Unified Modeling Style and Unified Process Architecture: Model-Driven Design and Model-Based Verification key to safety and cost-reduction

Ralf Fachet

Esterel Technologies GmbH
Otto-Hahn-Straße 13b
85521 Ottobrunn-Riemerling
ralf.fachet@esterel-technologies.com

Abstract: Safety-processes and standards such as IEC61508 and ISO26262 are increasingly dominating the world of Software Development, and becoming a serious challenge for traditional approaches. The broad deployment of diverse methods and toolsets calls for a unified approach to design, process and verification. A proprietary approach with a "one size fits all" single vendor philosophy will not last into the future.

1 Introduction

Stringent requirements from safety standards such as DO-178B for aerospace, EN50128 for railways, ISO (WD) 26262 for automotive, and the meta-standard IEC61508 require specific attention and measures.

We are going to present an approach, which provides seamless integration across tools and methodologies using a meta- model/ open interface approach, a unified modelling style to transparently integrate data- flow and control- flow algorithms on model level, and a unified process approach to fully cover the requirements and objectives from safety and documentation standards.

2 Metamodel approach

In theory and science, Metamodeling has been around for a long time. The basic idea is to have a model of models which can be transformed into each other using model-transformation techniques. A Metamodel can provide several views and can also be used as a repository to extract information. In the past UML models where typical examples of metamodeling. Recent research goes into the direction to open this approach to other methodologies as well.

The tool suite SCADE (Safety Critical Application Development Environment) from Esterel Technologies has been developed with safety standard objectives as main design factor. From the beginning it was built around a UML metamodel approach. Model transformation interfaces based on open and documented interface provide the capability for model transformation from other metamodel standards (such as UML) but also even a means to translate proprietary models like Matlab/Simulink® into a component in a model of models by transforming them for example into a SCADE model.

The advantage of a model of models is seamless integration of the different phases of a project as well as the various subsystems of a complex programmable electronic system (such as hardware, systems software and application software). For example as SysML Framework may be used to depict the overall systems design. A SCADE model inside the framework may describe the application layer of the system and be used as base for automatic code generation and production of all certification collaterals.

3 Unified modelling style

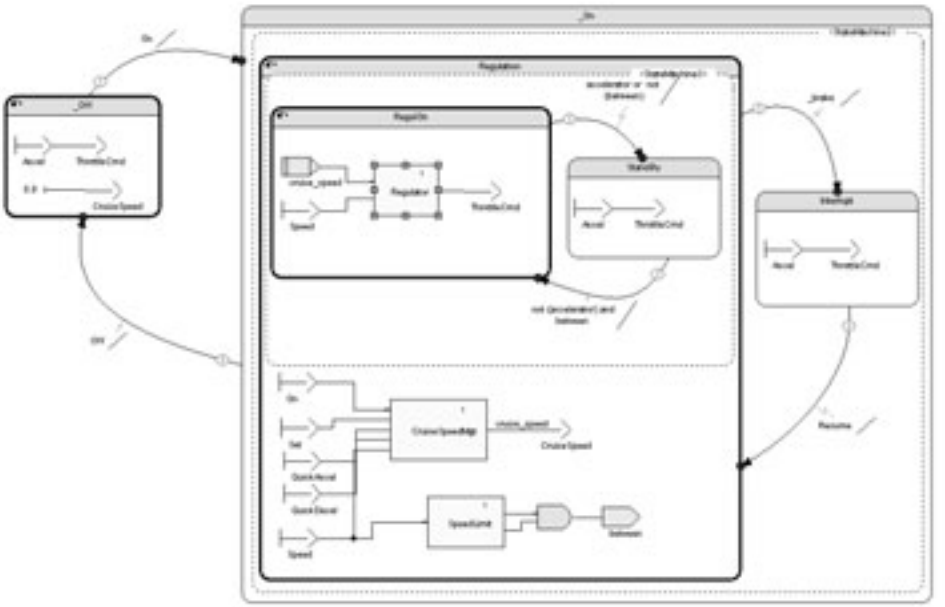
Model- based software engineering has evolved from traditional CASE tools to model-driven design methodologies. Since executable specifications have proven to be crucial for successful model- based design, pure documentation CASE tools have disappeared from the market.

Two tracks of modelling tools are widely deployed:

- Structure and analysis oriented tools, like the typical UML and SysML world
- Data-Flow oriented tools. Typically you see boxes that contain functionality and lines where the data flow between the boxes. Semantics might however vary widely.
- Control- Flow oriented tools: Typically you see state machines and event-triggered transitions from one state to the next.

While some of the existing tools require that the user moves to other methods in order to produce the software based on the analysis and design done in his tool (the other method often being handcoding), others provide means of autocoding. Some of the tools are either purely dataflow or control flow oriented, while others allow state-machine functionality to be plugged in by means of a separate tool which is coupled with the dataflow modelling environment.

SCADE now provides the possibility to seamlessly mix and stack dataflow and statemachines, and to integrate such a model into a system model of models so that for the first time the most complex applications can be fully expressed in a model- driven design flow.



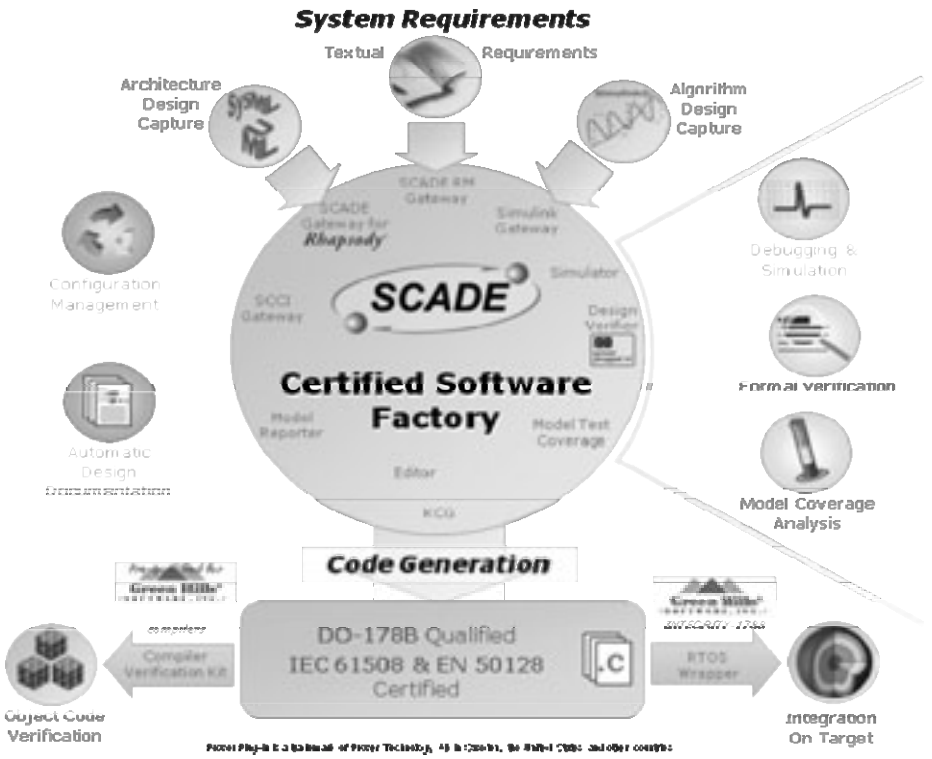
The dataflow and state- machines are not coupled on tool level but expressed in a strictly formalized modelling language. This formal model is then the source for automatic code generation and prerequisite for qualification of this automatic transformation step. The automatic code generator KCG 6 is therefore qualifiable to DO178B Level A, IEC 61508 and EN50128 as well as to all derived standards. The certification means that most code-level verification activities such as testing and reviews may be omitted in a safety critical project.

4 Unified process architecture

SCADE provides an open framework which serves as the backbone of as well the software development process as well as the validation and certification process. This open framework can be seen as the certification and software factory.

It takes in information from meta- models or functional prototypes and produces not only the certifiable software item but also manages the full certification workflow from system requirements to functional prototypes, algorithms and architecture done to the target- integrated application

Documentation, verification and validation are seamlessly connected as well as software development IDE, may the be vendor specific or open and eclipse- based.



As we see, this factory automates all steps that are necessary to produce safe software and also provide the safety proof. It follows the structure of the design, verification, validation, and certification processes but also provides structure and a efficient workflow to them.

The user can now ensure seamless interfacing to his system model, fully describe the needed functionality and model level and work in a fully integrated design, v&v and certification workbench.

SCADE provides the backbone and the open interfaces, enabling to use the right tools at the right place and allowing him to integrate his existing production islands into an efficient production cluster.