**ABSTRACT**

This thesis describes a plugin which was created for developers who intend to design their models using the Event-B language. Event-B is a formal language which uses mathematical techniques for system modelling and verification. The accuracy of the model is ensured by proof obligations. The main disadvantage of the Event-B is that it doesn’t have many well-developed modularization constructs and it is not easy to combine specifications in Event-B with those written in other formal languages. Developers can use the plugin described in this thesis if they want to make changes in the existing model such as element renaming or merging, without writing new elements from the scratch. Developers can use their knowledge of the institution theory and specification based operators to interact with the plugin.

Software development requires from the developer not only an accurate and clear structuring of the system, as well as efficient tests for finding bugs, but also a strong mathematical proof. All these components allow software to be reliable and eliminate the possibility of system failure. The more complicated the system is, the more difficult it becomes to make sure that it works correctly and, in this context, mathematical proof can help to show the absence of bugs.

**CHAPTER 1**

**Introduction**

Developing dependable systems is one of the most important targets in software development nowadays. Technologies are involved in nearly everyone’s daily life. People use smartphones, laptops, and different vehicles to solve their everyday problems. They rely on their gadgets which sometimes can work improperly and cause trouble. In those situations where the systems should be reliable and should work stably all the time, software, on which these systems are based, has to be verified. Verified software allows the user to be sure that it will work accurately in any situation. Reliable software usually is very expensive and is used in situations when any software fault can cause huge money losses or endanger people’s lives. To decrease the danger of money losses or security risks, scientists analyze all the possible variants of the system’s behavior and software developers design systems which work stably all the time. But analyzing the system is very time-consuming and difficult work, and requiring the developer to be sufficiently concentrated all the time is sometimes impossible.

To solve this problem and eliminate the human factor special tools have been developed. They allow the developer to verify their software easier and faster. One of these tools is the Rodin Platform, which provides effective support for refinement and mathematical proof [http://www.event-b.org]. Event-B is not the only language which can be used in verification, but is one of the most popular ones. The practical work of this thesis is based on creating a Plug-in which manipulates Event-B elements with the help of formal expressions. The Rodin Platform is Eclipse-based, so the Plug-in is written in Java. The work in this thesis should also help people who are familiar with the theory of institutions and specification-based operators (SBOs), but not familiar with Event-B syntax, to more easily manipulate Event-B elements by using SBOs inside the Rodin Platform.

* 1. **Motivation**

During the last couple of decades, the popularity of the software increased vastly. No one can imagine the work of banks, schools, hospitals without using modern technologies. Almost every single household appliance works under the control of software. Even the timetables for public transport are not created manually any more. People trust the software to control airplanes and train traffic. While life has become more convenient, it has also become more dangerous at the same time.

If software development is quite difficult work, then reliable software development is much more difficult. It requires not only accurate and clear structure and efficient tests to find the bugs, but also strong mathematical proofs. Software verification is very important, because the software testing can show the presence of the bugs, but never their absence [Dijkstra]. Software verification can be done using formal methods. While studying formal methods, I met the problem that knowing only theory of institutions is not enough to start working with tools which provide software verification. One should not only understand the logic of the verification, but although study the syntax and logic of the verification language and tool one uses. Each platform has its own features and to study them all, a person would have to spend lots of time. It is not often easy, because developer may want to try another language and another tool and should start studying formal language and verification tools from the very beginning. If there is code written in some formal language, it becomes another problem to translate this code to another formal language. Event-B is quite popular language, but there are some known concerns regarding the using of Event-B formal language:

* it doesn’t have well-developed modularization constructs and it is not easy to combine specifications in Event-B with those written in other formalisms [Marie’s paper];
* The Rodin Platform, which maintains the Event-B language is quite big and has lots of features, so it becomes quite difficult to start using it without knowing Event-B;
* If the developer is familiar with the theory of institutions, but not familiar with the Event-B, it will be hard to start working with Rodin Platform.

This theme for the thesis was chosen to decrease developers’ efforts in writing dependable software and to make creating it as easy as possible. The best way of doing this is to make it possible to use the Rodin Platform to write some specification-based operators and manipulate with elements, written in Event-B. This will allow the user to save time and to speed up the software development. Developers, using formal methods to prove their programs will have the opportunity to get a flexible tool which can be used to write proof obligations not only in Event-B, but also with the help of specification-based operators, and then to manipulate Event-B elements without knowing its syntax. The main currency nowadays is time, so studying lots of formal languages and understanding the main features of the tools, which use these languages, requires lots of time that can be spent on better software design.

* 1. **Overall project objective**

This thesis will provide a solution for the problem, which has been described in the previous part. The benefit for developers will be in the opportunity to use the Rodin Platform to make changes in Event-B models not only using the Event-B formal language, but also using the specification-based operators. One of the most important features of the created plugin is the renaming Event-B model elements (e.g., machines, events, variables), as this becomes a huge problem, when the model is quite big and the renamed object is used in different places. Renaming can also cause problems in proof obligations, one of the specific parts of formal languages, so it was important to keep this part valid and avoid errors caused by the renaming. The second big part of the plugin is merging two machines together, combing their variables, events, etc. This feature will allow two machines to combine their properties into one machine without creating new machine from scratch. Despite the fact that separate renaming (refactoring) and composition plugins already exist, our new plugin will combine these two features and will be scriptable using by specification-based operators. The developed plugin will simplify the verification of software in formal languages and save time during the development of reliable software systems.

**1.3 Research question**

The main question of the project is **RQ1**, *how can software verification be simplified for the developers?* This question is divided in two separate research questions, RQ1.1 and RQ1.2.

* **RQ1**: how can software verification be simplified for the developers?
* **RQ1.1**: how can developers, using different formal languages use the Rodin Platform without the necessity of studying the Event-B language?
* **RQ1.2**: how can renaming and machine composition be implemented without any errors in the corresponding proof obligations?

These questions describe the main idea of the current project. Understanding of what is done in this field and studying the existing plugins and projects will be the first step in answering these questions. The existing plugins may help in designing the new one in a simpler and more efficient way. With a firm understanding of the work done in this research field, the work that should be done will become more precise. The resulting developed plugin will provide developers with short and easy to use tool which will allow them to use Event-B models without spending long time studying and understanding all the Rodin Platform features.

**1.4 Solution**

To solve the above stated questions, the plugin for the Rodin Platform was designed and developed. This plugin will simplify the development of reliable software systems and help developers to start using the Rodin Platform simply and without huge effort. The plugin will use the existing Event-B models and manipulate their underlying representation. The plugin supports input validation and indicates if some problems can occur during the execution of the operations (renaming or composition). The plugin is developed in Java and uses the Event-B abstract syntax tree in the syntax analysis part of the development. This approach allows user to make necessary changes without the necessity of parsing the XML-files, which Rodin uses to store the Event-B project. The plugin is addressed to developers who want to verify software and who are familiar with the theory of institutions and specification-based operators.

**1.5 Structure of the thesis**

The project is separated into six chapters:

*Chapter 1:* the current chapter, introduces the initial problem, describes the motivation of the current project, states the research questions and solution of the problem in brief. This part also describes the current problems of using the Rodin Platform.

*Chapter 2:* this chapter presents the background research, it names and describes in detail two plugins that are most closely related to the current project and shows their advantages and disadvantages. This information is used in the next chapter a comparison between this project and existing plugins.

*Chapter 3:* this part defines the key requirements for the project and describes the design and implementation phases of the development process.

*Chapter 4*: this chapter represents the evaluation the work and states if all the key requirements were met and includes the comparison with existing plugins, mentioned in chapter 2.

*Chapter 5*: this part describes the case study.

*Chapter 6*: the last chapter of the thesis contains conclusions, where the value of the work is described and the future possible work is outlined.

**CHAPTER 2**

**Background and related work**

Formal reasoning is a very ‘strict’ type of reasoning, and it helps to find answers and make decisions between the conflicting sentences, ideas or opinions of different people. Formal reasoning is based on a certain form of arguments, which are declared to be true. Those arguments which contradict these arguments, become false accordingly. The conclusion, which is based on true statements, is supposed to be true as well. Formal reasoning usually reasons in terms of formal logic, not simple words. There are several languages, based on formal reasoning, in existence. One of the most popular languages based on formal reasoning is Event-B. It was developed by  [Jean-Raymond Abrial](https://en.wikipedia.org/wiki/Jean-Raymond_Abrial) ([France](https://en.wikipedia.org/wiki/France)) and is based on the B language. The main difference between B and Event-B is that Event-B has simpler notation, it is easy to learn and use and it has more features. It is used in many industrial projects and allows users to create systems and verify them.

**2.1 Event-B**

Event-B is a notation for formal modelling based around an abstract machine notation [Rodin User’s Handbook]. It allows the user to verify difficult real-life tasks. There are some examples of using verification in daily life: smart-grid modelling and railway interlocking models. Verification of systems is used to ensure the safety of people or to avoid costs caused by the improper operation of the system. The main advantage of using Event-B is that all development errors in the model can be easily found since in incomplete and inaccurate models some proofs cannot be done.

**2.1.1 Contexts and machines**

Event-B models consist of two main parts: contexts and machines. The context shows all static parts of the model, while the machine represents the dynamic parts of the model. These two main parts allow the user to create efficient models and to describe the behavior of the system. The key feature of Event-B is that the primary model can be really simple, but with the help of refinements, it can be gradually improved and become sufficiently complicated. The term “refinement” applies to the dynamic parts of the model, so-called machines. One of the most famous introductory example of Event-B modelling is the “Controlling Cars on a Bridge” model [5]. It describes a set of traffic lights for cars crossing the bridge from the mainland to an island and vice versa. The first model developed for this study case was really simple, it had island and bridge joined together and only two colors in the traffic lights: red and green, while the final model had not only traffic lights, but also car censors and all three parts of the case study – island, bridge and mainland. This example shows the idea of the refinement – gradual improvement of the model using refinements.

**2.1.2 Events**

The main part of machines in Event-B is the event. At the beginning of development there is just one event in each created machine – the INITIALISATION event. This event is used for initializing any variables shared between the events. No one model can work properly without this event. When developing the final model, different events can be created to describe the model. Each event should describe one action in real life. In the given example “Controlling Cars on a Bridge” there are different events describing “A car is leaving the mainland and entering the Island-Bridge”, “A car leaving the Island-Bridge and re-entering the mainland”, etc. The more precise a model becomes, the more events it usually includes. Events can either have no guards, or they can be also simple and guarded (keyword where) or they can be parameterized and guarded (keywords **any** and **where**) [2].

**2.2 Theory of institutions and SBOs**

Despite the fact that Event-B is a quite popular language and is used in industry, it has a great disadvantage - it doesn’t have well-developed modularization constructs and it is not easy to combine specifications in Event-B with those written in other formalisms [Marie’s paper]. Modularization constructs are the basis of the general theory of institutions. What is an institution? The concept of institution is introduced to formalize the informal notion of “logical system”. Institutions enable abstracting away from syntactic and semantic detail when working on language structure “in-the-large”; for example, language features can be defined for building large structures from smaller ones, possibly involving parameters, without a commitment to any particular logical system. This applies to both specification languages and programming languages. Institutions also have applications to such areas as database theory and the semantics of artificial and natural languages [1]. A specification is the main modelling unit in an institution, but specification language is not a programming language, this is a collection of sentences about programs [1]. For a (pure) logical programming language, the specification is also a program [1].

The key concepts in the theory of institutions are:

* A specification is the main modelling unit in an institution.

In terms of Event-B, a specification is referred to as a component: i.e. it is the description for either a machine or a context. In the theory of institutions, a specification consists of a signature along with a set of sentences over that signature.

* The signature of a specification is the set of names used in that specification.

For an Event-B machine this is the set of (global) variables and event names. For an Event-B context this is the set of constant and set names. We don't worry about the names of invariants, guards and axioms, since these are just labels for information and can't be seen by other specifications.

* The sentences in a specification are just the predicates that define things.

In Event-B machines these are the invariants, guards and actions; in Event-B contexts they are the axioms.

**2.3 Existing Event-B plugins**

The Rodin Platform, which supports the Event-B language, is a simple and easy-to-use tool, but its’ functionality is limited. This limitation doesn’t allow users to manipulate Event-B elements and use all the features of this language. Developers from all over the world try to make the use of this tool as simple as is possible. They provide plugins which allow user not only to edit the text of Event-B program (Camille editor), but also to create visual representations of the models (UML-B plugin), animate proofs (ProB animator), rename model elements and make compositions of several models. These plugins allow developers to create very precise and smart models and discover new features of the Event-B language. More details about two plugins closely related to the plugin described in this thesis are given in the following subsections.

**2.3.1 Refactoring framework**

The initial work of the Refactoring framework was done by Sonja Holl [3]. The author identified the problems related to refactoring in formal specification languages like B (and Event-B) due to the presence of proofs. The refactoring of such languages would need to be very good in order to avoid breaking proofs. This plugin was created to provide a possibility of renaming elements of the models written in Event-B. Users can rename not only machines and contexts, but also variables, variants, invariants, events, etc. via this plugin. To do so, the user should right click on the element he wants to rename and choose the new name. This simplicity allows the user not to worry about the proof obligations becoming inconsistent, because the plugin works very carefully and renames elements in such a way that proofs don’t break.

The plugin has several updates, the latest version is 1.3.0 and based on Rodin 3.0.x. During the dozens of updates, the plugin became powerful tool with good functionality and user-friendly interface. It includes not only renaming for main parts of the Event-B model such as machines and contexts, but also small parts of these parts, such as variables, invariants, events, constants, axioms, etc. It also allows users to keep the proofs valid during the renaming. During its execution, the plugin operates with three trees: a dependency tree to match all the dependencies between the renaming object and other objects in model (such as variables in invariants or theorems), an abstract syntax tree of the Event-B language to get access to all of the elements of the model, and a proof tree to make changes in proof obligations without breaking them. Even though the plugin’s main functionality is simple renaming, it allows users not to waste their time on creating new elements with other names and deleting unnecessary elements which can cause the crash of the whole system. Figures 2.1-2.4 contain screenshots of the user interface of this plugin showing the main flow of the interaction between user and the system. Figure 2.1 represents the plugin call, caused by right-clicking on the renaming element, and Figure 2.2 shows the dialog window asking user to input the new name. After the valid input of the new name, the plugin checks if any problems can appear during the renaming (Figure 2.3) and then starts renaming (Figure 2.4).

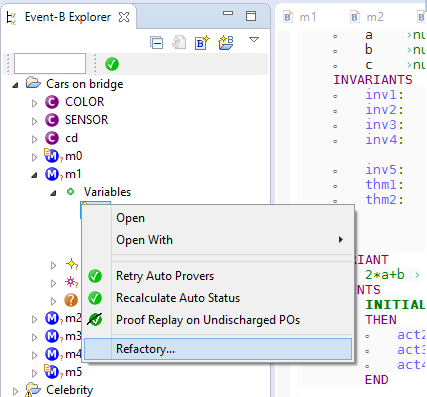


Fig. 2.1 Refactoring (renaming) plugin call

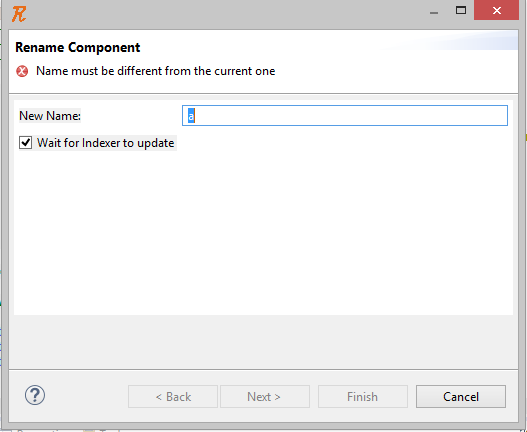


Fig. 2.2 New name input

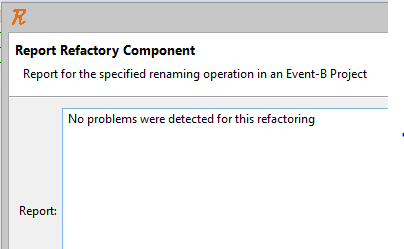


Fig. 2.3 Problem report

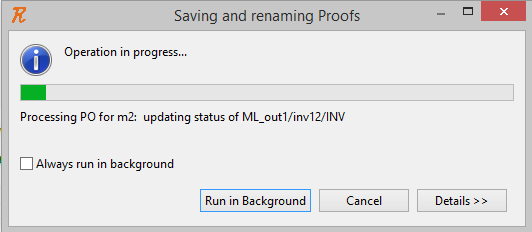


Fig. 2.4 Renaming in progress

**2.3.2 Feature composition plugin**

A feature composition plugin was developed by Ali Gondal (University of Southampton) and compatible with Rodin 2.0. This plugin allows user to build a composition model of the input models. The new model is also an Event-B model and is saved in Rodin database. This smart plugin highlights potential conflicts when joining models such as declarations of the same events or variables in both models. It also allows the user to resolve conflicting situations by removing the repeating/redundant information in different models. The composition editor also provides option for merging events [http://wiki.event-b.org/index.php/Feature\_Composition\_Plug-in].

The composition of several models created by this plugin allows the user to obtain a model with the necessary properties without long manual development. The dialog window of the feature composition plugin shows all available elements such as variables, invariants, events, etc. which can be used in the final composition model. The user can select/deselect these elements depending on planned idea of the final model. Besides allowing for the possibility of making a composition, the plugin allows the user to merge two or more events by creating a new event. However, the plugin doesn’t allow the user to compose variants and theorems. The tool is also capable of composing features at different refinement levels. The composite feature is a typical Event-B model and is automatically checked by the Rodin static checker for any errors [4]. This plugin is a prototype project of the feature composition tool and the developers claim it will be improved in future versions. It was created because the feature composition tools that existed before didn’t use all of the capabilities of the Event-B language and only provided user with small number of features. The developers claim that new versions of this plugin will be able to deal with proof obligations and create compositions based on existing proof obligations.

**2.4 Summary**

In this chapter we talked about Event-B language features, the Rodin Platform and its plugins which can be used to manipulate Event-B models. Two existing plugins were described to show key points of the renaming and composition of Event-B models. Some basics of the institutional theory were given to represent the advantages of using SBOs while operating with different formal languages. As the main problem of Event-B is its’ ‘non-standard’ syntax, the next chapter represents the solution which is based on implementing the Event-B editor which supports SBOs and has a functionality of two plugins described above.

**CHAPTER 3**

**Solution**

**3.1 Requirements specification**

The requirements to the generated plugin based on the research questions, introduced in chapter 1 and existing projects, which were mentioned in chapter 2. There are 5 requirements stated below.

**R1 – The plugin should be easy to use for all the users of Rodin Platform**

Despite the fact that all verification languages based on the same principles and use the same logic laws, the syntax of these languages can vary significantly. The user of the plugin should have some idea of working with Event-B and be able to manipulate its elements. The plugin will help any user to rename any element of the existing model without difficult and time-consuming manipulations. Even if the user hasn’t been working with the Rodin Platform for a long time, he will be able to call the plugin and write commands, based on specification-based operators. If the Rodin Platform user is more advanced, he will be able to learn specification-based operators and combine Event-B specifications with other languages specifications easily.

**R2 – The plugin should allow the user to rename Event-B elements and compose machines**

The main features of the plugin are renaming of Event-B elements and composing of machines. As there are existing plugins with the same functionality, but working separately, the goal of this plugin development was to combine features of these two plugins into one plugin and to make unusual way of communication with the system. The implementation of the specification-based operators in Rodin Platform will help to make the Event-B language more ‘standard’ and will allow to combine specifications in Event-B with other formal languages specifications. This standardization will allow developers using different formal languages to work on one project simultaneously.

**R3 – The plugin should not allow to make changes if the input is incorrect**

The main idea of this part is to prevent program execution if the user input is incorrect. As Event-B provides the proofs of the system, incorrect data input can make these proofs inconsistent. The plugin should not only be user-friendly and simplify models development, but it also should keep the system stable and not allow to execute operations which can make proof obligations inconsistent. Despite the fact that Rodin core catches some exceptions, the plugin should now allow the user to come over Rodin limitations and make harm changes in the working model.

**R4 – The plugin should give user information about incorrect data input**

This part is very important in software development. The feedback from the program shows the user any possible mistake he could make. There are several common mistakes that could be identified by the plugin. First of all, user can write element name incorrectly and the plugin display the message that the element with the given name doesn’t exist. Another way of making a mistake is to specify the same name for the renaming element as it already has or do not specify new name at all. Third possible mistake is misspelling of the key words or placing them in the wrong place of the command. As the Event-B language is case-sensitive, all the commands should be written in lower-case and the names of renaming elements should match the elements name in the model. In other case the plugin will not identify elements.

**R5 – The plugin should manipulate Event-B models with the help of specification-based operators**

As was mentioned above, the main disadvantage of the Event-B language is that it doesn’t have well-developed modularization constructs and it is not easy to combine specifications in Event-B with those written in other formal languages. The main feature of this plugin is the support of the specification-based operators. This feature allows developers not to worry about the Event-B language structure. Plugin executes all the operations using the Event-B abstract syntax tree, so all the dependencies between elements are considered and in case of valid input, no one machine will break during the renaming. Within the project, not all of the specification-based operators were implemented in the plugin, only part of them, but even this part could show the advantages of the chosen approach. After the renaming, elements in the tree will change their names automatically, without the necessity of refreshing the model tree. The one thing user will need to do is to open the renamed element (or machine/context if the element is inside them) and save it manually. After the saving, some errors can occur in the model tree, but after the full build of the workspace, all errors will disappear. If user changes the name of the element which is used somewhere in the model (e.g. variable can be used in invariants or events), after the renaming it will be changed in all occurrences. This is the main advantage of the renaming with the help of this plugin. During the manual renaming of the elements, user can forget to change the name somewhere and this will cause errors. Manual renaming is very time-consuming as well.

**3.2 Overall Project Concept**

To meet requirements described above, new plugin has been developed. The user interface of this plugin is a multi-page editor. The multi-page editor allows the user not only to write commands into one tab, but also to get a feedback from the plugin in another tab. Answering the research question **RQ1.1** (Section 1.3), the idea of the solution is to develop a tool which can manipulate Event-B elements with the help of SBOs. Any formal language developer, familiar with the theory of institutions, will be able to use this plugin to work on Event-B model. The plugin allows the user to rename not only machines and contexts of Event-B model, but also their elements, such as carrier sets, axioms, events, invariants, etc. Another useful feature of the plugin is machine composition, which allows the user to combine variants, invariants and events of one machine with those of another machine. SBOs can be applied to any formal specification. They are specification-independent and this is their main advantage. These operators are ‘standard’ and all operators in formal languages are based on them. To work with another language, the developer should find analogues of these ‘standard’ operators in another language and compare with those in the language he works with, which seems to be difficult work. The main concept of this plugin is to make possible to work on Event-B model using basic SBOs such as **with** and **and**. These key words will allow the user to make changes into Event-B models without deep knowledge of Event-B syntax. This project also will become a start point of Event-B ‘standardization’. The more standard the formal language is, the easier it becomes to work with it. Simple ‘standard’ syntax for this plugin requires from the user only correct input of names of elements one works with.

**3.3 System implementation**

This section is one of the biggest sections in this thesis. It describes the main phase of the development - making decisions about the implementation of the key features of the plugin. In the next few paragraphs some of the implementation decisions will be discussed. We will pay attention on the most important decisions which were made during the development, such as plugin type, the selection of SBOs, etc.

**3.3.1 Short summary of the system implementation decisions**

One of the most important phases in software development is a design phase. After the phase of analysis, when the developer examines existing solutions and find all their advantages and disadvantages, he should find his own approach of solving the problem or decide to use the existing solution. During the design phase of the current project, two existing plugins were examined and their advantages and disadvantages were notices. Among the advantages of the refactoring (renaming) plugin we can name the using of three types of trees – a dependency tree, an abstract syntax tree and a proof tree. This is an ideal solution for the problem of renaming elements and saving the consistency of proof obligations. This solution was kept in this project’s plugin with some rework. Despite the fact that second plugin’s functionality meets the requirements of our work, the solution used in the existing plugin is quite unusual and complicated. This was the reason to make our own decision and design a brand new solution for composition problem.

As a result, the user is able to make changes in Event-B elements with the help of our plugin without the necessity of installing and searching installed plugins within the Rodin Platform. He also doesn’t have to click several buttons and select/deselect necessary elements to be included into the machine composition. The functionality of two existing plugins was combined and implemented in multi-page editor plugin. Key words **copy**, **with** and **and** allow the user to manipulate Event-B elements and get a feedback from the plugin within one editor (in two different tabs). We chose these three key word, because they cover all the necessary functionality and play important role in institutional theory, being main two SBOs. Each word is responsible for certain operation. The word **copy** is in charge of creating a copy of the existing machine, the word **with** is responsible for renaming both machines/contexts and their elements, and the word **and** helps the user to create a composition of two machines, having elements from both of them.

The access to Event-B elements is proceeded through the abstract syntax tree. This tree is the foundation of the EMF (Eclipse Modelling Framework) model, which includes all the elements of Event-B formal language. This approach allows the plugin decrease the time of executing the code compare to making changes in the model through the simple XML-parsing of Event-B project files. The number of these files increases dramatically in big projects for industrial use. When using any application, the user expects immediate response from the program and the back-end of the current plugin manages to handle the information in reasonable amount of time. When manipulating elements using the AST, there is no need to worry about missing any action or guard where the element is used, which is important for the current problem related to proof obligations.

We implemented front-end part of the plugin using Standard Widget Toolkit (SWT) – one of the most popular Java plugin API. The user interface of the plugin is quite simple, it is a multi-page editor with two tabs – one for entering commands and another for output results from the plugin. The editor supports three basic SBOs. The key word **copy** creates a new file containing the newly created machine, while two other words don’t create new files, they only make changes in existing ones. With this design we can answer research question **RQ1.1** as having a possibility to use SBOs in this plugin to manipulate Event-B elements without deep knowledge of Event-B language syntax. Our plugin uses multi-page editor in order to have an access to Event-B elements without using any buttons or checkboxes and it provides efficient interaction between the user and the Event-B model. The solution of using three types of trees, which was mentioned above, can help to answer the research question **RQ1.2**. When the proof tree is created, it becomes easy to change names of elements and create compositions without making proof obligations inconsistent. As the Rodin tool and plugin are written in Java, it is possible to run them on any operation system, having JVM.

**3.3.2 SBOs and CASL**

During the studying of basics of the institutional theory and specification-based operators, main features of the specification language CASL were examined. CASL, the Common Algebraic Specification Language, has been designed by CoFI, the Common Framework Initiative for algebraic specification and development. CASL is an expressive language for specifying requirements and design for conventional software [7]. As the foundation of the plugin functionality is specification-based operators and CASL is well-structured formal language, this section of the thesis is dedicated to the comparative analysis of used in plugin key words and operators of CASL language. All examples used for the analysis are small and simple, but large and complex specifications are easily built out of simpler ones by means of (a small number of) specification-building operations [8]. Operators, used in this part belong to Structuring Specifications [8]. Combined together, they allow the user build complex and structured programs.

**3.3.2.1 Union**

First operator, which can be used to structure specification is union operator **and**. The Figure 3.1 represents simple piece of program, creating a union of two specifications – List\_ Selectors and Generated\_Set. Union is generally used to combine two self-contained specifications. Union of specifications is obviously associative and commutative [8].

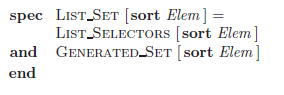
****

Fig. 3.1 CASL syntax for making union of two specifications

There is a principle ‘same name, same thing’ [8], existing in the CASL language. The main idea of this principle is that if two specifications have elements with the same name, they will not be duplicated. If these two elements have different content, one of these elements should be extended with the help of another CASL operator.

Let’s have a look at the created plugin and syntax for manipulating Event-B elements. It is less formal than CASL syntax and doesn’t need key words **spec** and **end**, but it has the same key word for creating a composition of two machines (Figure 3.2).

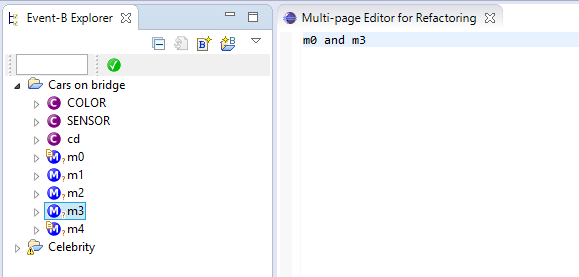


Fig. 3.2 The plugin syntax for creating a composition of two machines

As can be seen from the above two screenshots, the newly created syntax for manipulating Event-B machines matches CASL syntax, which means that Event-B elements control becomes more formal and well-structured.

**3.3.2.2 Renaming**

Renaming may be used to avoid unintended name clashes, or to adjust names of sorts and change notations for operations and predicates [8]. While the ‘same name, same thing’ principle is used in the union operation, it still can happen that during the combining of two specifications, this principle leads to unintended name clashes [8]. This can happen when two specifications with two elements with same names are intended to combine. If both of these elements should be remained in the final specification (they have the same name, but not the same ‘thing’), then one of these elements should be renamed to avoid unintended name clashes. The Figure 3.3 represents the syntax for renaming elements in CASL language.

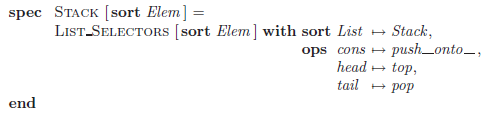


Fig. 3.3 CASL syntax for renaming element of one specification

In this piece of code key word **with** is responsible for renaming the element sort *List* into *Stack*, operation *cons* renamed into *push\_onto\_* and finally selectors *head* and *tail* are renamed into *top* and *pop*, respectively [8]. Let’s have a look at the renaming operation in the created plugin. It calls with the help of key word **with** as well. The syntax for this operator is similar to the key word **and** and requires name of the existing machine/context and new name, which should not be null or the same. Figure 3.4 represents the syntax of the plugin, which can be used to rename context.

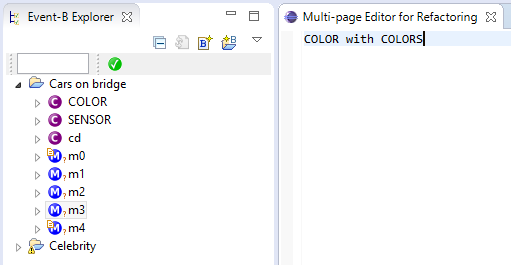


Fig. 3.4 The plugin syntax for renaming context COLOR

This syntax allows the user to rename both machines and contexts, but not internal elements. To rename Carrier Set/Constant/Axiom in context or Variable/Invariant/Event in machine, the syntax, represented on the Figure 3.5 should be used.

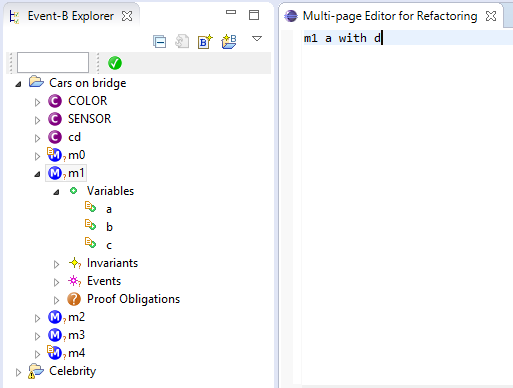


Fig. 3.5 The plugin syntax for renaming Variable *a* in machine m1

The syntax presented on the screenshot above can be used to rename Variable *a* in machine m1. It is clear that syntax for renaming elements in CASL and renaming element inside machines/contexts by created plugin are very similar. Of course, some differences can be noticed as well. In CASL it is possible to rename several elements at the same time, while in our plugin only one element could be renamed during the execution of one operation. Benefits of our plugin includes the possibility of changing machines and contexts, which is impossible to do in CASL.

**3.3.2.3 Copying**

This operator is not represented in CASL specification language, but in our opinion it is important to have a possibility of creating a copy of the existing machine, because sometimes the user needs to have several machines with similar properties, but having insignificant differences in the structure. The creating of such machines from scratch could be very complicated and time-consuming, considering the fact that models, used in industrial projects may have hundreds lines of code. The copying operation creates copy of the existing machine with another name. This machine could be used in future manipulations such as composition and renaming. Changes in the newly created machine will not affect the original one, which can be very useful in creating closely related machines. As it was with the renaming operator, only one machine could be created during the execution of this operator. To create another machine, new command should be written. This feature allows the user to avoid making silly mistakes in machine names and reduces efforts of searching these mistakes. The Figure 3.6 represents the syntax of copying machine in the plugin.

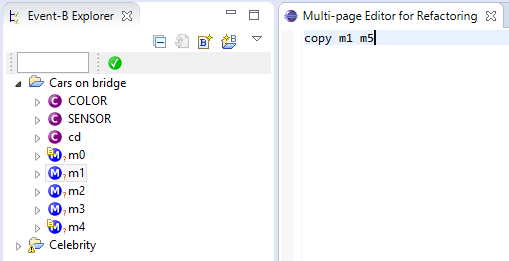


Fig. 3.6 The plugin syntax for creating a copy of machine m1

**3.3.2.4 Summary**

As can be seen from the overview of these three main operators, the first step of Event-B ‘standardization’ has been done. New plugin allows not only to create a composition of two machines, rename elements of Event-B models and copying existing machines, but also makes it possible to manipulate these elements, having basic knowledge of CASL language. All the operators are quite simple, but powerful enough to make significant changes in Event-B models. the next step of this ‘standardization’ should be done by implementing the rest of operators such as then, hide (or reveal) and construction ‘local… within… ’. The implementation of all listed operators will fully cover the structuring specifications.

**3.3.3 Back-end development**

Back-end development includes all the functionality features of the plugin. During the plugin development, several techniques were used. The main framework used for creating the structure of Event-B is an Eclipse Modelling Framework (EMF). EMF is a modelling framework which allows the developer to create models of systems and describe relationships between components. Although the description of EMF and main features of its models are close to UML diagrams, a model in EMF is less general and not quite as high level as the commonly accepted interpretation [6]. This framework unifies Java, XML and UML and its main benefit is the decreasing of costs of the development. As Event-B is well-structured formal language, its EMF model is logical and well-structured as well. This model was used to define all structural elements of Event-B and find dependencies and all relationships between Event-B components. The following screenshot (Figure 3.1) represents Event-B .ecore model built with the help of EMF.

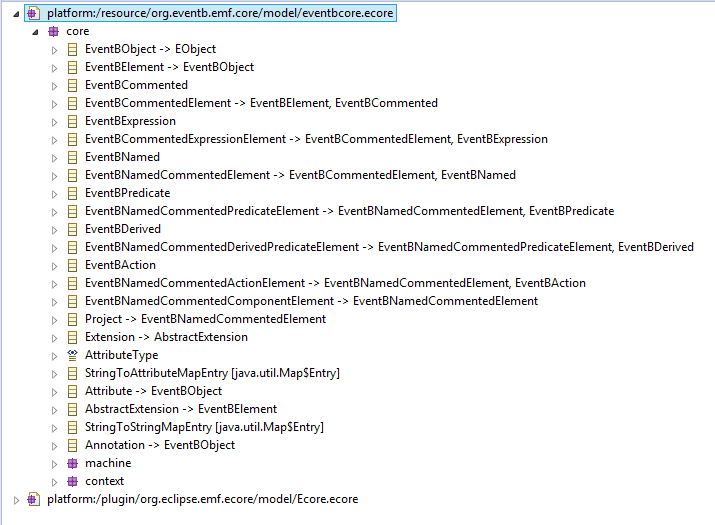


Fig. 3.2 Event-B EMF model

As can be seen from the model, there are not so many special classes, but all of them define Event-B components. The structure of Event-B components is represented on the Figure 3.2.

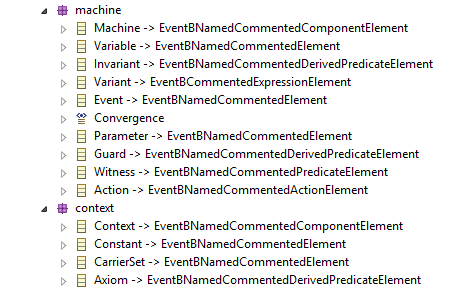


Fig.3.3 Event-B main components

Besides the possibility of creating models of systems, EMF allows the user to generate the source code from the model. This feature is very useful when the developer is intended to create his own programming language, as it creates all the necessary classes and relationships between them. Because of this bi-directionality, EMF has successfully bridged the gap between modelers and Java programmers [6]. The created EMF model let us not only fully understand the structure of Event-B, but also helped to build the strategy of manipulating Event-B components. This was very helpful due to the fact that Event-B stores its data in XML files and it is not clear at the beginning how to make changes of components or add something new into Event-B model.

One of the backend design approaches used in the project was the breaking of the text into tokens. The text entered into the editor, was split into separate words and these words were checked by the plugin. If they matched the key words defined by plugin, certain operations were performed, otherwise a warning was showed.

**3.3.4 Front-end development**

As the plugin is one of the means of connecting the user and the system internal structure, its interface should be clear and easy to use. It should not contain redundant panels or tabs; the names of the tabs should match the tab functionality, etc. For creating the plugin Standard Widget Toolkit (SWT) library was used. This library contains all visual elements of the applications such as buttons, labels, dialogue windows and so on. As was mentioned above, the foundation of the created plugin is a multi-page editor. Newly created file of this editor is stored in the project folder and has .mpe extension. It has two tabs containing information about the current operation. The user enters certain command into the first tab and when he switches to the second tab, the method activates and the feedback from the plugin appears on the second tab. The user doesn’t have to press anything else to execute operations. If there are no errors occurred during the program execution, the plugin will display the successful result on the screen and make any necessary changes in the model. The user can see changes performed by the plugin immediately after the execution. Renamed or composed machines will appear in the Event-B explorer tree. The copying of the machine takes more time and the Progress bar in the Rodin Platform will indicate how much of the work has been done. The renaming is very important capacity of this plugin. As in involves changes inside the model, so some errors can appear in other machines or contexts or even in proof obligations. To fix this problem, the user should open the error machine/context and simply save it. After the saving, all errors should disappear. These errors are related with the changes inside models, but they don’t affect the correctness of the model and don’t make proof obligations inconsistent. As proof obligations are the most important part of Event-B language, the ability of keeping them correct makes this plugin important in the work with manipulating Event-B elements. As can be seen from the next section, all the commands for this multi-page editor are simple and easy to remember and use.

**How does the Refactoring plugin work?**

To run the plugin, the user should choose it in the main menu of the Rodin Platform. To do so press File – New – Other… – Refactory Wizards – Multi-page Editor File. The dialog window should appear. It contains two fields available for changing. First field is designed for the name of Container. This name can be selected only from existing projects in the current workspace. The message above this field shows the user if the entered name is valid. The second field is purposed for the name of the creating file. It has value ‘Commands.mpe’ by the default. This name will appear on the first tab of the editor. If the user entered correct names for both fields, the button Finish will become active. After clicking this button, the main window of the editor will appear. The editor is case-sensitive, so all the key words should be entered in a lower case, while all the names of model elements should match existing elements in the current model. All the commands should be entered by the user in the first tab. The results of the execution will appear in the second tab called “*Results*”.

To copy the existing machine, the user should type “**copy** [machine\_1] [machine\_2]” command, where copy is a key word, machine\_1 is a name of existing machine and machine\_2 is a name of newly created machine. There are some restrictions put on this command. Firstly, the machine\_1 name should obligatorily be the name of existing machine. The input of the wrong name will cause an error “*The file [machine\_1] doesn't exist*”. Secondly, the machine\_2 name should not exist. The input of the existing machine will cause an error “*The file [machine\_2] already exists, choose another name*”. If everything entered correctly, the message “*The machine [machine\_1] exists. The file [machine\_2] doesn't exist, start copying*”. To rename the existing machine/context, the user should enter the following command: “[machine\_1/context\_1] **with** [machine\_2/context\_2]”. As with the **copy** key word, all restrictions remain the same. If the [machine\_1/context\_1] entered incorrect, an error “*No such machine or context exist*” will occur. If the [machine\_2/context\_2] is null or equal to the existing name, the following error will occur: “*Select another name. The name cannot be null or be equal to existing name*”. If everything entered correctly, the message “Context [machine\_1/context\_1] exists. Renaming of the context [machine\_2/context\_2] is done!” will appear. To rename components of the machine/context enter command “[machine/context] [component\_1] **with** [component\_2]”, where [machine/context] is the name of parent machine/context of the element, [component\_1] is existing component intended to be renamed and [component\_2] is a new name of the component. Restrictions for this variation of renaming are remaining the same as for the renaming machines/contexts. To create a composition of two machines, the user should first copy the first machine of the composition, as all the changes will be made into it. after this step is done, the following command should be entered: “[machine\_1] **and** [machine\_2]”, where [machine\_1] and [machine\_2] are existing machines which intended to be merged. This command will copy into [machine\_1] all missing variants, invariants and events, existing in [machine\_2]. The mandatory condition for this command is the existence of both machines.

**3.4 Dependability attributes**

Before we start to evaluate dependability of the project, let’s have a look on the dependability definition to learn what dependability actually is. According to the dictionary [9], dependability is an ability to perform as and when required. In other words, dependability shows the user’s trust in the system. It represents the coincidence between the system behavior and user’s expectations. Dependability has several attributes, such as system's **availability**, **reliability**, and its **maintainability**, and **maintenance** **support** **performance**, and, in some cases, other characteristics such as **durability**, **safety** and **security** [9]. In this thesis attention will be paid on the first three attributes: availability, reliability and maintainability of the system.

**3.4.1 Availability attribute**

Availability is an ability to be in a state to perform as required [9]. According to this definition, the system should be in active state during the whole process of the using. This means that execution of one particular operation should take satisfactory amount of time. Among all the operations performed by the plugin, only one operation takes significant amount of time. This operation is copying. Copying is time-consuming operation, because new machine is crated from scratch, so it takes some time to copy all variables, invariants and events, build the syntax tree, and make sure that new machine is available and ready to use. The more elements the original machine has, the more time it will take to recreate it. Despite the fact that copying takes some time, it is possible to continue working on the rest of elements in the model. They will be available for changing even during the copying operation. However, the manual creation of the machine will definitely take much more time from the user, and could cause problems of missing any elements or creating new proof obligations, which takes significant amount of time.

One more point about availability within different operation systems can be noticed. As the Rodin Platform is Java-based open source project, it could be run on all operation systems having JVM. Respectively, the plugin’s jar-file could be put in the Plugins folder in the directory where Rodin was installed. The plugin works fine with Windows and Linux operation systems, which makes it possible to work on Event-B projects from different machines, having the same amount of operations and functionality. Of course, the user can rely only on himself during the operation execution, the system doesn’t allow to avoid all the possible errors, but some errors from the user side are caught and showed in the Results tab of the multi-page editor.

To conclude, the availability attribute of the plugin was showed for two points of view – within the system itself and within several operation systems. According to the information above, the plugin may be considered as reliable software, which provides the user with access to internal elements of Event-B model all the time.

**3.4.2 Reliability attribute**

Reliability is an ability to perform as required, without failure, for a given time interval, under given conditions [9]. The correspondence to this attribute could be traced according to the requirements **R2**, **R3** and **R4**, mentioned in Section 3.1. The requirement **R2** describes the first factor of reliability – *correctness*. It sounds like “The plugin should allow the user to rename Event-B elements and compose machines” and describes the main functionality of the system. The correctness of the system is provided by execution of the system according to the specification. The requirement **R3** sounds like “The plugin should not allow to make changes if the input is incorrect”. This requirement confirms the second factor of the reliability – *robustness*. This factor helps to prevent damages if the use of the system is outside the specification. The plugin shows a warning message about the incorrect input, but doesn’t make changes in the system. The third requirement **R4**, which states that “The plugin should give the user information about incorrect data input”, provides the third factor of the reliability – *security*. This requirement prevents not only damage caused by deliberately use of the system outside the specification, but also unintended incorrect use of the system by the user.

**Incorrect data input**

Despite the fact that all factors of reliability were considered in system requirements, the situation when the user enters incorrect data still can occur. It is almost impossible to avoid incorrect data input from the user, as the names of all elements in Event-B model are in the responsibility of the user. There is no spelling check in multi-page editor, so the user should be very careful while entering new or existing names. Even in the situation when the user entered incorrect new name and noticed it after the execution, he always can delete incorrect element from the model and execute the command with correct data again. The high speed of the operations execution allows the user to call them quite frequently without any delays.

One of the most frequent examples of the incorrect input is the violation of the language syntax rules. The created plugin supports a scriptable language, which has certain rules required for calling proper methods. These rules are defined for each operation and the misspelling even of one word or incorrect order of words in command can cause errors in the execution. As was mentioned in the previous sections, the operation of renaming can be written in two variations: for machines/contexts and for their elements. It is very important to keep the correct order of the words in this operation as these two variations of the renaming call two different types of renaming. The same situation holds for two other operations. They can only be called if the command is written properly. Even wrong case of commands causes errors in the execution. The user is responsible for correct call of functions and name specifying, which influence on correct execution of the whole system and changes in the structure of Event-B model.

**3.4.3 Maintainability attribute**

Maintainability is an ability to be retained in, or restored to a state to perform as required, under given conditions of use and maintenance [9]. This is a characteristic, which can be evaluated after some time of the use of software. Technologies nowadays change so fast, so it is quite difficult to say how much will requirements to software change after certain period of time. Some of them could become outdated and will be required to change, some new requirements could appear. One of the possible solutions of this problem could be an open source platform.

**Open source**

Software development nowadays is completely different compare to software development even 10 years ago. A lot of open source projects appear and all developments interested in particular field of development can take part in it. This allows developers from all over the world to work on important problems of the humanity and maintain projects, which haven’t any sponsorship from big companies. We believe that open source projects increased the maintainability of software. This project will be maintained by developers, interested in formal languages standardization and searching for the current development decisions. The plugin is stored in jar-file and could be easily used by any developer. It can be changed or completed by other operations and developed till the full functional scriptable language. Both developers and the project will have benefits of the open source status of this projects.

**CHAPTER 4**

**Overall project evaluation**

This chapter is dedicated to the evaluation of the contribution given by this project. This can be done by reviewing requirements mentioned in Section 3.1. The comparison of the current project and existing plugins with the same functionality will also be conducted, as well as benefits of created plugin.

**4.1 Requirements**

**References**

[1] J. A. Goguen and R. M. Burstall. Institutions: Abstract Model Theory for Specification and Programming. Journal of the A.C.M., 39(1):95{146, January 1992

[2] J.-R. Abrial. The Event-B Modelling Notation, October 2007

[3] S.Holl. Refactoring of B models. Bachelor thesis, 2007, pp.1-52

[4] A. Gondal, M. Poppleton, C. Snook. Feature Composition – Towards product lines of Event-B models

[5] J.-R. Abrial. Modeling in Event-B. System and Software Engineering, Cambridge University Press, 2010

[6] D. Steinberg, F. Budinsky, M. Paternostro, E. Merks. EMF: Eclipse Modelling Framework. Addison-Wesley, 2009.

[7] Peter D Mosses, editor. CASL Reference Manual, volume 2960 of Lecture Notes in Computer Science. Springer, 2004.

[8] Michel Bidoit and Peter D Mosses. CASL User Manual, volume 2900 of Lecture Notes in Computer Science. Springer, 2004.

[9] IEC*, Electropedia del 192 Dependability*, [http://www.electropedia.org](http://www.electropedia.org/), select 192 Dependability, see 192-01-22 Dependability.