cadence®

Enabling ISO 26262 Qualification By Using Cadence Tools

By Randal Childers, Software Engineering Director, Cadence Design Systems

This document describes how to approach the software tool qualification outlined in ISO 26262 when developing automotive electrical and electronic systems using Cadence® tools. Cadence provides an ISO 26262 Tool Qualification Kit, also described in this document, that can help developers through the process with common use cases and reference workflows. Following these guidelines speeds development while ensuring compliance to functional safety standards.

Contents

Introduction

ISO 26262 focuses on the functional safety of electrical and electronic systems that are installed in series production passenger cars. This adaptation of IEC 61508 is for the automotive sector and affects all systems containing software- or hardware-based electrical, electronic, or electromechanical components. ISO 26262 covers many aspects of safety-related automotive software production, including the qualification of tools in the development process.

Neither IEC 61508 nor ISO 26262 require development tools to be certified or compliant to the safety standards because tools are not systems and are therefore outside the scope of both safety standards. However, both standards require the system developer to establish that all tools used during development do not violate any system safety requirements according to the appropriate system safety integrity level (SIL) or automotive safety integrity level (ASIL).

This document provides an overview of the software tool qualification approach outlined in ISO 26262 as it pertains to Cadence software tools. It also describes documentation that will be provided to help the system developer develop a valid safety argument for the tool chain that includes Cadence tools.

Software Tool Qualification Approach

The objective of ISO 26262 tool qualification is to ensure that software tools are suitable for use in developing safety-related items. If a software tool or a software tool chain is used for activities or tasks required by ISO 26262 that rely on the software tool's function, and relevant outputs are not fully examined or verified, the tool or tool chain needs to be assessed, classified, and potentially qualified.

The system developer needs to provide a valid safety argument for the tool chain—supported by appropriate evidence—that shows that no single failure in any tool could leave an undetected critical flaw in the system. The evidence required depends on the level of confidence that the tool performs its function correctly without introducing or failing to detect errors into the item, and on the ASIL of the safety-related item to be developed.

ISO 26262-8 clause 11 provides guidance on software tool classification and qualification, including the conditions under which no qualification is necessary. The approach can be divided into two steps: tool classification and tool qualification.

Software Tool Classification

The first step is to document, analyze, and evaluate the intended use of the tool in the development flow to discover:

- The possibility that a malfunction in the software tool can introduce or fail to detect errors in a safety-related item or system being developed, expressed by the classes of tool impact (TI1 or TI2)
- The confidence in measures that prevent the software tool from malfunctioning and producing corresponding erroneous output, or in measures that detect that the software tool has malfunctioned and has produced corresponding erroneous output, expressed by the classes of tool error detection (TD1, TD2, or TD3)

A tool confidence level (TCL) is determined based on tool impact (TI) and on the tool error detection level (TD) (see Figure 1).

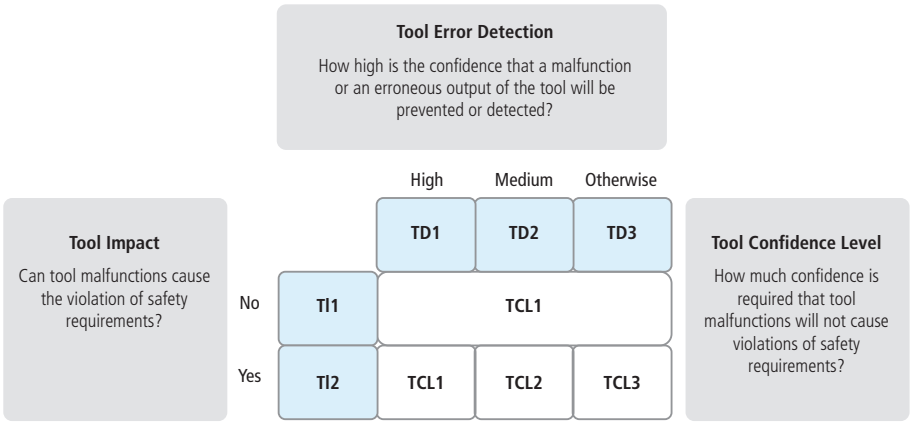

Figure 1: Tool evaluation according to ISO 26262:2011-8

Software Tool Qualification

Tools with the lowest possible TCL (i.e., TCL1) do not require subsequent tool qualification because a malfunction cannot cause a violation of the safety requirements. All other TCLs require formalized tool qualification. It is possible to improve the tool confidence level to TCL1 by enriching the development process with additional checks, redundancies, and restrictions.

Documentation Required for Qualification

The system developer will need to choose the appropriate methods for tool qualification depending on the required TCL and on the ASIL of the development object. The ISO 26262 process of tool qualification requires the creation of two documents: a Software Tool Criteria Evaluation Report documents the tool classification, and a Software Tool Qualification Report documents the tool qualification.

Software Tool Criteria Evaluation Report

Tool classification results for the Software Tool Criteria Evaluation Report depend on how the tool is used during the development of the safety-related system, and whether a malfunction in the software tool can introduce or fail to detect errors in the system being developed.

For software tools classified as TCL2 or TCL3, at least one of the following tool qualification methods must be applied:

- Increased confidence from use
- Evaluation of the tool development process
- Validation of the software tool
- Development in accordance with a safety standard

Software Tool Qualification Report

The Software Tool Qualification Report documents the tool qualification methods, results, and actual qualification, providing evidence that the tool qualification methods were carried out as planned. The specific recommendations for all TCL/ASIL combinations are listed in ISO 26262-8, tables 4 and 5.

It is important to note that the ISO 26262 tool qualification approach takes the interdependencies of tools in the tool chain into account. If a software tool X is used to verify the output of another tool Y, the interdependency between these tools needs to be considered when evaluating X (i.e., the downstream tool).

Cadence ISO 26262 Tool Qualification Kit

As previously stated, the system developer needs to provide a valid safety argument for the tool chain, supported by appropriate evidence. ISO 26262 calls for a project-specific classification and qualification of software tools where applicable, depending on the project-specific use case and the tool workflow to be used when developing or verifying safety-related items.

Users of these tools expect the tool vendor to provide assistance with the assessment, classification, and potential qualification of the tools. To reduce the effort and costs associated with tool qualification, Cadence provides an ISO 26262 Tool Qualification Kit that follows a generic qualification approach based on one or more common use cases and reference workflows. The tools are then classified assuming that they are being used as specified in the typical use case(s) and tool usage is being supported by the error prevention and detection methods described in the reference workflows. Table 1 provides a mapping between the documentation and the ISO 26262 requirement.

Item	ISO 26262 Reference	Description
Software Tools Classification Analysis	8-11.4.2, 3	Defines the TCL
Software Tool Qualification Plan	8-11.4.2, 4	Identifies what qualification methods are required, given the TCL and the ASIL for the current product
Software Tool Documentation	8-11.4.2.2	Description of features, functions, and technical properties (including during anomalous operating conditions), as well as installation process, user manual, required environment, known malfunctions and avoidance measures, and measures for fault detection

Table 1: Tool Qualification Kit Documentation

If the user applies the product differently than the referenced workflows, the tool classification needs to be carried out according to the actual use case(s), but can leverage the documentation contained in the ISO 26262 Tool Qualification Kit. If the required TCL derived from the actual use cases is equal to or lower than the TCL that resulted from the typical use cases, the software tool qualification in the kit can still be used. Each of the documents in the ISO 26262 Tool Qualification Kit is described in more detail below.

Software Tools Classification Analysis

The Software Tools Classification Analysis document contains information about TCL evaluation and determination for Cadence tools, based on TI and TD (see Figure 1). Any software tool used in the development of a system or its software or hardware elements needs to minimize the risk of systematic faults in the developed product due to malfunctions of the software tool leading to erroneous outputs. Any activities or tasks required by ISO 26262 that rely on the correct functioning of the software tool used must also have an adequate development process that is compliant with ISO 26262.

The Software Tools Classification Analysis document analyzes and justifies the TCL of Cadence tools with respect to ISO 26262. The TCL evaluates the probability that a tool malfunction and its corresponding output can introduce or fail to detect errors in a safety-related element being developed, and the confidence in preventing or detecting these errors.

When evaluating the confidence in prevention or detection, measures internal (e.g., monitoring) and external (e.g., guidelines, tests, reviews) to the software tool used when developing the safety-related element are considered and assessed. Depending on the ASIL of the safety-related item under development, an independent confirmation review may be necessary.

The system developer will use the Software Tools Classification Analysis together with the specific use cases for a tool to determine the TCL. When multiple use cases for a tool exist, there can be multiple TCLs. The tool classification process and its results are to be documented in the system developer's Software Tool Criteria Evaluation Report.

Software Tool Qualification Plan

The selected tool qualification methods must be documented in the Software Tool Qualification Report, with corresponding evidence that the tool qualification methods were carried out as planned. Cadence's Software Tool Qualification Plan focuses on two areas: planning for software tool qualification, and listing the use cases that demonstrate the tool is classified with the required level of confidence.

Software Tool Documentation

Several pieces of information must be provided to ensure proper software tool usage:

- Description of features, functions, and technical properties
- Description of the installation process
- User manual
- Operating environment
- Expected behavior in abnormal conditions

Summary

Automotive software designers need to understand how to implement ISO 26262 tool qualification requirements. This document reviewed the ISO 26262 tool qualification approach and outlined assistance Cadence provides system developers to support the tool qualification process. System developers can effectively evaluate their compliance with ISO 26262 by using Cadence's ISO 26262 Tool Qualification Kit, which includes common use cases and reference workflows to help designers more quickly develop compliant designs.