Verification of SCADE models

Brice Gombault
Systerel

November 21, 2013

Abstract

This document describes the verification and validation processes applicable to SCADE models.

Contents

1 Introduction

SCADE is a model-based development environment dedicated to critical embedded software. It allows the modelling of a software specification using a graphical editor. It includes a code generator certified to the international safety standards EN 50128. This document describes the verification processes applicable to SCADE models. The verification of SCADE model is composed of the forth following parts.

- The verification of modelling rules that the SCADE model shall respect (SCADE rules and other specific rules such as naming or modelling rules applicable to openETCS project).
- The verification of the compliance between the specification requirements and the SCADE model.
- The verification of the compliance between the simulation of the SCADE model and the functional requirements defined in the specification.
- The writing of the report.

2 Verification processes applicable to a SCADE model

The verifier shall be independent and shall neither be Requirements Manager, Designer nor Implementer as defined in the safety standards EN 50128 v2011.

The input documents needed are all the necessary System and Software Documentation used for the SCADE design activity and all the documentation produced during this phase, such as the SCADE Design Description, the SCADE Design Test Specification and the SCADE Design Test Report.

2.1 Respect of modelling rules

Syntactic rules of SCADE language are verified with the Quick Check tool available in the publisher. If an error is detected it must be corrected or justified in the SCADE Design Description document by the designer. The verifier shall ensure that no error remains or the justification associated is correct.

For specific modelling rules the verification has to be made manually by the verifier and described in the Verification Report. A grid of verification may be created in order to prove the compliance of the model with the rules. On some cases, dedicated tools can be developed.

2.2 Specification traceability check

The verification of the compliance of the SCADE model with each requirement has to be made manually, by the verifier.

The Scade model shall be correct according to the informal requirements and the informal specification shall be completely covered : each specification requirement must be traced in the SCADE model. The specification requirements which are not covered by the SCADE model must be listed and justified in the SCADE Design Description document by the designer.

2.3 Testing and Validation of the model

The verifier shall control the activity of software testing performed by the tester.

The software testing uses the Model Test Coverage (MTC) and the Generic Qualified Testing Environment (QTE) tools from SCADE. Five steps are performed.

- Establish the Test Specification document.
- Writing scenarios in order to test the different functions independently.
- Running scenarios on the SCADE model.
- Extraction and analysis of results and the associated coverage.
- Establish the Test Report.

3 Results

All these different verifications activities shall be described in the Verification and Validation Plan, and their results shall be record in a Verification Report. Each disparity must be corrected or justified.

3.1 Verification report content

The verifier shall produce a Verification Report containing the proof of the compliance of the SCADE model. It shall include the following points:

- the identity, version and configuration of SCADE model;
- the verifier name;
- the goal of the Verification Report;
- the result of each verification process with:
  - items which do not conform to the specifications;
  - components, data, structures and algorithms poorly adapted to the problem;
  - detected errors or deficiencies.
- the fulfilment of, or deviation from, the Software Verification Plan;
- assumptions if any;
- a summary of the verification results.

4 Conclusion

The use of SCADE with its verification processes is compliant with the CENELEC norm but as it is not developed as open-source it is not compliant with the goal of openETCs project.