Integrating formal approaches in Human-Computer Interaction methods and tools: an experience

Patrick Girard[1], Mickaël Baron[1], Francis Jambon[2]

[1] LISI/ENSMA, 1 rue Clément Ader, Téléport 2,
BP 40109, 86961 Futuroscope Cedex, France
{girard,baron}@ensma.fr

[2] CLIPS-IMAG, 385 rue de la bibliothèque,
BP 53, 38041 Grenoble cedex, France
Francis.Jambon@imag.fr

Abstract: Formal methods are increasingly used by HCI researchers. Nevertheless, their usage in actual interactive developments is not so common. In this paper, we describe the use of a specific formal method from two viewpoints. On the one hand, we demonstrate how it is possible to use a formal method on real development from specification to actual code. Doing so, we notice that HCI concepts, such as architecture models, may have to be adapted. On the other hand, we show how it is possible to bring more usability to formal methods by the way of a complete integration into HCI tools. We conclude in eliciting the lessons learned from these works.

Keywords: Formal methods, HCI tools, interactive development

1. Introduction

Software engineering (SE) methods are well known to be relatively far from Human Computer Interaction (HCI) methods and tools. From the HCI point of view, we can say that beyond use case models in UML, task-based approaches are not really in use in most projects. From the SE point of view, HCI tools and methods remain partial and somewhere "anecdotal".

In this contribution, we would like to introduce our experience in attempting to incorporate formal methods (issued from SE point of view) in interactive design and development. Doing so, we try to elicit the points that make all the difficulty of actually realizing our goals.

Our approach is based on the use of the formal B method in HCI, in order to address security in critical interactive applications, such as traffic air control or nuclear power plant supervision. We do not intend to focus on the use of this particular formal method. Adversely, we only use this experience to illustrate the gap between the two fields.

In the next part –part 2– we give a short list of formal approaches that have been used in HCI, and we give several points that explain their poor usage in that field. In part 3, we relate the first attempts in applying the B method in interactive design. We particularly focus on architectural problems, which might constitute a solid bridge between SE and HCI. In part 4, we show how actual HCI tools might incorporate secure development methods by the way of leaning on formal semantics all along the HCI design and development. Last we conclude on discussing the lessons learned in these works.

2. Formal approaches in HCI

Formal specification techniques become regularly used in the HCI area.

On the one hand, user-centred design leans on semi-formal but easy to use notations, such as MAD (Scapin and Pierret-Golbreich, 1990) and UAN (Hix and Hartson, 1993) for requirements or specifications, or GOMS (Card et al., 1983) for evaluation. These techniques have an ability to express relevant user interactions but they lack clear semantics. So, neither dependability nor usability properties can be formally proved.

On the other hand, adaptation of well-defined approaches, combined with interactive models, brings partial but positive results. They are, for example, the interactors and related approaches (Duke and Harrison, 1993, Paternò, 1994), model-oriented approaches

(Duke and Harrison, 1993), algebraic notations (Paternò and Faconti, 1992), Petri nets (Palanque, 1992), Temporal Logic (Brun, 1997, Abowd et al., 1995). Thanks to these techniques, some safety as well as usability requirements may be proved.

However, these formal techniques are used in a limited way in the development process, mainly because of three points:

Few of them can lean on usable tools, which allow real scaled developments. Case studies have been demonstrated, but no actual application has been completely designed with these methods.

Formal notations are currently out of the scope of HCI designers. Their usage by non specialists it everything but easy.

Formal studies are currently disconnected from usual HCI tools. No commercial tool and very few research one really incorporates semantically well defined approaches.

In this paper, we relate our studies one model-oriented approach, the B method (Abrial, 1996), whose one great advantage is to be well instrumented. But we do not allege it is the best nor the perfect formal method to be used. Our claim is that this model-oriented technique that uses proof obligations can be used with profit in a HCI context; more, it might be used together with model checking techniques, where automatic proofs of properties can be performed.

3. The B method and interactive design and development

This section presents the different steps that have been made in the attempt to use the B method in the field of HCI. Starting from the reduced aspect of verifying software specifications, we show how it has been possible to reach the implementation step in a complete formal development. Then, we focus on architecture problems. Last, we conclude in analyzing the difficulty of this extreme approach.

3.1. Using B for HCI specifications

In (Aït-Ameur et al., 1998a, Aït-Ameur et al., 1998b), the authors use for the first time the B method for the verification of interactive systems. Lying on a pure interactive case study (see below), these works suggest formally based solutions which allow solving difficulties that are inherent to interactive systems specification, such as reachability, observability or reliability.

The case study is a co-operative version of a Post-It[®i] Note software. With this case, it is possible to address highly interactive problems due to the direct manipulation style, such as drag and drop, Iconfication/Deiconification, resizing, and so on. A special attention is paid on mouse interaction.

This use of the B method on a non-trivial case study has illustrated the capability of B to handle different aspects of the software life cycle in the area of interactive systems. The described approach demonstrates:

Complete formalisation: the approach is completely formalised and most of the proof obligations are automatically proved. The other ones need only few steps of manual proof.

Property checking: it is possible to check properties on specifications, thanks to the weakening of preconditions.

Reverse engineering aspects can be handled with this approach and the specifications of already existing programs can be used to develop new ones. Therefore, reusability issues appear.

Incremental design: the specifications are incrementally. Indeed, programming in the large operator allows to compose abstract machines and therefore to build more complex specifications. Yet, this process needs to follow a given methodology issued from the area of interactive system design.
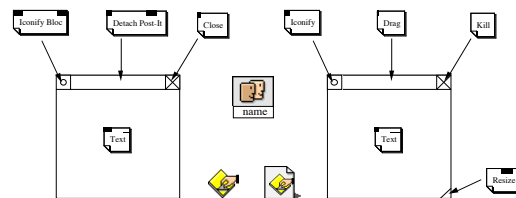

Figure 1: From the left to the right, The Post-It[®] block, the three icons (Post-It[®] block, User, and Post-It[®]), and the Post-It[®] Note itself.

One can object that this case study is situated at a too low level for the interactive viewpoint. Properties such as keeping the mouse pointer into the screen are not relevant in current graphical systems where this is ensured –or supposed to be ensured– by the operating system. In fact, this emphasizes the problem of using formal methods in actual interactive environments. Is it acceptable to use formal techniques when we lean on graphical layers that are not formally defined? One

---

i   "Post-it" is a registered trademark of 3M

solution, as described in this work, might be to make a reengineering analysis of such tools.

The first step reached by this study is the one of a complete specification of an interactive system, with respect to some interactive properties. As many works in the field of formal methods in HCI, it is possible to concentrate on some properties, but two drawbacks can be given:

Because of the strong relation to the coding activities, interactive properties are not related to the user activity;

Formally ensuring that specification are consistent, and respect properties, does not ensure that the actual code will respect specification, without a link between implementation and specification.

One of our major goals in exploring the usage of formal methods in the context of HCI design and development was to ensure that other people than pure formal methods specialists could use the method. So, with help of B tools, we tried to realize the whole development of an interactive application, from high-level specifications to running code. We first propose a architecture model to assist the designer (3.2), and then define heuristics to implement this model (3.3).

3.2 Formal development versus software architecture models

The case study is here a control panel for a set of three rechargeable batteries. It is an elementary safety-critical process-control system: the operator can control side effects on hardware –the switches– whereas the hardware state –the batteries levels– is altered asynchronously. Both safety and usability properties have to be ensured. This required first step of the design process consists in modeling the battery control panel requirements with the B language. Three kinds of requirements must be fulfilled:

The system must be safe, i.e., the system must avoid shortcuts and it must not be possible to switch on an empty battery.

The system must be honest, i.e., the user interface widgets must display exactly the batteries levels and switches positions.

The system must be insistent, i.e., the system must warn the operator when a battery is going to be empty.

Our first idea for designing such a system was to use a well-known multi-agent model, such as MVC (Goldberg, 1984) or PAC (Coutaz, 1987), because acceptability of formal methods is greatly influenced by using domain standard methods. The interactive system specifications must however stay in the boundaries of the B language constraints. We selected three kinds of constraints that relate to our purpose. These main constraints are:

Modularity in the B language is obtained from the inclusion of abstract machine instances –via the INCLUDES clause– and, according to the language semantics, all these inclusions must build up a tree.

The substitutions used in the operations of abstract machines are achieved in parallel. So, two substitutions –or operations– used in the same operation cannot rely on the side effects of each other.

Interface with the external world, i.e. the user actions as well as the updates of system state, must be enclosed in the set of operations of a single abstract machine.

Classic software architecture models such as PAC or MVC are not compliant with these drastic B language constraints. That is why we proposed a new hybrid model from MVC and PAC to solve this problem. The design of this new software architecture model –CAV– cannot be detailed here. The reader should refer to (Jambon et al., 2001) for a more detailed description of the model design.
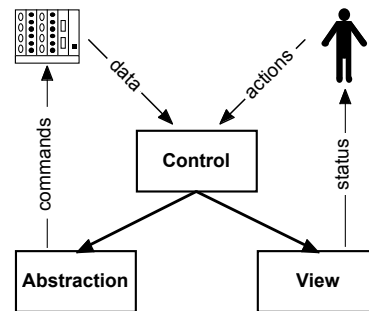

Figure 2: The three components of the Control-Abstraction-View software architecture model

The CAV model uses the external strategy of MVC: the outputs of the system are devoted to a specific abstract machine –the View– while inputs are concerned by another one –the Control– that also manages symmetrical inputs from the reactive system which is directed by the third abstract machine –the Abstraction. The Control machine synchronizes and activates both View and Abstraction machines in response to both user and reactive system events.

Among the usability properties, the system is in charge of warning the user if a battery is going to be empty. This usability requirement has to be specified as: if the battery switch is in position ON and the level is below or equal 10%, a warning message must

be shown. This is specified in the INVARIANT clause of the View. As a consequence, the operations of the View must be specified to fulfil this invariant whatever the way they are computed. This insistence property specification is restricted to the View abstract machine. So, it is fairly easy to handle. On the contrary, the Conformity property requires the Control mediation between Abstraction and View. Its specification is similar to the specification of safety below.

Among the safety requirements, we detail now the prevention of user error: the operator must not be able to switch on an empty battery. At first, this safety requirement deals with the functional core of the system, i.e., it must be specified in the Abstraction. Moreover, this requirement is not a static but a dynamic property: the battery can become empty while switched on, but an empty battery must not be switched on. This requirement is not static predicate, so, it cannot be specified in the invariant clause of the abstract machine. In the B language semantics, this category of requirement must be specified in a precondition substitution of operations.

In fact, we delegated to the Control abstract machine –that includes the Abstraction– this safety requirements, i.e. the Control is in charge of the verification of the semantic validity of the parameters when it calls the operation of the Abstraction abstract machine. We name this technique the delegation of safety. This generates two consequences: (1) The operator cannot be aware of the fact that a battery could not be switched on ; (2) An action on a pushbutton can be generated with a empty battery number as parameter, so some required proofs obligations cannot be proved.

The first consequence is easy to set up. We have to improve the interface layout and to update the state of the button: enabled or disabled. Of course, if a button is disabled, it is well known that this button cannot emit any action event. This assertion may seem to be sufficient to solve the second consequence above. That is not exact: the B semantics cannot ensure that a disabled button cannot emit events because the graphic toolkit is not formally specified. So, the Control abstract machine must filter the input events with the button states specified in the View abstract machine. This is required by the formal specification. The benefit of this consequence is that our system is safe whether the user interface is defective.

3.3. From formal specifications to implementation

The final program must be a set of software modules in which some of them are formally specified and implemented, and some others are developed with classic software engineering methods. In order to dissociate these two antagonist types of modules, interfaces have been inserted in between. So, at the implementation step, the CAV architecture supports some add-ons as shown on figure 3. We now focus on these three types of modules: secure code, interface and native modules.
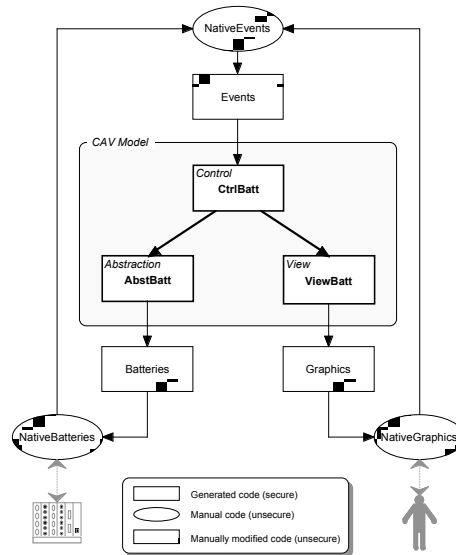

Figure 3: The CAV software architecture with interface and native modules

3.3.1. Secure Code

The core of the interactive system has been specified in three B abstract machines. These machines specify the minimum requirements of the system but do not give any implantation solution. To do so, the B method uses implementation machines that refine abstract machines. The implementation machines are programmed in BØ pseudo-code that shares the same syntax with the B language, and is close to a generic imperative programming language. In implementation machines, the substitutions are executed in sequence. BØ pseudo-code can be automatically translated into C code.

As implementation machines refine abstract machines, they must implement all the operations of the abstract machines. Moreover, the B method and semantics ensure that the side effects on variables of the implementation machine operations do respect the invariant as well as the abstract machine operations they refine. Providing the proof obligations are

actually proved, the implementation machines respect the safety and usability requirements. So, the code is secure providing the specifications are adequate.

3.3.2. Native Code and Interfaces

A working program cannot be fully developed with formal methods because most of graphic widgets and hardware drivers libraries are not yet developed with formal methods. As a consequence, the battery control panel uses three native modules:

The NativeGraphics software module controls the graphic layout of the user interface. It uses the GTk library.

The NativeBatteries software module simulates the batteries with lightweight processes. It uses the POSIX thread library.

The NativeEvents software module is in charge of merging the events coming from the user or the hardware and formats them to the data structure used by the BØ translator.

These three modules are not secure. However, the modules can be tested with a reduced set of test sequences because the procedures of these modules are only called by the secure code that does respect the formal specification. For example, the bar graph widget of NativeGraphics module is to be tested with values from 0 to 100 only because the secure modules are proved to use values from 0 to 100 only. Abnormal states do not have to be tested.

The interfaces module roles are to make a syntactic filtering and translation between native modules and secure code:

The Events software module receives integer data and translates them to 1..3 or 0..100 types. This module is secure because it as been specified and fully implemented in BØ but is called by non-secure modules.

The Graphics and Batteries modules are specified in B and the skeleton of the modules is implemented in BØ and then manually modified to call the native modules NativeBatteries and NativeGraphics respectively.

3.3.3. Programming Philosophy

At last, the project outcome is a set of C source files. Some of these files are automatically generated from the BØ implementation, while others are partially generated or manually designed. The formal specification and implantation require about one thousand non-obvious proof obligations to be actually proved. All these proof obligations can be proved thanks to the automatic prover in a few dozen of minutes with a standard workstation.

The core of the system is formally specified and developed. The programming philosophy used is called the offensive programming, i.e., the programmer does not have to question about the validity of the operations calls. The B method and semantics ensure that any operation is called with respect to the specifications. Most of the dialogue controller as well as the logic of the View and the Abstraction are designed with this philosophy. As a consequence, most of the dialog control of the system is secure.

On the opposite, the events coming from the real-word –user or hardware– have to be syntactically and semantically filtered. This programming philosophy is defensive. On the one hand, the syntactic filtering is done by the Event module that casts the parameter types –from integer to intervals. On the other hand, the semantic filtering is achieved by the Control module, which can refuse events coming from disabled buttons. So, the system is resistant to graphic libraries bugs or transient errors with sensors. This filtering is required by the proof obligations that force upon the operation calls to be done with valid parameters.

There is no need to use the defensive programming philosophy in native modules. The procedures of these modules are called only by secure modules, so the parameters must be valid anytime. Neither verification nor filtering is necessary. The programming philosophy looks like the offensive philosophy except that the native modules are not formally specified but must be tested, so we name this philosophy half-offensive. As a consequence the development of high-quality native code can be performed with a reduced programming effort.

3.4. Formal method in HCI: what kind of user?

As we write upper, one of our first goals was to ensure that other people than pure formal method specialists could use the method. Did we succeed?

We must admit that this goal is not reached today. In our first attempts on the Post-It® case study, even if the B tool automatically demonstrated most proofs, it remained some of them to be demonstrated by hand. This task cannot be made by non B specialists.

In the second case, for the battery case study, we obtained a fully automated process with the B tool. But it required to pay strong attention on condition writing; more, despite of the smallness of the study, the number of generated proof obligation let us think that a much more example might "explode" the tool.

4. Incorporating formal methods in HCI tools

Another way to allow cooperation between SE and HCI is to lean on formal semantics while building a tool for HCI. We describe in this section such an approach, and show how it can bring different solutions.

In section 4.1, we shortly review the area of HCI tools, mainly GUI-Builders and Model-Based tools. Section 4.2 describes the fundamentals of our proposal: connecting directly and interactively a GUI-Builder to a functional core, by the way of formal semantics. Section 4.3 relates how to incorporate task-based analysis in this process.

4.1. A glance at HCI tools

HCI tools for building interactive software are numerous. In the meantime, few of them handle formal approaches.

On the one hand, GUI builders and tools from suites such as Visual Basic® or Jbuilder® do not provide any way to handle any kind of formal method. Code generation is another difficulty, because it enforces a code organization that does not conform to good SE practices.

On the other hand, Model-Based tools (Puerta, 1996, Puerta et al., 1999) deal with models, but are currently not usable for actual software development. Some research tools such as Petshop (Ousmane, 2001) incorporate formal methods, for some parts of software development.

Our goal is to try to incorporate formal methods in HCI tools in a deep way, with respect to usability for HCI user.

4.2 A semantic link between the functional core and the HCI tool

The basic idea of our approach is to build HCI tools that lean on formal semantics to ensure that properties are maintained all along the development process. At the same time, we do not expect the user to become a formal method specialist

Our first step was to demonstrate how it is possible to build a tool that ensures a semantic formal link. We start from a formally developed functional core. We assume that this functional core, which has been specified with the B method, delivers services through an API. It is possible to automatically link such a

functional core to a tool that exploits function signatures and formal specifications to help building interactive software.

In figure 4, we can see a screen copy of the GenBUILD tool. On the left, the animator consists in fully generated interface that allows to interactively run the functional core. Every function of the functional core is usable through button activation. When parameters are required, a dialog box appears to allow the user to enter them. Functions are textually described, and current state of the functional core can be estimated through the result of all functions. It is important to notice that all that part is fully automatically generated. It allows the user to "play" with his/her functional core, and to be aware of functional core state.

In the right part of the figure, we can see the GUI-Builder view, where widgets can be dropped to build the concrete user interface. In the center, as in any GUI-Builder, we can see a property window, which allows the user to finalize the presentation. Below this window, the last window permits associating events to functions from the functional core.

The great two originalities at this point are: first, at any time, we can switch from design mode to test mode where functional core can be called from either the presentation or the animator (the context of the functional core remains consistent); second, the
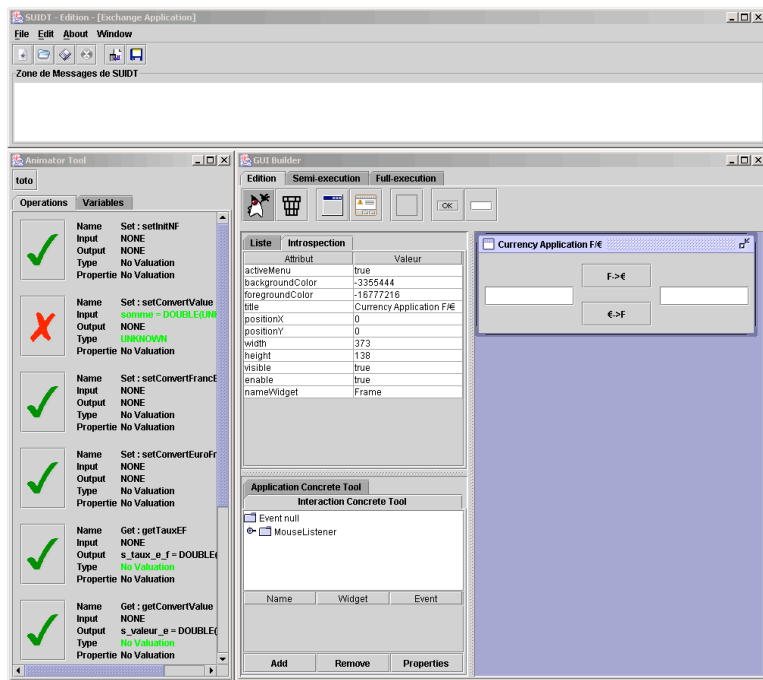

Figure 3: the GenBUILD system

system leans on formal specifications from the functional core to ensure that calls are correct.

This study demonstrates that it is possible to incorporate formal approaches in interactive tools. The benefit is not very important at this stage, because interactive model is poor: we assume that the link between widgets and functional core is direct. In the next part, we show how it is possible to enhance this model.

4.3. Linking task based analysis and formal semantics

The second step of our study consists in focusing on task-based analysis. We incorporated task-based analysis into our system by the way of two task models (abstract and concrete task models) using the CTT formalism (Paternò, 2001). In figure 5, we see on the upper left a view of the abstract task model. While CTTE (Paternò et al., 2001) provides a purely graphical view of CTT trees, we chose to draw them in a tree widget. This avoids many problems like sizing or beautifying. The original part of the study consists in the link that exists between the abstract task model and the functional core. In tools such as CTTE, we can animate the task model, in order to ensure that the specifications of the system are consistent. In GenBUILD, we can go one step further. We can animate the system itself; we exploit the possibility to interactively run the functions of the

functional core, with respect to the formal specifications of this one. More, we can also link the pre- and post-conditions of CTT to functions, in order to dynamically control the execution. This is shown in the front window on figure 5.

We do not illustrate here the concrete task model, which allows the same kind of links, but on the presentation (widget) side (Baron and Girard, 2002).

With GenBUILD, we use formal specifications in an interactive way that allows non-specialists to take advantage of formal methods without heavy learning or careful usage.

5. Lessons learned

5.1. Consideration about methods

Our studies bring partial solutions in the field of formal methods for HCI. On the one hand, they demonstrate how formal methods are really usable in HCI design. In the meantime, their usage is restricted to specialists that come to grips with mathematical fundamentals. Automatic proving is not possible in real developments. "Manual" proving is mandatory. Incorporating formal approaches into HCI tools may bring a solution: hiding formal language complexity allows HCI designers to use these methods in a blink mode.

On the other hand, we did not work on a global method to build application with such tools. We assumed that functional cores have to be designed first. In many cases, this is not the best way to work. In some cases, task analysis may turn up new needs. Modifying the functional core and its formal specifications to rebuild a new solution might be difficult. Is the opposite way possible? Is it possible to start form task analysis, to design the presentation, and then to develop the functional core, with respects to properties that might be enforced in the functional core by strong formal methods?

5.2. What is the user

One of the strongest questions that have been raised by these studies is: what kind of user for formal methods in HCI?

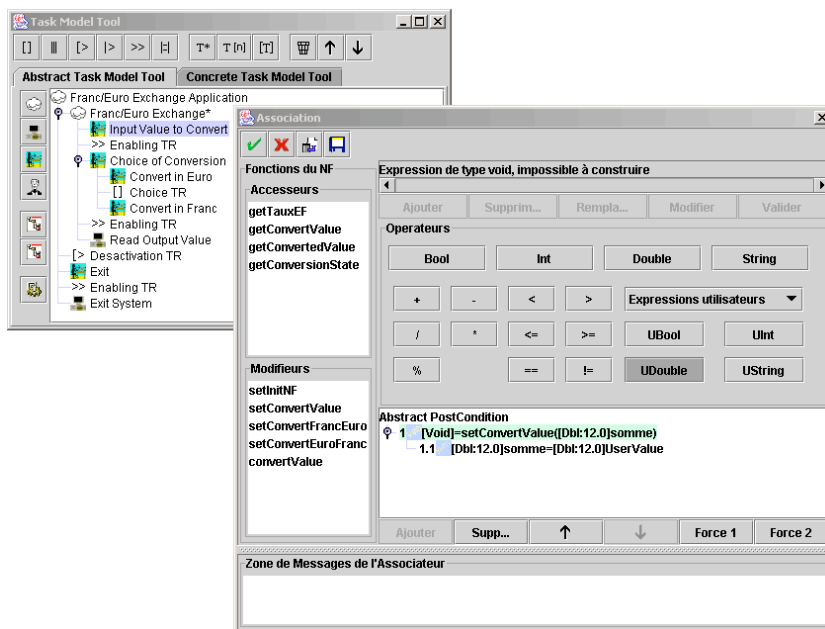One the one hand, manipulating formal methods

Figure 5: task-based aspects of GenBUILD

themselve is often hard. Complete formal development is very difficult, and formal tools such as "Atelier B" are not really able to manage real scaled applications.

On the other hand, manipulating formal methods through HCI tools seems very interesting. But wher is the place for formal development? And who might make it?

All these points are to be discussed, and solutions to be bring by further work.

6. References

Abowd, G. D., Wang, H.-M. and Monk, A. F. (1995) A Formal Technique for Automated Dialogue Development, in DIS'95, Design of Interactive Systems (Eds, Olson, G. M. and Schuon, S.) ACM Press, Ann Arbor, Michigan, pp. 219-226.

Abrial, J.-R. (1996) The B Book: Assigning Programs to Meanings. Cambridge University Press.

Aït-Ameur, Y., Girard, P. and Jambon, F. (1998a) A Uniform approach for the Specification and Design of Interactive Systems: the B method, in Eurographics Workshop on Design, Specification, and Verification of Interactive Systems (DSV-IS'98), Vol. Proceedings (Eds, Markopoulos, P. and Johnson, P.), Abingdon, UK, pp. 333-352.

Aït-Ameur, Y., Girard, P. and Jambon, F. (1998b) Using the B formal approach for incremental specification design of interactive systems, in Engineering for Human-Computer Interaction, Vol. 22 (Eds, Chatty, S. and Dewan, P.) Kluwer Academic Publishers, pp. 91-108.

Baron, M. and Girard, P. (2002) SUIDT : A task model based GUI-Builder, in TAMODIA : Task MOdels and DIAgrams for user interface design, Vol. 1 (Eds, Pribeanu, C. and Vanderdonckt, J.) Inforec Printing House, Romania, Bucharest, pp. 64-71.

Brun, P. (1997) XTL: a temporal logic for the formal development of interactive systems, in Formal Methods for Human-Computer Interaction (Eds, Palanque, P. and Paternò, F.) Springer-Verlag, pp. 121-139.

Card, S., Moran, T. and Newell, A. (1983) The Psychology of Human-Computer Interaction. Lawrence Erlbaum Associates.

Coutaz, J. (1987) PAC, an Implementation Model for the User Interface, in IFIP TC13 Human-Computer Interaction (INTERACT'87) North-Holland, Stuttgart, pp. 431-436.

Duke, D. J. and Harrison, M. D. (1993) Abstract Interaction Objects. Computer Graphics Forum, 12, 25-36.

Goldberg, A. (1984) Smalltalk-80: The Interactive Programming Environment. Addison-Wesley.

Hix, D. and Hartson, H. R. (1993) Developping user interfaces: Ensuring usability through product & process. John Wiley & Sons, inc., Newyork, USA.

Jambon, F., Girard, P. and Aït-Ameur, Y. (2001) Interactive System Safety and Usability enforced with the development process, in Engineering for Human-Computer Interaction (8th IFIP International Conference, EHCI'01, Toronto, Canada, May 2001), Vol. 2254 (Eds, Little, R. M. and Nigay, L.) Springer, Berlin, pp. 39-55.

Ousmane, S. (2001) Spécification comportementale de composants CORBA. PhD of Univ. Université de Toulouse 1, Toulouse.

Palanque, P. (1992) Modélisation par Objets Coopératifs Interactifs d'interfaces homme-machine dirigées par l'utilisateur. PhD of Univ. Université de Toulouse I, Toulouse.

Paternò, F. (1994) A Theory of User-Interaction Objects. Journal of Visual Languages and Computing, 5, 227-249.

Paternò, F. (2001) Model-Based Design and Evaluation of Interactive Applications. Springer.

Paternò, F. and Faconti, G. P. (1992) On the LOTOS use to describe graphical interaction, Cambridge University Press, pp. 155-173.

Paternò, F., Mori, G. and Galimberti, R. (2001) CTTE: An Environment for Analysis and Development of Task Models of Cooperative Applications, in ACM CHI 2001, Vol. 2 ACM Press, Seattle.

Puerta, A. (1996) The MECANO project : comprehensive and integrated support for Model-Based Interface development, in Computer-Aided Design of User interface (CADUI'96) (Ed, Vanderdonckt, J.) Presse Universitaire de Namur, Namur, Belgium, pp. 19-35.

Puerta, A. R., Cheng, E., Ou, T. and Min, J. (1999) MOBILE : User-Centered Interface Building, ACM/SIGCHI, Pittsburgh PA USA, pp. 426-433.

Scapin, D. L. and Pierret-Golbreich, C. (1990) Towards a method for task description : MAD, in Working with display units (Eds, Berliguet, L. and Berthelette, D.) Elsevier Science Publishers, North-Holland, pp. 371-380.