Le développement de logiciels (et autres choses) avec B

Thierry Lecomte

CLEARSY, Aix en Provence, France,
thierry.lecomte@clearsy.com

Abstract. Les méthodes formelles sont aujourd'hui un pilier discret mais essentiel du développement logiciel dans les systèmes critiques pour la sécurité. Cet article présente un retour d'expérience industriel par CLEARSY sur l'utilisation de la méthode B dans les secteurs ferroviaire, des cartes à puce et de la mobilité autonome. Il décrit les processus développés autour de la spécification, de la preuve de systèmes, de la validation de données, et de la génération de code certifiable. Il discute également des défis rencontrés, des standards existants, ainsi que des opportunités futures dans des domaines émergents comme l'intelligence artificielle certifiée.

Keywords:

1 Introduction

Depuis plusieurs décennies, les méthodes formelles sont utilisées pour garantir l'exactitude des logiciels embarqués dans les systèmes critiques. L'approche repose sur une modélisation mathématique rigoureuse, accompagnée de preuves formelles permettant de démontrer que le système respecte ses exigences de sécurité. Malgré leur efficacité démontrée, ces méthodes peinent à se généraliser dans l'industrie en dehors de domaines spécifiques comme le ferroviaire ou les cartes à puce. Le présent article décrit l'expérience acquise chez CLEARSY, en s'appuyant sur des applications concrètes et des résultats industriels significatifs.

2 Développement logiciel avec la méthode B

Le développement logiciel avec la méthode B [2] permet d'atteindre un niveau de sûreté extrêmement élevé. L'approche consiste à spécifier mathématiquement le comportement attendu du logiciel et à prouver formellement que l'implémentation est correcte vis-à-vis de cette spécification. Cette démarche permet, dans certains cas, d'éviter les tests unitaires classiques et de réduire les tests d'intégration.

L'environnement Atelier B (www.atelierb.eu/en/) est utilisé comme outil principal. Il permet de générer du code C à partir de modèles formels et de vérifier la cohérence entre la spécification et l'implémentation. Cette approche est couramment appliquée pour le développement d'équipements critiques, comme les calculateurs de sécurité ferroviaires (ex. : CLEARSY Safety Platform).

3 Validation formelle des systèmes et des données

Le B événementiel est utilisé de manière extensive pour valider le raisonnement de sûreté de grands systèmes industriels. Par exemple, la preuve de correcte-interopérabilité de la nouvelle signalisation ERTMS Niveau 3 Hybride sur la ligne Marseille – Vintimille a pour objectif de démontrer de manière irréfutable que le système Contrôle – Commande – Signalisation satisfait ses exigences de sécurité, en s'appuyant sur des garanties attendues des différents sous-systèmes.

Outre le logiciel, les systèmes critiques [7] reposent sur de grandes quantités de données paramétriques. CLEARSY a mis en place des processus de validation formelle de ces données, utilisant l'outil ProB [4] pour la vérification automatique de milliers de règles métier sur des jeux de données de plus de 100 000 éléments.

L'importance de cette validation a été soulignée par des accidents réels : en 2019, un TGV a franchi un aiguillage à 170 km/h au lieu de 100 km/h à La Milesse (France), en raison d'une erreur de données non détectée lors d'une validation manuelle. Les rapports officiels recommandent désormais l'usage de méthodes de validation automatisées fondées sur des approches formelles.

4 Intégration dans les systèmes de sécurité

La CLEARSY Safety Platform [6] illustre l'intégration complète de ces méthodes dans un calculateur de sécurité. Cette plateforme combine redondance matérielle (2oo2) et logicielle (4oo4) avec un développement fondé sur B, permettant une maîtrise des pannes systématiques et aléatoires. Ce produit, développé depuis plus de cinq ans, est aujourd'hui déployé dans divers projets ferroviaires.

L'expérience montre qu'un cycle de développement bien huilé, incluant des audits de modèles et une acceptation contractuelle des livrables formels, peut éviter des régressions et instaurer une confiance durable avec les exploitants.

5 Autres domaines d'application

5.1 Cartes à puce et sécurité

Le domaine des cartes à puce est l'un des rares où les méthodes formelles sont imposées par les standards, notamment via les critères communs (Common Criteria). Les niveaux EAL6+ et EAL7 exigent un lien formel entre la spécification de sécurité et l'implémentation, y compris pour des produits certifiés tels que des microkernels ou des machines virtuelles Java. Des travaux de recherche récents [1] explorent la génération automatique de circuits (VHDL) à partir de modèles formels.

5.2 Mobilité autonome

Dans le contexte de la mobilité autonome, la situation est plus contrastée. Les projets concernent des navettes routières ou ferroviaires, des drones de sauvetage ou sous-marins. Si la perception basée sur l'IA ne se prête pas encore

aux méthodes formelles, ces dernières sont adaptées aux composants binaires (ON/OFF, ouvert/fermé). L'absence de standard clair, les incertitudes sur la responsabilité en cas d'accident, et le faible retour sur investissement freinent toutefois les déploiements industriels.

5.3 Retour d'expérience industriel

Le retour d'expérience industriel indique que :

- Les appels d'offres mentionnent de plus en plus les méthodes formelles, souvent à la suite de défaillances passées ;
- La pression économique pousse à l'externalisation mais pas nécessairement à l'abandon des méthodes formelles, surtout lorsqu'elles sont déjà intégrées au cycle de développement ;
- Les standards (notamment dans le ferroviaire) ne se dégradent pas, au contraire ils stabilisent l'usage des méthodes formelles ;
- L'injection de méthodes formelles dans des cycles existants est recherchée à condition d'un impact minimal.

6 Conclusion

Les méthodes formelles offrent une réponse rigoureuse et éprouvée aux exigences de sûreté des systèmes critiques. Leurs applications dans le ferroviaire et la sécurité des cartes à puce ont démontré leur efficacité. Le défi actuel est leur extension vers de nouveaux domaines, notamment la mobilité autonome, tout en maintenant un bon compromis entre exigence, coût et acceptabilité. Les expériences accumulées avec B et Event-B montrent qu'il est possible de concilier rigueur mathématique, contraintes industrielles et innovation technologique.

L'enseignement des méthodes formelles en général, et de B [5][3] en particulier, doit être encouragé.

References

1. Benveniste, M.: A correct by construction realistic digital circuit. In: Proc. of the Workshop on Recent Innovations and Applications in B,, Eindhoven, Netherlands, November 3, 2009. (2009)
2. Butler, M., Körner, P., Krings, S., Lecomte, T., Leuschel, M., Mejia, L.F., Voisin, L.: The first twenty-five years of industrial use of the b-method. In: ter Beek, M.H., Ničković, D. (eds.) Formal Methods for Industrial Critical Systems. pp. 189–209. Springer International Publishing, Cham (2020)
3. Carvalho, G.: Teaching formal methods for 10 years: Reflections on theories, tools, materials, and communities. In: Sekerinski, E., Ribeiro, L. (eds.) Formal Methods Teaching. pp. 58–74. Springer Nature Switzerland, Cham (2024)
4. Hansen, D., Schneider, D., Leuschel, M.: Using B and prob for data validation projects. In: Butler, M.J., Schewe, K., Mashkoor, A., Biró, M. (eds.) Abstract State Machines, Alloy, B, TLA, VDM, and Z - 5th Int'l Conf., ABZ 2016, Linz, Austria, May 23-27, 2016, Proc. LNCS, vol. 9675, pp. 167–182. Springer (2016)

5. Lecomte, T.: Teaching and training in formalisation with b. In: Dubois, C., San Pietro, P. (eds.) Formal Methods Teaching. pp. 82–95. Springer Nature Switzerland, Cham (2023)
6. Lecomte, T., Déharbe, D., Sabatier, D., Prun, E., Péronne, P., Chailloux, E., Varoumas, S., Susungi, A., Conchon, S.: Low Cost High Integrity Platform. In: ERTS 2020 - 10th European Congress on Embedded Real Time Systems. Toulouse, France (Jan 2020), https://hal.archives-ouvertes.fr/hal-02446132
7. Sabatier, D.: Using formal proof and B method at system level for industrial projects. In: Lecomte, T., Pinger, R., Romanovsky, A. (eds.) Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification - 1st Int'l Conf., RSSRail 2016, Paris, France, June 28-30, 2016, Proc. LNCS, vol. 9707, pp. 20–31. Springer (2016)