Refinement-Preserving Translation from Event-B to Register-Voice Interactive Systems

Denisa Diaconescu\(^2\), Ioana Leustean\(^2\), Luigia Petre\(^1\),
Kaisa Sere\(^1\), and Gheorghe Stefanescu\(^2\)

\(^1\) Åbo Akademi University, Finland
\(^2\) University of Bucharest, Romania

Abstract. The state-based formal method Event-B relies on the concept of correct stepwise development, ensured by discharging corresponding proof obligations. The register-voice interactive systems (rv-IS) formalism is a recent approach for developing software systems using both structural state-based as well as interaction-based composition operators. One of the most interesting feature of the rv-IS formalism is the structuring of the components interactions. In order to study whether a more structured (rv-IS inspired) interaction approach can significantly ease the proof obligation effort needed for correct development in Event-B, we need to devise a way of integrating these formalisms. In this paper we propose a refinement-based translation from Event-B to rv-IS, exemplified with a file transfer protocol modelled in both formalisms.

1 Introduction

Event-B \([2,9,14,15,16,17,18]\) is a state-based formalism dedicated to the refinement-based development of parallel and distributed systems. This amounts to developing an abstract model into more concrete ones, so that we are sure that a more concrete model correctly develops a more abstract one. A central advantage of Event-B is the associated Rodin tool platform \([27,3]\) employed in discharging the proof obligations that ensure this correct development. In addition to providing a user interface for editing Event-B models, the proving process is closely integrated with the modelling process, encouraging proof-based model improvement. Event-B is currently successfully integrated in several industrial developments, for instance at Space Systems Finland \([13]\) and at SAP \([8]\).

The register-voice interactive systems \([24,25,21,11,12,23]\) (rv-IS) formalism is a recent approach for developing software systems using both structural state-based as well as interaction-based composition operators. Interactive computation \([29]\) is an important computer science topic, often related to human-computer interaction, the particular case when one of the interacting entities is human. While able to deal with such cases as well, the rv-IS formalism is more oriented to the process-to-process interaction. There are already many successful formalisms for this, including Petri nets \([26]\), process algebras \([5]\), \(\pi\)-calculus \([20,19]\), dataflow networks \([6,7]\), etc. The approach used in this paper integrates a dataflow-like interaction model with a classical state-based computation model.
One of the most interesting features of the rv-IS formalism is the structuring of the component interactions.

Our aim is to study whether a more (rv-IS inspired) structured approach of an interactive, modular system has any effect on the correct development as designed in Event-B. More precisely, we are interested in uncovering whether the proof obligations are significantly eased when a certain structure is assumed in the model. For this, we need to devise an integration of Event-B and rv-IS, up to a level where the key features of each formalism can be easily translated into the other. We have set up the following working plan for integrating the Event-B and the rv-IS formalisms:

1. Define a notion of refinement in rv-IS models based on a combination of the refinement of state-based systems and of Broy-style refinement of dataflow-based interactive systems.
2. Define a translation $\text{eb2is}$ from Event-B models to structured rv-IS models.
3. Prove the translation $\text{eb2is}$ preserves refinement.
4. Use one of the known translations to pass from structured rv-IS models to unstructured rv-IS models, e.g., the translation in [12].
5. Define a refinement preserving translation $\text{is2eb}$ from unstructured rv-IS models to Event-B models.
6. Use these translations $\text{eb2is}$ and $\text{is2eb}$ to: (1) improve the discharging of proof obligations in Event-B based on rv-IS structural operators and associated decomposition techniques; (2) get tool support to develop and analyze rv-IS models.

In this paper we present a double-folded contribution. First, we introduce a refinement-preserving translation $\text{eb2is}$ from Event-B models to structured rv-IS models. Second, we argue our translation by analyzing an example: we present three refinement steps for modeling a simple file transfer protocol in Event-B and show the associated refined structured rv-IS models. This means we are addressing items 2. and 3. in our working plan above. We have already addressed item 1. in [10] and item 4. in [12].

We proceed as follows. In Section 2 we outline Event-B and rv-IS. In Section 3 we introduce a general translation from Event-B models to rv-IS models and briefly put forward the concept of rv-IS refinement. In Section 4 we present an example of a file transfer protocol and in Section 5 we conclude the paper.

## 2 Preliminaries

In this section we overview the formalisms to integrate to the extent needed in this paper.

### 2.1 Event-B

Event-B [2] is a state-based formal method focused on the stepwise development of correct systems. This formalism is based on Action Systems [4,28] and the B-Method [1]. In Event-B, the development of a model is carried out step by step from an abstract specification to more concrete specifications.