Alessandro Cimatti et al.: From Informal Safety-Critical Requirements to Property-Driven Formal Validation, Proceedings of The Sixth NASA Langley Formal Methods Workshop, p.7–8

From Informal Safety-Critical Requirements to Property-Driven Formal Validation

Alessandro Cimatti, Marco Roveri, Angelo Susi, Stefano Tonetta

Fondazione Bruno Kessler - Istituto per la Ricerca Scientifica e Tecnologica, Trento, Italy
{cimatti,roveri,susi,tonettas}@fbk.eu

Extended Abstract

Most of the efforts in formal methods have historically been devoted to comparing a design against a set of requirements. The validation of the requirements themselves, however, has often been disregarded, and it can be considered a largely open problem, which poses several challenges.

The first challenge is given by the fact that requirements are often written in natural language, and may thus contain a high degree of ambiguity. Despite the progresses in Natural Language Processing techniques, the task of understanding a set of requirements cannot be automatized, and must be carried out by domain experts, who are typically not familiar with formal languages. Furthermore, in order to retain a direct connection with the informal requirements, the formalization cannot follow standard model-based approaches.

The second challenge lies in the formal validation of requirements. On one hand, it is not even clear which are the correctness criteria or the high-level properties that the requirements must fulfill. On the other hand, the expressivity of the language used in the formalization may go beyond the theoretical and/or practical capacity of state-of-the-art formal verification.

In order to solve these issues, we propose a new methodology that comprises of a chain of steps, each supported by a specific tool. The main steps are the following. First, the informal requirements are split into basic fragments, which are classified into categories, and dependency and generalization relationships among them are identified. Second, the fragments are modeled using a visual language such as UML. The UML diagrams are both syntactically restricted (in order to guarantee a formal semantics), and enriched with a highly controlled natural language (to allow for modeling static and temporal constraints). Third, an automatic formal analysis phase iterates over the modeled requirements, by combining several, complementary techniques: checking consistency; verifying whether the requirements entail some desirable properties; verify whether the requirements are consistent with selected scenarios; diagnosing inconsistencies by identifying inconsistent cores; identifying vacuous requirements; constructing multiple explanations by enabling the fault-tree analysis related to particular fault models; verifying whether the specification is realizable.

The methodology aims at increasing the confidence in the correctness of the requirements. On one hand, with the adoption of a property-based approach, every requirement is associated with a formal counterpart; on the other hand, a semi-formal language is exploited to narrow the gap with the natural language. The verification techniques are optimized in order to deal with large sets of requirements. The granularity of the formalization allows to focus on different types and levels of abstraction based on the hierarchy and on the modularity of the requirements; furthermore, it makes it possible to perform what-if analysis, based on hypothetical changes to the

specification; finally, the diagnostic information helps in localizing the formalization mistakes and the corresponding specification ambiguities.

This methodology has been proposed in response to the call to tender ERA/2007/ERTMS/OP/01 "Feasibility study for the formal specification of ETCS functions". The European Train Control System (ETCS) is a huge set of requirements that defines a control system to guarantee the interoperability between the European rail system and trains. Due to its complexity, ETCS presents the mentioned issues at a high level of magnitude.