Towards CamilleX 3.0

Thai Son Hoang, Colin Snook, Asieh Salehi Fathabadi, Dana Dghaym, and Michael Butler

ECS, University of Southampton, Southampton, U.K.
{t.s.hoang, cfs, d.dghaym, a.salehi-fathabadi, m.j.butler}@soton.ac.uk

The CamilleX Framework [3] provides a textual representation of Event-B models for the Rodin Platform (Rodin) platform. It supports both (1) direct extensions of the Event-B syntax to support modelling extensions such as machine inclusion [2] and record structure [1], and (2) indirect extensions via *containment* mechanism to such as UML-B diagrams [4]. In this presentation, we will take a look at some of the remaining issues and proposal to address them in the next release of CamilleX.

Element Ordering. Currently, CamilleX relies on the Event-B Eclipse Modelling Framework (EMF) framework to store the semantics model of the Event-B machines and contexts. Modelling elements of the Event-B constructs are stored in different "collections", one for each carrier sets, constants, axioms, variables, invariants, events, and "extensions" (e.g., record structure). As a result, there is no ordering information is kept between the different modelling elements. For example, the current implementation of record structure generates the record-related invariants after all normal context axioms (similarly for records in a machine). This could cause problems when the order of the elements matter. Consider the following declarations of a record r with a field A of type S. Axiom @axm1 indicates the surjectivity of S with respect to field A.

```
// CamilleX context with Record
sets S
axioms
  @axm1: ∀s · s ∈ S ⇒ s ∈ ran(A)
record r
  A : one S
```

```
// Translated Rodin context
sets S r
constants A
axioms
  @axm1: ∀s · s ∈ S ⇒ s ∈ ran(A)
  // record field translation axiom
  @axm_r_A: A ∈ r → S
```

This translated model is ill-formed as the type for A can not be determined for axiom @axm1. We will need to be able to interleave the record declaration and axioms as necessary.

As result, the new version of Event-B EMF (currently under development) will store the modelling elements in a generic collection, named orderedChildren (the other collections will become derived attributes to minimise the impact of the changes). The syntax of CamilleX for XMachines and XContexts can be updated to allow the interleaving of modelling elements. We are working on updating the record-structure generator to take advantage of the new ordering.

Identifier Declaration Taking advantage of the ordering allowing us to interleave the modelling elements, we can eliminate the block such as **axioms**, **invariants**,

events. Each element will be prefixed with a singular keyword, such as **axiom**, **invariant**, **event** (notice that the **event** keyword already exists). Moreover, identifier elements such as **constants**, **variables**, and parameters can be declared together with their types and their (initial) values. This allows all information related to the constants and variables in one place. For example, instead of

```
variables a
invariants
 @a−typeof: a ∈ ℕ
event INITIALISATION
begin
 @a−init: a := 0
end
```

we can have

```
variable a : ℕ := 0
```

and the relevant invariants can be generated accordingly.

Support Context Instantiation For context instantiation [5], we will need to distinguish between the abstract sets and constants that need to be instantiated and the properties of them that need to be proved during the instantiation. These elements can be added to the syntax of CamilleX for instantiated and instantiating contexts.

```
context c0
abstract sets S
abstract constants c
axiom A(S, c)
```

```
context d0
sets T
constants d
axiom A(S, c)
instantiates c0(T, d)
```

The translation from CamilleX will flatten the instantiated and instantiating contexts into the facility provided by the instantiation plug-in [5].

Acknowledgement. This work is supported by the following projects:

- HiClass project (113213), which is part of the ATI Programme, a joint Government and industry investment to maintain and grow the UK's competitive position in civil aerospace design and manufacture.
- HD-Sec project, which is funded by the Digital Security by Design (DSbD) Programme delivered by UKRI to support the DSbD ecosystem.

References

1. Asieh Salehi Fathabadi, Colin Snook, Thai Son Hoang, Dana Dghaym, and Michael Butler. Extensible record structures in Event-B. In *ABZ 2021*, 2021.
2. Thai Son Hoang, Dana Dghaym, Colin F. Snook, and Michael J. Butler. A composition mechanism for refinement-based methods. In *ICECCS 2017*, pages 100–109. IEEE Computer Society, 2017.
3. Thai Son Hoang, Colin Snook, Dana Dghaym, Asieh Salehi Fathabadi, and Michael Butler. The CamilleX framework for the Rodin Platform. In *ABZ 2021*, 2021.
4. Mar Yah Said, Michael J. Butler, and Colin F. Snook. Language and tool support for class and state machine refinement in UML-B. In Ana Cavalcanti and Dennis Dams, editors, *FM 2009*, volume 5850 of *Lecture Notes in Computer Science*, pages 579–595. Springer, 2009.
5. Guillaume Verdier and Laurent Voisin. Context instantiation plug-in: a new approach to genericity in Rodin. (in Rodin Workshop 2021), 2021.