SpaceSystems
Finland

TITLE:

Training Evaluation Document

Deploy

	FUNCTION	NAME	DATE	SIGNATURE
PREPARED BY	SW Engineer, SW Engineer	Tuomas Räsänen Laura Nummila	30.09.2010	
CHECKED BY	Quality Manager	FirstName LastName	30.09.2010	
APPROVED BY	Project Manager	Timo Latvala	30.09.2010	

REF:	XXX-OF-SSF-499
ISSUE:	0.1
DATE:	30.09.2010

Document Status Sheet

Issue	Date	Modified Items / Reason for Change
0.1	30.09.2010	First draft issue of the document.

Table of Contents

Document Status Sheet 2
Table of Contents 3
List of Figures 4
List of Tables 4
1. Introduction 5
1.1 Abstract 5
1.2 Abbreviations and Definitions 5
1.3 References 5
1.4 Document Overview 5
2. Background of the Engineers 7
2.1 Ms. Nummila 7
2.2 Mr. Räsänen 7
3. Progress of the work 8
3.1 Tools, Training and Assistance 8
3.2 The Effort in Different Phases of the Work 8
3.2.1 Timeline and Events 8
3.2.1.1 Mr.Räsänen 8
3.2.1.2 Ms. Nummila 9
3.2.2 Current Status 10
4. Assessment 11
4.1 Training Materials 11
4.2 Tools 11
4.3 Notable Difficulties 12
4.4 Suggestions 12
4.5 Learning Effort 13
4.6 Hypotheses about Event-B 13
5. Summary 14
Distribution 15

List of Figures

Error! No table of figures entries found.

List of Tables

Error! No table of figures entries found.

1. Introduction

1.1 Abstract

The purpose of this work was to find how much effort is needed for an engineer without background in formal methods to become a competent user of Event-B, and to evaluate the currently available training material, documentation and tools. The work also provides input for analyzing some hypotheses (TSP-HM-1, TSP-EA-1) [RD2] concerning the use of formal methods.

Two engineers without previous background in formal methods learned to use Event-B in the Rodin environment. They studied until they were able to independently build simple models. At a later stage, also Modularization Toolbox was studied, and a model built. The Record Types plugin was also studied to some extent, but the modeling work was mainly learning from the existing examples.

Depending on the engineer, it took about one man-month (1.3, respectively 0.9 months) of partly tutored study to be able to work with reasonable independence. By 'reasonably independent', we mean an ability to design and implement simple models and also to learn more by consulting documentation and occasionally an expert. The tools used in the learning process (Event-B, Rodin, plugins) were generally considered good for their purpose, but the available training material appeared to be incomplete. The use of Modularization Toolbox seems to help in building of complicated models, but at least from a new-beginners point of view also complicates the modeling process.

1.2 Abbreviations and Definitions

Abbreviation	Description
AABO	Åbo Akademi
FM	Formal Methods
SSF	Space Systems Finland
TBD	To Be Defined

1.3 References

[RD1] http://www.event-b.org/

[RD2] D30 – Initial Evidence Repository (Pilot Phase) – V1.4, Project DEPLOY, 17.02.2010

1.4 Document Overview

Chapter 1 Is the introduction.

Chapter 2 Describes the process of the work, and the methods used.

Chapter 3 Contains an assessment of materials and tools used, and some discussion about the usefulness of the method.

Chapter 4 Contains the conclusions.

2. Background of the Engineers

2.1 Ms. Nummila

Ms. Nummila is a software engineer having M.Sc. degree in computer engineering. The university studies were focused on embedded systems and software production.

Except for an introductory university course in formal logic and fundamental structures, Ms. Nummila has no background in use of formal methods. Most recent work experience is on onboard SW component implementation, unit and validation test design, unit and validation test implementation and quality assurance in high reliability software projects. She has been working at SSF since October 2006.

2.2 Mr. Räsänen

Mr. Räsänen is a software engineer with a M.Sc. degree in medical physics and electronics. The studies included a substantial portion of digital signal processing.

He has no formal background in Computer Science; the programming skills are a result of a long practice of building computer-controlled measurement and test systems. At the time of the study, he had worked about 11 years at SSF, doing mainly functional testing of space software. This work included building test environment. Recently, he has also worked in qualifying an embedded system according to industry standards. The current study is his first contact with formal methods.

3. Progress of the work

3.1 Tools, Training and Assistance

The basic modeling environment was the Eclipse based Rodin platform. The platform is continually being updated to answer the needs of the users and the development of Event-B.

The Rodin platform has an internal Event-B editor. It is interactive; the user can create templates for different Event-B language components and fill them in. The editor also contains a Pretty Print –tool that displays the Event-B code with all its special symbols.

Another alternative for editor is Camille that looks and behaves like a text editor with syntax highlighting.

Since the spring 2010, two new plugins have been added: Modularization and Record Types. Some documentation for them can be found in the Event B Wiki [RD1].

The training material consisted of the Event B Wiki, teaching material from the training course held in Zürich in April 2008, Web, and general University teaching material about formal logic. The Zürich course contains lectures, exercises, summary presentations and Rodin models. Some material about the B Method was used as a reference. Assistance from more experienced Event-B programmers was needed, especially in the beginning of the training phase. From SSF, Dr. Dubravka Ilic and Dr. Timo Latvala were the persons to contact for help. Also Prof. Elena Troubitsyna and Dr. Linas Laibinis from Åbo Akademi (AABO) were available for assistance via email.

3.2 The Effort in Different Phases of the Work

3.2.1 Timeline and Events

3.2.1.1 Mr.Räsänen

In the early part of the study, Mr. Räsänen consulted colleagues, who had experience with Event-B and the Rodin environment, particularly Dr. Ilic. He acquired the above mentioned learning materials gradually, over the early spring 2010 (the Modularization Toolbox material was produced later).

04.01.2010 – Mr. Räsänen joined the project, and started the studies by installing the Rodin platform and learning the basics of its use. The work went on intermittently, other projects allowing, and continued in gathering and reading different types of Event-B material. A major part of the work was studying lecture notes of an example, which at the same time made an extensive tutorial of the Event-B language. This phase took the effort of 66.5 h, or about nine days.

24.03.2010 – Mr. Räsänen continued training by writing in the Rodin environment a complete example that was described in the lecture Bound Retransmission Protocol. The work was finished, when all proof obligations were satisfied. This took 32.3 h, or about 4.5 days.

06.04.2010 – The next phase for Mr. Räsänen was to independently build an own model based on what was then understood to be a packet exchange protocol in another project. This phase included a 3 h tutorial session, where more advanced viewpoints and methods were explained. The model in question was repeatedly rewritten, and two out of three refinements were ready, when this phase ended. This phase took 111.2 h, or about 15 days.

05.05.2010 – **Meeting**, concerning mainly training with Prof. Troubitsyna and Dr. Laibinis from AABO. Mr. Räsänen had a presentation explaining his progress so far, as well as some analysis of the process.

06.05.2010 – Mr. Räsänen continued refining the previously mentioned packet protocol model, until he considered it as ready. This phase took 22.5 h or about three days.

20.05.2010 – **Meeting**: A training session organized by Prof. Troubitsyna and Dr. Laibinis. The training in to morning consisted of basic concepts of Event-B. Mr. Räsänen had caught cold, and was obliged to leave after the lunch.

24.05.2010 – Mr. Räsänen studied the Modularization Toolbox, using the material delivered during the meeting 20.05.2010 (a parking gate example). This phase included downloading the model implementing the example and investigating it in the Rodin environment. The effort of this phase was 24.4 h, or a bit over three days.

3.2.1.2 Ms. Nummila

Ms. Nummila joined the project at a later phase in May 2010. Due to Dr. Ilic's commitments to other projects she wasn't available for consultancy, and the learning process was mainly self-study. In case severe problems were encountered in the modeling work, Dr. Laibinis and Dr. Latvala were available for getting the assistance needed.

05.05.2010 – Meeting: Ms. Nummila joined the Deploy project by attending a meeting with Prof. Troubitsyna and Dr. Laibinis. The meeting mainly concerned training and planning of the future activities.

18.-19.05.2010 – Training: To prepare for the following training session, Ms. Nummila spent 14.5 hours installing the Rodin platform and getting familiar with the available documentation (Event B Wiki, university teaching material).

20.05.2010 – Meeting: A training session organized by Prof. Troubitsyna and Dr. Laibinis. The first part of the training consisted of learning the basics of the Rodin platform and building a couple of simple models with some assistance from Dr. Laibinis. The latter part was concentrated on a presentation of a modular model description (Parking Lot).

21.05. – 28.06.2010 – Modeling: Based on the description of the modular model, Ms. Nummila first built a monolithic model of the Parking Lot. When the monolithic model was ready and she was more experienced in using the Rodin platform and the Event B language, the modular plugin was installed and a modular model of the same Parking Lot example was built. The work was quite independent, but a few questions were asked from Dr. Laibinis and Dr. Latvala about some problems faced in the use of the Rodin platform and the Modularization plugin. The amount of time used for building of the two models was 109 hours or approximately 14.5 days.

3.2.2 Current Status

The engineers have acquired an ability of independently developing Event-B models, and implementing them in the Rodin environment. They are able to study further the Modularization Toolbox, and to use it, at least slowly in the beginning, in developing more complex models.

4. Assessment

4.1 Training Materials

The lecture materials and presentations in the Zürich Course are good in explaining many different aspects of Event-B and showing its use by examples. The examples are also implemented as ready models.

Event B Wiki is a fairly comprehensive tutorial for both the Rodin platform and the Event B language, but documentation for some of the latest plugins (record types, teamworking) seems unfinished. Any information not available in the Event B Wiki was very difficult to find elsewhere either.

At present, a student will have difficulties in deciding where to begin. An outline telling about the general features of Event-B, and showing from which material to start, would be useful for the student.

A systematic reference material going through all features of the Event-B language would be very helpful. During the work, no description was found for EQL, a fairly common proof obligation. This was the only obvious omission, although it was rather difficult to find detailed information about other proof obligations as well.

4.2 Tools

The basic features of the Rodin environment are easy to use, once the user is familiar with the Eclipse platform (it's a good idea to go through the Eclipse tutorial). The Event-B Editor is interactive, and supports new features (currently modularization). Camille is quicker to use for the experienced people, and the code is much easier to read than in the Event-B Editor or Pretty Print. On the other hand, Camille doesn't show all symbols used by Event-B. Currently neither Camille nor Pretty Print supports the Modularization Toolbox.

The Rodin platform, and the tools and the documentation incorporated into it follow closely the development of Event-B. However, the tools and the documentation haven't had the time to catch up with the development of the method. Some issues worth noting are:

- Some minor practical matters about the use of the platform seem to be omitted that are self-evident to the writer of the documentation, but far from obvious to a novice user (e.g. how the action numbering does not start from zero in a refined Initialization Event etc.).
- Camille editor has some stability problems. One must also be very careful, when copying and pasting – the structure of the code may get mixed. With mysterious errors, it is worthwhile to check in the Event-B Editor, what the code actually looks like.
- The Rodin platform Help is not quite complete. This is particularly obvious in the Proof Control part.
- At least on Windows, the Rodin platform sometimes gets frozen. The usual cause for this was having several machines/contexts open at the same time, and then trying to expand one of them. The only recovery is then restarting the whole platform.

4.3 Notable Difficulties

At the beginning, it is difficult to learn the right approach. A programmer's instinct is to start from a basic functionality, and expand the system to have more and more properties. On the other hand, the approach of Event-B is to look at the whole system from the beginning, first from a very general, abstract outline. The general, abstract features are then gradually filled in with finer detail.

It is not easy to find information for a particular need from the current material. The most effective way is often to search Internet for the answer; this tends to lead to Event-B Wiki. Sometimes the answer is not found. At the current stage of the documentation, help from a more experienced user is vital. One advantage brought by the graphical user interface is that some of the problems could also be solved with trial and error method. Of course this is more time consuming, but is also the only option left if the documentation doesn't provide the answer and no experienced colleagues are available for consultancy.

While working on the modular model, some of the Rodin problems (errors/warnings) were difficult to track. The error messages were too vague, and didn't clearly specify in which part of the model the problem was. After gaining some more experience of using the modularization plugin it became easier to associate the errors with their origin, but this was only based on simple knowledge of which trigger to pull to make a certain error message disappear.

4.4 Suggestions

A comprehensive Event-B and Rodin reference material, including *e.g.* the complete Event-B notation and all types of proof obligations fully explained, would be very useful, when the learning user begins to gain independence. This reduces the need to consult an expert every once in a while. The documentation would need to be organized so that leads to all the different topics can be found from a central chapter or a document.

Event B wiki page has a short FAQ, but it might be useful to expand it by adding some generally known problems in the use of the Rodin platform. This would help the new users to overcome some of the difficulties the others have already encountered.

Proving is largely an automatic mechanism, but it is central to Event-B. For novice users, it is largely a black box. Even somewhat more advanced users cannot yet understand how the proof obligations get proven. Therefore, one should put a special emphasis on the documentation about proving and of the Proof Control part of Rodin.

It should be noted, that as both Event-B and the Rodin platform are still under development, it is understandable that the documentation for all the latest plugins is not always up-to-date. Anyway, from a novice user's point of view it might be better to omit the new features until their documentation has been completed. On the other hand it is assumable that the group of researchers working on the development of Rodin wants to get the latest updates from everybody as soon as possible, documented or not. This problem could be solved by clearly declaring which plugins are suitable for a regular user with all the existing features explained in their documentation. The newly added plugins that are still beta versions could still be available for the developers to test and improve the latest additions, but then the novice user would not get confused about unfinished features.

4.5 Learning Effort

It took about a month's worth (1.3 resp. 0.9) of working time to learn Event-B and Rodin well enough for reasonably independent work. Because both students were at the time occupied by other projects, the calendar time was about four resp. two months. This information has been used to give numerical values to the hypothesis TSP-HM-1.

4.6 Hypotheses about Event-B

TSP-HM-1-Hyp3 - For developers and analysts with no background in FM, a training programme and/or individual coaching needed to become autonomous with Event-B modelling and proofing takes at most XXX months and requires YY% of effort (per engineer) over that period.

The participants of the current study used approximately 2 – 4 months with 50 % - 25 % effort to achieve a reasonable independence.

TSP-EA-1-Hyp2 - An engineer with no or little FM background takes at least 6 months to become autonomous when spending at least 50% of her/his time on training and practicing with a new formalism. (Some advanced training or monthly individual coaching from experts will also be required during these 6 months).

The experience from the current study suggests that the time of 6 months can be cut into half. Consultation with an expert user will occasionally be necessary in order to obtain advice and feedback.

5. Summary

It has taken the hours of about one working month to attain the ability of working with Event B and Rodin in a reasonably independent fashion. Consultation with expert users is still needed at this level.

Almost all necessary information can be found from the documentation listed in Ch. 3.1. but searching for it can be quite difficult. Organized documentation is needed, including a full reference material, where all the details of Event-B and properties of the tools can be found. This will help disseminating Event-B and its tools to wider circles, as the need for expert consultation is reduced.

The skills learned during the period of this study may be of use, when designing a complex system. It is not possible, however, to estimate the benefits with the present level of experience.

Distribution

Nr	Destination
1 original + XXX copies	XXX

(End of the document)