Using BDD and SBVR to Refine Business Goals into an Event-B Model: A Research Idea

Fabio Levy Siqueira
University of São Paulo
(levy.siqueira@usp.br)

Thiago C. de Sousa
State University of Piauí
(thiago@uespi.br)

Paulo Sérgio Muniz Silva
University of São Paulo
(paulo.muniz@usp.br)

FormaliSE 2017

05/27/2017

Agenda

- ☐ Introduction
- ☐ Background
- ☐ BDD2EVENT-B
- ☐ Related Work
- ☐ Final Considerations

Introduction::Motivation

- We worked at Alstom Transport in Brazil with Event-B few years ago.
- After 4 months of the Door Control System project, the team summarized the folowing issues:
  - How do I start the model?
  - How do I trace the requirements to the model?
  - What is the next step?
  - When should I refine the model?
- The transition from the requirements phase to the formal specification phase is one of the most painful steps and is still an open issue.

Introduction::Proposal

A method based on BDD combined with the formalism provided by SBVR in order to obtain a refinement from requirements into an Event-B model.

What are BDD and SBVR!?

Background::Event-B

- Event-B is a state model-based formal method for modelling systems based on predicate logic and set theory where the refinement mechanism is guaranteed by formal mathematical proof obligations.
- This method has two components :
  - Contexts: used for static specification, including global sets, constants and axioms
  - Machines: applied to dynamic specification, containing variables, invariants, variants and events

Background::BDD

- Behavior-Driven Development (BDD) is an agile software development approach with an emphasis on requirements analysis and testing.
- The BDD process has 5 steps:
  - Start by determining a set of high-level business goals;
  - Based on these goals, describe the features that the system must deliver;
  - Features are then broken into user stories;
  - The user stories are illustrated with examples, called scenarios;
  - Scenarios are translated to automated tests.

Background::SBVR

- Semantics of Business Vocabulary and Business Rules (SBVR) is an OMG standard that allows documenting the semantic of business vocabularies and business rules.

- The specification includes the description of SBVR Structured English, which use four font styles to represent the following concepts: Term, Name, Verb and Keyword.

- From a logical perspective, SBVR allows expressing quantification, logical operations and modal operations.

BDD2EVENT-B::Overview(1)

- Why BDD?
  - BDD suggests applying a sequence of refinements;
  - BDD template is similar to Event-B template;
  - BDD is a popular agile method.

- Why SBVR?
  - SBVR is ready for automation;
  - SBVR allows using quantification, logical operators, and modal operations;
  - SBVR is understood by business specialists (vocabulary).

BDD2EVENT-B::Overview(2)

- The customer, a domain specialist and a requirements analyst (with background in formal methods) work together

- The method is composed of four steps, based on the BDD process:
  - Step 1 - Determining the high-level business goals;
  - Step 2 - Determining the software features;
  - Step 3 - Refine the features into user stories;
  - Step 4 - Define the acceptance criteria of the user stories.

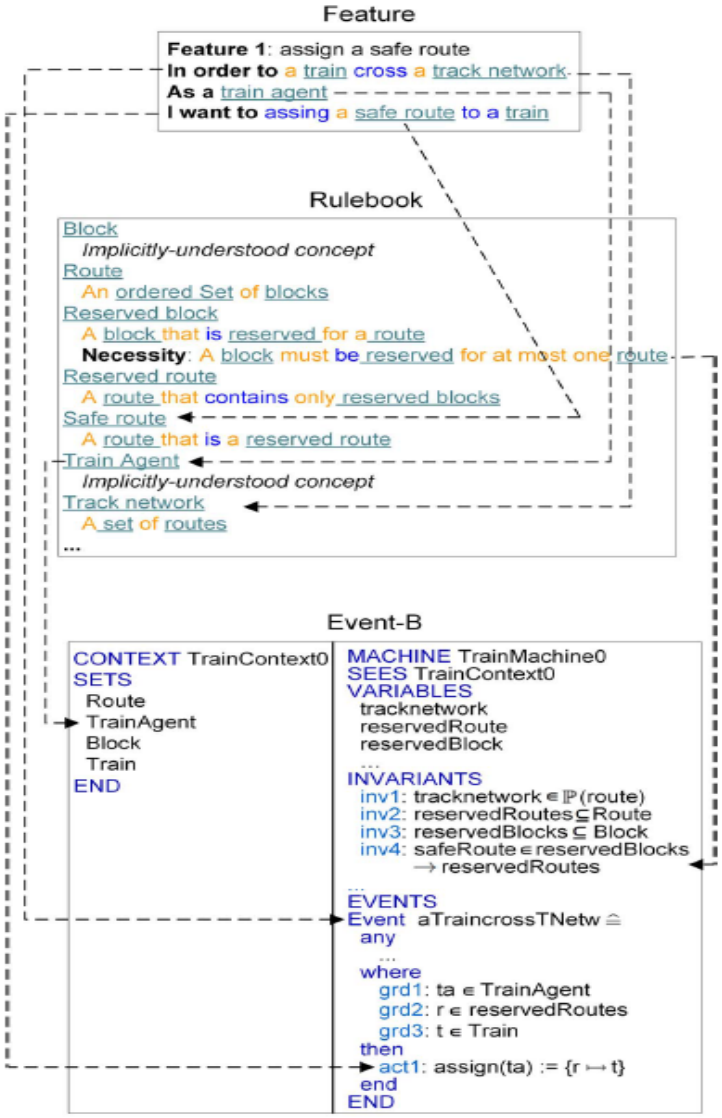
BDD2EVENT-B::Example

- The track network is made of blocks, and contains points (a device that splits a track in two directions) and crossings (a device that makes two tracks cross each other);
- The paths trains may follow in the network are called routes, and they are defined as a sequence of blocks;
- A signal is located before the first block of the route, protecting it. If the signal is red, the train cannot use the corresponding route; if it is green, the train can move safely in the route.

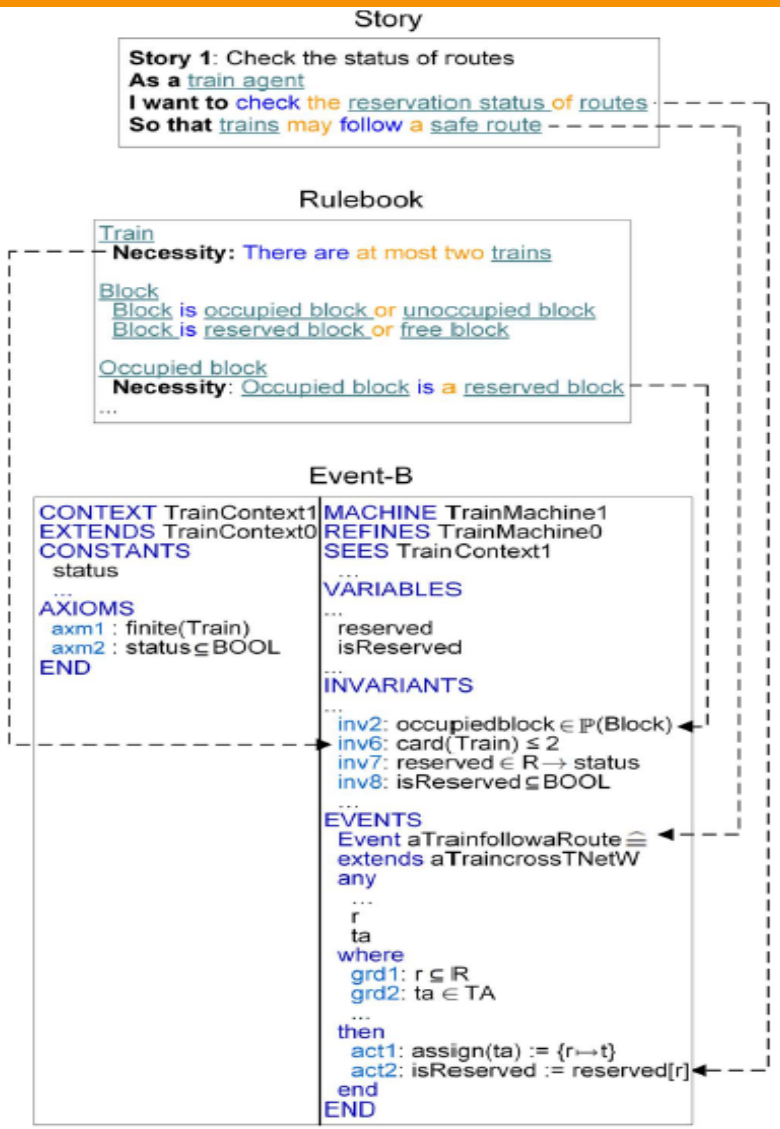
BDD2EVENT-B::Step 1

The goal of the train system is to safely control trains moving on a track network.

BDD2EVENT-B::Step 2



BDD2EVENT-B::Step 3



BDD2EVENT-B::Step 4

Related Work::Transformation

- R. Murali, A. Ireland, and G. Grov, "UC-B: Use Case Modelling with Event-B," in Abstract State Machines, Alloy, B, TLA, VDM, and Z: 5th International Conference, ABZ 2016, Linz, Austria, May 23-27, 2016, Proceedings, M. Butler, K.-D. Schewe, A. Mashkoor, and M. Biro, Eds. Springer International Publishing, 2016.
- C. Ponsard and X. Devroey, "Generating high-level Event-B system models from KAOS requirements models," Actes du XXIXe`me Congre`s INFORSID, pp. 317–332, 2011.

Related Work::Refinement

- E. Alkhammash, M. Butler, A. S. Fathabadi, and C. Cırstea, "Building traceable Event-B models from requirements," Science of Computer Programming, vol. 111, Part 2, pp. 318 – 338, 2015, special Issue on Automated Verification of Critical Systems (AVoCS 2013).
- M. Jastram, S. Hallerstede, M. Leuschel, and A. G. Russo, Jr., "An approach of requirements tracing in formal refinement," in Proceedings of the Third International Conference on Verified Software: Theories, Tools, Experiments, ser. VSTTE'10. Berlin, Heidelberg: Springer- Verlag, 2010, pp. 97–111.

Final Considerations::Discussions(1)

- The main benefit of this proposal is to bridge the gap between a formal specification and high-level business goals:
  - The use of SBVR, a controlled language created to help the business community, allows a direct involvement of domain specialists in this process;
  - Formal models in Event-B are obtained by transformations of requirements artifacts, with the support of SBVR formalism;
  - The use of a method based on BDD allows successive refinements of the requirements model, from goals to scenarios.

Final Considerations::Discussions(2)

- Another benefit is to allow intermediate verification in requirements artifacts:
  - The vocabulary consistency, since it was built along the dialogues and during the process of learning the application domain;
  - The consistency between the features and the stories, based on the definitions provided by the features (stories introduce more elements in the vocabulary) and, evidently, with the vocabulary already made consistent;
  - The consistency between stories and scenarios, based on the stories (for the similar reason) with the vocabulary already made consistent.

Final Considerations::Ongoing Work

- Make analysis on SBVR and a mapping from its formal model to Event-B constructs;
- Improve the method, providing guidance for each step;
- Investigate which proof obligations can be done in the intermediate models in order to make the requirements analyst task easier.

That's all!

THANKS!