Choose certainty.
Add value.

Technical report

of the

Type testing

of the Configuration Environment SLS

Applicant

Siemens AG

Gleiwitzer Straße 555

D-90475 Nürnberg

Germany

Manufacturer

Siemens AG

Report no. SN84689T

Revision: 1.3, Date 2018-05-22

Test body

TÜV SÜD Rail GmbH
Rail Automation

Barthstraße 16
D-80339 Munich

Revision history

Revision	Date	Author	Status	Modifications
0.1	2012-11-28	P. Weiß	Initial	-
0.5	2012-12-18	P. Weiß	Ongoing	Test Report included
0.9	2013-02-21	P. Weiß	Ongoing	Chapter 4 and 5 updated
1.0	2013-03-06	P. Weiß	Final	Chapter 4 and Chapter 5.4
1.1	2016-05-24	F. Seika	Update	Migration to STEP 7 V13, S7-1500 and ET 200MP
1.2	2018-05-17	P. Weiß	Update	Modified concept Updated standard IEC 62061 Chapter 1, 3.1, 4, 5.1, and 6
1.3	2018-05-22	P. Weiß	Update	Table 4: Document-No./ File identifier of [D7] corrected

Table 1: Revision history

Content

List of Tables

List of Figures

1 Target of Evaluation (ToE)

On July 2012 Siemens AG requested TÜV SÜD Rail GmbH to test and certify the Configuration Environment SLS from Siemens AG. The Project No. related to this Technical Report was as follows: 717506369.

On March 2016 Siemens AG requested TÜV SÜD Rail GmbH to test and certify the modifications related to the migration of the environment to STEP 7 V13, S7-1500 and ET 200MP. The Project No. related to this was as follows: 717512386.

On April 2018 Siemens AG requested TÜV SÜD Rail GmbH to test and certify the modification of the Configuration Environment SLS. The Project No. related to this modification was as follows: 717516806.

The ToE is a Configuration Environment within the SIMATIC families. The non-safety related HMI shall be used to configure safety related electrical drive systems.

2 Scope of Testing

2.1 Test specimen

The safety related configuration shall be performed via the non-safety related HMI and the safety related F-CPU. The configured safely limited speed values will be provided from the HMI and verified before downloading. After configuration the connected drive system shall operate with these SLS values, as shown in Figure 1.

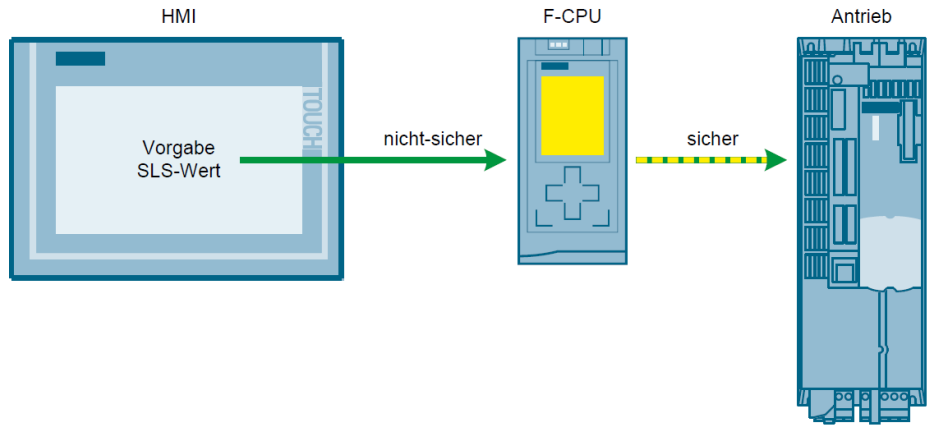

Figure 1: Overview of the Configuration Environment SLS

The basic functionality of the Configuration Environment SLS is depicted in Figure 2.

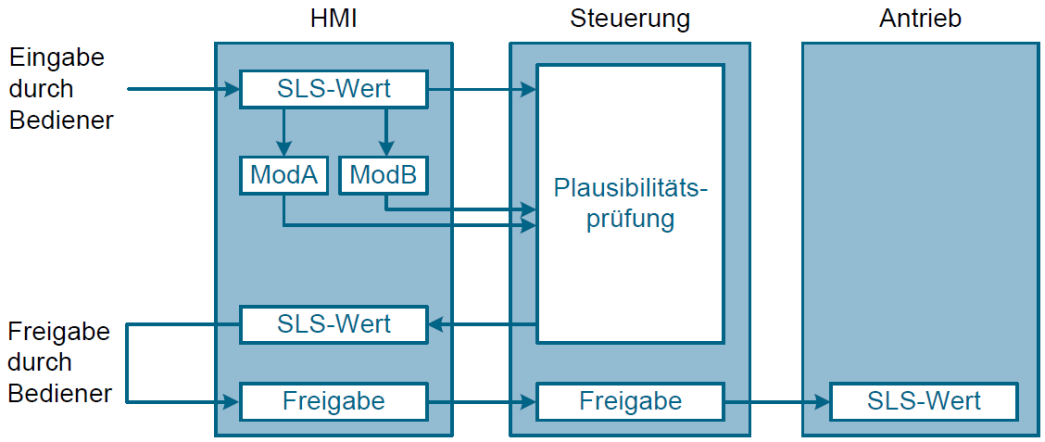

Figure 2: Basic functionality of the SLS

2.1.1 Nomenclature of SLS

The following terms are used in this report with a meaning defined as follows:

F-CPU	Safety related CPU of the certified SIMATIC S7 Safety System
F-Program	Safety related programmed user application
HMI	Human Machine Interface
SLS	Safely Limited Speed

Table 2: Nomenclature

2.2 Tests

The Configuration Environment SLS were examined with regard to the following testing operations:

I. Functional safety including
- Analysis of the architecture (System-FMEA)
- Analysis of the fault detection measure
- Analysis of the error prevention measures
- Review of documented functional tests

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

3 Basis of Testing

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

3.1 Functional safety

No.	Standard	Title
[N1]	IEC 62061: 2015	Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems
[N2]	EN ISO 13849-1: 2015	Safety of machinery - Safety-related parts of control systems Part 1: General principles for design

Table 3: Functional safety

4 Documents provided for testing of SLS

Following documents were provided by Siemens AG to be checked and evaluated by the test house.

No.	Title	Document-No./ File identifier	Revision	Date
[D1]	Vorgabe von Grenzwerten für Sichere Geschwindigkeit (SLS) von einem nicht-sicherem HMI	67634251_SLS_over_HMI_DOC_V20_de	-	02/2013
[D2]	Systemtestprotokoll	Systemtestproto-koll_SLS_over_HMI_V10	-	2013-02-08
[D3]	Systemtestprotokoll	Systemtestproto-koll_inkl_Nachtrag		2013-03-06
Modification: Migration to STEP 7 V13				
[D4]	Vorgabe von Grenzwerten für Sichere Geschwindigkeit (SLS) von einem nicht-sicherem HMI	67634251_SLS_over_HMI_DOC_V20_de	2.0	05/2016
[D5]	Systemtestprotokoll	Systemtestproto-koll_SLS_over_HMI_V11	1.0	2016-01-08
[D6]	Einflussanalyse der Änderungen am Sicherheitskonzept	67634251_SLS_over_HMI_Einflussanalyse_V10	1.0	2016-04-08
Modification: Modified concept and updated standard IEC 62061				
[D7]	Vorgabe von Grenzwerten für Sichere Geschwindigkeit (SLS) von einem nicht-sicherem HMI	67634251_SLS_over_HMI_DOC_V30_de	3.0	03/2018

No.	Title	Document-No./ File identifier	Revision	Date
[D8]	Funktionstestprotokoll	67634251_SLS_over_HMI _DOC_V30_FunctionTest	3.0	15.03.2018

Table 4: Documentation

5 Performance and result of tests

5.1 Test reports

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

No.	Title	Document-No./ File identifier	Revision	Date
[R1]	Review Report	Review_SLS_HMI	1.3	2013-02-21
[R2]	Review Report System Test	Review_Systemtest	1.2	2013-03-06
Modification: Migration to STEP 7 V13				
[R3]	Review Report - Checklist	Review_SLS_HMI_Checklist_1.0	1.0	2016-04-26
[R4]	Review Report - Documents	Review_SLS_HMI_Dokumente_1.1	1.1	2016-05-24
Modification: Modified concept and updated standard IEC 62061				
[R5]	Review Protocol	Review Protocol	1.1	2018-05-17
[R6]	Checklist for safety of machinery Conformity evaluation according IEC 62061-A2:2015	IEC 62061	1.0	2018-04-19

Table 5: Test results

5.2 Project Management

The project specific activities for the Configuration Environment SLS have been identified and documented see [D1].

Result:

The relevant requirements for the Configuration Environment have been identified and verified, see [R1].

5.3 System Failure Mode and Effects Analysis (System-FMEA)

The Configuration Environment SLS consist of safety related and non-safety related components. Fault detection is assured by means of following basic techniques:

- Redundant transmission of SLS value (ModA / ModB)
- Plausibility Check of redundant SLS values within the safety component
- Confirmation of SLS values from the user

In case of a detected failure an error message will be announced to the user. As a result, the re-configuration of SLS values will not be accepted and the drive system is still relying on the original stored values.

Result:

The system- and function block FMEA as depicted in the document [D1] was made by Siemens AG and reviewed by TÜV SÜD Rail GmbH. The results of this FMEA for the Configuration Environment meet the requirements according to [N1] and [N2]. The result is recorded in [R1].

5.4 Qualitative Analysis and Fault Simulations (FIT)

All function-related faults in components or component groups were examined to assess their effects on the safe functioning of the configuration environment.

Practical fault simulations were carried out by Siemens AG to provide subsequent evaluation of the knowledge obtained from the theoretical failure mode and effect analysis. The performances of these fault simulations provide information on the fail-safe characteristics of the configuration environment.

The documented results of these faults were compared with the required characteristics which had been stipulated in the theoretical failure mode and effect analysis for the fault detection mechanisms and the fault reaction.

Result

All fault models according to [N1] and [N2] were covered. The FMEA [D1], the FIT [D2] and the impact analysis [D6] demonstrated that the safety concept of the Configuration Environment meets the requirements of the standards listed in clause 3 of this Technical Report.

The results of the fault insertion tests have been reviewed [R2] and are documented in the test report [D2].

5.5 Software evaluation

The safety related software of the Configuration Environment is related to the identified safety measures derived from the FMEA. This software is realized via the already certified library elements within the F-program.

The Configuration Environment SLS shall be realized with “key switch” verification in the F-Program see [D1].

5.5.1 Realization of the software

The F-Program part related to the safety measures of the configuration environment has been engineered and realized for an F-CPU using the required programming environment of the safety system.

5.5.2 Software tests

Based on the above mentioned FMEA (see chapter 5.3) the software within the F-Program as documented in [D1] has been tested.

Result:

The performed Software tests as indicated in test [D2] did not result in any deviations from the anticipated results.

5.6 Electrical Safety

Not applicable for configuration environment.

5.7 Climatic stress tests

Not applicable for configuration environment.

5.8 Mechanical stress tests

Not applicable for configuration environment.

5.9 Electrical stress tests

Not applicable for configuration environment.

5.10 Testing of the noise immunity

Not applicable for configuration environment.

5.11 Testing of the noise emission

Not applicable for configuration environment.

5.12 Verification of the degree of protection

Not applicable for configuration environment.

5.13 Inspection of the technical documentation

The user manual [D1] was examined to verify the completeness of the technical documentation.

Result:

The results are documented in report [R1].

The technical documentation fulfils the requirements in accordance with the required standards.

6 Modification

6.1 Migration to STEP 7 V13

The modification described in [D6] has been realized according to the test basis.

Result:

The updated documents [D4] and [D5] have been reviewed, see [R4]. In addition, the test basis has been updated, see [R3].

The modification has been carried out and the validation activities have shown that the changes did not raise any safety relevant objections.

6.2 Modified concept and updated standard IEC 62061

The modification described in [D7] has been realized according to the test basis.

Result:

The updated documents including testing have been reviewed (see [R5]) and the product compliance to the updated standards has been checked too, see [R6].

7 Application Conditions

The configuration environment SIMATIC SLS with HMI can be used for safety related applications if the following items are met:

- The application example documented in [D1] shall be included into the F-Program without safety related modifications
- The manual [D1] with its references has to be applied
- The final F-Program shall be evaluated, verified, and validated in accordance to the application standards

  Remark: The evaluation, verification, and validation of the F-Program shall include all safety functions, although those defined and identified for the configuration environment.

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, if the above mentioned application conditions (see chapter 6) are met. Therefore the Configuration Environment SLS can be used for applications in accordance to IEC 62061 up to SIL 3 and in accordance to ISO 13849 up to Cat 4 PL e.

Technical Certifier

Digital unterschrieben von Peter Weiß
Datum: 2018.05.22 09:38:31 +02'00'

P. Weiß

Project Manager

Digital unterschrieben von Franz Seika
Datum: 2018.05.22 09:45:35 +02'00'

F. Seika