Choose certainty.
Add value.

Report

to the

Certificate

Z10 078930 0003 Rev. 00

Software tool for safety-related development

TESSY

Manufacturer
Razorcat Development GmbH
Witzlebenplatz 4
D-14057 Berlin

Report no. RB 84018 C
Revision: 1.6, Date 2018-08-20

Testing Body:
TÜV SÜD RAIL GmbH
Barthstraße 16
D-80339 München
Germany

Certification Body:
TÜV SÜD Product Service GmbH
Ridlerstraße 65
D-80339 München
Germany

Content

Content **2**
List of Tables **2**
List of Figures **2**
Revision history **3**
1 Purpose and Scope **4**
2 Identification **7**
3 Basis of Testing **7**
4 Scope of Testing **8**
5 Tool Classification and Qualification Requirements **8**
5.1 IEC 61508 ..... **8**
5.2 ISO 26262 ..... **8**
5.3 EN 50128 ..... **9**
5.4 IEC 62304 ..... **9**
6 Testing Results **9**
7 Conditions of Use **10**
8 Summary and Certificate Number **11**

List of Tables

Table 1: Revision history 3
Table 2: Identification 7
Table 3: Normative basis of testing 7

List of Figures

Figure 1: TESSY Core Workflow 4

Revision history

Revision	Date	Author	Status	Modifications
1.0	2011-12-07	K. Leupold	-	initial
1.1	2013-05-16	J. Dong	-	Release 3.0.x Chapter 1, 2, 6
1.2	2014-06-17	J. Dong, S. Waldhausen	-	Release 3.1.x Chapter 1, 2, 6
1.3	2014-12-02	J. Dong	-	RB84018T Rev. 1.3 Chapter 1, 6
1.4	2015-06-22	W. Schlögl, S. Waldhausen	-	Release 3.2.x Chapter 1,2,6
1.5	2016-11-10	W. Schlögl	-	Release 4.0.x Chapter 1,2,6
1.6	2018-08-20	W. Schlögl	active	Release 4.1.x Chapter 1,2,3,5,6

Table 1: Revision history

1 Purpose and Scope

Contract

Razorcat Development GmbH has contracted TÜV SÜD Rail GmbH in August 2011 to perform an assessment on TESSY with respect to Functional Safety. The aim of the testing was the certification of TESSY to be suitable to be used in safety-related developments according to IEC 61508 and ISO 26262. In August 2018 the certification has been extended to also cover the railway standard EN 50128 and the medical standard IEC 62304.

System under test

TESSY provides an integrated suite for automated dynamic testing. A typical workflow using TESSY can be seen in Figure 1:

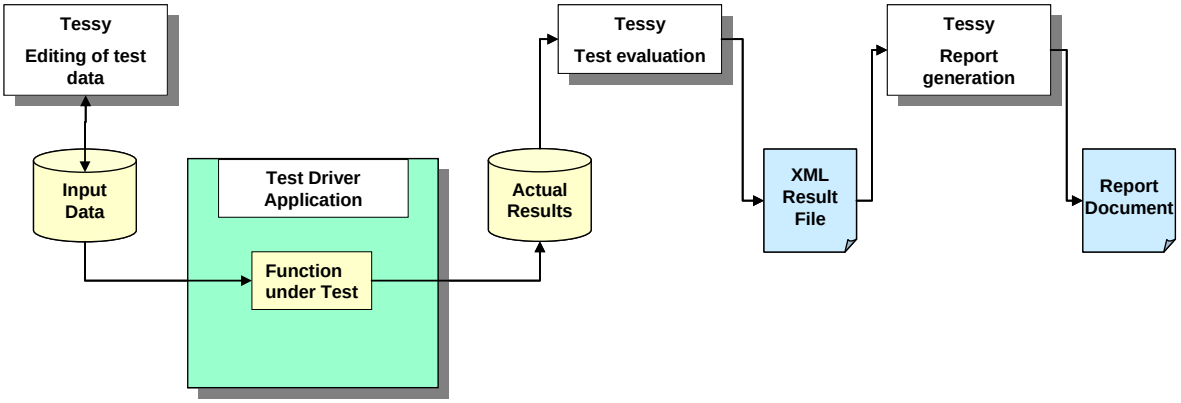

Figure 1: TESSY Core Workflow

Test scope

The following features were under investigation during this assessment:

- The construction of test harnesses in a simulated and target environment for the execution of unit tests testing single C-functions.
- The execution of test cases, along with the streaming of test data into and out of the unit under test.
- The measurement of branch coverage (C1) and MC/DC as well as MCC coverage (also referred to as C2) achieved during a unit test.
- The comparison of test results with expected values.
- The production of test reports on the operation and outcome of the tests.

Test Report

The detailed results of the testing have been documented in the Technical Report RB84018T, Rev. 1.0.

Release 3.0.x

Razorcat Development GmbH has contracted TÜV SÜD Rail GmbH in October 2012 to perform an assessment on the modification of TESSY to release 3.0.x with respect to Functional Safety.

The following features and changes were under investigation during this assessment:

- Perspective improvements
- Traceability of requirements
- Enhanced coverage handling
- Improved integration of the Classification Tree Editor (CTE)
- Enhanced component testing
- Application Programming Interface (API) and command line interface
- Reports only in PDF format

The detailed results of the testing have been documented in the Technical Report RB84018T, Rev. 1.1.

Release 3.1.x

Razorcat Development GmbH has contracted TÜV SÜD Rail GmbH in May 2014 to perform an assessment on the modification of TESSY to release 3.1.x with respect to Functional Safety.

The following features and changes were under investigation during this assessment:

- Enhanced coverage handling: statement coverage (C0), decision coverage (DC), entry point (EPC) and function coverage (FC) added
- headless mode using command line interface
- New development tools JIRA (for change request management) and Git (for version management)

The detailed results of the testing have been documented in the Technical Report RB84018T, Rev. 1.3.

Release 3.2.x

Razorcat Development GmbH has contracted TÜV SÜD Rail GmbH in May 2015 to perform an assessment on the modification of TESSY to release 3.2.x with respect to Functional Safety.

The following features and changes were under investigation during this assessment:

- Static code analysis support with PC-Lint

The detailed results of the testing have been documented in the Technical Report RB84018T, Rev. 1.4.

Release 4.0.x

Razorcat Development GmbH has contracted TÜV SÜD Rail GmbH in October 2016 to perform an assessment on the modification of TESSY to release 4.0.x with respect to Functional Safety.

The following features and changes were under investigation during this assessment:

- C++ Support
- Management of code variants
- Support of test driven development
- Optimized test execution
- Auto-reuse in command line execution
- UUIDs for TESSY objects
- Exclusion of single tests

The detailed results of the testing have been documented in the Technical Report RB84018T, Rev. 1.5.

Release 4.1.x

Razorcat Development GmbH has contracted TÜV SÜD Rail GmbH in July 2018 to perform an assessment on the modification of TESSY to release 4.1.x with respect to Functional Safety.

The following features and changes were under investigation during this assessment:

- Calculation of the McCabe metric and derived metrics
- Automated fault injection
- Introduction of a new scripting language for editing tests
- New Classification Tree Editor
- Review of test changes
- Arithmetic expressions as test data
- Stimulating and measuring of hardware signals

Additionally the certification was extended to also cover the requirements for tools from EN 50128:2011 and IEC 62304:2015.

The detailed results of the testing have been documented in the Technical Report RB84018T, Rev. 1.6.

2 Identification

The following table identifies the tool releases that have been considered for the assessment.

Software Product	Release	Standards considered for Certification			
		IEC 61508:2010	ISO 26262:2011	EN 50128:2011	IEC 62304:2015
TESSY	2.9.x	✓	✓	-	-
TESSY	3.0.x	✓	✓	-	-
TESSY	3.1.x	✓	✓	-	-
TESSY	3.2.x	✓	✓	-	-
TESSY	4.0.x	✓	✓	-	-
TESSY	4.1.x	✓	✓	✓	✓

Table 2: Identification

3 Basis of Testing

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

No.	Standard	Title
[N1]	IEC 61508-3: 2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements
[N2]	IEC 61508-4: 2010	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations
[N3]	ISO 26262-1: 2011	Road vehicles - Functional safety - Part 1: Vocabulary
[N4]	ISO 26262-2: 2011	Road vehicles - Functional safety - Part 2: Management of functional safety
[N5]	ISO 26262-6: 2011	Road vehicles - Functional safety - Part 6: Product development at the software level
[N6]	ISO 26262-8: 2011	Road vehicles - Functional safety - Part 8: Supporting processes
[N7]	EN 50128: 2011	Railway applications - Communication, signaling and processing systems Software for railway control and protection systems
[N8]	IEC 62304: 2015	Medical device software - Software life-cycle processes

Table 3: Normative basis of testing

4 Scope of Testing

The testing of TESSY comprised the following steps:

I. Functional safety
- Functional safety management,
- Analysis of the Safety Requirements Specification
- Relevant aspects of the development lifecycle:
  - Quality assurance measures
  - Modification, configuration and release management
  - Bug lifecycle procedures
- Verification and Validation procedure & results

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

5 Tool Classification and Qualification Requirements

5.1 IEC 61508

IEC 61508 demands the assessment of offline support tools (7.4.4.2).

TESSY supports the verification of source code, where errors in the tool can fail to reveal defects but cannot directly introduce errors in the executable software.

According the definitions in [N2], TESSY can be classified as an off-line software support tool of class T2.

For T2 tools, IEC 61508-3: 2010 requires that:

- The tool functionality and behavior, as well as any instructions or constraints, shall be documented.
- For T2 as well as for T3 tools, only qualified versions shall be used.

5.2 ISO 26262

The ISO 26262 standard classifies software development tools according to their tool impact (TI) and the probability of tool error detection (TD).

TESSY, being a diagnostic tool, cannot introduce errors into the application. Nevertheless, the tool impact is TI = 2, because in the case of a failure, it may mask existing errors in the code being tested. TI2 requires an estimation of the tool error detection TD on customer side.

So, tool error detection always depends – besides the tool provider – also on measures of fault avoidance and error detection on the customer side.

Depending on the applied measures of error prevention and error detection in the user development process, i.e. the applied techniques and intensity of validation activities, the resulting tool error detection can vary.
In order to achieve tool qualification for all ASIL levels, the measures

- evaluation of the development process,
- validation of the software tool

have been applied, following the requirements of ISO 26262-8.

5.3 EN 50128

EN 50128:2011 is an application standard derived from IEC 61508. The requirements for software tools are derived from the requirements on software tools according to IEC 61508-3:2010. Due to the equivalence of the requirements for software tools, no separate testing has been performed with respect to EN 50128.

The part of the audit covering the development process, quality assurance measures, verification and validation, modification and bug handling can be taken over. For SIL up to SIL 4 according to EN 50128, caveats and mitigation measures to potential failure mechanisms are described in the Safety Manual for Tessy.

5.4 IEC 62304

IEC 62304:2015 provides a framework of life cycle processes for the safe design and maintenance of medical device software. IEC 62304 does not itself place specific requirements on software tools, or on the qualification of tools, but IEC 62304 advises that “IEC 61508 can be looked to as a source of methods, tools and techniques that can be used to implement the requirements in IEC 62304” (IEC 62304:2015, C.1).

IEC 62304 requires tools to be “suitably validated” (Table C.3). The tool validation according to IEC 61508 is a main aspect of the testing described in this report. Since IEC 62304 does not define how suitable validation is achieved, but refers to IEC 61508 with respect to tools, the validation can be considered suitable also in the sense of IEC 62304, if the development process follows the safety documentation in its current version.

6 Testing Results

The assessment comprised the testing activities as given in paragraph 4. As a basis for testing, the standards given in Table 3 (paragraph 3) have been considered. The results are documented in the Technical Report RB84018T, Rev. 1.0.

The testing results related to the modification of TESSY to release 3.0.x are documented in the Technical Report RB84018T, Rev. 1.1.

The testing results related to the modification of TESSY to release 3.1.x are documented in the Technical Report RB84018T, Rev. 1.3.

The testing results related to the modification of TESSY to release 3.2.x are documented in the Technical Report RB84018T, Rev. 1.4.

The testing results related to the modification of TESSY to release 4.0.x are documented in the Technical Report RB84018T, Rev. 1.5.

The testing results related to the modification of TESSY to release 4.1.x are documented in the Technical Report RB84018T, Rev. 1.6.

I. Process audit:
   - The quality assurance procedures of Razorcat Development GmbH fulfill the requirements applicable for software tool development.
   - The modification and release management of Razorcat Development GmbH is suitable to ensure reliability and quality of the released software products.
   - Razorcat Development GmbH provides user support that allows customers to be aware of actual known bugs, bug fixes and workaround recommendations.
   - The analysis of the verification and validation procedures of Razorcat Development GmbH has shown that the requirements of the underlying standards are fulfilled.

II. The technical documentation fulfills the normative requirements. The relevant information for safety-related development is clearly formulated and well-structured.

To ensure adherence to the existing process quality procedures, as well as to survey further quality improvements, the software modification process is audited once a year by TÜV SÜD.

7 Conditions of Use

- The Safety Chapter of the User Manual bundles information that has to be considered in a safety-related development.
- In order to benefit from the tool qualification, developers of safety-related application software should follow the registration hints in the user's guide.
- Compiler options should be used consciously, and their potential interference with the testing should be analyzed (e.g. code instrumentation may influence code optimization).

8 Summary and Certificate Number

This report specifies the conditions of use and restrictions for the application of the TESSY product of Razorcat Development GmbH. It is part of the certificate.

Z10 078930 0003 Rev. 00

Munich, 2018-08-20

Digital unterschrieben von Christian Dirmeier
Datum: 2018.08.22 12:36:32 +02'00'

Christian Dirmeier
(Technical Certifier)