the specification, see protocol [R3].

7.5 System operation and maintenance

The operation and commissioning activities as well as the maintenance activities necessary to assure the safety of the system is described in the user documentation, see /D43/ and /D44/.

Result:

All requirements addressed to the user, implementer and operator are described in the user documentation, see [R6].

7.6 System safety validation

System safety validation shall confirm that the safety functions are implemented as specified. The validation activities have been assessed at appropriate stages of the development, the overall result is collected in /D10/.

Result:

The system validation report /D10/ shows that all requirements specified in /D2/ are implemented and tested against the specification. The result of the review is documented in [R3].

7.6.1 Environmental conditions, electrical stress test and EMC

The system shall withstand the specified environmental conditions as listed in /D2/. EMC test procedures to meet requirements (increased test levels) of functional safety have been addressed in the test plan, see /D1/.

Result:

The test against environmental conditions is performed in accredited test labs, see reports /D40/, the summary of the reports is documented in [R6].

7.6.2 Functional testing against specification

The system functional test shall confirm that the E/E/PE System functions as specified in the system requirements specification, /D2/.

Result:

The system is tested against its specification in several phases of the life cycle. All test as specified in the V&V plan have been reviewed, for system functional testing see protocols [R6] and [R7].

7.6.3 Documentation

The user documentation addresses requirements for the installation, commissioning and operation of the system, see user documentation /D43/ and /D44/.

Result:

All requirements addressed to the manual are implemented, see review [R6].

7.7 System modification

To modify the system, applicable phases of the lifecycle have to be considered, this is described in the safety plan, /D1/.

Result:

As the system is a newly developed system, this clause is not applicable.

7.8 System verification

The system shall be verified against the specification to confirm that all specified requirements have been correctly implemented. This is shown by several test reports listed in clause 4 and specially tracked by requirements tracking table /D46/.

Result:

The review of test reports as listed in the previous clauses showed that the system behaves as specified. The completeness of implementation of all requirements is confirmed in the protocol [R6].

8 Functional safety assessment

The development of the safety system TREI 5B-04 is assessed at appropriate stages of the lifecycle either by internal reviews or in conjunction with TÜV SÜD Rail GmbH. The independence of internal reviews of parties involved is shown in the safety plan /D1/.

Result:

Where applicable, internal reviews have been reviewed for independence and completeness, lifecycle assessments related to functional safety have been conducted with external test laboratory TÜV SÜD Rail GmbH, see checklists [R8] to [R12].

9 Summary

The test results of clause 5 showed that the ToE, as specified in clause 2.1, fulfils the requirements of clause 3 and the related standards and guidelines.

Technical Certifier

Günter Greil

Project Manager

Franz Seika