25 YEARS OF FORMAL METHODS AT RATP

FROM MANUAL APPROACH FOR PROOF OF PROGRAMS TO INSTRUMENTED DEMONSTRATION OF RAILWAY SYSTEMS SAFETY

David Bonvoisin

Engineering department – Railway transportation systems – Head of RAMS division

RATP

SUMMARY

The RATP Company operates one of the most important multimodal transportation network in the world. As soon as the first software-based train control system was deployed on this network at the end of the 80's, RATP has experienced the use of formal methods to master the safety critical part of the software. Since then, RATP has kept on developing, improving and promoting the use of formal proof for validation or assessment purpose, with a constant target to extend its scope. The next step considered by RATP is the application of formal proof at system level for the demonstration of railway systems safety by using a composite methodology combining top-down and bottom-up approaches.

INTRODUCTION

The RATP Company operates one of the biggest and most complex urban multimodal transportation network in the world. The only railway part of this network gathers mass transit, metro and tramway lines, allowing to achieve about 2.2 billion travels a year. Since the end of the 1990's, the need for increasing transport capacity in Paris area has resulted in a vast program of line extensions. Meanwhile, a program for the renewal of the railway network has been launched in order to reach the high level performance level required for the transportation systems to meet the needed transport capacity.

These long term and still ongoing programs have already made RATP's engineering department an important actor in the railway domain and one of the world experts in automating existing lines. Indeed, the required level of performance means developing and using advanced technologies as well as designing, qualifying, deploying and maintaining complex systems and architectures. Besides, all the renewal operations have to be done without traffic interruption, making the task schedules very constrained, imbricated and hard to build and tune.

Formal methods/formal proof: what does it mean?

Formal methods are system design techniques that use rigorously specified mathematical models to build software and hardware systems. In contrast to other design approaches, formal methods use mathematical proof as a complement or alternative to system testing in order to ensure correct behaviour. As systems become more complicated, and safety becomes a more important issue, the formal approach to system design offers a higher

level of insurance. To sum up, the value of formal methods is that they provide a means to examine the entire state space of a digital design (whether hardware or software) and establish a correctness or safety property that is true for all possible inputs.

HISTORICAL OUTLINE OF URBAN RAILWAY SAFETY RELATED SYSTEMS

Urban railway system families

The operation of a high performance urban transportation system nowadays means developing and installing 3 categories of systems: interlocking systems, operation and supervision aiding systems, and command and control systems for aided and safe driving (ATO/ATP). Of course the first category of systems has existed for a long time. And if the second one exists since the 1950's, the third one, i.e. ATOs and ATPs, was born in the 70's from the wish of increasing the performance of the metro in order to respond to the need for improving its transport capacity.

From analogue to digital electronic equipment

At first designed with relay-based or electronic analogue technology, the step to numeric technology was passed at the end of the 80's (SACEM system), setting the milestone of the entrance of the embedded safety critical software in the urban railway domain. This trend was validated in 1998 by the success of the METEOR project consisting in the deployment of a UTO system on the new line 14 of the Paris metro. The use of numeric technologies (i.e. embedding software) has since been generalized: 15 computer-based interlocking systems and 5 CBTC systems have already been installed in Paris and several projects of automated driving systems involving the use of such technologies are ongoing at RATP (CBTC, GOA2 and GOA4).

EXPERIENCE AND PROMOTION OF FORMAL METHODS AT RATP

First experimentation of formal proof: the SACEM project

However, the mastery of software technics was not immediate. The SACEM project has hinted RATP the possibility of the weakness of validation processes based on the use of tests. Indeed, after the end of the validation stage, unsafe behaviours have been highlighted during on site tests. A first attempt, without any tool but driven by some software high level experts, to use formal proof has allowed to fix the safety related bugs that had not been revealed by test campaigns. This experience not only made the SACEM a new standard with regards to safety (zero unsafe behaviours detected after 26 years of operation) but also emphasized the potential superiority of the formal proof over test-based approaches.

METEOR project: the confirmation of the efficiency of formal methods

This first experience led RATP in 1993 to fund the industrialization of a software development toolkit aimed at supporting the B method called "Atelier B" and to impose to its supplier Matra Transport International the use of the B method[1] for the development of the ATP of METEOR (CBTC of Paris line 14) in 1995. Once again, this policy resulted in a success [1]: once put in revenue service in 1998, the METEOR software has never needed any modification.

[1] The inventor of the B method, J.-R. Abrial, was one of the software experts who had been involved in the SACEM project.

A posteriori formal proof

The birth of the EN50128 CENELEC standard in 2001 has brought a rigorous canvas to the railway system suppliers for building their software development process. Yet, if the EN50128 standard highly recommended the use of formal methods for the safety critical part of software (SIL 3 and 4) [2], it did not forbid the use of "classical" fully test-based processes.

At the beginning of the Paris metro renewal program, i.e. at the beginning of 2000's, only 2 suppliers of signalling systems, ALSTOM and SIEMENS (formerly Matra Transport International), were using the B method. And because of the European regulation that required competition balance for public procurement, it was not possible for RATP to formally instruct for the B method in its tender. Then the clause used in tender documents was: "… the proof for obtention of the adequate safety level shall be brought either using B method, either another method should it present an equivalent proving capacity (to be demonstrated by the tenderer)…"

The European regulation, the recommendation of the use of formal methods and the legitimacy of test-based processes given by the EN50128 standard finally resulted in the use of semi-formal[2] approaches such as SCADE or Petri nets by some of the signalling systems suppliers.

However, RATP still wished the use of formal proof wherever possible and was convinced it would be worth providing its suppliers advanced proof tools. RATP has thus developed and procured a formal proof tool-chain based on a tried-and-tested proof engine combining model checking and inductive proof techniques, bringing the ability to perform formal proof over a software developed with a semi-formal approach. This toolkit, called "Prover Certifier", has been provided to Ansaldo and Thales respectively for the validation of the Paris line 3 zone controller[3] and the computer based interlocking systems of Paris lines 1, 4, 8 and 12. In those 2 cases, the proof-based validation processes had to be designed and applied without impacting the usual development process of the supplier, resulting in so-called *a posteriori* proof approaches, which were found to be effective [3,4].

PERF approach

From 2010, RATP finally appropriated the formal proof techniques and skills. The new experiences brought by the *a posteriori* proof approaches conducted by Ansaldo and Thales had highlighted the possibility to use formal proof independently from the development process. RATP then chose to apply on its own the *a posteriori* proof approach for its internal software safety assessment of Paris line 5 CBTC carborne controller and Paris line 13 CBTC, independently from the validation processes used by its suppliers. From a safety point of view, this methodology, called PERF, share with B method the same following strong features: the exhaustiveness brought to the verification of considered properties, and the validation of requirements themselves by means of a formal modelling that reveals any ambiguity or lack of accuracy. PERF approach proved to be very efficient: each time it has been used, unsafe bugs that had not been discovered during validation phase have been revealed, making it possible to fix them before commissioning. PERF was also found to be cost-effective[4] on the long term. It has been used by RATP for internal purpose (CBTC) but also for external missions [6,7].

---

[2] i.e. without proof. In the case of semi-formal methods, the underlying mathematical models are used to offer features such as automatic checks and code generation, but not formal proof.

[3] The zone controller is the wayside equipment of the CBTC in charge of processing the train tracking and the movement authority limits to be transmitted to the carborne controller.

[4] The cost of implementing PERF is, for the first shot, equivalent to conventional assessment/validation methodologies. This initial cost is largely due to the necessary adaptation of the tools to the development methodology used by the supplier and to implementation of a suitable process. On the other hand, the cost of formal proof falls sharply when dealing with changes (non regression and impact assessments), which makes PERF more advantageous over the lifetime of the project. RATP noticed that the use of *a posteriori* formal proof instead of validation tests reduced the overall validation workload by roughly 25% while at the same time significantly improving the confidence level as regards the safety of software based systems.

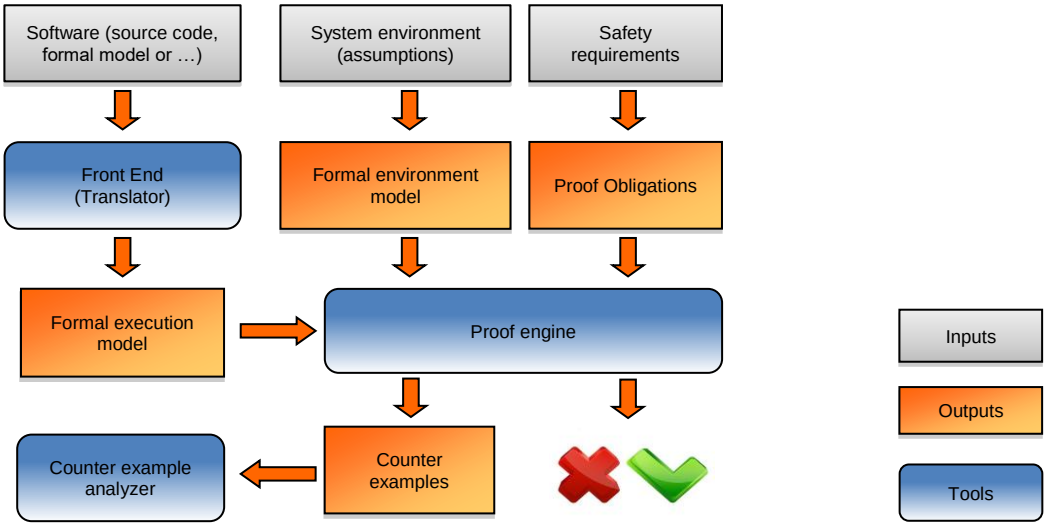

Figure 1. PERF verification workflow

Validation of CBTC configuration data: OVADO®

For SACEM and METEOR project, RATP had developed project-specific configuration data validation tools that later revealed to be very difficult to maintain and master on a long period. As PERF was being designed by RATP for the safety assessment of generic application software, a similar methodology has been considered by RATP for the validation of CBTC configuration data. Built upon a B language predicate evaluation engine, the OVADO® tool which had initially been intended for the Paris line 13 CBTC has been re-designed in 2009 to become as versatile as possible. The abstraction possibilities brought by the B language to express requirements to be evaluated by the tool allowed rubbing implementation details and specificities. It was then possible to use the same tool and methodology for different projects and situations [5]. From there, RATP has been using OVADO® for the validation of the configuration data of Paris lines 1, 3, 5, 9 CBTC systems, continually improving its methodology (efficiency, versatility, ease of skill capitalization).

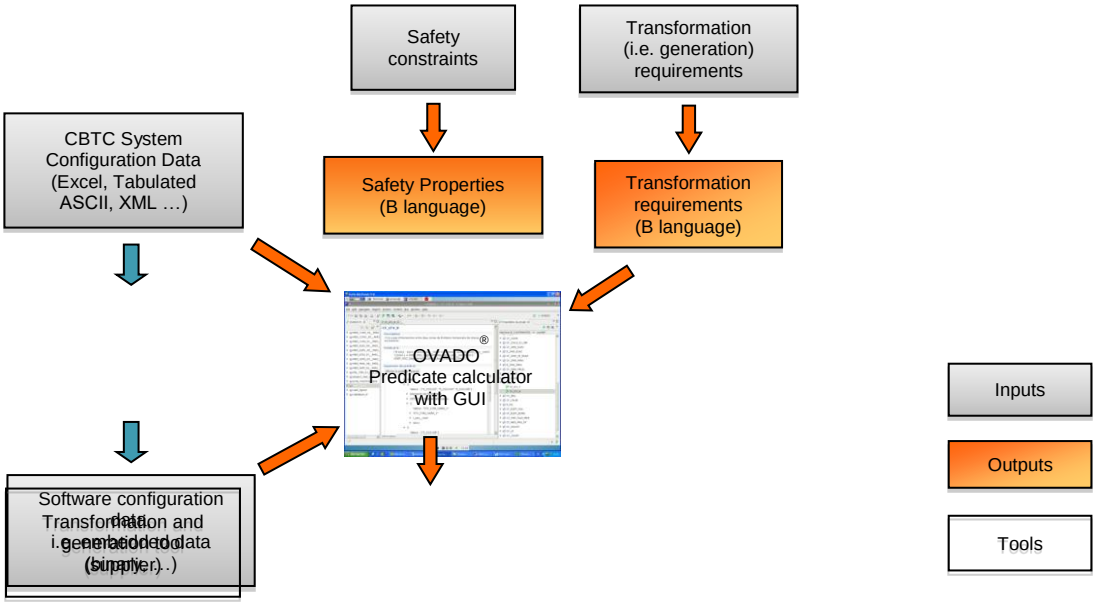

Figure 2. OVADO workflow

The end of the skill iss

Until the middle of the 2000's, finding people skilled at formal methods was rather difficult. But these methods are now widely taught at University worldwide. Furthermore, some companies are now specialized in such methods and can offer skilled resources as well as the high level expertise needed to solve a problem or to design smart and efficient processes. In France, RATP, like many railway suppliers, has built partnership with such companies: Clearsy, Systerel, Prover Technologies, Saferiver, bringing life to a constantly increasing skill ecosystem. The formal proof toolkits now available are also easier to master than they used to be. Finally, the versatility of approaches like PERF allows a strong capitalization of skills, since the same tools and techniques are used for different situations and by different users. For these reasons, and thanks to a recurrent workload in the considered domain, RATP is confident in its capacity in managing competences regarding the formal methods.

TO GO FURTHER...

Building on these achievements, RATP still aims to extend the scope of the formal proof techniques (i.e. not only for software validation or assessment).

New generation of relay-based interlocking: PHPI

At the end of the 2000's, RATP initiated a research and development project regarding the possible use of formal proof to demonstrate the safety of a relay-based interlocking design. At the same time, RATP released the prototype of a new safety relay (CRIS[5]) aimed at replacing the legacy so-called "NS1 relay". These two steps, combined with the experience of the deployment of Thales computer-based interlocking have paved the way for the next generation of interlocking systems at RATP: the PHPI. This new concept gathers several innovative features: CRIS type relays, very short installation delay, ease of evolution/upgrade, remote relay supervision, HIL

[5] The CRIS relay is no longer built with clockwork techniques but with industrial off the shelf electronic components. This makes the CRIS relay easy to produce, cheaper than NS1 and potentially multi-sources.

factory testing facilities for functional validation and last but not least, a safety validation process based on formal proof.

Therefore, although the first PHPI interlocking equipment will be put in revenue service at the end of 2016 in Paris (but with "traditional" verification and validation process), the first deployment of the full concept of PHPI will take place by 2019. The formal proof process will then be used for the demonstration of safety of this new generation of relay based interlocking systems aimed to be used for the renewal of RATP interlocking infrastructures during the next decades.

Formal proof at system level

The RATP's CBTC product, OCTYS, is said to be "interchangeable", i.e. one onboard or wayside equipment can be replaced by an equivalent[6] equipment produced by another supplier. Though it allows multi-sourcing, this genericity, as well as industrial ownership issues, makes it very difficult to guarantee the completeness of the safety demonstration. As this product will be deployed again in Paris metro, at least on line 6 and 11, RATP has decided to invest in a new approach aimed at ensuring this completeness. This approach has already been conducted by Clearsy for the installation of a CBTC in the New York metro [8]. It consists in the use of Event-B[7] method at system level in order to formalize the safety demonstration and proof its soundness with a dedicated tool such as Atelier B. This project has been launched in April 2016 and should finish by the end of 2017. This experience may lead to other uses of Event-B to master the increasing complexity of railway systems that RATP engineering department have now to design and install, with a new level of integration.

The Grail

Lastly, RATP engineers aim at reaching, at middle term, their Grail: achieving the complete and global formal demonstration of the safety of the CBTC to be deployed in Paris in the future. For this, a composite approach is under consideration, combining a top-down approach based on the use of Event-B at system level and a PERF inherited bottom-up approach based on model checking, induction, abstraction and composition methods applied at software level. The top-down part of the process would allow to formally derive safety requirements to be met by sub-systems, configuration data and operating regulation, whereas the bottom-up approach would allow to prove that the safety critical software of each sub-system does fulfil these safety requirements. Despite many technical issues still to be solved, reaching this Grail is no longer a dream: the foundations of this approach are already built.

6 Equivalent here means meeting the generic requirements of the OCTYS product and being configured to match the specific configuration of the line.

7 Event-B refers to a method using B features and proof mechanisms but applied at system level, and without code generation goal.

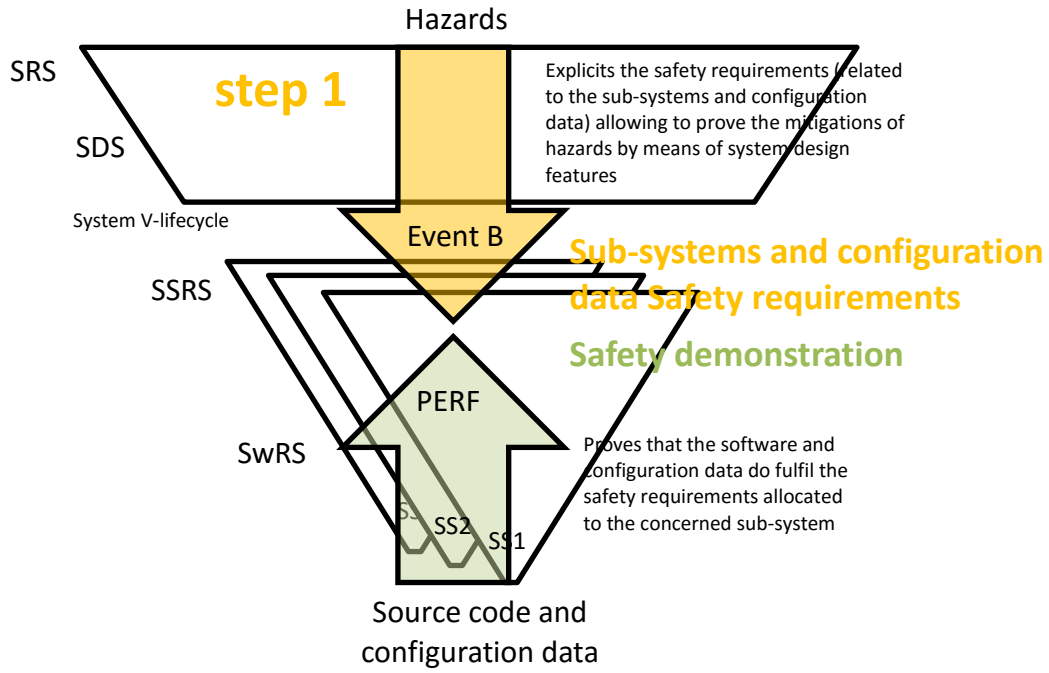

Figure 3. Hybrid approach to reach the Grail

SRS: System Requirement Specification
SDS: System Design Specification
SSRS: Sub-System Requirement Specification
SwRS: Software Requirement Specification
SS: Sub-System

CONCLUSION

Since the end of the 80's with its first use of a software-based train control system, RATP has been experimenting, using, improving and promoting formal proof techniques while drawing benefits from its efficiency. Considered by RATP as one of the pillars of the demonstration of railway systems safety, these techniques can be now considered as a part of RATP's DNA. RATP is still driving or collaborating to several research projects aimed at improving these cutting edge techniques and extending their scope. And if the safety critical software can now almost be considered as mastered, this is, by far, not the case for the system level. And since the system architectures tend to become more and more complex, formal proof at system level is considered by RATP as a focus for the next decade.

REFERENCES

1 Behm P, Benoît P, Faivre A, Meynadier JM: Météor: a successful application of B in a large project. In: LNCS 1708, FM'99 – Formal methods, pp. 369-387 (1999)

2 CENELEC EN-50128: Railway applications - Communication, signalling and processing systems - software for railway control and protection systems (2011)

3 Mota JM, Dmitrieva E, Mammar A, Caspi P, Behnia S, Breton N, Raymond P: Safety demonstration for a rail signalling application in nominal and degraded modes using formal proof. In: Formal methods applied to industrial complex systems, pp. 71-114 (2014)

4 Fioroni S: An innovative approach and an adventure in rail safety. In: Formal methods applied to industrial complex systems, pp. 27-36 (2014)

5 Abo R, Voisin L: Formal implementation of data validation for railway safety-related systems with OVADO. In: SEFM, LNCS 8368, pp. 221-236 (2014)

6 Bonvoisin D, Benaissa N: Utilisation de la méthode de preuve formelle PERF de la RATP sur le projet PEEE. In: Revue générale des chemins de fer 250 (2015)

7 Benaissa N, Bonvoisin D, Feliachi A, Ordioni J: The PERF approach for formal verification. In: LNCS 9707, Reliability safety and security of railway systems, pp. 203-214 (2016)

8 Sabatier D: Using formal proof and B method at system level for industrial projects. In: LNCS 9707, Reliability safety and security of railway systems, pp. 20-31 (2016)

NOTATION

ATO: Automatic Train Operation.

ATP: Automatic Train Protection.

CBTC: Communication Based Train Control.

CRIS: Safety industrial relay board (“Carte Relais Industriel de Sécurité”).

GOAx: Grade Of Automation x. This scale goes from 1 to 4 and corresponds to the level of automation of the train control system.

GUI: Graphical User Interface.

HIL: Hardware In the Loop (testing facilities).

METEOR: Eastern-western rapid Metro (“METro Est Ouest Rapide”). The UTO which has been put into revenue service on line 14 in 1998 in Paris.

OCTYS: Open Control of Trains, Interchangeable & Integrated System (i.e.: Interchangeable CBTC).

OVADO®: Configuration data validation tool (“Outil de Validation de DOnnées”).

PERF: Proof Executed over a Retro-engineered Formal model. RATP’s own formal proof approach used for safety assessment purposes.

SACEM: drive, operate and maintain aiding system (“Système d’Aide à la Conduite, l’Exploitation et la Maintenance”), equipping the line A of the Paris transportation network.

SIL: Safety Integrity Level.

UTO: Unattended Train Operation system. Fully Automated train control system, allowing operation without any onboard staff.