Introduction

Les systèmes à base d'électronique programmable sont utilisés de plus en plus et rendent encore plus difficile la maîtrise de la sécurité (tant du point de vue de la *safety* que du point de vue de la *security*). En effet, ce type de système combine les qualités et les défauts de l'électronique et des logiciels. L'électronique est caractérisée par des défauts qui sont dits aléatoires, ce type de défaut peut apparaître à tout moment, mais il est probabilisable. Le logiciel est caractérisé par des défauts systématiques. Le logiciel n'est pas soumis au vieillissement, mais il est soumis à la notion de bug (défaut logiciel). On peut dire que tous les logiciels contiennent des défauts, seuls les logiciels ayant suivi des processus de développement particuliers peuvent tendre vers le zéro-défaut.

L'objectif de ce livre est de décrire les principes généraux pour réaliser un système à base d'électronique programmable qui soit sûr de fonctionnement. Nous rappellerons les concepts de base de la sûreté de fonctionnement et les définitions de base (chapitre 1) ainsi que leurs mises en place (chapitre 4). Ce livre peut s'appliquer à différents référentiels normatifs (voir le chapitre 3), même si le domaine ferroviaire est pris comme fil conducteur.

La maîtrise de la sûreté d'un système à base d'électronique programmable se base sur la maîtrise de l'électronique (chapitre 5) et la maîtrise du logiciel (chapitre 6). Dans le cadre de ce type de système, il est à noter que l'on peut aller jusqu'à la certification (chapitre 7).

Pour finir cette introduction, je tiens à remercier tous les industriels qui m'ont fait confiance depuis plus de dix années.