Potpourri of what? One year in a DA's life

Aryldo G. Russo Jr.[1], Thiago C. de Sousa[1] Haniel Barbosa[1], Paulo Muniz[2], and David Déharbe[3]

[1] AeS Group
{agrj, thiago.sousa, haniel}@aes.com.br
[2] University of São Paulo
paulo.muniz@poli.usp.br
[3] University of Rio Grande do Norte
david@dimap.ufrn.br

Abstract. In this article we present a collection of what we have been doing so far in the context of DEPLOY Associate program. Besides the progress of the pilot project, the development of a specification of a simple railway system called "dead man control", we also present some parallel developments, some theorical, some practical of the use of formal methods in industry. As the space is restrict, we present only some superficial information about what we are doing in these different but convergent projects.

1 Introduction

Due to the advances in technology, many safety functions that were handled by hardware are now responsibility of the embedded software. This fact triggered motivation to use formal methods in standards relevant to software safety [1]. Some standards can be followed to increase the equipment safety level. One of the most widely used is the IEC 61508 [2]. This standard presents four levels of safety (higher level, higher safety), the so called Safety Integrity Levels - SIL, and above the level 2, the use of formal method is required or suggested to achieve a certain level of completeness, robustness, and safety, that grows as the level grows. The goal of using formal methods is to produce an unambiguous and consistent specification that is as complete, error-free and with less contradictions as possible, however simple to verify.

The remainder of this paper is organized as follows: a brief AeS history and the reason for the use of formal methods in Section 2, the description of our ongoing projects in Section 3, and finally we reserve Section 4 for further discussions.

2 The AeS Group and Formal Methods

AeS Group is a Brazilian company and was created in 1991, and at that time it was working in the building automation field. By the year of 1998, it began his

involvement in the railway field, when the first Brazilian General Door Control System (GDC) for Rolling stock doors were developed. To address concern with safety, the AeS group decided to identify a formal method that would best fit the current GDC SIL 3-level requirements and railway industry standard practices and standards (as is the case of CENELEC EN 50128[3], an IEC 61508-like for railway systems).

Based on these previous information, and the constraints such as, the size of the company (at that date, AeS counted only with 15 employees, and most of them working on administrative tasks) and the lack of deep knowledge of the method itself, the AeS group decided, first, to study and use the B method[4] and, second, to look for assistance from academia, which was obtained from two Brazilian Universities (University of São Paulo and University of Rio Grande do Norte).

From that time, and after facing several pitfalls, AeS Group has acquired a reputation as a company that has the needed know-how to develop safety critical applications, and, nowadays, it is in charge of several training courses around the world teaching software development process for safety systems based on a formal method mind.

3 Ongoing work

In this section we present a summary of ongoing works of AeS R&D team. At this moment, we have five projects, all of them related to the use of B/Event-B languages in industry.

3.1 A Methodological WRSPM Approach to a B Formalization in an Industrial Setting

Requirements are often expressed in a natural language. Building a formal model of such requirements is still an open issue in software development. We propose a systematic approach to understand and organize requirements so that the construction of a formal specification is facilitated. We present an intermediate model that stands between the natural language requirements and the abstract model for the functional specification. This intermediate model facilitates traceability between the different artifacts produced in the software development process, which is a requirement for fulfilling international safety standards. Subsequently we present and analyze the results of trying to produce a formal specification from this intermediate model incrementally, along with descriptions and alternative solutions to the complications we faced. We present the application of this method to the requirements of a real public transportation system.

3.2 Lost & Found in Requirements - A Formal Help

In an industrial world, it's known that the requirement documentation is frequently poor, in the sense that only the essential information is presented. Moreover, this essential sense is based on the specifier feeling, normally an expert in

the subject, where fundamental information is not presented based on the hypothesis that is basic enough to be suppressed. On the other hand, when trying to implement the specification a lot of gaps emerge, even if when implementing in a non formal way. But, thanks to the necessity of proofs that come with the formalism, it becomes clear that some specification can not be implemented until the moment that all gaps are solved and the specification can be proved. In this paper we present, briefly, our experience during the DEPLOY Associate Program where we are in charge to specify and implement a project called "Dead Man Control". During this first year, we could see how the formalism could help us in find requirement problems, and, mainly, how to prepare the questions to the customer to fulfill this gaps.

3.3 UPside Down, Another way to see the same thing - LADDER to B

It's common to see several proposition to formalize a process in order to generate a source code, like, for example, from B to C or ADA. But, in industry, to force or to convince people to change the development process is always a difficult task. In this work we propose to use a common front end development environment, LADDER, and introduce the formalism behind the scene. In this way, instead of generating LADDER diagrams from a formal language, we propose to formalize the LADDER diagram, and prove that this is correct in relation to the specification.

3.4 A UML-based Method for Event-B Refinement

Event-B is a formal method that allows flexible modelling and refinement of systems. However, it is hard to convince developers to adopt it because they are not used to mathematical models. On the other hand, UML has become the de facto standard for software modelling since it provides an easy graphical notation. In this project we propose a method for Event-B refinement using UML. At this moment, we address refinement steps involving decomposition of events and machines using three popular artifacts: use cases, activity and sequence diagrams. We show a case study of an auto teller machine (ATM) to demonstrate how a use case realization by an activity diagram can be used to decompose events (also to introduce control flow) and, after that, how a sequence diagram can be used as complementary technique for splitting a machine into sub-machines.

3.5 Using the B Formal Method in the process of traditional software development for critical systems

Mass transport systems are considered the most effective and efficient public transport both in terms of population thoughts are the government bodies. Among them, the railway environment is highlighted by the speed of transport,

amenities, number of persons carried, among other factors. However, to guarantee the effectiveness of this transportation modality, they must provide this transport safely. To ensure such safety, various standards were created, some of them of general aspects and others dedicated to a specific domain. These standards require, for certain levels of security that formal methods are used during the development process to ensure that certain safety features are achieved.

Currently the traditional development process is not prepared, due their empirical characteristics, for a direct adoption of these formalisms. This point and counter-point, ie, the distance between the currently used and required by the standards should be eliminated so that the systems developed can be used in the railway domain.

This work presents techniques for using these formal methods, based on a structured development process. A method of application is presented, and the use of this method as well as the techniques described is validated w.r.t. its application in a pilot project, and subsequent comparison with the traditional development development. This comparison use certain metrics such as, for example, development time, number of software revisions until final acceptance by the customer and time required for testing for final validation of the system.

4 Discussions

In this short article we present, briefly, what's been done so far in the sense of application of formal methods in an industrial process in South America. We only pointed out some ongoing, future and past work to show the difficulties, but, moreover, the achievements of this attempt. Despite of all odds, we could see during this last year that a lot of people in the development process were not afraid to try something different and , moreover, they were willing for something to help to develop better (and easy to test and validate) products.

References

1. Bowen, J.P., Stavridou, V.: The industrial take-up of formal methods in safety-critical and other areas: A perspective. In: FME '93: Industrial-Strength Formal Methods, First International Symposium of Formal Methods Europe. Volume 670 of Lecture Notes in Computer Science., Odense, Denmark, Springer (1993) 183–195 1
2. Commission, I.E.: IEC 61508 - Functional safety of electrical/electronic/programmable electronic safety-related systems. International Electrotechnical Commission Standards (1998) 1
3. CENELEC: Software for Railways Control and Protection Systems. EN 50128. (1995) 2
4. Abrial, J.: The b-book: Assigning programs to meanings. books.google.com (Jan 1996) 2