Using Model-Driven Engineering to Support Safety Assurance

Software Engineering and Technology (SET) Group

Safety certification is one of the most costly and time-consuming tasks in the safety-critical domain, such as automotive, railway and avionics. OPENCOSS [1] is a FP7 large-scale integrated project, started since October 2011. It aims to devise a conceptual certification framework for those safety-critical domains.

We have implemented our approach using Eclipse Modeling Framework work with certain plug-ins. For our demonstrations, we use two case studies: ISO 26262 and company X. Our key results are two different editors, which are shown in Figure 3 and Figure 4. In the two different editors, different domain concepts are added to the GMM.

An overview of our approach is shown in the Figure 1. We begin with GMM, then if needed, some domain concepts can be introduced into it. To support it, a MetaModel Refine Language (MMRL) is defined [3]. It is a simple domain specific language, which allows the user to describe their domain concepts using the provided operators. After this, a metamodel transformation could be executed to get SMM. Finally, a graphical editor, based on the SMM, could be automatically generated, which facilitates the user to build their models using those concepts from their own domain. According to different scenarios, our approach can be divided into two steps: updating and specialization (shown in Figure 2).

One of the key challenges of this project is to define a common certification framework as a core for specifying certification assets. As a result, a Generic MetaModel (GMM) of safety standards has been built [2], which allows patterns of certification assessment to be shared and supports cost-effective re-certification between different standards. Because the concepts in GMM are generic, it will bring some extra cost to interpret them and some ambiguities when using them. To address this, Specific MetaModel (SMM) is proposed.

We present a model-driven engineering approach to facilitate safety assurance. By using this framework, domain concepts or project related concepts can be kept, users do not need to change their current way of working, and the traceability from GMM to SMM is maintained using our MMRL. Besides, it could be used for mapping between different specific metamodels [4].

References