Choose certainty.
Add value.

Report

on the

Certificate

Z10 11 12 78930 001

Software tool for safety-related development

Tessy

Manufacturer
Razorcat Development GmbH
Witzlebenplatz 4
D-14057 Berlin

Report no. RB 84018 C
Revision: 1.1, Date 2013-05-16

Testing Body:
TÜV SÜD RAIL GmbH
Ridlerstraße 57
D-80339 München
Germany

Certification Body:
TÜV SÜD Product Service GmbH
Ridlerstraße 57
D-80339 München
Germany

Dissemination, distribution, copying or any other use of any information in this report in part is strictly prohibited.

Content

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

List of Tables

Table 1: Revision history 3
Table 2: Identification 6
Table 3: Normative basis of testing 6

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	active	Release 3.0.x Chapter 1, 2, 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.

System under test

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

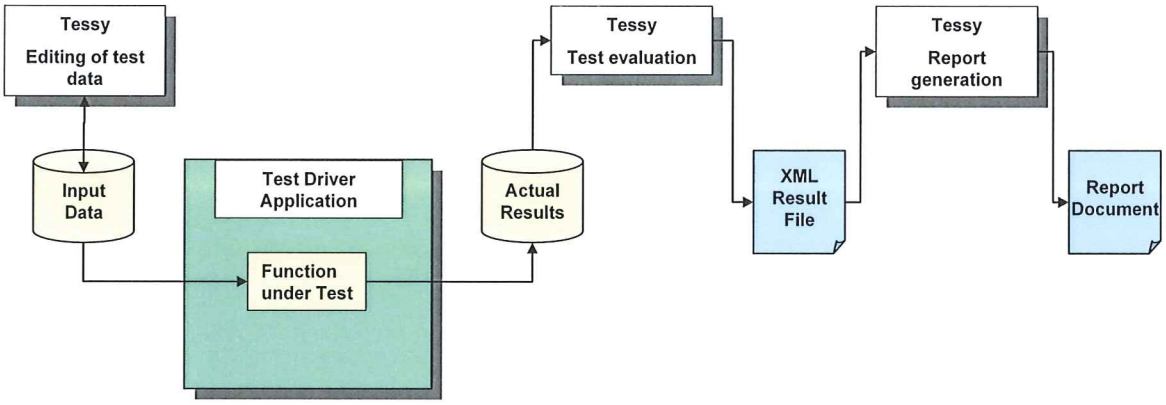

Figure 1: : Tessy Core Workflow

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 RB 84018 T, 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 RB 84018 T, Rev. 1.1.

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
Tessy	2.9.x	✓	✓
Tessy	3.0.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, ASIL D	Road vehicles - Functional safety - Part 8: Supporting 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.

As the intention of the customers who will use Tessy cannot be foreseen, ASIL = D is assumed.

The tool error detection level has to be assumed to TD = 3[1], this yields a Tool Confidence Level of TCL = 3.

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.

[1] ISO 26262-8:2011, Clause 11.4.5.2 b)

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 RB 84018 T, Rev. 1.0. The testing results related to the modification of Tessy to release 3.0.x are documented in the Technical Report RB 84018 T, Rev. 1.1.

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 11 12 78930 001

Munich, 2013-05-16

Guido Neumann
Rail Automation
Technical Certifier