Validation des logiciels de sécurité ferroviaire

De l'utilisation de la méthode B

Le souci de sécurité est devenu au fil du temps une véritable seconde nature dans le monde du ferroviaire. Et puisque l'informatique touche désormais tous les domaines, jusqu'à s'insinuer dans les foyers, il était logique que la sûreté de fonctionnement des transports requière, elle aussi, ce nouveau sésame.

La sécurité informatique est devenue aujourd'hui un enjeu fondamental où la moindre erreur peut avoir des conséquences catastrophiques.

Mais si programmer un logiciel de sécurité n'est pas simple, que dire alors de la validation de ce type de logiciel… Car pour vaincre la réticence à l'utilisation d'équipements programmables, de nombreux travaux ont dû être menés dans le domaine de la vérification et de la validation. Et en particulier sur l'applicabilité des techniques formelles au développement du logiciel critique - lequel sera, à la fin de ce développement formel, considéré comme logiciel de sécurité.

La méthode B est une des techniques formelles les plus utilisées à la SNCF. Elle semble en effet très adaptée à la construction du logiciel critique du fait de sa bonne couverture du cycle de développement (de la phase de spécification à la production automatique du code) et de ses possibilités de vérification formelle.

Une stratégie d'intégration de B originale

Mais comme quoi rien n'est simple dans cette discipline, un gros travail a dû être réalisé pour fournir une stratégie d'intégration de la méthode B dans le développement du logiciel critique... En effet, la pratique de B ne respecte pas l'ordre classique des étapes de la construction d'un logiciel. On remarque, par exemple, que l'élaboration de la spécification formelle des besoins et la conception d'une architecture logicielle se font simultanément et sans distinction.

Il arrive ainsi que l'organisation du modèle soit remise en cause alors que le développement est déjà très avancé. Cette étude, menée dans le cadre d'un doctorat avec l'École nationale supérieure des télécommunications, a donc débouché sur le besoin d'adapter le cycle de vie de la méthode B et d'y associer un support méthodique approprié au ferroviaire.

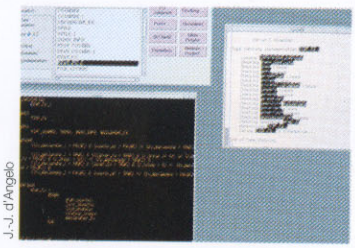
Il est ainsi paru nécessaire, pour répondre aux exigences de sécurité, de distinguer lors de la conception du logiciel critique les besoins de fonctionnement des besoins de sécurité. Ainsi, la thèse préconise que les contraintes de sécurité soient formalisées en amont - ce que n'impose pas la seule utilisation de B - pour constituer les éléments structurants de la modélisation formelle.

Une démarche validée sur un cas réel

La faisabilité de ces propositions a ensuite été démontrée sur un cas concret : le contrôle des limitations de vitesse. Il en ressort que la démarche proposée fournit la "traçabilité" précise, correspondant aux exigences de développement du logiciel critique, en tirant profit de la technique de vérification formelle inhérente à la méthode B.

Reste à appliquer cette démarche sur d'autres cas réels. Car même s'il s'agit là d'une bonne méthode d'utilisation d'une méthode, encore faut-il savoir bien l'utiliser... ●

Souad Traverson/Eric Maunoir



J.-J. d'Angelo