Choose certainty.
Add value.

Technical report

of the

Type testing

Software Tool for Safety Related Development SIMATIC Automation Tool

Applicant

Siemens AG

Gleiwitzer Str. 555
90475 Nürnberg
Germany

Manufacturer

Siemens AG

Östliche Rheinbrückenstraße 50
76187 Karlsruhe
Germany

Report No.: SJ91567T
Version 1.1 of 2018-05-17

Test Body

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

This report may be represented only in complete wording. The use for promotion needs written permission. It 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 agency.

Table of Contents page

1 Target of Evaluation (ToE) 3

2 Scope of Testing 4

2.1 Test specimen 4

2.2 Nomenclature of SIMATIC Automation Tool 4

2.3 Tests 5

3 Standards and guidelines 5

3.1 Functional safety 5

3.2 Susceptibility to environmental errors 5

3.3 Safety information in the product documentation (safety manual, operating instructions) 6

4 Documents provided for testing of SIMATIC Automation Tool 6

4.1 Product level 6

4.2 Tests and Manual 7

5 Performance and result of tests 8

5.1 Test reports 8

6 Functional Safety Management and Lifecycle Audit 8

6.1 Validation planning of the safety of the SIMATIC Automation Tool 8

6.2 Product design and development of SIMATIC Automation Tool 8

6.2.1 Software design 8

6.2.2 Engineering System – Application development 9

6.3 Product integration 9

6.4 Product operation and maintenance 9

6.5 Product safety validation 9

6.6 Product modification 9

6.7 Product verification 10

7 Functional safety assessment 10

8 Summary 11

List of tables page

Table 1: Revision history 3

Table 2: Abbreviations 3

Table 3: Identification of SIMATIC Automation Tool 5

Table 4: Functional safety 5

Table 5: Safety information 6

Table 6: Documentation product level 7
Table 7: Documentation Tests and Manual 7
Table 8: Test reports 8

List of figures page

Figure 1: Product overview of SIMATIC Automation Tool 4

Revision history

Revision	Status	Date	Author	Modification / Description
1.0	Active	2017-10-26	P. Weiß	Released
1.1	Active	2018-05-17	P. Weiß	Chapter 1, 4, 5.1, and 7.1

Table 1: Revision history

List of abbreviations

Abbreviation	Description
SAT	SIMATIC Automation Tool

Table 2: Abbreviations

1 Target of Evaluation (ToE)

On 2017-04-24 Siemens AG requested TÜV SÜD Rail GmbH to test and certify the SIMATIC Automation Tool according to the standard listed in clause 3 of this report. The project numbers related to this technical report are 717513580 and 717515765.

In March 2018 Siemens AG requested TÜV SÜD Rail GmbH to test and certify the new version of the SIMATIC Automation Tool. The project number to this modification is 717515765.

2 Scope of Testing

2.1 Test specimen

The SIMATIC Automation Tool is a PC based software application that is able to operate, configure, and control a variety of Siemens S7Plus series products including S7-1200 and S7-1500 fail-safe CPUs.

A limited number of operations initiated by this tool have been deemed to have safety relevance. Only components listed in the annex to the report of the certificate are supported by the tool. All these possible safety relevant operations are shown below:

- Reset-to-Factory
- Restore from Backup
- Program Update
- Format Memory Card

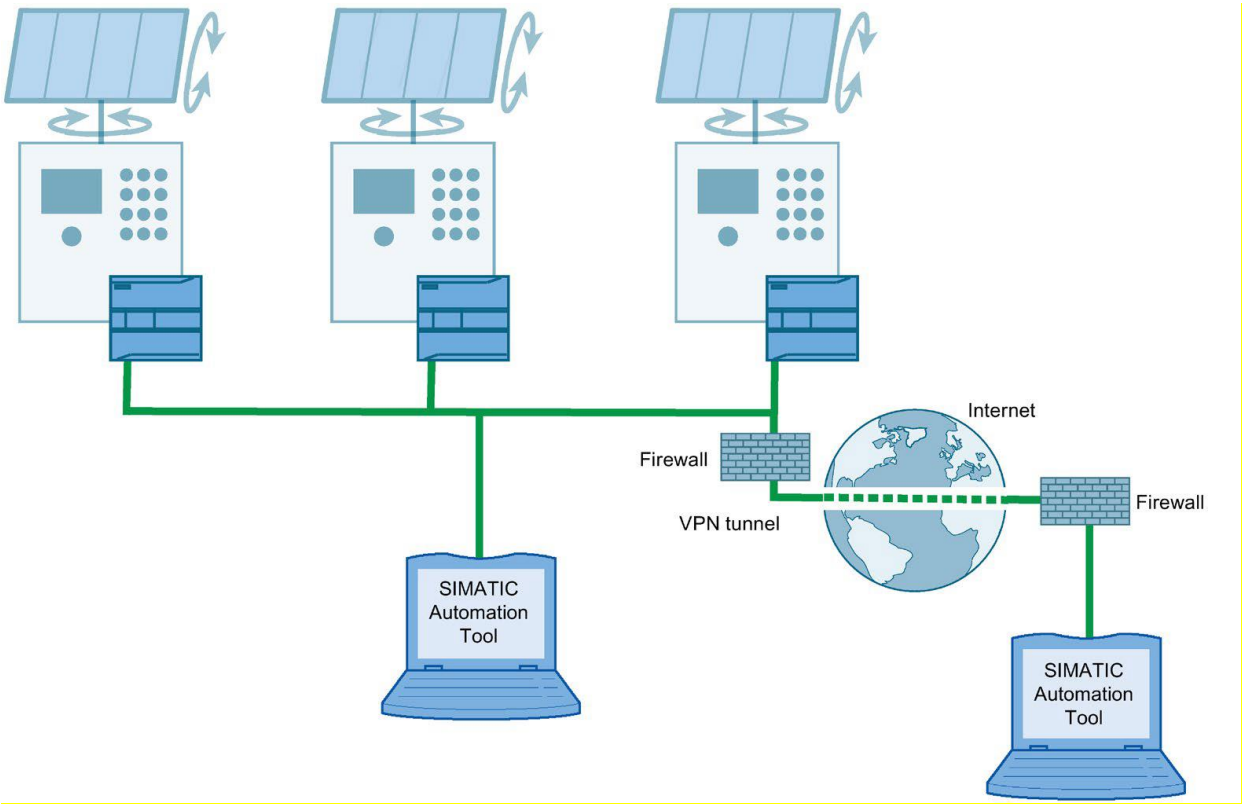

Figure 1: Product overview of SIMATIC Automation Tool

2.2 Nomenclature of SIMATIC Automation Tool

The SIMATIC Automation Tool tested is identified by software version as follows:

Name	
SIMATIC Automation Tool V3.1, build number V03.01.01.00_08.13.00.01	see annex SJ91567C-A

Table 3: Identification of SIMATIC Automation Tool

2.3 Tests

The SIMATIC Automation Tool was examined with regard to the following testing operations:

I. Functional Safety including
   - Functional safety management (FSM) und safety lifecycle
   - Analysis of the software
   - Error simulations and software tests
   - Test of the error prevention measures
   - Functional tests

II. Safety information in the product documentation (safety manual, user manual, installation and operating instructions).

3 Standards and guidelines

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

3.1 Functional safety

No.	Reference	Description
/N1/	IEC 61508-1:2010 (SIL 3)	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements
/N2/	IEC 61508-3:2010 (SIL 3)	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements
/N3/	IEC 61508-4:2010 (SIL 3)	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations
/N4/	IEC 62061:2005/A2:2015 (SIL CL 3)	Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems
/N5/	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 4: Functional safety

3.2 Susceptibility to environmental errors

Not applicable for a tool.

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

No.	Reference	Description
/N6/	EN ISO 13849-1:2015 (PL e, Cat. 4)	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design
/N7/	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 5: Safety information

4 Documents provided for testing of SIMATIC Automation Tool

4.1 Product level

No.	Title	Document number / ID	Rev.	Date
/D1/	FSM Plan	FSM_SIMATIC_Automation_Tool_V1_01R	1.01	2017-08-18
/D2/	Configuration Management plan	CM_Plan_Simatic_Automation_Tool	1.1	2017-09-28
/D3/	Safety Requirement Spec.	Safety_Requirements_SIMATIC_Automation_Tool_V102R	1.02	14-06-2017
/D4/	API Specification	API_Specification_SIMATIC_Automation_Tool_V3_1_1	3.1.1	2017-08-23
/D5/	Graphic User Interface V 3.1	GUI_Changes_SATV31_R1_11	1.11	2017-08-08
/D6/	SW Design Spec.	SafetySoftwareDesign_SATV31_R1_11	1.11	2017-08-14
/D7/	HAZOP Analysis	Hazard_Operability_Analysis_V1_00R.pdf	1.0	2017-08-17
/D8/	FIT Spec	SAT_FaultInsertion_Test_Specification	2.0	2017-08-23
/D9/	Integration Test Spec.	SAT_Integration_Test_Specification	2.02	2017-10-10
/D10/	SIMATIC Automation Tool	Automation-Tool_Summary	03.01.00.00_09.12.00.01	2017-10-16

No.	Title	Document number / ID	Rev.	Date
Documents related to Release 3.1 SP1				
/D11/	Change Request	ChangeRequestForm	001	05-02-2018
/D12/	CM-Plan	CMPlan	1.2	06-12-2017
/D13/	Functional Safety Management Plan	FSM	1.2	21.02.2018
/D14/	Safety Requirements Specification	SRS	1.3	21.02.2018
/D15/	Programming API Specification	APISpecification	3.2	16.03.2018
/D16/	Feature Specification: GUI changes for V3.1 SP1	GUIChanges	1.2	27.03.2018
/D17/	Fault Insertion Test Specification	FaultInsertionTestSpecification	2.1	05.03.2018
/D18/	Safety Integration Test Specification	SafetyIntegration-TestSpecification	2.4	15.05.2018

Table 6: Documentation product level

4.2 Tests and Manual

No.	Title	Document number / ID	Rev.	Date
/D19/	FIT Report	SAT_FaultInsertion_Test_Report_V1_04	2.01	2017-10-17
/D20/	Integration Test Report	SAT_Integration_Test_Report_V1_10	2.03	2017-10-17
/D21/	Manual	simatic_automationtoolusergui de_V3_1_201710_en-US	-	2017/09
/D22/	Static Code Analysis	StaticCodeAnalysis	1.0.1	2017-09-29
Documents related to Release 3.1 SP1				
/D23/	S7/HMI SIMATIC Automation Tool V3.1 SP1 User Guide	simatic_automationtoolusergui de	A5E4361 6265-AA	05/2018
/D24/	Fault Insertion Test Report	FaultInsertionTestReport	2.2	03.05.2018
/D25/	Safety Integrity Test Report	SafetyIntegration-TestReport	2.5	15.05.2018

Table 7: 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]	Review protocol	Review Protocol	1.4	19.10.2017
[R2]	Checklist	Tool Checkliste IEC 61508	1.0	16.10.2017
Documents related to Release 3.1 SP1				
[R3]	Review protocol	Review Protocol	1.3	17.05.2018

Table 8: Test reports

6 Functional Safety Management and Lifecycle Audit

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

Result:

The analysis of the organization and procedures of Siemens AG has shown that the requirements for SIL 3 according to IEC 61508 (see /N1/ to /N3/) are covered, see [R2].

6.1 Validation planning of the safety of the SIMATIC Automation Tool

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 [R1], all specified requirements are addressed to be validated.

6.2 Product design and development of SIMATIC Automation Tool

The SIMATIC Automation Tool incorporates means to fulfill the required risk reduction level.

6.2.1 Software design

The architecture of the software fulfils the requirements addressed by the specification, see /D6/ and /D20/.

Result:

The software architecture is described in separate charts for each functionality via flow diagrams. A HAZOP (see /D7/) has been performed by Siemens AG and reviewed by TÜV SÜD Rail GmbH (see [R1]), to analyze the software design and the related safety measures.

6.2.2 Engineering System – Application development

The engineering system is already certified, see related references in the safety manual.

6.3 Product integration

Product integration test shall prove that the internal interfaces for the different functionalities as well as external interfaces to the overall system interact as specified. The hardware and software integration planning is documented in /D8/ and /D9/.

Result:

Based on test concept and product integration testing the SIMATIC Automation Tool complies to the specification, see protocol /D20/

6.4 Product operation and maintenance

The operation and commissioning activities as well as the maintenance activities necessary to assure the safety of the SIMATIC Automation Tool is described in the user documentation, see /D21/.

Result:

All requirements addressed to the user and implementer are described in the user documentation, see [R1].

6.5 Product safety validation

Product 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 [R1].

The product functional test shall confirm that the product functions as specified in the safety requirements specification, see /D3/ have been realized.

Result:

The product is tested against its specification in several phases of the life cycle. All tests as specified in the V&V plan have been performed and reviewed, see protocol [R1] and test reports /D19/ and /D20/.

6.6 Product modification

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

Result:

The modification procedure has been explained in more detail by Siemens AG, see [R2].

6.7 Product verification

The product 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 in /D21/.

Result:

The review of test reports as listed in the previous clauses showed that the product behaves as specified. The completeness of implementation of all requirements is confirmed in the protocols /D19/ and /D20/.

7 Functional safety assessment

The development of the SIMATIC Automation Tool 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, /D2/.

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 checklist [R2].

7.1 SAT Release 3.1 SP1

The modification in the non-safety related code (see /D11/) of the SIMATIC Automation Tool has been documented realized and tested (see /D11/ to /D18/ and /D23/ to /D25/) by Siemens AG.

Result:

The review of the documents as listed above showed that the modified product behaves as specified. The completeness of implementation of all requirements is confirmed in the protocols /D24/, /D25/, see [R3].

8 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

Digital unterschrieben von Christian Dirmeier
Datum: 2018.05.22 16:00:38 +02'00'

C. Dirmeier

Project Manager

Digital unterschrieben von Peter Weiß
Datum: 2018.05.22 12:54:12 +02'00'

P. Weiß