ISO26262 confidence in SW Tools for EB Tresos Studio

DECEMBER 2021

EB Tresos Studio use in NXP safety SW development lifecycle

How is it used in the development lifecycle of a ASIL D software safety product ?

EB Tresos Studio is used to configure the driver and to generate the source code containing the driver configuration parameters. The generated source code files are compiled with other driver source code files in order to create the production object code.
Also used to perform conformity checks for configuration schema (VSMD report) and used in plug-in builder to convert configuration schema format.

Can a tool failure produce erroneous output that eventually results in a presence of error(s) in the element being developed?

Yes, the tool can introduce errors in the software being developed.
Tool Impact is TI2

What is the level of detecting or preventing potential tool errors?

There is a high probability of detecting or preventing potential tool errors through testing and peer review.
EB Tresos Studio output is tested and reviewed.
Tool Detection is TD1.

EB Tresos Studio failures detection examples

Failure modes	Effect	Detection
Calculate and store wrong configuration parameter values into epc files or source code configuration files while the driver is tested	Test fails due to wrong configuration (false positive).	Detected by testers. Dedicated test defined and included in regression test plan.
Calculate and store wrong configuration parameter values into epc files or source code configuration files while the driver is tested	Test passes while the configuration files are wrong (false negative)	When different Tresos version is used, then faulty configuration can be generated but likely detected at user integration and testing phase. Overall, this requires two faults, a bug in cfg files and a Tresos bug, so the overall detection is high.
Conformity check between driver configuration schema and Autosar schema template generate a wrong report	Driver configuration schema is reported as correct although it is wrong(false negative)	Use a second independent schema ckecker: AMDC tool from Vector
Conformity check between driver configuration schema and Autosar schema template generate a wrong report	Driver configuration schema is reported as wrong although it is correct(false positive)	Use a second independent schema ckecker: AMDC tool from Vector
Conversion of the configuration schema from .xdm(Elektrobit Tresos specific) format to .epd(Autosar) format is wrong	Insert into driver plugin a wrong configuration schema represented according to Autosar format(.epd file)	Identified when loaded by Tresos or other tool. Configuration results are reviewed when used in production. Configuration generated from both epd and xdm and compared.

Establishing Tool Confidence Level

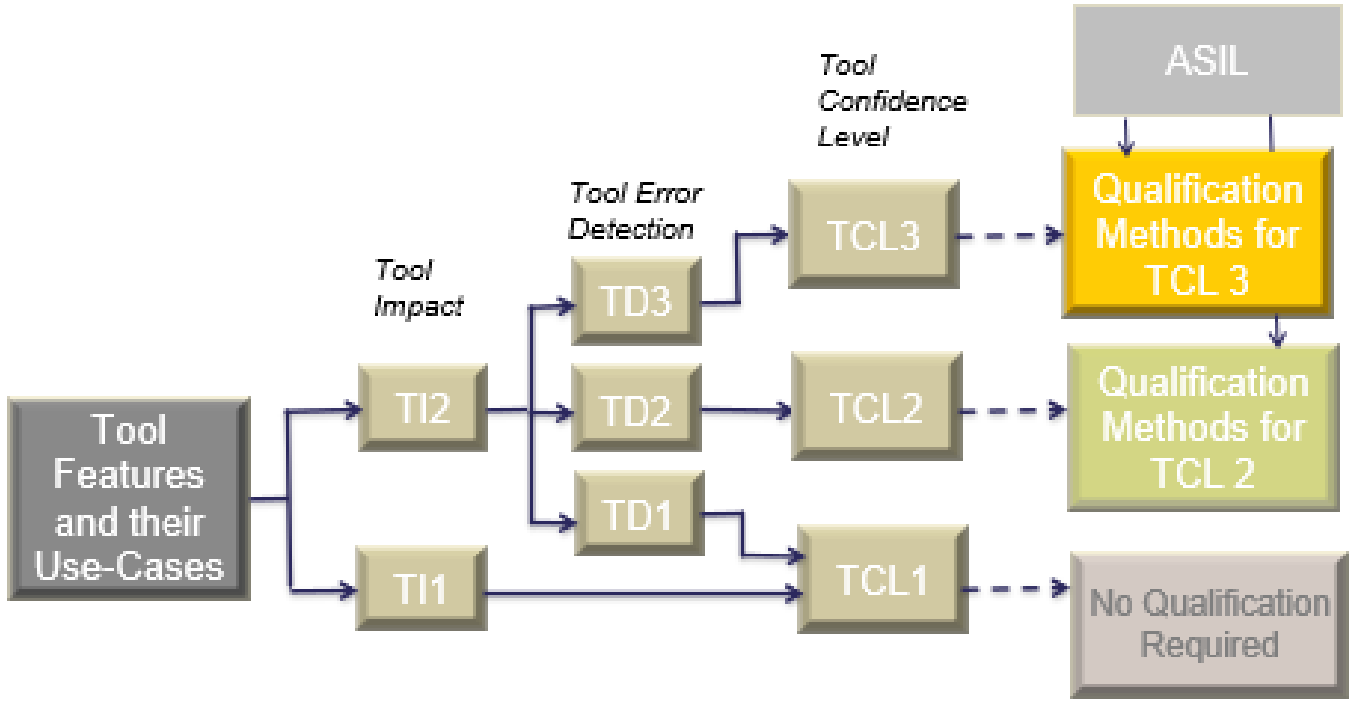
		Tool error detection		
		TD1	TD2	TD3
Tool impact	TI1	TCL1	TCL1	TCL1
	TI2	TCL1	TCL2	TCL3

Tool Impact (TI)
if a software tool can introduce or fail to detect errors

- TI1: No impact
- TI2: Impact

Tool Detection (TD) in usage of tool

- TD1: High probability of detecting/preventing potential tool errors
- TD2: Medium probability of detecting/preventing potential tool errors
- TD3: All other cases (Low or unknown)



According to ISO26262 - 8- 2018, clause 11.4.5.4 Tool Confidence Level is TCL 1.

No qualification method needed to increase confidence in use.