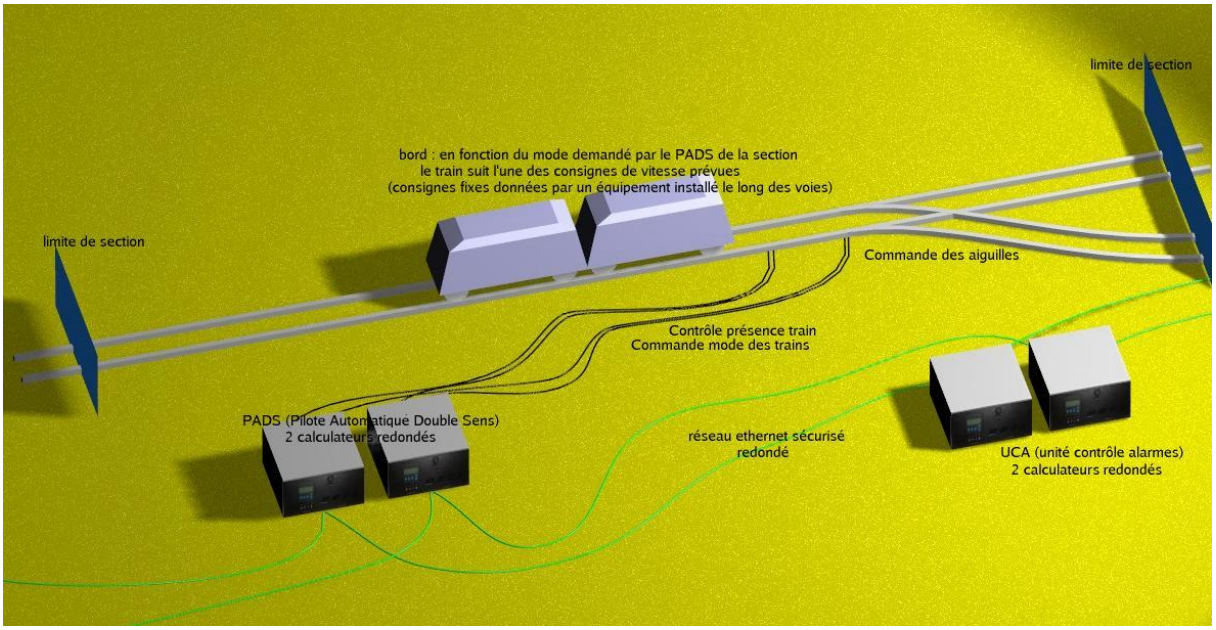
# Développement du logiciel de pilotage automatique SIL4 du VAL de ROISSY

## Introduction

Siemens Transportation Systems (STS) sous-traite à ClearSy la réalisation avec B du logiciel de pilotage automatique du VAL de ROISSY. Ce projet est actuellement en cours. Les tailles principales sont les suivantes :

| | |
|---|---|
| Durée prévue du projet | environ 15 mois |
| Lignes de B écrites (hors B généré par EDITHB/BERTILLE) | environ 40 000 lignes |
| Taille du programme obtenu | 156 000 lignes de code ADA hors commentaire |
| Nombre d'obligations de preuve B (y compris sur les parties auto-générées) | environ 44 000 |
| Nombre d'obligations de preuves à démontrer interactivement | environ 1 300 |
| Nombre de règles ajoutées | environ 100 (80% démontrées avec les outils de preuve de règle) |

Les éléments logiciels à réaliser avec B sont la logique d'itinéraire, la logique de cantons et la logique de modes de marche des trains. Ces éléments, avec le système de communication constituent le logiciel PADS (Pilote Automatique Double Sens). Chaque section du VAL de ROISSY est contrôlée par une instance de ce logiciel générique, configuré en fonction de la géométrie de la voie et des équipements installés. Le PADS commande et contrôle le mouvement des aiguilles et le mode de marche des trains (qui détermine la vitesse demandée à chaque rame en fonction de sa position). ClearSy réalise également les éléments logiciels de l'Unité de Contrôle des Alarmes (UCA).




Les spécifications logicielles détaillées du VAL de ROISSY sont issues de celles du VAL de l'aéroport de Chicago (également réalisé par STS), avec un certain nombre d'évolutions concernant en particulier la constitution des rames et les zones de garage. La formalisation en B de ces spécifications fait partie des travaux demandés à ClearSy. Les spécifications issues du projet Chicago sont très détaillées et très stables ; les spécifications des éléments nouveaux ont déjà évolué ou été complétées au cours du projet.

Les éléments concernés sont réalisés en B logiciel. La spécification formelle B décrit les traitements à effectuer à l'aide de variables abstraites (ensembles, relations, fonctions...). Les raffinements de conception sont obtenus avec l'outil de raffinement automatique EDITHB/BERTILLE paramétré avec un certain nombre de règles de raffinement, jusqu'au niveau B0 traduisible en code ADA. On ajoute ensuite les éléments externes (modules de communication) pour obtenir l'ensemble des sources. La traduction de B0 vers ADA et la compilation sont effectuées avec les mêmes chaînes d'outils redondés qui ont été employées sur METEOR (ligne 14 du métro Parisien), pour une exécution sur Processeur Sécuritaire Codé (PSC).

ClearSy a également procédé à la mise en place d'un niveau B *au dessus* des spécifications logicielles formelles décrivant les traitements : les *propriétés globales de cycle* ont été formalisées dans un niveau B dont ces spécifications deviennent un raffinement. Ceci permet la preuve mathématique de la correction des traitements choisis par rapport à ces propriétés, en plus de l'assurance donnée par l'expérience du VAL de Chicago. Cette preuve assure également que l'assemblage de ces traitements préserve ces propriétés, ce qui est primordial. Les propriétés choisies (environ une quinzaine) ont été sélectionnées par STS.

Les outils B employés sont l'Atelier B version 3.6.4 et EDITHB/BERTILLE. La preuve interactive a été faite avec l'interface graphique de l'Atelier B ou avec l'interface EMACSPRI (suivant les préférences des utilisateurs). De nombreux "scripts" ont permis d'automatiser certaines tâches. Concernant le langage B, notons que la nouvelle clause "opérations locales" a été employée intensivement, permettant une réduction de la complexité du découpage en composants B. Notons également que de nombreuses règles de raffinement automatique (configuration de BERTILLE) ont été ajoutées.

La date de fin de ce projet n'étant pas encore échue, nous ne pouvons que formuler les conclusions actuelles. Le projet se déroule suivant les plannings prévus. La phase de conception en particulier est grandement facilitée par les outils automatiques de raffinement (BERTILLE) ; la preuve ne pose pas

de difficultés spéciales. Un nombre important d'échanges entre ClearSy et STS ont été nécessaires, en particulier pour la partie des spécifications qui concerne les éléments nouveaux par rapport à Chicago ; il est manifeste que la formalisation B de ces spécifications suscite un flux de questions qui participe grandement à leur stabilisation et à la découverte des éventuels problèmes qu'elles pourraient contenir.

Pour les entrées / sorties, la méthode employée consiste à encapsuler les API fournies par l'environnement et vues via des machines de base B par des niveaux B plus abstraits dont les variables représentent plus sémantiquement les informations consolidées échangées avec l'extérieur et sur lesquelles se basent la définition B des traitements à faire. L'effort de développement B concernant ces entrées / sorties abstraites et leur raffinement jusqu'aux machines de base n'est pas à négliger. Il s'avère que celui-ci représente environ 20% de l'effort global. En fait, on prouve ainsi avec B l'ensemble des traitements de mise en forme et consolidation qui sont effectués sur ces entrées sorties.

Résumé des conclusions :

- Avec les outils automatiques de raffinement, la production d'un logiciel prouvé à partir de spécifications détaillées est assez facile ;
- La formalisation de spécifications logicielles détaillées aide leur élaboration ;
- A partir des spécifications logicielles détaillées formalisées en B, nous avons pu ajouter facilement un niveau de spécification qui assure, par preuve, des propriétés globales établies par l'assemblage des modules.