Verification of SCADE models with S3 model-checker

Marielle Petit-Doche, Matthias Güdemann, Roméo Courbis
Systerel

February 23, 2015

Abstract

This document describes the verification and validation processes applicable to SCADE models usin the S3 model-checker.

Contents

1 Introduction

This document gives a description of the VnV process applied on a Scade design model. The Scade model covers two functions of the ETCS on-board unit:

Level Management function , described in SRS-26 §5.10

Mode Management function , described in SRS-26, §4.6, §5.4, 5.6, 5.7, 5.9, 5.11, 5.13, 5.19

2 Verification processes applicable to a SCADE model

The principe of verification consists in the definition of properties in textual languages, and verification of these properties by model-checking techniques on a textual translation of the Scade Model.

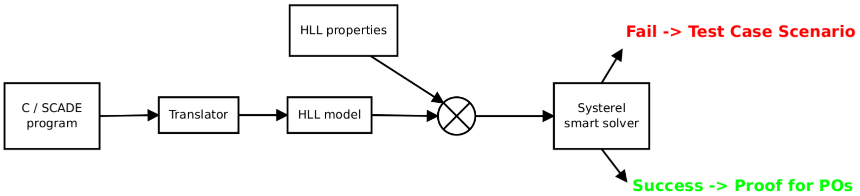

Figure 1: Procedure of verification of Scade model

Figure 1 describes the process:

- the main input is a Scade model to verify (same approach and tool can be applied to a C program) which is translated in a High Level Language (a textual description of the model)
- the second input is the propreties to verify, written in HLL
- these both inputs are merged in aunique HLL file, used directly as input of the Systerel Smart Solver (S3 model-checker) for verification
- result of the S3 tool is Success or Failure; in case of failure counter-example is provided for analyse.

The S3 tool is a model-checker which manages as well an internal SATs solver as external SAT solvers.

This process can be apply to cover three purposes:

Properties of an HLL Model: The prover may be used to prove or disprove properties of an HLL model. Those properties are modeled as proof obligations.

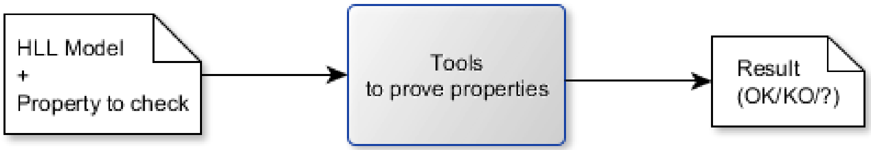

Figure 2: Properties of an HLL Model

Solving Properties of an HLL Model: The prover may be used as a solver, by finding values for the streams that comply with some property P. To do so, just put the negation of P as a proof obligation. If the prover succeeds to disprove the proof obligation, it will provide a solution solving P. If the prover succeeds to prove the proof obligation, then this proves that the property cannot be solved.

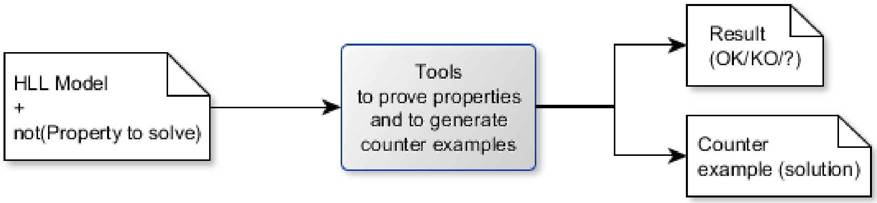

Figure 3: Solving Properties of an HLL Model

Proving the Equivalence of 2 HLL Models: The prover may be used to prove that 2 HLL models with the same interface (the same input streams and output streams) are equivalent. To do so, an equivalent model is produced with proof obligations stating that for all input streams values, each output of the first HLL model is equal to the output of the second model with the same name.

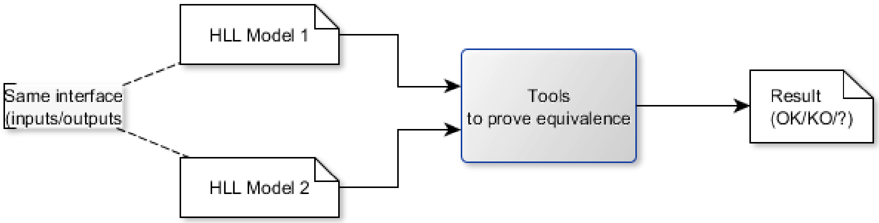

Figure 4: Proving the Equivalence of 2 HLL Models

3 Results

3.1 Proof of simple properties

Conditions to isolate, non-leading, unfitted,...

3.2 Verification of use case

Start of mission to describe

3.3 Comparison of Scade models

levels

4 Conclusion