Approche formelle pour la réalisation d'un système sécuritaire de contrôle commande de façades de quais

4ème Conférence Annuelle d'Ingénierie Système
« Efficacité des entreprises et satisfaction des clients »
Centre de Congrès Pierre Baudis, TOULOUSE, 2-4 mai 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

Résumé

Clearsy est une société d'ingénierie qui réalise ses prestations avec des techniques et outils de modélisations formelles centrés autour de la technologie B.

Cette présentation décrit la méthodologie qui a été mise en œuvre lors de la réalisation d'un système sécuritaire de contrôle et de commande de façades de quais pour la RATP.

Nous présentons ici les différentes activités menées ainsi que les avantages tirés lors des différentes étapes du processus de développement et d'intégration.

Présentation du projet

Depuis quelques années, la RATP utilise un système de portes palières permettant d'empêcher l'accès aux voies du métro depuis les quais. Ce système a été mis en place sur le métro automatique METEOR (ligne 14) lors de sa mise en service. Il permet d'améliorer considérablement la disponibilité et la fluidité de la ligne.

Afin d'améliorer la qualité de son service et la sécurité dans son réseau, la RATP souhaite disposer de ce type de protection sur d'autres lignes, qu'elles soient entièrement automatisées ou non. Pour des raisons pratiques et de coût, elle ne souhaite toutefois pas avoir à modifier le matériel roulant.

Avant de déployer un nouveau système de portes palières sur une ligne entière, la RATP a lancé un projet prototype concernant une installation sur trois quais de la ligne 13 pendant 8 mois. Ce projet se décompose en deux :

- La partie mécanique des façades de quais
- La partie de contrôle et de commande du système des façades baptisée COPPILOT

Clearsy est en charge de la seconde partie qui consiste à :

- Concevoir un système sécuritaire de niveau SIL3,
- Détecter l'arrivée, la présence, et le départ d'un train sans contact avec celui-ci,
- Détecter l'ouverture et la fermeture des portes du train,
- Produire les ordres d'ouverture et de fermeture sécuritaires des portes palières.

Bien entendu, étant donné que la solution est destinée aux voies de métro, le système doit être conforme aux différentes normes très strictes appliquées aux systèmes ferroviaires mis en œuvre par la RATP.

Notre stratégie

La difficulté dans ce projet concerne des délais de réalisations très courts : 10 mois entre le lancement du projet et la mise en service du système.

Notre stratégie devait donc s'orienter autour d'un système permettant de produire une architecture de sécurité pouvant être qualifiée rapidement et dont les résultats dépendraient peu des différentes technologies et modèles de capteurs utilisés.

Ainsi, nous avons choisi une architecture constituée de composants industriels du commerce : un automate de sécurité Siemens dont le fonctionnement est certifié SIL3, des capteurs infra-rouge (Leuze, DataSensor, …) et radars.

La sécurité du système repose sur la technologie sécuritaire de l'automate ainsi que sur la redondance des mesures données par les différents capteurs et non pas sur la sécurité en tant que telle des capteurs.

Cette solution permet ainsi :

- De diminuer les coûts du matériel, car les capteurs du commerce sont beaucoup moins chers que les capteurs certifiés de sécurité,
- d'avoir des délais d'approvisionnement beaucoup plus courts, car ils sont beaucoup plus répandus,
- d'être beaucoup moins dépendant d'un fournisseur
- et d'assurer une diversité des sources d'approvisionnement.

Notre méthodologie

Afin d'atteindre le niveau de sécurité requis dans les délais imposés, nous avons mis en œuvre une méthode de développement permettant d'atteindre une très bonne fiabilité et une très bonne traçabilité entre les différentes étapes pour permettre de gagner du temps en validation.

Clearsy utilise la méthode formelle B, très adaptée au développement de logiciel SIL3 ou SIL4. Par exemple, nous l'utilisons pour écrire le logiciel du pilote automatique du Val de Roissy, programme devant être hautement sécuritaire (SIL4).

Dans ce projet, cette méthodologie a été utilisée pour la première fois sur tout le cycle système : lors des phases de spécifications du système et de la sécurité puis sans rupture à tous les niveaux du processus de développement de l'application.

Grâce au langage B, qui se base sur la théorie mathématique des ensembles, il est possible de décrire un système sous forme d'expressions logiques, puis de vérifier sa cohérence. Cette vérification se fait sous la forme de preuves mathématiques. Ce langage a été mis en œuvre sur différents systèmes demandant une très grande sécurité (SIL4) principalement dans le milieu ferroviaire sur des projets tels que le pilote automatique du métro METEOR (RATP, ligne 14).

Le langage B permet notamment de :

- Vérifier qu'un système respecte bien certaines propriétés (fonctionnelles, de sécurité, …),
- Vérifier qu'un système est bien cohérent intrinsèquement, c'est-à-dire qu'il n'y a pas de contradiction,
- Vérifier qu'un système tel qu'il est défini ne possède pas de « zones d'ombre » dans lesquelles il pourrait y avoir des comportements mal ou non définis,
- Obtenir une traçabilité très forte (intégrée au langage lui-même et par preuve mathématique) entre les phases de spécification, de conception puis d'implémentation.

Durant le processus de développement du projet COPPILOT, nous avons donc fait le choix, en accord avec la RATP, d'intégrer cette méthodologie formelle lors des principales phases afin d'assurer la cohérence de nos travaux avant d'avancer dans les étapes suivantes.

Le processus de développement

La méthode B a été utilisée durant tout le cycle de développement comme représenté sur le schéma suivant.

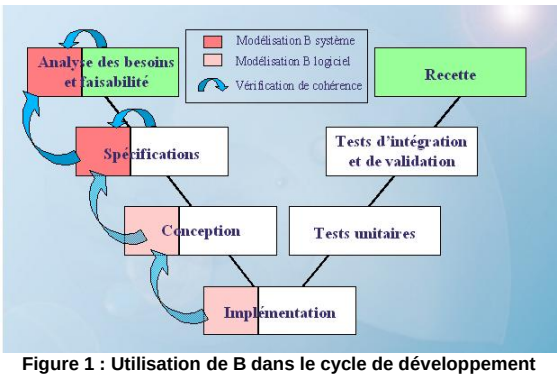

Figure 1 : Utilisation de B dans le cycle de développement

Analyse des besoins et faisabilité. Dans un premier temps, la RATP nous a confié l'analyse fonctionnelle et formelle du système pour garantir la complétude et l'univocité du cahier des charges.

La solution qui avait été imaginée à ce stade reposait sur deux télémètres lasers fonctionnant en parallèle sur les portes de parts et d'autres du quai. Grâce à une reconnaissance d'image réalisée par deux systèmes totalement indépendants, il était possible de reconnaître l'arrivée, le départ et l'arrêt d'un train en gare ainsi que l'ouverture et la fermeture des portes du train.

La première étape consistait à faire une vérification sur l'ensemble du système, c'est-à-dire sur le système de contrôle/commande (COPPILOT) et sur les façades de quai :

- que les contraintes fonctionnelles étaient bien respectées,
- que les propriétés de sécurité attendues par la RATP étaient vérifiées, c'est-à-dire qu'il n'est pas

possible de créer de connexions interdites entre la voie et le quai ou entre le train et la voie,

et à étudier quels sont les événements perturbateurs pouvant conduire à un fonctionnement dangereux du système.

Dans un second temps, nous avons étudié la solution retenue à base de télémètres lasers afin de vérifier qu'elle répondait bien aux contraintes du projet.

La méthodologie B utilisée dans ce contexte permet facilement de répondre à ces problématiques. De plus, en l'utilisant à ce niveau dans le processus de développement, nous nous assurions que le système était complet et univoque avant de poursuivre le processus et qu'ainsi, par la suite, il ne devrait pas y avoir de modification à apporter dans les spécifications fonctionnelles.

Spécifications systèmes et logicielles. La RATP a ensuite retenu Clearsy pour assurer la maîtrise d'œuvre de la partie contrôle/commande (COPPILOT). La méthode B a été utilisée lors de l'étape de spécification afin de valider la cohérence du choix de l'architecture du système vis-à-vis des spécifications fonctionnelles fournies par la RATP.

La solution initiale imaginée en phase d'étude a été remplacée par une architecture basée sur un automate sécuritaire et un ensemble de capteurs utilisant des technologies différentes (hyperfréquence, infrarouge, lasers, …) ayant chacun une fonction bien particulière : détecter la présence, les déplacements du train et les mouvements de portes, …

Dès les spécifications systèmes et logicielles de cette solution écrites, nous avons poursuivi par deux actions complémentaires :

- une modélisation B de ces spécifications dans le cas de fonctionnement nominal des capteurs (en absence de toute perturbation) réalisée par l'équipe de développement,
- une étude de sécurité, menée par l'équipe indépendante de sécurité, permettant de déterminer de manière précise l'influence des différentes perturbations sur le fonctionnement de l'application (fonctionnement dégradé).

Pour réaliser les modèles B, nous sommes repartis des résultats de la première étape d'étude système réalisée dans la phase précédente. Ainsi, nous avons pu vérifier que la nouvelle solution était cohérente avec le système tel qu'il avait été imaginé. Nous avons modélisé toutes les fonctionnalités du système (arrivée et départ du train, détection de l'ouverture des portes du train, détection de la fermeture des portes du train, …)

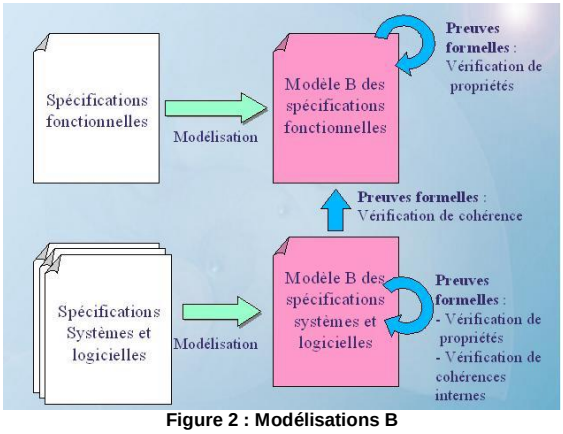

Figure 2 : Modélisations B

Grâce à cette méthodologie, à la fin de la phase de spécification, nous avions les certitudes suivantes grâce à la preuve mathématique :

- L'architecture système choisie est conforme avec les spécifications fonctionnelles de la RATP.
- Il n'y a pas dans les spécifications de « zones d'ombre » dans lesquelles on ne sait pas comment doit se comporter le système.
- Toutes les règles définies sont cohérentes entre elles et avec le système physique (métro).

Conception et implémentation. La méthode B permet de produire automatiquement du code logiciel prouvé issu de la modélisation de spécifications.

Dans ce système, nous n'avons dû rompre ce processus de développement basé sur B. En effet, l'automate de sécurité Siemens retenu ne supporte qu'un seul type de programmation dans son environnement de développement certifié et celui-ci est graphique.

Nous avons donc mis en place une méthode manuelle de traduction de la modélisation B vers des diagrammes d'état qui sont ensuite traduits en LADDER (schéma à contact), langage utilisé dans l'automate.

De cette manière, la traçabilité du cycle de développement reste complète car :

- La traduction du B en diagrammes d'état est quasiment littérale, nous avons simplement optimisé un peu la traduction afin qu'elle respecte les contraintes temporaires,
- Le traitement de chaque état est décrit sous forme de diagramme de flux où chacune des branches correspond à un ou plusieurs événements B,

- La traduction de ces derniers vers le langage à contacts est littérale,
- En phase de validation, nous pouvons faire correspondre chaque chemin du programme en LADDER à un événement du modèle B.

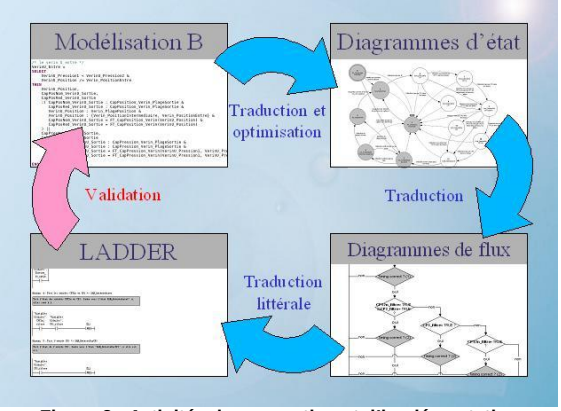

Figure 3 : Activités de conception et d'implémentation

Tests unitaires, d'intégration et de validation. L'utilisation de la méthode B lors du développement d'une application peut, dans certain cas, rendre inutile les tests unitaires. Il faut pour cela avoir généré le code automatiquement grâce à un traducteur certifié.
Dans notre cas, ces tests restent nécessaires à cause de la rupture du processus de développement en B

Donc, dans ces dernières étapes du processus, deux solutions se sont présentées :

- Produire un banc de test à partir de la modélisation B,
- Ecrire un banc de tests de manière classique à partir des documents de conception, de spécification fonctionnelle.

La première solution, bien que plus intéressante dans notre processus, n'a malheureusement pas pu être mise en place, à cause de l'indisponibilité de l'outil d'animation de modèle B, encore en développement à ce moment-là. Nous avons donc dû utiliser une méthode traditionnelle basée sur :

- les exigences des spécifications fonctionnelles, systèmes et logicielles,
- les exigences de la conception.

Finalement, seulement quelques mois après le lancement du projet, nous avons obtenu une application fonctionnelle entièrement testée et validée. Le processus de développement basé sur le B que nous avons utilisé nous a permis d'obtenir un logiciel testé à 100% sans erreurs vis-à-vis des spécifications et cela lors du premier passage du banc de test.

Tests d'intégration sur les voies. Nous avons ensuite testé l'ensemble du système, composé de l'automate et des différents capteurs sur une plate forme de test installée sur un des quais de la ligne 14 de la RATP. L'accès aux voies et aux différents capteurs étant déjà protégé par des portes palières, cette disposition nous permet de mesurer le comportement de l'ensemble du système (sécurité, disponibilité, temps de réponse, …) sur une durée de plusieurs semaines.

Nous avons pu alors valider le système ainsi que les différentes technologies utilisées.
Métriques. Voici quelques chiffres permettant d'estimer l'importance du projet :

- En phase d'analyse système, nous avons écrit environ 130 pages de documents d'étude.
- De notre étude de sécurité résultent environ 15 documents comptant 300 pages au total.
- Nous avons ensuite écrit plus de 600 pages de documentation de développement représentant une trentaine de documents.

Nos modèles représentent environ 3500 lignes soit environ 1000 preuves prouvées à 100 %. Les preuves interactives (10 %) ont demandé environ deux jours de travail.
Nous avons utilisé l'outil *CompoSys* (www.composys.fr) lors de la modélisation système afin de pouvoir générer la documentation automatiquement.
Nous avons prouvé nos modèles B avec « *B4free* (version gratuite de l'atelier B pour les académiques, www.b4free.com) puis avec l'*Atelier B* (www.atelierb.societe.com). Le premier nous a apporté beaucoup de souplesse lors de l'écriture du modèle alors que le second nous a permis de valider les résultats.

Avantages de la méthodologie

La méthodologie employée et basée sur des techniques formelles nous a permis dans un temps très court et avec un minimum de personnes travaillant sur le projet d'obtenir en quatre mois un système sécuritaire, justifié et vérifié par un organisme indépendant. Pour être précis, l'équipe comprenait :

- Un chef de projet,
- Un ingénieur pour le développement,
- Un ingénieur pour la validation,
- Et un ingénieur pour la sécurité.

En l'espace de quatre mois (juillet à octobre), après que les choix architecturaux aient été faits :

- toutes les spécifications systèmes et logicielles ont été écrites, modélisées et validées,

- toute la conception logicielle a été faite, relue et validée,
- l'ensemble du banc de test (tests unitaires, tests d'intégration et de validation) a été écrit, validé et passé sur le système cible avec 100% de réussite dès le premier essai,
- l'ensemble du dossier de sécurité a été écrit et envoyé aux autorités de tutelle de la RATP.

De plus, le système présente souplesse et robustesse :

- Souplesse : Il a été développé de manière à ce qu'il soit possible de changer certaines technologies de capteurs du système (capteurs de position, de déplacement, …) dans la mesure où l'élément de substitution puisse remplir la même fonction et qu'il reste cohérent avec les analyses et les contraintes de sécurité. Ainsi, nous avons pu remplacer un télémètre hyperfréquence par un télémètre laser infrarouge sans modifier de manière conséquente les différents dossiers.

- Robustesse : Nous avons lancé un banc de test pendant plusieurs jours dont le but est de présenter de fortes perturbations aléatoires générées sur les différentes entrées de l'automate afin de valider sa résistance à un environnement perturbé. Nous n'avons pas encore réussi à ce jour à mettre le fonctionnement du système en défaut.

Enfin, il faut aussi préciser que le choix de l'utilisation de la méthode B a été fait par ClearSy lors du développement de l'application et que son utilisation n'était pas exigée par la RATP.
Ce choix a été vu de manière très positive par la RATP qui connaît déjà les apports de cette méthodologie et qui compte déjà parmis ses employés des personnes capables de valider les différents modèles.

Nos perspectives

Nous estimons que la méthodologie utilisée est très efficace et totalement adaptée à ce type de projet alliant contraintes de temps et contraintes de sécurité.

Elle n'est pour l'instant pas totalement finalisée car il nous reste un chaînon manquant. Nous travaillons d'ailleurs actuellement sur des outils pouvant nous aider dans ce domaine :

- un traducteur de B vers un assembleur pour automate, afin de relier de manière automatique le modèle B écrit en phase de spécification vers le code de l'automate
- et en l'absence de traducteur, développer un animateur de modèle B qui permettrait de produire de manière automatique le banc de tests et de valider sur le système cible l'application écrite manuellement.