TPT - QUALIFICATION

according to ISO 26262

Overview

Version 1.5

February 2016

PIKETEC
software engineering

TABLE OF CONTENTS

1 Introduction

Time Partition Testing (TPT) is a model-based solution for software testing of embedded control systems. TPT allows functional software tests. It is real-time enabled, thus capable of test execution in real-time test environments.

Test modeling, test execution, test management and test documentation are fully supported.

TPT tests MATLAB/Simulink, TargetLink or ASCET models efficiently and automatically. TPT also enables consistent testing from Model-in-the-Loop, Software-in-the-Loop, Hardware-in-the-Loop, CAN, LIN and other main test environments.

A tool qualification according to [ISO 26262] is required to use TPT within the automotive industry.

2 ISO 26262

[ISO 26262] "Functional Safety - Road vehicles" has replaced the international standard IEC 61508 valid for developing electrical, electronic and programmable electronic (E/E/PE) systems in various application areas. [ISO 26262] is worldwide mandatory for the development of road transport vehicles since November 2011.

3 Confidence in use of software tools

Both IEC 61508 and ISO 26262 require the qualification of the tools that are used in the development of software in safety-related systems. [ISO 26262-8] Chapter 11 - “Confidence in the use of software tools” - specifies the conditions which have to be met by a tool to reach the „required level of confidence“. In addition – if needed - methods for qualification are defined.

The qualification of a tool means increasing its usage confidence, preventing that tool errors can cause safety-critical or safety-related failures in the developed system.

Qualification is done in two steps. First an analysis and classification of the tool has to be done. Here the use cases and potential error cases are considered. A malfunction of a particular software tool can introduce or fail to detect errors in a safety-related item or element being developed. This possibility must be determined. Thereafter the measures that prevent the software tool from malfunctioning, or the measures that detect that the software tool has malfunctioned and produced corresponding erroneous output are determined.

Based on these measures, the required software tool confidence level (TCL) can be determined. The methods required for the qualification of software tools are derived from the TCL. The steps that have to be taken for analysis and qualification are, summarized:

> As prerequisites, a safety plan and the information regarding the phases of the safety lifecycle in which the software tool is involved shall be available. In addition, the usage of a software tool shall be planned (version number of the tool, configuration, environment in which the software tool is executed and the maximum ASIL of all relevant safety requirements (See [ISO 26262-6] 11.3, 11.4).

1. The first step consists of „Evaluation of a software tool by analysis“ ([ISO 26262-8] 11.4.5).
   “Here the intended usage of the software tool is analyzed and evaluated.
   1.1 The Tool Impact (TI) and
   1.2 The Tool Error Detection (TD) are determined ([ISO 26262-8] 11.4.5.2)
   1.3 Based on TI and TD the „Tool Confidence Level“ (TCL) is identified”
   ([ISO 26262-8] 11.4.5.5])
2. The qualification itself can be done with four methods, depending on the TCL of the tool and the ASIL of the system to be developed (see [ISO 26262-8] 11.4.6).

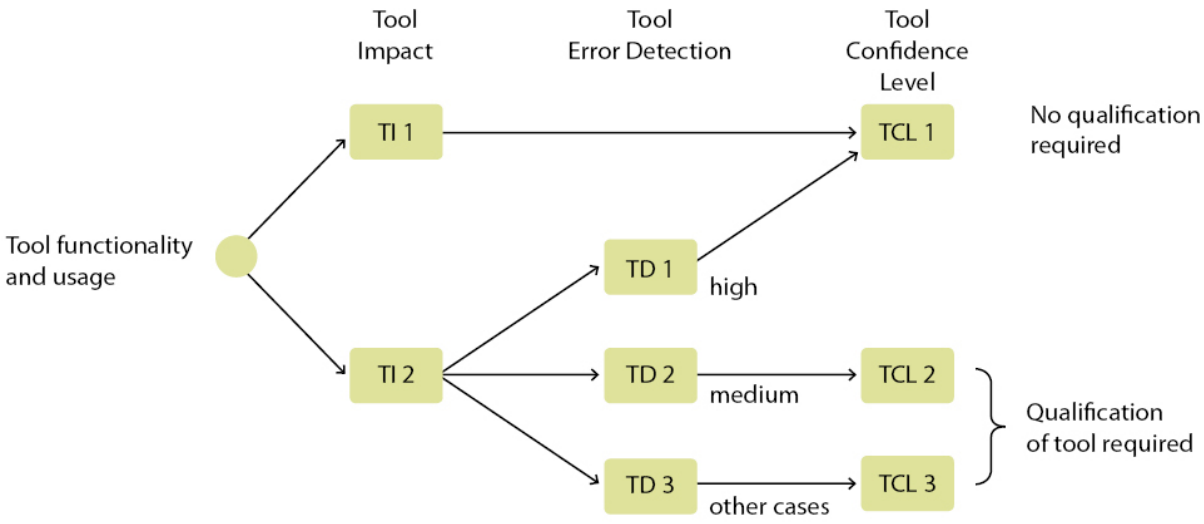

Figure 1: Determination of TCL

As any test tool, TPT has a tool impact TI=2, because a failure of the test tool can lead to violations of safety requirements which are not detected.

To determine the Tool error Detection (TD), the entire tool chain must be taken into account. This may lower the TD level considerably.

4 TPT Qualification

A tool like TPT can only be qualified by embedding it into a specific development process, which also means integrating the tool into a specific safety lifecycle (see [ISO 26262-6] 5.4.1, Figure 2).

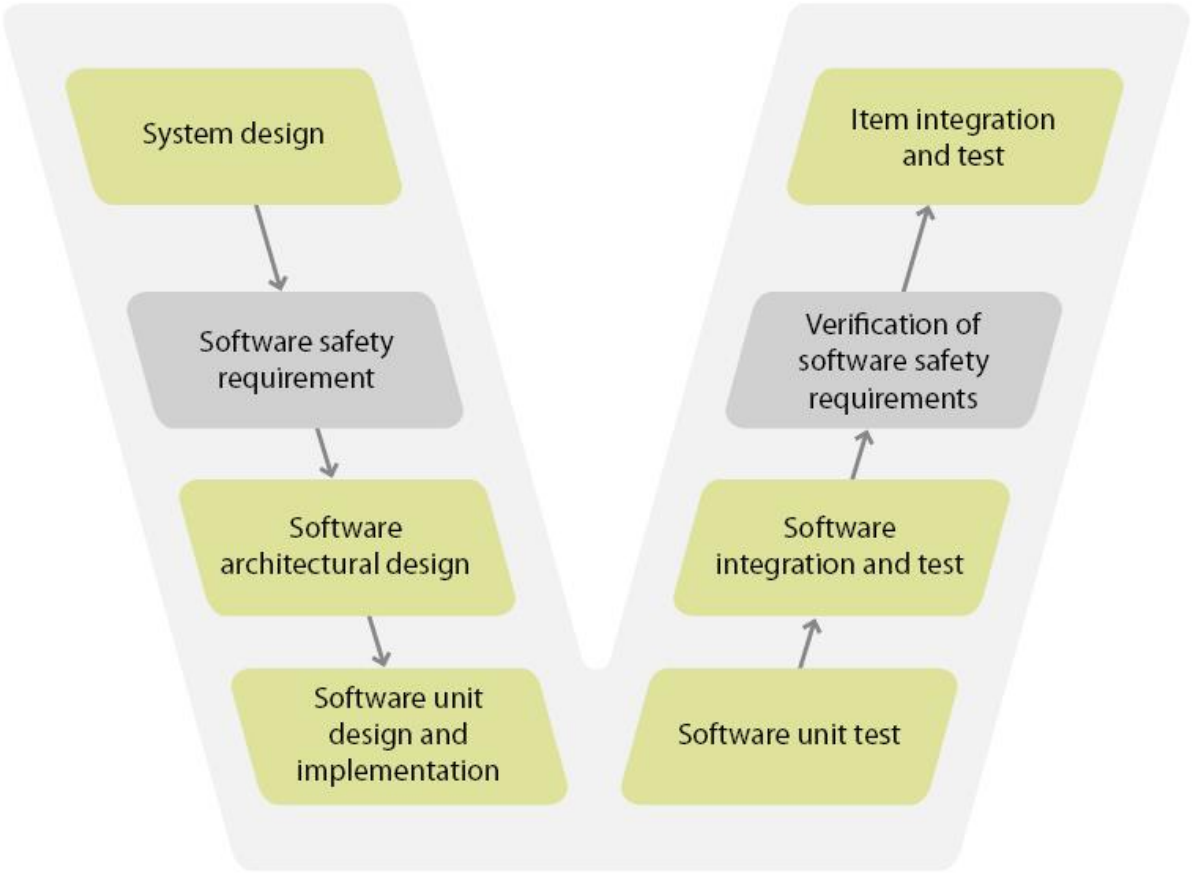

Figure 2: Safety lifecycle

This implies that the user must perform a qualification of the tool in the specific project environment. The tool manufacturer/producer has to show that the tool is qualifiable.

To ease the qualification process and to reuse knowledge, a preliminary tool qualification is reasonable for the tool's standard use cases, given the use of the tool can be derived from a standard configuration. This simplifies the qualification process according to [ISO 26262-8] noticeably (see [Klarmann] p. 28).

TPT can be qualified preliminary for standard (TPT) use cases. The use cases given in every TPT usage can be generically determined. This can be shown by an analysis of TPT, as required within the scope of [ISO 26262-8].

Four qualification methods are defined [ISO 26262-8] Section 11.4.6:

1a. "Increased Confidence from Use",
1b. "Evaluation of the Development Process",
1c. "Validation of the Software Tool" and
1d. "Development in Compliance with a Safety Standard".

For TPT, two of the methods are not applicable:

1a. "Increased Confidence from Use" is excluded since this method can only be used if the specification of the tool has not been modified (cf. [ISO 26262-8], 11.4.7.2). For TPT, in principle, three releases per year are planned. For every new release, due to the modified specification, the use of the previous releases cannot be considered for an "increased confidence for use".

1b. "Development in Compliance with a Safety Standard" must be excluded as a qualification method, since TPT is and will not be developed based in a safety standard, although it is developed systematically.

TPT can be qualified by using the methods

1b. "Evaluation of the development process" and
1c. "Validation of the software tool".

Method "1c Validation" is highly recommended for ASIL D. To be prepared for this case the generic qualification of TPT was done according to the method "1c. Validation".

TPT can be qualified for TCL2 and TCL3 and for systems from ASIL A to ASIL D.

In practice TPT has always been qualified by method (1c), regardless of minor TCL or ASIL determination.

The use of TPT can be derived from a standard configuration. To show this and to minimize the tool user´s effort, PikeTec offers a TPT-„Qualification-Kit".

To qualify TPT with specific use cases, the generic use cases, which were derived in the Qualification-Kit, must be consolidated with the project-specific use cases. If applicable, detailed use cases must be specified.

5 Qualification-Kit

For a fast and efficient qualification of TPT, PikeTec provides a Qualification-Kit consisting of two parts:

1. Support regarding the qualification

- Support[1] to determine the use cases, if the use cases go beyond the generic scope.
- Support[1] to determine the Tool Confidence Level.
- Support[1] to create a qualification-report, for which solely the tool user is responsible for.

2. Scope of delivery

- Gap-Analysis, to analyze whether additional use/error cases and tests within the specific project have to be taken into account.
- Test execution of generic and additional tests done by PikeTec
  - Manual tests
  - Validation Suite, which contains about 10.000 test cases at the present.
- All needed documents, for example
  - Validation and verification plan
  - Test plan
  - Validation and verification report

[1] If desired by the tool user

- Guidelines (Safety manual) to recognize or avoid possible errors

The Qualification-Kit shows that TPT is qualifiable and makes the qualification process easy and efficient. The Qualification-Kit provides a significant contribution to the qualification of TPT, reducing time and effort significantly.

6 References

[ISO 26262]	ISO 26262:2011-11: Road vehicles - Functional safety. International Standard, Part 1-9, 15.11.2011
[ISO 26262-6]	ISO 26262-6:2011-11: Road vehicles - Functional safety. Part 6: Product development at the software level. International Standard, 15.11.2011
[ISO 26262-8]	ISO 26262-8:2011-11: Road vehicles - Functional safety. Part 8: Supporting processes. International Standard, 15.11.2011
[Klarmann]	Klarmann, Kriso, Gebhardt 2010: REALTIMES 1/2010 http://www.etas.com/data/RealTimes_2010/rt_2010_1_28_de.pdf
[TPT Quali-Kit]	TPT - Qualification-Kit in accordance with ISO 26262, Analysis and Qualification measures. Version 1.3, PikeTec, November 2014