TASKING®

TASKING Compiler Qualification Kit

ASIL-D

CERT C

IEC 62304

EN 50128 ISO 26262 ASIL-D

ISO 25119

ASIL-D ISO 26262 ASPICE

CERT C IEC 61513

MISRA C

ASIL-D

ASIL-D

CERT C

Overview

SUMMARY

The TASKING Compiler Qualification Kit provides development organizations with the required evidence to demonstrate compliance with ISO 26262 and similar safety standards. It covers the software tool qualification process and demonstrates that TASKING toolsets are capable of developing safety critical software up to the highest safety integrity levels (ASIL-D for automotive) when used as described in the safety manual.

FUNCTIONAL SAFETY

The ISO 26262 functional safety standard targets electrical and electronic systems within road vehicles under 3500kg (7700lbs). Automotive OEMs and their suppliers are required to comply to this standard. To prove compliance the OEM and its suppliers must compile a set of evidence, i.e. documents, that prove that all criteria listed in the standard have been fulfilled.

Functional safety, defined as absence of unreasonable risk due to hazards caused by malfunctioning behavior of electrical and electronic (E/E) systems, is moving away from a specialist requirement to become normality as the number of complex applications that rely on electronics is increasing. Nevertheless, functional safety remains a complex issue that influences all lifecycle processes, requires specialized tool support and tool usage, and increases product development time and costs. Strict compliance to safety standards pays of when safety issues arise, normally legal accountability will be waived when system development has been done according to the latest safety standards, such as ISO 26262 or others depending on the industry sector.

RESPONSIBILITIES

The supplier of an E/E system is responsible for obtaining certification. TASKING toolsets have been used for many years in safety related applications across a wide range of vertical markets, including automotive, industrial, railway, and medical. To simplify and accelerate the development and certification of safety-certified systems by our customers, TASKING delivers:

- Static code analysis features built into the compiler to verify compliance with MISRA and CERT guidelines;
- Safety Checker, a tool to detect interference between software elements with different automotive safety integrity levels (ASIL);
- Compilers developed using an ASPICE CL2 compliant development process;
- Safety Kits that provide confidence-building evidence for toolset qualification;
- Services to help customers pass certification in cases where the customers use-case deviates from the use-case described in the safety manual.

MISRA AND CERT STATIC CODE ANALYSIS

Static code analysis is a method used to verify all possible paths within a software program without actually executing the program. It efficiently locates defects that go unnoticed during dynamic tests or peer reviews.

The European Motor Industry Software Reliability Association (MISRA) has created a set of software development guidelines, MISRA C, that helps to facilitate code safety, security, portability and reliability for embedded systems. The CERT Division of the Software Engineering Institute, founded by US government to address cybersecurity threats, created the CERT C Coding Standard. Both standards are used across a wide variety of industries and applications including the automotive, rail, aerospace, military and medical sectors.

Safety standards such as ISO 26262 recommend the use of automated static analysis tools, such as available in TASKING VX toolsets, to find violations of the MISRA C and/or CERT C standards.

SAFETY CHECKER

Safety Checker automatically detects interference between software elements with different Automotive Safety Integrity Levels (ASIL) by checking access restrictions on the memory of single and multi-core systems.

This is very important in today's automotive system designs where multiple functionalities with different safety requirements (ASILs) are integrated in one domain controller, where an error in a non-safety-critical software component may cause the failure of safety critical components. Safety standards such as ISO 26262 prescribe that it shall be ensured that such interference does not occur. Safety Checker is the only ASIL-partition-aware static analysis tool that performs the proper analysis to ensure freedom from interference.

For the highest safety level (ASIL-D) safety standards prescribe the use of dedicated hardware, a memory protection unit, to ensure freedom from interference. Also in this case a Safety Checker is a valuable tool, since it detects interferences at software-construction-time, i.e. it prevents interferences from occurring, whereas the memory protection unit only mitigates the effects of interferences that occur at runtime, possibly after a system has been shipped to the customer.

TASKING TOOLSETS ARE DEVELOPED USING ASPICE LEVEL 2 CERTIFIED PROCESSES

The Automotive SPICE® (ASPICE) maturity model has been derived from the ISO 15504 International Standard for software process assessments, for suppliers to the (European) automotive industry it is a mandatory method for objective process evaluation and process improvement. It is comparable to the widely used CMMI model developed in the US and Asia.

TASKING VX Compiler Toolsets are developed using ASPICE level 2 certified processes. This simplifies and accelerates the certification of our customers systems. It eliminates the need for any further toolchain qualification effort for lower safety integrity levels up to ASIL-B.

ID	PROCESS NAME	PA 1.1	PA 2.1	PA 2.2	CAPABILITY LEVEL
MAN.3	Project management	F	F	F	2
ENG.4	Software requirements analysis	F	F	F	2
ENG.5	Software design	F	F	F	2
ENG.6	Software construction	F	F	F	2
ENG.7	Software integration test	F	F	F	2
ENG.8	Software testing	F	F	F	2
SUP.1	Quality assurance	F	F	F	2
SUP.8	Configuration management	F	F	F	2
SUP.9	Problem resolution	F	F	F	2
SUP.10	Change request management	F	F	F	2

TASKING Processes have been assessed at ASPICE CL2 ("F" denotes Fully achieved)

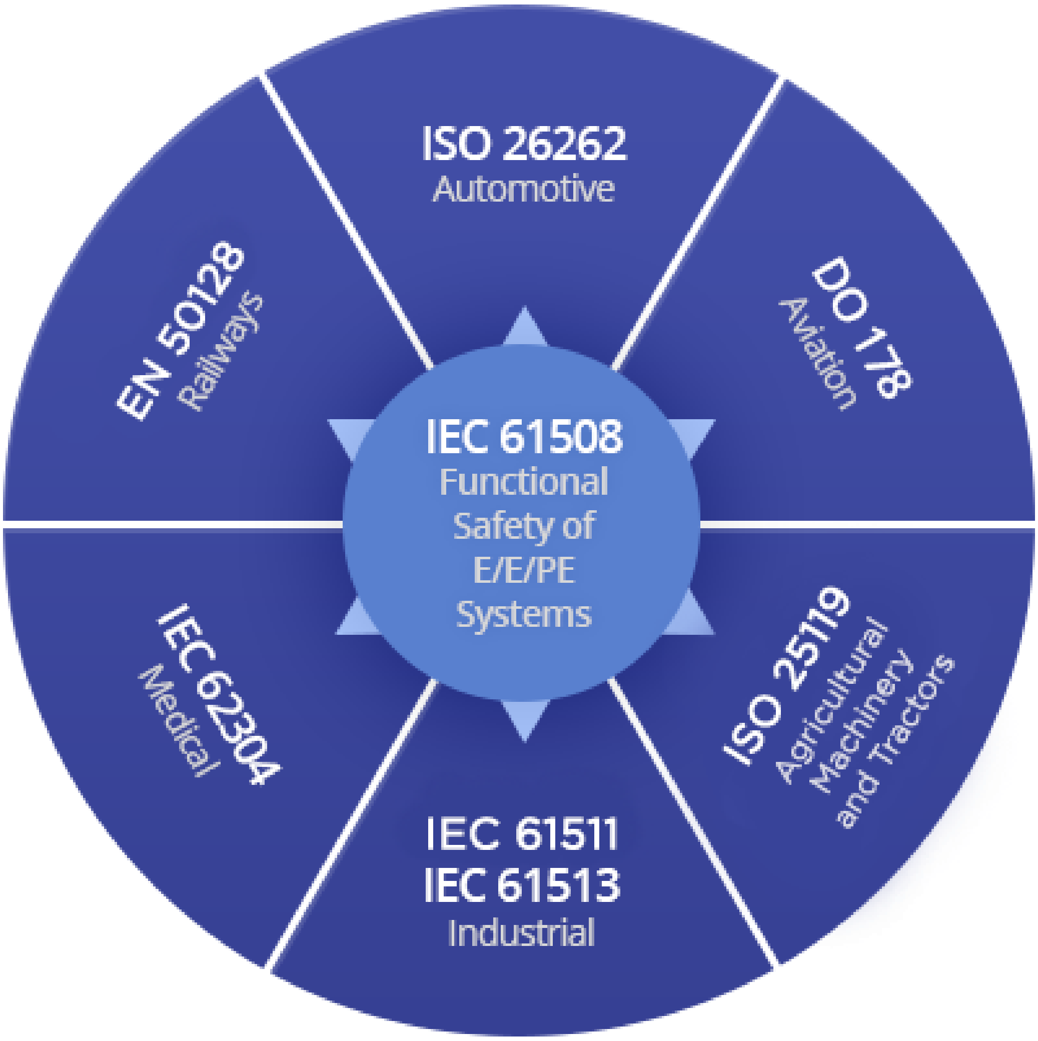
Higher ASIL levels require additional qualification evidence which is included in the TASKING Compiler Qualification Kit.

TASKING COMPILER QUALIFICATION KIT

The TASKING Compiler Qualification Kit provides the required evidence with supporting documentation to demonstrate that the compiler is fit to develop safety-related software up to ASIL-D when used as described in the safety manual. A Safety Kit contains the following:

- A safety manual, which provides guidance about how to use the toolset for safety related development, and contains evidence to support tools qualification methods “Evaluation of the tool development process” for lower safety integrity levels, and “Validation of the software tool” for higher safety integrity levels.
- A license to access all information on TASKING’s defect reports and mitigations database that contains up-to-date information about all known tool issues reported by TASKING and customers.
- Scripts and instructions about how to execute “Validation of the software tool” qualification method which is only needed if the customer’s use of the tools differs from the use cases described in the safety manual.

A safety kit is needed if you develop safety-critical software that should pass some formal certification process. It provides the evidence to satisfy your certification authority’s to prove that the compiler and the way it is used match with the safety requirements of your system.



TASKINGS ISO 26262 SERVICES

Services are relevant for customers that must meet high safety integrity levels ASIL-C or ASIL-D, **and** whose particular use of the tool does not match a use case that is described in the safety manual.

In such case a customer can decide to do an in-house tool qualification, or can ask TASKING to update the safety kit based upon the customer's use case. The benefits for the customer of using the TASKING ISO 26262 services are:

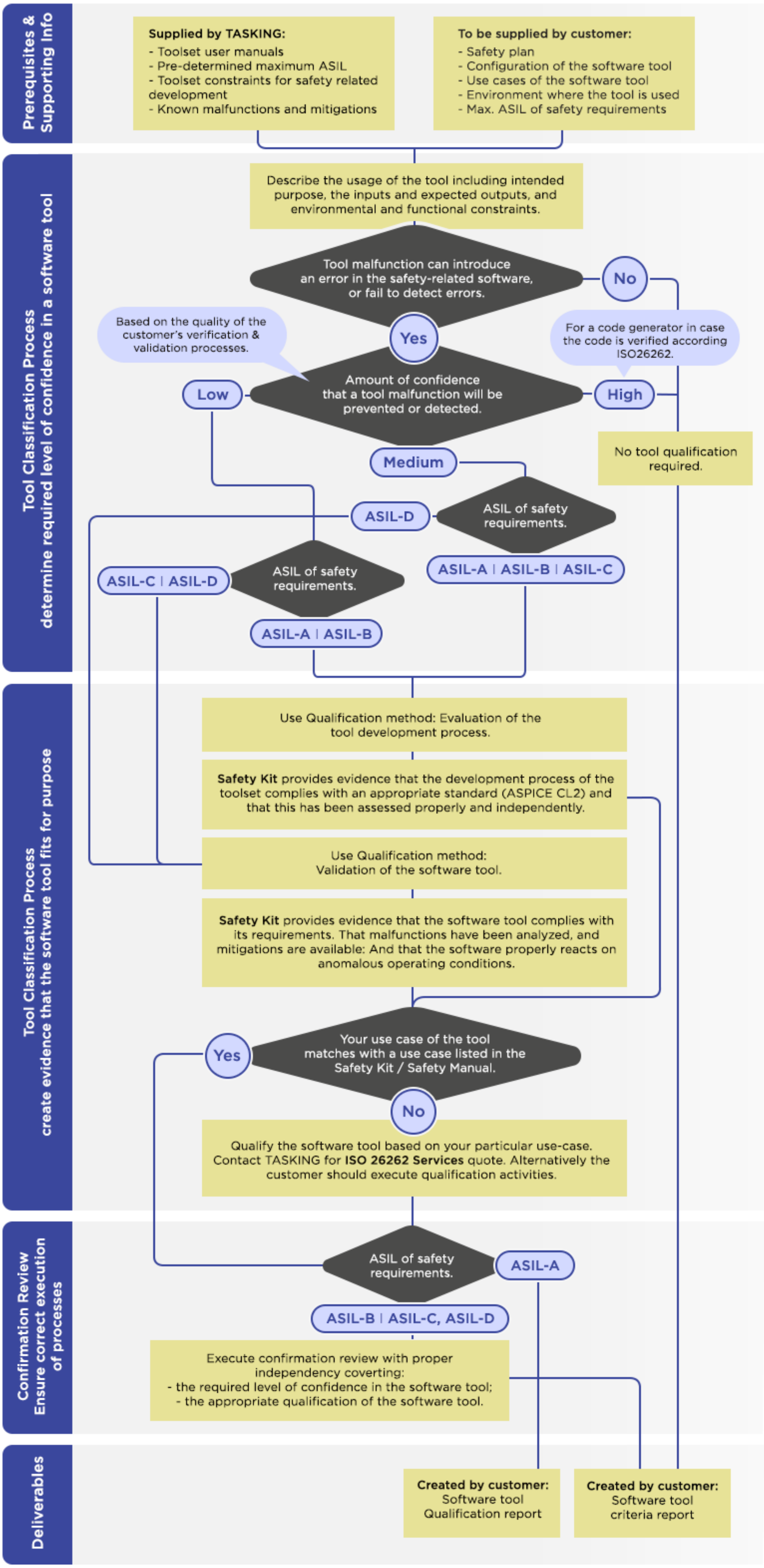
- No investment in compiler test suite(s) needed.
- No or less investment in test-infrastructure needed.
- No or less investment in training needed.
- Work is carried out by experts with deep knowledge about the tools.

STANDARDS COVERED

TASKING VX compiler toolsets fulfill the requirements for development tools in accordance with ISO 26262, EN 50128, and ISO 25119. The toolsets can be used for any Safety Integrity Level, provided the safety-related item is developed in accordance with the respective requirements.

Other safety standards can be supported as well, however no specific cross-referencing between the content of the Safety Kit and the requirements of other standards has been developed.

Tool Qualification in Accordance with ISO 26262 Functional Safety Standard



Prerequisites & Supporting Info

Supplied by TASKING:
- Toolset user manuals
- Pre-determined maximum ASIL
- Toolset constraints for safety related development
- Known malfunctions and mitigations

To be supplied by customer:
- Safety plan
- Configuration of the software tool
- Use cases of the software tool
- Environment where the tool is used
- Max. ASIL of safety requirements

Tool Classification Process
determine required level of confidence in a software tool

Describe the usage of the tool including intended purpose, the inputs and expected outputs, and environmental and functional constraints.

Tool malfunction can introduce an error in the safety-related software, or fail to detect errors.

No

Yes

Based on the quality of the customer's verification & validation processes.

For a code generator in case the code is verified according ISO26262.

Amount of confidence that a tool malfunction will be prevented or detected.

Low

High

Medium

No tool qualification required.

ASIL of safety requirements.

ASIL-D

ASIL-A | ASIL-B | ASIL-C

ASIL of safety requirements.

ASIL-C | ASIL-D

ASIL-A | ASIL-B

Tool Classification Process
create evidence that the software tool fits for purpose

Use Qualification method: Evaluation of the tool development process.

Safety Kit provides evidence that the development process of the toolset complies with an appropriate standard (ASPICE CL2) and that this has been assessed properly and independently.

Use Qualification method: Validation of the software tool.

Safety Kit provides evidence that the software tool complies with its requirements. That malfunctions have been analyzed, and mitigations are available: And that the software properly reacts on anomalous operating conditions.

Your use case of the tool matches with a use case listed in the Safety Kit / Safety Manual.

Yes

No

Qualify the software tool based on your particular use-case. Contact TASKING for **ISO 26262 Services** quote. Alternatively the customer should execute qualification activities.

Confirmation Review
Ensure correct execution of processes

ASIL of safety requirements.

ASIL-A

ASIL-B | ASIL-C, ASIL-D

Execute confirmation review with proper independency coverting:
- the required level of confidence in the software tool;
- the appropriate qualification of the software tool.

Deliverables

Created by customer:
Software tool
Qualification report

Created by customer:
Software tool
criteria report

Distributed by Hitex GmbH
www.hitex.de
Fone +49 721 9628 0
Email sales@hitex.de