**Noname manuscript No.**
(will be inserted by the editor)

# Tasking Event-B: A Code-Generation Extension for Event-B

**Andrew Edmunds · Michael Butler**

Received: date / Accepted: date

**Abstract** Event-B is a formal set-theoretic approach to modelling systems in the safety-critical, and business-critical, domains. This article describes an extension to the Event-B approach, called Tasking Event-B, which facilitates automatic generation of source code from annotated Event-B models. Tasking Event-B allows specification of multi-tasking implementations. We believe that automatic code-generation makes a useful contribution to the Rodin tool-set, by contributing a link in a coherent tool-chain. Automatically generating code from the Event-B model can be seen as a productivity enhancement. It removes a source of errors, that of manually coding for each development. To validate the approach we have undertaken case studies and taken part in an industrial collaboration. We present a number of case-studies to illustrate our work, in this article.

**Keywords** Formal Methods · Event-B · Code Generation · Concurrency · Embedded Systems

Andrew Edmunds
School of Electronics and Computer Science,
University of Southampton, UK
E-mail: ae2@ecs.soton.ac.uk

Michael Butler
School of Electronics and Computer Science,
University of Southampton, UK
E-mail: mjb@ecs.soton.ac.uk

## 1 Introduction

Event-B [6] is one of a number of formal methods that may be used to model systems where a high degree of reliability is required. Event-B was inspired by its predecessor, *Classical-B* [3]. It is a modelling language, used with a supporting tool platform, Rodin [4]; so named from the project in which it was developed [25]. Further work was undertaken in the DEPLOY [35] project to assess the approach with a number of the industrial partners. To derive the greatest benefit from the formal modelling approach, it is desirable to use the formal modelling artefacts to generate implementations for, at least, some parts of the system being modelled. During the latter stages of the DEPLOY project, automatic generation from Event-B models began to evolve, as the platform stabilized, where we targeted multi-tasking, embedded control systems. Initially, we chose Ada [9] as a basis for our approach. This was not only because of it's suitability for the application domain, but also because the programming constructs are well-considered programming abstractions. Ada maps well to Event-B modelling elements, which is easy for modelling, and simplifies the translation to code. We do not attempt to model all aspects of the system, e.g. time; but we model the evolution of the system state, and are able to specify properties relating to the state, that are important for system safety. In current work, in the Advance project [34], we are concerned with modelling and co-simulation of Cyber-physical systems. We can, again, make use of automatic code-generation techniques to provide implementations for use in co-simulation.

In this section we introduce Event-B to the reader, and compare Event-B with some other formal approaches. We discuss automatic code-generation from formal models, and discuss some of the potential target programming language targets.

In Sect. **??** we... In Sect. **??** we...

### 1.1 Overview

The formal methods related to the work presented here can be categorized as state-based formal methods. Alternative, but not unrelated, approaches are categorized as process-based methods. Classical-B [3, 7, 11, 12] and its successor, Event-B are said to be state-based, since they focus on modelling the changes of state, not the behaviour of processes. In Classical-B, state updates are modelled by guarded operations, where the operation is an analogue of a procedure call in a programming language.

### 1.2 Event-B Modelling

In Event-B, state updates are modelled by guarded events, providing a more abstract view of the way a system evolves. Event-B can be used to model systems at an abstract level; and by adding more detail (using a technique called refinement) it can model the software aspects of systems too. Both methods are set theoretic modelling approaches that incorporate a notion of proof to show that important system properties are maintained. The former is primarily an approach to software systems development, the latter more widely applicable to system-modelling. In an effort to make modelling and proof easier, Event-B was developed to overcome some of the difficulties encountered when using in Classical-B. The main differences between Classical and Event-B are highlighted in [19], and inspiration was also drawn from action systems [8].

It is fair to say that Event-B is not just a formal modelling language; the name is used to describe both a notation, and a methodology. In addition to this a mature tool-platform called *Rodin*, named after its development programme, complements the methodology. The main modelling components of Event-B are contexts and machines. Contexts are used to model static features using sets, constants, axioms, and theorems. Machines are used to model variable state using *variables.* A third, more recent addition, is the Theory component; where a developer can augment the bundled mathematical language, and rule-base, with new (inference and re-write) rules, data types, and operators. During the modelling process, changes to the components result in automatic generation of proof obligations, which must be discharged in order to show that the development is consistent. The proof obligations generated in classical-B are often complex, the Event-B approach results in simpler proof obligations as described in [19], since Event-B consists of a simplified action syntax, giving rise to simpler proof obligations. A further simplification was made by adopting an event-based approach, where each atomic event has a predicate guard and an action consisting only of assignment statements. Events correspond to operations in the B-method; operation specification was more expressive, and included constructs for specifying operation preconditions (as part of its Design by Contract approach), operation calls, return parameters, and more complex structures for branching and looping. These constructs are not features of Event-B. Due to these simplifications (and more efficient proof tools) a large number of the proof obligations may be discharged automatically, by the automatic provers. Where un-discharged proof obligations remain, the user has, at their disposal, an interactive prover. Various techniques can be applied, to discharge the proof obligations, such as adding hypotheses; or making use of the hyperlink-driven user interface, for rule and tactic application. In the early stages of development with Event-B, a developer will begin by abstracting, and modelling, the observable events occurring in a system. Event-B, as the name suggests, takes an event-based view of a system; where events occur spontaneously from the choice of enabled events. An event is said to be enabled when the guard is true, and the state updates, described in the event actions, can take place; otherwise it is disabled, and none of its updates can occur.

### 1.3 An Event-B Example

An example of an Event-B machine can be seen in Fig. 1. It shows an abstract model of a pump controller, used in one of the case studies. We will use this model to describe some features of Event-B. But first we introduce the case study, which models a discrete *pumpController*. The model describes a system where the controller receives a value of the fluid level, and a boolean value representing a user-request to turn the pump. Based on the inputs to the controller, a command to turn the pump on may be issued, or a warning is issued if a minimum level *MIN* has been reached. In Fig. 1, we see that machine *M1* refines another machine *M0*; we will discuss refinement in Subsect. 1.4. It also has a *SEES* clause; this makes the contents of a context visible to a machine. Contexts may contain sets, constants, axioms and theorems, and example context can be seen in Fig. 2. There are variables representing the internal state of the controller, and invariants providing type information for variables. Invariants are also used to describe the safety properties of the system. This describes a required safety property, that if the level is at or below *MIN*, and a user's pump-on request is detected, then a warning will be issued. Also, if the level is OK and a pump-on is requested, then the state *pumpOnCmd* = *TRUE* is set. Following the *INVARIANTS* clause are the model's *Events*. The *Initial-*

```
MACHINE m1 REFINES m0 SEES ctx
VARIABLES m_level, c_level, e_level, m_pumpOnReq, c_pumpOnReq, e_pumpOnReq,
   m_pumpOnCmd, c_pumpOnCmd, e_pumpOnCmd, m_warn, c_warn,
e_warn,
  c_level_internal, c_pumpOnReq_internal
INVARIANTS
 (c_level_internal ≤ MIN ∧ c_pumpOnReq_internal = TRUE ⇒ c_warn
= TRUE)
  ∧ (c_level_internal > MIN ∧ c_pumpOnReq_internal = TRUE
    ⇒ c_pumpOnCmd = TRUE)
  ∧ (c_level_internal ∈ ℤ)
  ∧ (c_pumpOnReq_internal ∈ BOOL) . . .
EVENTS
INITIALISATION c_level := 100 ∥ m_level := 80 ∥ c_pumpOnReq :=
FALSE ∥ . . .
EVENT fmiSetBoolean_c REFINES fmiSetBoolean_c
 ANY p
 WHERE p = c_compound ∧ p ∈ BOOL
 THEN m_pumpOnCmd := p
 END
. . .
```

**Fig. 1** An Event-B Pump Controller Model

```
CONTEXT ctx
CONSTANTS MIN
AXIOMS MIN = 10
```

**Fig. 2** An Example Context

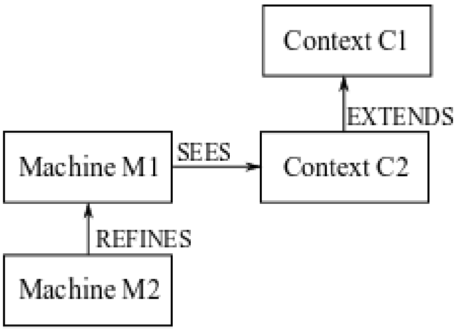

**Fig. 3** Refinement and Extension

*isation* event is special event, since it has no guards. The initialisation event of a machine must occur before any other event in the machine is enabled. The event in the figure has a parameter $p$, in the *ANY* clause. Parameters can be used to represent information flow, in and out of events, or they can represent a *local* variable within the scope of the event. The event guard is defined in the *WHERE* clause, in the example, where $p$ is typed as a Boolean. The guard relates the parameter to a machine variable *c_pumpOnCmd*, in the predicate $p = c\_compound$. The event action appears in the *THEN* clause, where the parameter is assigned to the variable *m_pumpOnCmd*, in the expression $m\_pumpOnCmd := p$.

### 1.4 Refinement and Extension

As we mentioned earlier in the section, Event-B makes use of a technique called refinement, where a machine can be refined by another. Fig. 3 shows this relationship. The refined machine is augmented with state variables, events and invariants, to provide a more detailed specification satisfying the properties, specified in the invariants, of the abstract specification. The counterpart to refinement of machines, is extension of contexts. It is then possible to build upon pre-existing contexts, using the *EXTENDS* clause, by adding more sets, constants, axioms and theorems. When a machine *SEES* a context, the contexts that it extends are also accessible to the machine. In a refinement, new variables, events and invariant properties can be added. Existing events can be modified, but in a restricted manner. Machine refinement is transitive and leads to a hierarchical structure. Refinements are related to their more abstract counterparts in such a way that, a valid refinement always satisfies the specifications higher in the refinement hierarchy. In this way, important system properties can be specified at a high level of abstraction, and maintained down through the refinement chain. The Event-B tools are responsible for generating the proof obligations relating to refinement; these must be discharged in a similar way to those generated for proof of machine consistency. It is often necessary to specify a linking invariant, to describe the relationship between the variables of the abstract and refinement machines. Inspection of the proof obligations can assist in this task since some of the un-discharged proof obligations provide information about this link. In some cases we may model entities in an abstraction that are defined in the event parameters; and in the refinement these entities may be introduced to the model as machine variables. To assist with the proof effort we have a slightly different strategy to that of refining abstract variables with concrete variables. We link the parameters of the abstract event, with their concrete counterpart, using a $WITNESS$. This construct is a predicate describing the relationship between an event parameter (that disappears) from an abstract model, and the corresponding (refining) variable in the concrete model. Another feature of Event-B is the ability to refine one atomic event with a number of events, thus breaking the atomicity, as described in [10]. Eventually, at the end of a refinement chain the models are detailed enough to accurately describe an implementation. But Event-B is a modelling language, and there is a disjunction between the description of the system in Event-B, and commonly used programming languages, such as Java, C and Ada. Addressing the semantic gap between Event-B and programming constructs is the subject of this article, which we will introduce more fully, later in the article.

### 1.5 Targets for Code-Generation

Initial development of the code-generation approach began from an object-oriented perspective, with the implementation-level notation, object-oriented, concurrent-B (OC-B) [14]. The focus of this work was to use Event-B to model and generate code for safe multi-tasking with object-oriented languages. We initially targeted the Java [18] language. We found, however, that this approach gave rise to a notation where the semantic gap between Event-B and the OC-B was quite large. This was not optimal for developers of Event-B models, who then wanted to write implementation-level specifications, from which code could be generated. We also found that models quickly became large and intractable; we recognized the need for decomposition of models into smaller units. At that time, Event-B tools were at an early stage of development, and machine decomposition was still in development.

We decided to modify the approach, to use the newly developed decomposition approach [29,30], and use an implementation-notation more closely related to Event-B (than OC-B, which was an object-oriented notation). The focus, then, became generating safe concurrent implementations, rather than targeting object-oriented technology, per se. This gave rise to our approach, known as Tasking Event-B. Our interest in safe, concurrent implementations drove us towards the Ada tasking model. At the implementation-level, an Event-B model is effectively a detailed model of an implementation. We found that the Ada [9] programming language provides clearly defined constructs, that map well to Event-B, see Fig. 4. Ada tasks and protected objects can be modelled by Event-B machines in a one-one mapping. We distinguish between

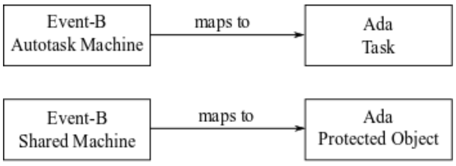

**Fig. 4** Mapping between Event-B and Ada

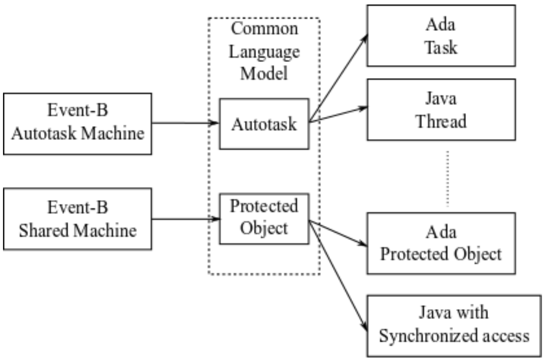

**Fig. 5** The Common-Language Model

the two entities by annotating the machines with the AutoTask and Shared keywords. We describe the mapping in more detail in Sect. **??**.

Before we proceed with a more detailed description of Event-B we provide an overview of the target languages that we wish to generate. Ada provides the basis for the code-generation approach as described in [15]. Ada tasks are processing units, known to the run-time system. Protected objects provide an encapsulation mechanism, that prevents interference. In Java the processing unit is provided by Thread class, and encapsulation is provided by synchronized methods and blocks. In C, there is some choice about the method of thread implementation, such as OpenMP [37] threads, or POSIX threads[1]. In its most basic form, the encapsulation mechanism for protected regions must be coded explicitly. Our final code-generation target arises from our work on co-simulation of Cyber-Phsyical systems in the Advance project [34]. In this approach we generate a specialized form of C code, conforming to the FMI standard for model co-simulation [36]. This can be used to simulate the software running on an embedded controller, in a simulation of its environment. In order to provide some commonality in the code generation process we formulated a two-stage code-generation process, as shown in Fig. 5, which is a modified from Fig. 4; with the first step translating to a common-language model, containing an abstraction of the required implementation. The second stage is a back-end processor, translating to the various target implementation languages. The semantics of the common-language model are formulated using Event-B, and provides a formal basis for the translation. We will discuss the semantics of Tasking Event-B in Sect. **??**.

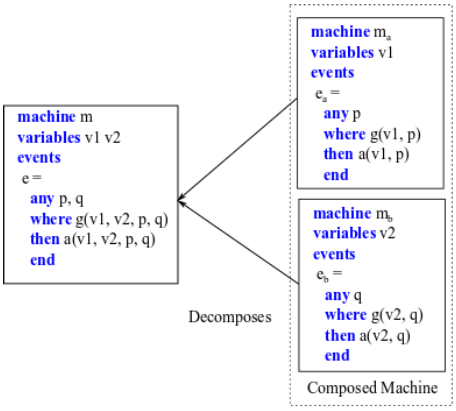

**Fig. 6** Decomposition

## 2 More about Event-B

### 2.1 Decomposition and Composition

Decomposition and composition are two related approaches, that we use to partition a system, to allow us to work on smaller, manageable sub-models. Figure 6 illustrates the shared-event decomposition approach [29] which we make use of in our code generation approach. An alternative shared-variable approach is described in [5]. In the shared-event decomposition approach the system is partitioned so that each variable is allocated to a single machine. In the figure, the variables of machine $m$ are partitioned into the sets $v1$ and $v2$ and decomposed into $m_a$ and $m_b$ respectively. The events ....

### 2.2 Theories

### 2.3 ProB

## 3 Tasking Event-B

### 3.1 The Language and Semantics

When modelling certain aspects of a system we may wish to impose an ordering of events. However, there is no sequence operator provided in the Event-B approach. It is therefore necessary to make appropriate use of guards and and state variables to model this aspect of a system. For example if we wish to impose an ordering on two events *evt1* and *evt2* so that $evt1$ occurs before $evt2$ we can use the following approach. Introduce an enumerated set $Grds = \{one,\ two,\ stop\}$ and a variable $step\ \in\ Grds$. Initially $step\ :=\ one$; and we make use of $step$ in the event guards as follows,

$$evt1 = \textbf{WHEN}\ step = one\ \textbf{THEN}\ \ldots \parallel step := two\ \textbf{END}$$
$$evt2 = \textbf{WHEN}\ step = two\ \textbf{THEN}\ \ldots \parallel step := stop\ \textbf{END}$$

This ensures that initially $evt1$ is enabled and $evt2$ is disabled since $step = one$; only after $evt1$ has updated the $step$ variable to $two$ is $evt2$ enabled. At this time $evt1$ is no longer enabled since its guard is now false. Finally no events are enabled since $step = stop$ and all guards are false.

### 3.2 Theories for TEB

### 3.3 State-machines

## 4 Tooling

### 4.1 The Rodin Platform and Eclipse

### 4.2 IL1/CLM

### 4.3 Templates

### 4.4 Interfaces

## 5 Conclusions

### 5.1 Discussion

### 5.2 Related Work

As we mentioned in the introduction, the main driver for this work has been to derive the greatest benefit from the formal modelling approach, by making use of the formal modelling artefacts to generate implementations. There are many formal notations and many have support for automatic code-generation.

The Classical-B [3] approach made use of an implementation-level notation called *B0*, described in [13]. B0 is similar to a programming language, and consists only of concrete programming constructs. These constructs map to programming constructs in a number of programming languages. *B0* forms part of the Classical-B refinement chain, so the implementation-level specification refines the abstract development. Translators are available targeting programming languages such as C [22], and *High Integrity Ada* (based on *SPARKAda* [2]).

The *Z-notation* is a state-based specification notation (actually a distant ancestor of Event-B).

The VDM-SL is a state-based formal specification language, related to $Z$, and has tool support for automatic code generation.

VDM++ is an object-oriented extension to Models can be described textually; or using a graphical interface using UML diagrams, in much the same way as UML-B does for B and Event-B. VDM++ can be used with the VDM++ Toolbox to generate C++ and Java code. VDM++ can be used to model and implement developments with concurrently executing processes, using threads.

*Object-Z* [31] is an object-oriented approach to development using $Z$. A route to implementation is described using a translation to *PerfectDeveloper* [16] in [33]. *PerfectDeveloper*'s approach is to use verified-Design By Contract, where verification conditions are generated from a specification using constructs such as pre and postconditions, class and loop invariants, and assertions. The verification conditions must be shown to hold in order to show the specified contracts are satisfied by the implementation. They are generated for each method entry to show that the precondition holds, for each method exit to show that the postcondition holds, and wherever an assertion appears. *PerfectDeveloper* provides automatic, and semi-automatic, translations to Java and C++ but appears not to support concurrent processing.

There are some combined formal approach where code-generation has been investigated. CSP [20,26] is a process algebraic approach to system specification in which the ordering of events occurring in a system play a major role. CSP specifications have been translated into Java code using JCSP [24, 38]. A hybrid CSP and Classical-B approach [27,28] combines the benefits of modelling, using both process-based and state-based techniques. In this approach, called $CSP \parallel B$, specifications are used to constrain the order that the state-changing operations may occur; and to specify points at which the processes may interleave. The B operations synchronize with CSP events with the same name, and provide an ordering of the occurrence of B operations. ProB [23] is an animator and model checker for Classical-B and Event-B, and can be used with the $CSP \parallel B$ combination. It is used in the JCSProB [40] approach, which combines CSP and Classical-B, and has a code generator inspired by JCSP. Another combined approach, amenable to model-checking, is *Circus* [39], which is combination of CSP and *Z-notation* [32]. CSP is used to order the $Z$ operations. It can be translated to Java as described in [17] and makes use of the JCSP library.

## References

1. POSIX.1c, Threads extensions, IEEE Std 1003.1, 2004 Edition
2. SPARKAda. URL `http://www.adacore.com/sparkpro/`
3. Abrial, J.: The B Book - Assigning Programs to Meanings. Cambridge University Press (1996)
4. Abrial, J., Butler, M., Hallerstede, S., Hoang, T., Mehta, F., Voisin, L.: Rodin: An Open Toolset for Modelling and Reasoning in Event-B. Software Tools for Technology Transfer **12**(6), 447–466 (2010). URL `http://dx.doi.org/10.1007/s10009-010-0145-y`
5. Abrial, J., Hallerstede, S.: Refinement, Decomposition, and Instantiation of Discrete Models: Application to Event-B. Fundam. Inform. **77**(1-2), 1–28 (2007)
6. Abrial, J.R.: Modeling in Event-B: System and Software Engineering. Cambridge University Press (2010)
7. Abrial, J.R., Cansell, D.: Clickn prove: Interactive proofs within set theory. In: D. Basin, B. Wolff (eds.) Theorem Proving in Higher Order Logics, *Lecture Notes in Computer Science*, vol. 2758, pp. 1–24. Springer Berlin Heidelberg (2003). DOI 10.1007/10930755_1. URL `http://dx.doi.org/10.1007/10930755_1`
8. Back, R., Sere, K.: Stepwise Refinement of Parallel Algorithms. Science of Computer Programming **13**(2-3), 133 – 180 (1990). DOI http://dx.doi.org/10.1016/0167-6423(90)90069-P. URL `http://www.sciencedirect.com/science/article/pii/016764239090069P`
9. Barnes, J.: Programming in Ada 2005. International Computer Science Series. Addison Wesley (2006). ISBN-10: 0321340787 / ISBN-13: 9780321340788
10. Butler, M.: Incremental Design of Distributed Systems with Event-B (2008). URL `http://eprints.ecs.soton.ac.uk/16910/`
11. ClearSy: B4Free. from http://www.b4free.com
12. Clearsy System Engineering: The Atelier B Tool. URL `http://www.atelierb.eu/en/`
13. ClearSy System Engineering: The B Language Reference Manual, version 4.6 edn.
14. Edmunds, A.: Providing concurrent implementations for event-b developments. Ph.D. thesis, University of Southampton (2010). URL `http://eprints.soton.ac.uk/141688/`
15. Edmunds, A., Rezazadeh, A., Butler, M.: Formal Modelling for Ada Implementations: Tasking Event-B. In: Ada-Europe 2012: 17th International Conference on Reliable Software Technologies (2012). URL `http://eprints.soton.ac.uk/335400/`
16. Escher Technologies: PerfectDeveloper. Available at http://www.eschertech.com
17. Freitas, A., Cavalcanti, A.: Automatic Translation from Circus to Java. In: J. Misra, T. Nipkow, E. Sekerinski (eds.) FM, *Lecture Notes in Computer Science*, vol. 4085, pp. 115–130. Springer (2006)
18. Gosling, J., Joy, B., Steele, G., Bracha, G.: Java Language Specification - Third Edition. Addison-Wesley (2004)
19. Hallerstede, S.: Justifications for the Event-B Modelling Notation. In: Julliand and Kouchnarenko [21], pp. 49–63
20. Hoare, C.: Communicating Sequential Processes. Prentice Hall (1985)
21. Julliand, J., Kouchnarenko, O. (eds.): B 2007: Formal Specification and Development in B, 7th International Conference of B Users, Besançon, France, January 17-19, 2007, Proceedings, *Lecture Notes in Computer Science*, vol. 4355. Springer (2006)
22. Kernighan, B., Ritchie, D.: The C Programming Language, Second Edition. Prentice-Hall (1988). URL `http://cm.bell-labs.com/cm/cs/cbook/`
23. Leuschel, M., Butler, M.: ProB: an automated analysis toolset for the B method. STTT **10**(2), 185–203 (2008). URL `http://dblp.uni-trier.de/db/journals/sttt/sttt10.html#LeuschelB08`
24. P.H.Welch, Aldous, J., Foster, J.: CSP Networking for Java (JCSP.net). In: Computational Science - ICCS 2002: International Conference (2002)
25. RODIN Project: at http://rodin.cs.ncl.ac.uk
26. Roscoe, A.W., Hoare, C.A.R., Bird, R.: The Theory and Practice of Concurrency. Prentice Hall PTR, Upper Saddle River, NJ, USA (1997)
27. Schneider, S., Treharne, H.: Communicating B Machines. In: D. Bert, J.P. Bowen, M.C. Henson, K. Robinson (eds.) ZB, *Lecture Notes in Computer Science*, vol. 2272, pp. 416–435. Springer (2002)

28. Schneider, S., Treharne, H.: CSP Theorems for Communicating B Machines. Formal Asp. Comput. **17**(4), 390–422 (2005)
29. Silva, R., Butler, M.: Shared Event Composition/Decomposition in Event-B. In: FMCO Formal Methods for Components and Objects (2010). URL `http://eprints.soton.ac.uk/272178/`. Event Dates: 29 November - 1 December 2010
30. Silva, R., Pascal, C., Hoang, T., Butler, M.: Decomposition Tool for Event-B. Software: Practice and Experience (2010). URL `http://eprints.ecs.soton.ac.uk/21714/`
31. Smith, G.: The Object-Z specification language. Kluwer Academic Publishers, Norwell, MA, USA (2000)
32. Spivey, J.M.: The Z notation: A Reference Manual. Prentice-Hall, Inc., Upper Saddle River, NJ, USA (1989)
33. Stevens, B.: Implementing Object-Z with Perfect Developer. Journal of Object Technology **5**(2), 189–202 (2006)
34. The Advance Project Team: Advanced Design and Verification Environment for Cyber-physical System Engineering. Available at http://www.advance-ict.eu
35. The DEPLOY Project Team: Project Website. at http://www.deploy-project.eu/. URL `http://www.deploy-project.eu/`
36. The Modelica Association Project: The Functional Mock-up Interface. Available at https://www.fmi-standard.org/
37. The OpenMP Architecture Review Board: The OpenMP API specification for parallel programming. Available at http://openmp.org/wp/
38. Welch, P., Martin, J.: A CSP Model for Java Multithreading. In: Software Engineering for Parallel and Distributed Systems (2000)
39. Woodcock, J., Cavalcanti, A.: A Concurrent Language for Refinement. In: A. Butterfield, G. Strong, C. Pahl (eds.) IWFM, Workshops in Computing. BCS (2001)
40. Yang, L., Poppleton, M.: Automatic Translation from Combined B and CSP Specification to Java Programs. In: Julliand and Kouchnarenko [21], pp. 64–78