

A Formal Approach in the Implementation of a Safety System for Automatic Control of "Platform Doors"

4th Annual Conference on System Engineering
"Company efficiency and customer satisfaction"
Pierre Baudis Congress Centre, TOULOUSE, 2nd - 4th May 2006

Florent PATIN
ClearSy
20, rue Joubert
75009 Paris
Florent.patin@clearsy.com

Guilhem Pouzancre
ClearSy
20, rue Joubert
75009 PARIS
guilhem.pouzancre@clearsy.com

Thierry Servat
ClearSy
20, rue Joubert
75009 PARIS
thierry.servat@clearsy.com

Summary

Clearsy is an engineering company that performs its services with the use of formal modelling techniques and tools based on B-technology.

This presentation describes the methodology employed in implementing a safety system for automatic control of "platform doors" for the RATP, the Paris Transport Authority.

We present here the different activities carried out, as well as the benefits obtained over the various stages of the development and integration process.

Project presentation

For some years the RATP has been using a system of glass safety door barriers allowing the RATP to prevent access to its underground tracks from the platforms. This system was implemented on the fully automatic METEOR underground (line 14) when it was commissioned. It results in substantial improvement in line availability and traffic flows.

With the aim of improving the quality of service and the safety of its network, the RATP wants to use this kind of protection on other lines, no matter whether these are fully automated or not. For practical reasons as well as for reasons of cost, it does not, however, want to modify its rolling stock.

Before moving to deploy a new system of glass safety door barriers on a whole line, the RATP launched a prototype project for installation of the system on three platforms of line 13 for 8 months. This project has two parts:

- The mechanical component of the "platform doors"

- The automatic control component of the screen system, christened COPPILOT

Clearsy is in charge of the second part which involves:

- Design of an SIL3 level safety system
- Detection of the arrival, presence and departure of a train without there being any contact with the latter
- Detection of the opening and closing of the train doors
- Generation of the opening and closing safety sequences for the glass safety door barriers.

Of course, since the solution is intended for the Paris metro lines, the system must comply with the different standards that are very strictly applied to the rail systems in operation by the RATP.

Our strategy

The difficulty in this project relates to its very short realisation deadlines of 10 months between project launch and commissioning of the system.

Our strategy therefore had to be based on a system allowing production of a safety architecture for which validation could be quickly obtained and with results that would be fairly independent of the various technologies and sensor models used.

For this reason we chose an architecture based on standard industrial components - a Siemens safety controller with SIL3 certification, infrared sensors (Leuze, DataSensor etc.) and radars.

System safety is based on the safety technology of the controller as well as on the

redundancy of the measurements given by the various sensors, and not on the safety as such of the sensors.

This solution therefore allows:

- A decrease in materials costs, since the standard sensors are a lot less expensive than safety-certified sensors
- Procurement deadlines that are a lot tighter, since the sensors are a lot more widely available
- Much less dependence on a single supplier
- A variety of procurement sources

Our methodology

So as to attain the level of safety required within the timescales imposed, we have implemented a development procedure resulting in very good reliability and traceability between the different stages so as to gain time as regards validation.

Clearsy uses the formal B-method, which is well suited to development of SIL3 or SIL4 software. We are using it, for example, to write the software for the Val de Roissy driverless system, a program that has to meet a very high level of safety (SIL4).

In this project, this is the first time this methodology has been used in the full system cycle - in the system and safety specification stages and then seamlessly throughout all the levels of the development and application process.

Using the B language, which is based on the mathematical theory of sets, it is possible to describe a system using logical expressions and then to check its consistency. Such a check is performed using mathematical proofs. This language has been used on various systems requiring very high safety levels (SIL4) mainly in a rail environment, on projects such as the METEOR driverless system (RATP, line 14).

In essence the B language enables us to:

- Check that a system fully meets certain criteria (functional and safety etc.)
- Check that a system really is intrinsically consistent, in other words that there is no contradiction embedded within it
- Check that a system as defined does not have "grey areas" where there might be behaviour that is badly defined or not defined at all
- Obtain a very high degree of traceability (integrated into the

language itself and by mathematical proof) between the specification, design and implementation phases

During the development process of the COPPILOT project we have therefore taken the decision, in agreement with the RATP, to integrate this formal methodology in the main phases so as to ensure consistency of our work before moving on to the following stages.

The development process

The B-method was used throughout the development cycle as shown in the following flow chart.

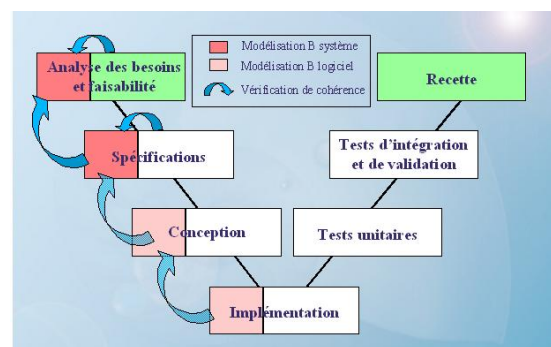


Figure 1: Use of B in the development cycle

Requirements and feasibility study. Initially, the RATP engaged us to carry out the functional and formal analysis of the system to ensure that the build specification was complete and unambiguous.

The solution as conceived at this stage was based on two laser telemeters working in parallel on the doors at different places on the platform. Using image recognition performed by two completely different systems it was possible to recognise the arrival, departure and stopover of a train in the station, as well as door opening and closure.

The first stage involved performing a check over the full system, i.e. over the automatic control system (COPPILOT) and over the platform doors, with a view to ensuring that:

- The functional constraints had been properly met
- The safety characteristics expected by the RATP had been checked, in other words that it was not possible to create impermissible connections between the track and the platform or between the train and the track

This stage also involved a study of what intrusive events might lead to the system functioning in a dangerous manner.

At the next stage we investigated the chosen solution that was based on laser telemeters so

as to check that it did in fact meet the project constraints.

The B-method used here makes dealing with these issues easy. In addition, by using it at this level in the development process, we could be sure that the system was complete and univocal before continuing the process, and that there would not therefore have to be any modification to be made to the functional specifications.

System and software specifications. The RATP then selected Clearsy to be project manager of the automatic control component (COPPILOT). The B-method was used in the specification stage to check consistency of the choice of system architecture with regard to the functional specifications supplied by the RATP.

The initial solution that had been conceived in the study phase was replaced with an architecture based on a safety controller and a set of sensors using different technologies (hyperfrequency, infrared, lasers, etc) each having a very specific function: Detection of the presence, of the movements of the train and of the door movements etc.

Once the system and software specifications for this solution had been written, we continued with two complementary approaches:

- B-modelling of these specifications for the case of nominal functioning of these sensors (without any adverse intrusions) undertaken by the development team
- A safety study, carried out by the independent safety team, allowing exact identification of the influence of the various adverse intrusions on the functioning of the application (fail soft).

To create the B-models we started from the results of the first stage of the system study carried out in the preceding phase. We were thus able to verify that the new solution was consistent with the system as it had been conceived. We modelled all the functionalities of the system (train arrival and departure, detection of opening of the train doors and detection of closure of the train doors etc.)

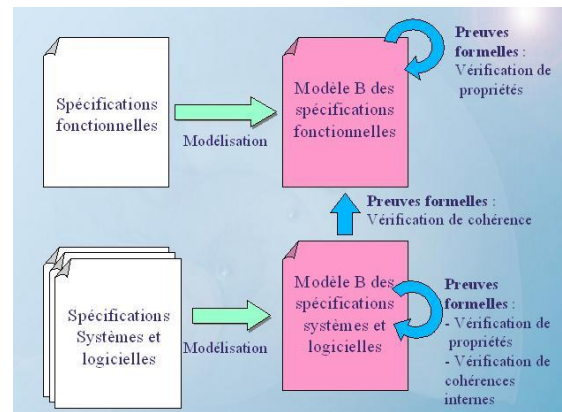


Figure 2: B-modelling

Thanks to this methodology, at the end of the specification phase, as a result of mathematical proof, we could be sure of the following:

- The chosen system architecture complies with the functional specifications of the RATP.
- There are no "grey areas" in the specifications where it is not known how the system will behave.
- All the rules defined are consistent with each other and with the physical system (Paris Metro).

Design and realisation. The B-method allows automatic production of the software code that has been subjected to proof resulting from the specification modelling.

In this system, we had to discontinue this development process based on B. In actual fact, the Siemens safety controller only supports one type of programming in its certified development environment and this is of a graphic kind.

We therefore set up a manual translation method from the B modelling to state diagrams that are then translated into LADDER (logic gate schema), the language used in the controller.

In this way, development cycle traceability is fully retained because:

- The translation of B into state diagrams is almost literal; all we did was optimise the translation somewhat to meet time constraints
- Processing of each state is described in flow diagram terms where each of the branches corresponds to one or several events in B
- Translation of these into logic gate language is literal
- In the validation phase we can get each program path in LADDER to correspond to an event of the B-model.

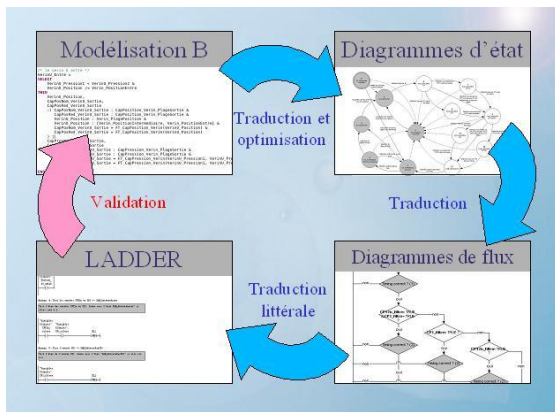


Figure 3: Design and realisation activities

Unit tests and integration and validation tests. Using the B-method in developing an application can, in certain cases, render unit testing superfluous. For this to be so, the code must have been automatically generated by means of a certified compiler.

In our case, these tests are still necessary due to the break in the B development process.

In these final stages of the process, therefore, two solutions became apparent:

- Production of a testbed based on B modelling
- Writing a testbed of traditional format based on the planning and functional specification documents.

Unfortunately, the first solution, though more interesting within our process, could not be implemented because of the non-availability of the B-model animation tool which was still under development at that time. We therefore had to use a traditional method based on:

- The requirements of the functional, system and software specifications
- The design requirements

Finally, only a few months after the project launch, we did obtain a functional application that was fully tested and validated. The development process based on the B-method that we used allowed us to obtain 100% tested software with no errors as regards the specifications, and this, moreover, on the first testbed run-through.

Track integration tests. We then tested the whole of the system made up of the controller and the various sensors on a test platform installed on one of the platforms of line 14 of the RATP. Since access to the tracks and the various sensors is already protected by glass safety door barriers, this allows us to measure the behaviour of the full system (safety, availability, reaction time etc.) over a period of several weeks.

We were therefore then able to validate the system as well as the different technologies used.

Metrics. Here are some figures that give an idea of the size of the project:

- In the system analysis phase, we wrote about 130 pages of study documents
- Our safety study resulted in about 15 documents amounting to 300 pages in total
- We then wrote more than 600 pages of development documentation amounting to about thirty separate documents

Our models involve about 3,500 lines, in other words around 1000 proofs, all with 100% proof. The interactive proofs (10%) required around two days of work.

We used the *CompoSys* tool (www.composys.fr) for modelling so as to be able to generate the documentation automatically.

We proved our B-models with “*B4free*” (free version of Atelier B for universities, www.b4free.com) and then with “*AtelierB*” (www.atelierb.societe.com). The former gave us a lot of flexibility in writing the model, whereas the second allowed us to validate the results.

Advantages of this methodology

Within a very short timeframe and with a minimum of personnel working on the project, the methodology used that was based on formal techniques allowed us within four months to obtain a safety system that was approved and checked by an independent agency. In exact terms, the team included:

- A project manager
- A development engineer
- A validation engineer
- A safety engineer

Within the space of four months (July to October), once the decisions relating to the architecture had been made:

- All the system and software specifications were written, modelled and validated
- All software design had been completed, revised and validated
- The full testbed (unit tests, integration and validation tests) was written, validated and run on the target system with 100% success on the first trial
- The full safety dossier was written and forwarded to the supervisory authority of the RATP

In addition, the system displays flexibility and robustness:

- Flexibility: It was developed in such a way that some system sensor technologies (position sensors, movement sensors etc.) may be changed provided the replacement item can fulfil the same function and that it remains consistent with the safety analyses and constraints. Thus we were able to replace a microwave frequency telemeter by an infrared laser telemeter without making important modifications to the various files.
- Robustness: We launched a testbed for several days with the aim of generating major random adverse intrusions on the different controller inputs so as to validate its resistance to a disordered environment. So far we have not yet managed to cause the system to fail

Finally, we should also point out that the decision to use the B-method was made by ClearSy when developing the application, and that there was no requirement from the RATP that it be used.

The RATP reacted very favourably to this decision, since it is already aware of the benefits of this methodology and has staff on its books capable of validating the various models.

Our views

We assess the methodology used to be very efficient and fully adapted to this kind of project that combines time constraints and safety constraints.

For the time being it is not fully finalised, as we have one missing link. Currently we are working on tools that can help us in this field:

- A compiler of B on to a machine assembler, so as to automatically link the B-model written in the specification phase with the automatic controller code
- And, in the absence of a compiler, to develop a B-model animator that would give automatic production of the testbed and validate the hand-written application on the target system.