Speculation towards a Confirmation Review QuickCheck/Erlang

Oskar Ingemarsson & Sebastian Weddmark Olsson

September 17, 2013

1 Introduction

To be able to confirm what ASIL level a software tool can reach a confirmation review must be written according to ISO26262. The confirmation review must take a number of sections in the ISO-standard in consideration. The section that must be considered are 11.1 until 11.4 in ISO26262-8. The goal is here is to reach the highest degree of Tool Confidence Level (TCL1) for a verification tool written in Erlang which uses QuickCheck as a ground stone. If this can be achieved one should be able to use the verification tool as a help to reach ASIL C and D.

Here follows speculations about what can be achieved using QuickCheck/Erlang as the keystones for the verification tool. The exact sentences for each section will be left out and replaced with a summery. For the exact definition of every section see the ISO-standard.

2 Requirements

ISO26262-8: 11 Confidence in the use of software tools

11.1 Objectives

Just the objectives, more or less what is described in the introduction.

11.2 General

This section emphasises that ...

11.3 Inputs to this clause

11.4 Requirements and recommendations

11.4.1 General requirement

11.4.1.1
This section just says that the verification tool should accomplish the requirements according to the ISO standard.

11.4.2 Validity of predetermined tool confidence level or qualification

11.4.2.1
To the verification tool to reach a certain ASIL level, depending on later achievements of the software, certain actions must be taken. This actions regards that different persons must to do same confirmation review of the software and come to the same conclusion.

11.4.3 Software tool compliance with its evaluation criteria or its qualification

11.4.3.1
Just about that all the required functionality of the verification tool also is used when using the software for verification.

11.4.4 Planning of usage of a software tool

11.4.4.1
The version of and other basic information for the verification tool must be written down in the confirmation review.

11.4.4.2
The verification review should contain documentation about the verification tool. Descriptions of function used, which environment the software is run in, etcetera.

11.4.5 Evaluation of a software tool by analysis

11.4.5.1
This section is about that one should document the verification tool for what purpose it should have. It should also be clear what the expected output is and which constraints the tool may have.

11.4.5.2
The first part of this section requires one to analyse the verification tool to find out if bugs can be introduced because of malfunctions of the verification tool.

Also if real bugs in the software, which is about to be tested, are missed because of bugs in the verification tool.

The verification tool should then be classified to a certain Tool Impact (TI). The verification tool companions TI1 if there are no possibility that errors are missed or introduced because of malfunctioning of the verification tool and otherwise TI2.

The second part is about the confidence of the verification tool. The meaning of this is how easy it is to find bugs in the verification tool. There are three classes of Tool error Detection (TD). A verification tool should be ranked TD1 if it has hight degree of confidence, TD2 if it has medium degree of confidence and TD1 otherwise.

11.4.5.3
This section only says that if the degree of TI or/and TD is unclear then the choice of degree should be conservative.

11.4.5.4
This section says that TD2 not should be chosen if the verification tool just is one part of a greater verification suit.

11.4.5.5
This part describes how the Tool Confidence Level (TCL) should be chosen according to the determination of TD and TI. See the table below.

	TD1	TD2	TD3
TI1	TCL1	TCL1	TCL1
TI2	TCL1	TCL2	TCL3

11.4.6 Qualification of a software tool

11.4.6.1
This section says that if a verification tool is classified as TCL1 no qualification are needed. Hence no further sections needs to be described. See discussion and conclusion.

3 Discussion/Conclusion

The only section that is worth any discussion are more or less the one which describes the evaluation of of TI and TD. This because it is the only section which may distinguishes different method. There are some confusion regarding what is actually meant in the choice of TI. Because QuickCheck uses random vectors for it tests all bugs may not be found. However if all properties are correct defined there will be no missed bugs if the environmental setup, where a bug exists, is generated by a test vector.

Even if it's only possible to achieve TI1 with QuickCheck as a ground stone for the verification tool it should still be possible to reach TD1 and hence be

able to achieve TCL1. The argumentation for this is that QuickCheck should be reliable to not contain bugs in its self. Also the verification tool will be implemented in Erlang. This makes it easy to produces compact and lucid code which are side effect free.

The bottle neck comes most certainly down to the modelling of the Autosar modules. Regardless of which software tools that will be used this step must be taken. There are also a reliable library for Erlang, developed by Quviq, which aim is to make it easy to implement a state based module of an Autosar module. This will certainly also reduce the number of bugs.

As a conclusion it should be possible to reach TCL1 with help of QuickCheck/Erlang.