A formal approach for correct-by-construction system substitution

Guillaume Babin

A formal approach for correct-by-construction system substitution

Guillaume Babin*‡
*Université de Toulouse ; INP, *IRIT* ; 2 rue Camichel, BP 7122, 31071 Toulouse Cedex 7, France
‡*CNRS* ; Institut de Recherche en Informatique de Toulouse ; Toulouse, France
guillaume.babin@irit.fr

***Abstract*—The substitution of a system with another one may occur in several situations like system adaptation, system failure management, system resilience, system reconfiguration, etc. It consists in replacing a running system by another one when given conditions hold. This contribution summarizes our proposal to define a formal setting for proving the correctness of system substitution. It relies on refinement and on the Event-B method.**

Keywords: system substitution, state recovery, correct-by-correction, Event-B, refinement

I. Motivation

Several efforts were devoted to the formal development of complex systems. Different formal approaches have been defined, they led to numerous system developments in real life applications like transportation systems, web applications, information and data management, etc.

One of the major concerns in system development relates to the substitutability of a system by another one. This capability can be seen throughout different concerns. Among these ones we are mainly interested in two of them: functional and behavioural concerns.

1) The *functional concern* deals with the function of the system i.e. what it does. We have identified three main substitutions:
   - a system may be replaced by an equivalent one;
   - a system may be degraded i.e. replaced by a system achieving less functions, the problem being to identify that the critical ones are still achieved;
   - a system may be upgraded i.e. replaced by a system achieving more functions.

   The functional concern relates to the preservation of the functions of the substituted system by the substitute one. This preservation is studied through property verification. Classical formal verification techniques guarantee that the substituted and the substitute systems refine the same specification.
2) The *behavioural concern* deals with the behaviour of a system in terms of execution sequences. We have identified two main substitutions:
   - a system may be replaced by another system, but it requires to restart the system from its initial state. This corresponds to a *cold start* substitution;
   - a system may be replaced at a given state by another system recovering this state and pursuing the execution of the system from this recovered state. This corresponds to a *warm start* or *hot start* substitution.

   The behavioural concern requires an explicit modelling of system states during execution.

Through these concerns several properties like dependability [1], adaptation [2] [3], resilience, self-healing systems [4], loss of QoS can be addressed.

System substitution is performed when an event requiring this change occurs. In several cases, this event is (or these events are) triggered by monitors in case of monitored systems, or by evaluating a given situation in autonomous systems (self-⋆ systems).

This paper overviews the formal approach we propose to handle system substitutions.

II. Our approach

In the following, we consider systems that are expressed as states and transitions describing state changes. Our approach is a correct-by-construction one, it relies on refinement and on the Event-B method [5] [6] [7] [8]. It addresses system substitution and covers both concerns, functional and behavioural.

A. The functional concern: refinement

Refinement relates an abstract system to a concrete one. The refined concrete system preserves the properties of the abstract one. Both of the three identified cases of the functional concern may be encoded by refinement. Indeed, several concrete representations of a given specification can be given at different abstraction levels, linked by a refinement relationship. Invariants represent the key feature for describing equivalent, degraded or upgraded systems.

B. The behavioural concern: refinement and variants

Once the functional concern has been addressed, it becomes possible to assert that a system may substitute another one in one of the three identified cases above. When a system runs, one obvious substitution case corresponds to a re-start of the substitute system. But, when the sequence of system running states is recorded, one may identify correlations between the states of the substitute system and the current state of the substituted system. Our proposal is to use explicit variants

to identify the substitution state and invariants to express such state correlation. Indeed, variants describe the sequence of running states. Correspondences between states of the substituted and of the substitute system are expressed by the variant values. Invariants define properties between the states of both systems, enabling the copy of the substituted state variables to the substitute state variables.

C. Why Event-B ?

The Event-B method is set-up in order to formalise our approach. Event-B is a state-based method that promotes correct-by-construction development paradigm and formal verification by theorem proving. Indeed, Event-B supports the definition of state-based systems where transitions recording state changes are encoded by events. Moreover, it offers the capability to explicitly express variants and invariants, and to build systems using refinements.

1) Event-B refinement for the functional concern: a top level machine, representing the main function(s) of a system may be refined by one or more other machines leading to different concrete system designs. All the obtained machines are possible system substitutes.

2) Event-B refinement and variants for the behavioural concern: it is possible to link two substitute systems of the same system into a single refinement. The idea consists in linking these two substitutes with a property establishing a relation between the state variables of one substitute system and the *corresponding* state variables of the other substitute system. We call this property an *horizontal invariant*. The corresponding state is defined thanks to explicit variants. Indeed, a state of the substitute system can recover the state of another substitute system if their variant values match. A specific event *switch* commutes to the substitute system in a single Event-B model of both systems.

III. Formalisation with Event-B

A. Functional concern

The first step consists in defining a top level specification Event-B machine. Each system, refining this specification is considered as a potential substitute. Obviously, the chosen invariant defines the nature of this substitution (equivalence, degradation or upgrade). Once these refinements have been conducted, we get a set of potential substitutes.

B. Behavioural concern

The behavioural concern requires the explicit manipulation of the current state of the system to be substituted. Therefore, our model defines systems as pairs $(sv, VarExp)$:

- sv being a subset of $Vars$ the set of system variables, such that $sv \subseteq Vars$
- an expression $VarExp = exp(v_1, \cdots, v_n)$ over $v_i \in sv$ evaluating to a natural number and defining a decreasing function. This expression describes a variant for the studied system.

This model, combining functional and behavioural concerns, is generic enough to enable the expression of a system together with an explicit representation of its states, if combined with a valuation of its variables. This explicit representation makes it possible to explicitly manipulate a state in an Event-B machine. As a consequence of this modelling, the expression of generic mechanisms combining variant values for recovering states becomes possible.

C. Fragment of the Event-B generic model

The following Event-B fragment results from the previously described model.

- $Variables$ defines the carrier set containing all the system variables
- $Values$ is the carrier set of the values of the variables
- $VariablesSets \subseteq \mathcal{P}(Variables)$ a set of sets of variables to identify the variables of each system (partition)
- $Valuations = Variables \rightarrow Values$ functions that give the value of a variable
- $Systems = VariablesSets \times (Valuations \rightarrow \mathbb{N})$ a system is a pair composed of a group of variables and a variant function
- $Systems\_states = Systems \times Valuations$: all the states of the systems, i.e. pairs (system – variables values)

IV. Case study

To illustrate our approach a case study issued from electronic commerce is shown. We consider an online purchase of goods composed of four steps: *selection* of goods by filling a cart, *payment*, *billing* and *delivery*. Solely the *selection* step is detailed below. Moreover, for this case study, we consider that the event triggering the system substitution is a system failure. A failure may occur while the client is filling his cart with goods during the *selection* step. Failure is the event that triggers system substitution.

Setting up our approach led to the following steps.

A. Functional concern

- an upper model level with an abstract selection of a set of goods in a cart has been designed (corresponding to the Event-B machine *M1*);
- a first basic selection system (*Sys1*) composed of one cart located on a website, has been created by refining *M1* (machine *M11*);
- a second basic selection system (*Sys2*) composed of two carts located on different websites, without failures, has been created by refining *M1* (machine *M12*);
- a system composed of the previous ones. The used system is chosen at initialisation (machine *M13* refining *M1*).

B. Behavioural concern

- The first step towards handling the behavioural concern was the creation of an abstract selection feature, refining *M1* and introducing the possibility to switch from *Sys1* to its substitute *Sys2* . Here, we detail the switching process only. (Machine *M14*)
- *Cold start.* *M14* is refined, by defining a mechanism that substitutes *Sys1* by *Sys2* with a reinitialisation on the

TABLE I
PROOFS STATISTICS

Event-B Machine	Total PO	Automatic proof	Interactive proof	
M1	31	27	4	(13%)
M11	28	27	1	(4%)
M12	57	56	1	(2%)
M13	99	97	2	(2%)
M141	133	129	4	(3%)
M142	230	214	16	(7%)
Generic model	37	28	9	(24%)
Instanciation	53	39	14	(26%)

initial state of *Sys2*. The event triggering the substitution re-initialises *Sys2* from its initial state. (Machine *M14*)

- *Hot or Warm start.* *M14* is refined to a machine where *Sys1* is substituted by *Sys2* with preservation of the previous *Sys1* executions. The event that triggers the substitution restores the current state of *Sys2* to a state that functionally matches with *Sys1* state before substitution. By functionally, we mean that there is no selected goods of *Sys1* cart that are lost. (Machine *M142*)

C. Instanciation of the generic model

We instantiated our model, according to the previously overviewed generic model, with the following definitions.

- $Variables = \{C1, C2a, C2b\}$ corresponding to the carts. $C1$ for *Sys1* and $C2a, C2b$ for *Sys2*;
- $ValueElements = \{Prod1, Prod2, Prod3, Prod4, Prod5\}$ is the set of goods;
- $Valuations = (\{C1\} \mapsto \mathcal{P}(ValueElements)) \cup (\{C2a, C2b\} \mapsto \mathcal{P}(ValueElements))$ associates a subset of goods to each cart;
- $VariablesSets = \{\{C1\}, \{C2a, C2b\}\}$ identifies the variables of each system *Sys1* and *Sys2*;
- $Sys1 = \{C1\} \mapsto (\lambda val \cdot val \in \{C1\} \to \mathcal{P}(ValueElements) \mid card(ValueElements) - card(val(C1)))$
- $Sys2 = \{C2a, C2b\} \mapsto (\lambda val \cdot val \in \{C2a, C2b\} \to \mathcal{P}(ValueElements) \mid card(ValueElements) - card(val(C2a) \cup val(C2b)))$
- $Systems = \{Sys1, Sys2\}$
- $Systems\_states = Systems \times Valuations$

We were then able to refine this machine with one expressing directly $C1$, $C2a$ and $C2b$ carts, and prove the refinement. Moreover, the following safety properties have been proved on each of the machines.

- All the desired products are selected after the *selection* action. If $P \subseteq PRODUCTS$ is the set of products to purchase, and $carts \in SITES \times PRODUCTS$ is the variable denoting the pair of selected products on a given website. This property is expressed as
$$selection\_done \Rightarrow \text{ran}(carts) = P$$
- There is no product selected twice i.e. no product in both of the two carts, expressed as
$$\forall p,\ p \in \text{ran}(carts) \Rightarrow \text{card}(carts^{-1}[\{p\}]) = 1$$

Here, the horizontal invariant is $val(C1) = val(C2a) \cup val(C2b)$, where val is the corresponding valuation.

This generic model together with this case study have been modelled on the RODIN platform [9] [10] and the statistics of table I (proof obligations PO) have been obtained.

V. ONGOING WORK

This paper presented a global view of our approach for system substitution. This approach exploits the notion of refinement, invariants and variants. System substitution has been illustrated with a use case from electronic commerce.

Currently, our work is pursued in two directions. On the one hand, we are building a generic model for system substitution formalised within the Event-B method. A set of generic machines, to be instantiated, defining system substitution is under construction. It is planned to study within this framework adaptation, self-healing, reliability, ... situations. On the other hand, we plan to integrate a monitor in order to monitor a property of the system behaviour and trigger system substitution. For example, monitored properties could be identification of system failures or loss of quality of service.

REFERENCES

[1] J.-C. Laprie, "Dependable computing and fault tolerance: Concepts and terminology," in *Fault-Tolerant Computing, 1995, Highlights from Twenty-Five Years., Twenty-Fifth International Symposium on*, Jun 1995, pp. 2–11.

[2] D. Weyns, M. U. Iftikhar, D. G. de la Iglesia, and T. Ahmad, "A survey of formal methods in self-adaptive systems," in *Proceedings of the Fifth International C* Conference on Computer Science and Software Engineering*, ser. C3S2E '12. New York, NY, USA: ACM, 2012, pp. 67–79. [Online]. Available: http://doi.acm.org/10.1145/2347583.2347592

[3] S. Kell, "A survey of practical software adaptation techniques," *Journal of Universal Computer Science*, vol. 14, no. 13, pp. 2110–2157, jul 2008. [Online]. Available: http://www.jucs.org/jucs_14_13/a_survey_of_practical

[4] M. Parashar and S. Hariri, "Autonomic computing: An overview," in *Unconventional Programming Paradigms*, ser. Lecture Notes in Computer Science, J.-P. Banâtre, P. Fradet, J.-L. Giavitto, and O. Michel, Eds. Springer Berlin Heidelberg, 2005, vol. 3566, pp. 257–269. [Online]. Available: http://dx.doi.org/10.1007/11527800_20

[5] J.-R. Abrial, *Modeling in Event-B: System and Software Engineering*, 1st ed. New York, NY, USA: Cambridge University Press, 2010.

[6] J.-R. Abrial and S. Hallerstede, "Refinement, decomposition, and instantiation of discrete models: Application to event-b," *Fundamenta Informaticae*, vol. 77, no. 1, pp. 1–28, 2007. [Online]. Available: http://iospress.metapress.com/content/C74274T385T6R72R

[7] Y. Ait-Ameur, M. Baron, and N. Kamel, "Encoding a process algebra using the event b method. application to the validation of user interfaces," in *Proceedings of 2nd IEEE international symposium on leveraging applications of formal methods (ISOLA)*, 2005.

[8] Y. Ait-Ameur, M. Baron, N. Kamel, and J.-M. Mota, "Encoding a process algebra using the event b method," *International Journal on Software Tools for Technology Transfer*, vol. 11, no. 3, pp. 239–253, 2009. [Online]. Available: http://dx.doi.org/10.1007/s10009-009-0109-2

[9] J.-R. Abrial, M. Butler, S. Hallerstede, and L. Voisin, "An open extensible tool environment for event-b," in *Formal Methods and Software Engineering*, ser. Lecture Notes in Computer Science, Z. Liu and J. He, Eds. Springer Berlin Heidelberg, 2006, vol. 4260, pp. 588–605. [Online]. Available: http://dx.doi.org/10.1007/11901433_32

[10] J.-R. Abrial, M. Butler, S. Hallerstede, T. Hoang, F. Mehta, and L. Voisin, "Rodin: an open toolset for modelling and reasoning in event-b," *International Journal on Software Tools for Technology Transfer*, vol. 12, no. 6, pp. 447–466, 2010. [Online]. Available: http://dx.doi.org/10.1007/s10009-010-0145-y