# Event-B: From Systems to Sub-systems Modeling

Kenza Kraibi(✉)

Institut de Recherche Technologique Railenium, 59300 Famars, France
kenza.kraibi@railenium.eu

## 1 Introduction

Event-B [3] is a formal method that allows the verification of critical systems properties. This method is based on the refinement reasoning which consists in adding more details step by step from the abstraction. Modeling critical systems in Event-B requires several steps of refinement in order to take into account all the details of the specification. Therefore, the whole system modeling and proof become more difficult because of the huge size of data and system properties like safety properties described in the system specification.

PRESCOM project (Global Safety Proofs for Modular Design/**PRE**uves de **S**écurité globale pour la **CO**nception **M**odulaire) is an IRT Railenium project in partnership with Clearsy Systems Engineering and under the supervision of Gustave Eiffel University (UGE/COSYS/ESTAS) and Polytechnic University of Hauts-de-France (UPHF/LAMIH). As part of this project, the goal of our thesis[1] is to answer the industrial need, i.e. find a solution to the models voluminosity issue in Event-B when we put the whole specification in the model progressively by the refinement mechanism. This conduces to: study what exists in the literature; apply these approaches on a railway case study, analyze the results and identify their limitations. Based on these identified limitations, we propose a new approach of decomposition called the *decomposition by refinement*.

## 2 Related Work and Analysis

Many approaches have been proposed to deal with the Event-B decomposition issue, among others one finds: the shared variable decomposition and the shared event decomposition. The shared variable decomposition [4], A-style, consists in distributing events of a system in several sub-systems. This approach proposes to manage shared variables between several events in different sub-systems. It is also used for decomposing parallel programs [6]. The shared event decomposition [5], B-style, is based on the variables partition in each sub-system. Each sub-system

[1] This thesis is supervised by: Rahma Ben Ayed (IRT Railenium), Joris Rehm (Clearsy), Simon Collart-Dutilleul (UGE/COSYS/ESTAS), Philippe Bon (UGE/COSYS/ESTAS) and Dorian Petit (UPHF/LAMIH).


A. Raschke et al. (Eds.): ABZ 2020, LNCS 12071, pp. 418–422, 2020.
https://doi.org/10.1007/978-3-030-48077-6_35

contains the chosen variables, and the shared events between the resulting sub-systems are defined in two different signatures for each sub-system. In addition to these two approaches, one finds others such as generic instantiation [4], modularization [7], fragmentation and distribution [10].

The aim of this work is to model the behavior of railway signaling systems in Event-B and at the same time manage the complexity of the resulting models. For this reason, we choose to proceed with the study and analysis of A-style and B-style, because the other cited approaches imply some classical-B [1] method semantics or use other languages.

The analysis of A-style and B-style leads to these results: both approaches require several steps of refinement in order to simplify the model decomposition. For A-style, the shared variables should be copied in the sub-systems and shouldn't be refined. The invariants involving the shared variables are not considered in the sub-systems. As for the shared events decomposition, the distribution of the variables is not always possible because of complex actions involving partitioned variables in different sub-systems or complex predicates (invariants and guards). This requires the separation of these variables by several steps of refinements with mathematical proofs. The detailed description of the state of the art, the application on a railway case study, the analysis and the identified limitations have been presented in [8].

## 3 Proposed Approach

On the basis of the industrial need and the identified limitations, we define a new approach called the *decomposition by refinement* method. The approach consists in the decomposition using the refinement technique for the purpose of keeping the semantic link between the system and the resulting sub-systems. So, a system is decomposed into one or more sub-systems in such a way they are refining this later. This can be applied to a system either in the abstraction level or in a certain level of refinement as shown in Fig. 1. By this way the sub-systems are still preserving the defined system properties in the abstraction through the refinement. Also, we define a new link between the sub-systems named REFSEES. This link will provide to each sub-system the visibility to the other sub-systems: the state of the private variables, the corresponding invariants, the constants, the sets and the properties.

Let us consider the example of Fig. 1 and let $M$ be the system to decompose[2]. $M$ defines the state variables $v$ where $v = (x, y, z)$ for example, the invariants to preserve involving the state variables $I(v)$ and the abstract events $ae$. The goal is to decompose $M$ into two sub-systems $M_a$ and $M_b$ where: $M_a$ (resp. $M_b$) is a refinement of $M$; $w_a$ (resp. $w_b$) are the state variables refining some state variables of $M$. For example, $w_a$ are refining $x$ and $y$, and $w_b$ are refining $y$ and

[2] Due to the limited place in this paper, we show a simple example, but we have already performed our approach on interesting case studies from the railway domain [8].

$z$; $J_a(w_a)$ (resp. $J_b(w_b)$) is the gluing invariant of $M_a$ (resp. $M_b$); The events $re_a$ (resp. $re_b$) are the events of $M_a$ (resp. $M_b$) refining a part of the abstract ones in $M$.

The clause *REFSEES* in $M_a$ (resp. $M_b$) allows to see the state of the private variables of $M_b$ (resp. $M_a$). So, the private variables of $M_a$ (resp. $M_b$) can be used in the guards of the events of the machine $M_b$ (resp. $M_a$). More details about *REFSEES* clause are in [8,9].

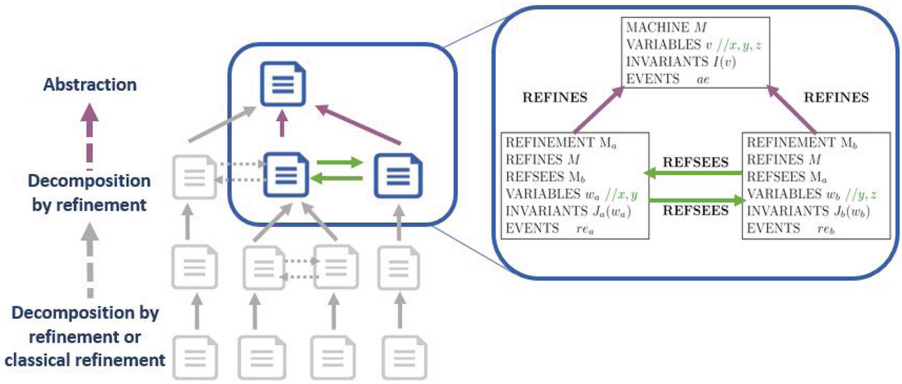


**Fig. 1.** Proposed approach: decomposition by refinement

Some rules should be considered in order to formalize this approach:

**Rule**$_1$: Some state variables of the decomposed system $M$ can only be in one of the sub-systems $M_a$ or $M_b$. But, these variables should all be present at least in one of the sub-systems.
**Rule**$_2$: The sub-system $M_a$ (resp. $M_b$) can refer in the guards of their events to the private variables of $M_b$ (resp. $M_a$).
**Rule**$_3$: The transition system of the resulting sub-systems $M_a$ and $M_b$ should correspond to one transition system of the behavior of $M$.
**Rule**$_4$: $M_a$ and $M_b$ transitions are not synchronized contrary to the decomposition by shared events. So, following what has been presented in [2], we can demonstrate that the theoretical re-composition/combination of the sub-systems is a refinement of the system $M$.
**Rule**$_5$: For each sub-system, a variant proof obligation rule VAR should be defined because a transition should not be triggered indefinitely. As for the deadlock freedom rules, there are two types: the weak deadlock freedom rule $DLF_w$ and the strong one $DLF_s$. $DLF_w$ verifies that at least one of the events is triggered. Whereas $DLF_s$ proves that each event is triggered at least one time. This verification should also be done in case of the definition of new events.

## 4 Conclusion and Future Work

Several approaches have been proposed to deal with the complex and huge system specifications issue in Event-B such as A-style and B-style. The realized analysis and the study conduce to the identification of some limitations of those approaches regarding the industrial need. So, we propose a new approach: the *decomposition by refinement* based on decomposing a system by the refinement technique into several sub-systems. A new clause REFSEES is defined to link the sub-systems to each other which allows the visibility of the state variables. This approach will ensure the preservation of invariants through the refinement technique. Currently, we are working on the definition of the strategy to follow for the application of the approach. This strategy will define: the way to decompose the state variables of the system and its events, and how to define, in each sub-system, new invariants, new state variables and new events. As a short-term perspective, we will demonstrate that the fact of combining -theoretically- the sub-systems constitutes a one refining component of the initial system regarding the theoretical definition of the refinement in B method. As a long-term perspective, new proof obligations will be specified, through the new defined link, to ensure the behavior preservation in each of the resulting sub-systems. for the purpose of its scaling up, the approach will be applied to a railway signaling system case study.

## References

1. Abrial, J.R.: The B-Book: Assigning Programs to Meanings. Cambridge University Press, New York (1996)
2. Abrial, J.R.: Event Model Decomposition. Technical report/[ETH, Department of Computer Science 626 (2009)
3. Abrial, J.R.: Modeling in Event-B: System and Software Engineering. Cambridge University Press, New York (2010)
4. Abrial, J.R., Hallerstede, S.: Refinement, decomposition, and instantiation of discrete models: application to event-B. Fundamenta Informaticae **77**(1–2), 1–28 (2007)
5. Butler, M.: Decomposition structures for event-B. In: Leuschel, M., Wehrheim, H. (eds.) IFM 2009. LNCS, vol. 5423, pp. 20–38. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-00255-7_2
6. Hoang, T.S., Abrial, J.-R.: Event-B decomposition for parallel programs. In: Frappier, M., Glässer, U., Khurshid, S., Laleau, R., Reeves, S. (eds.) ABZ 2010. LNCS, vol. 5977, pp. 319–333. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-11811-1_24
7. Hoang, T.S., Iliasov, A., Silva, R.A., Wei, W.: A survey on event-B decomposition. Electron. Commun. EASST **46** (2011)
8. Kraibi., K., Ben Ayed., R., Rehm., J., Collart-Dutilleul., S., Bon., P., Petit., D.: Event-B decomposition analysis for systems behavior modeling. In: Proceedings of the 14th International Conference on Software Technologies, vol. 1: ICSOFT, pp. 278–286. INSTICC, SciTePress (2019). https://doi.org/10.5220/0007929602780286

9. Kraibi., K., Ben Ayed., R., Rehm., J., Collart-Dutilleul., S., Bon., P., Petit., D.: Towards a method for the decomposition by refinement in event-B. In: Refinement Workshop at Formal Methods Congress (Refine@FM), Accepted paper but not yet published (2019)
10. Siala, B., Tahar Bhiri, M., Bodeveix, J.P., Filali, M.: Un processus de Développement Event-B pour des Applications Distribuées. Université de Franche-Comté (2016)