1

Introduction

1.1. Objectif

Le domaine ferroviaire est soumis à un référentiel normatif et à un référentiel légal (lois, décret, arrêté) qui dépend des pays. Au niveau européen, le référentiel légal est composé de textes européens et de textes nationaux. A noter que ce référentiel normatif et législatif est assez jeune (les premières normes datent du milieu des années 1990 et les premières lois de 2004). La figure 1.1 présente les principales normes applicables à la réalisation d'un système ferroviaire.

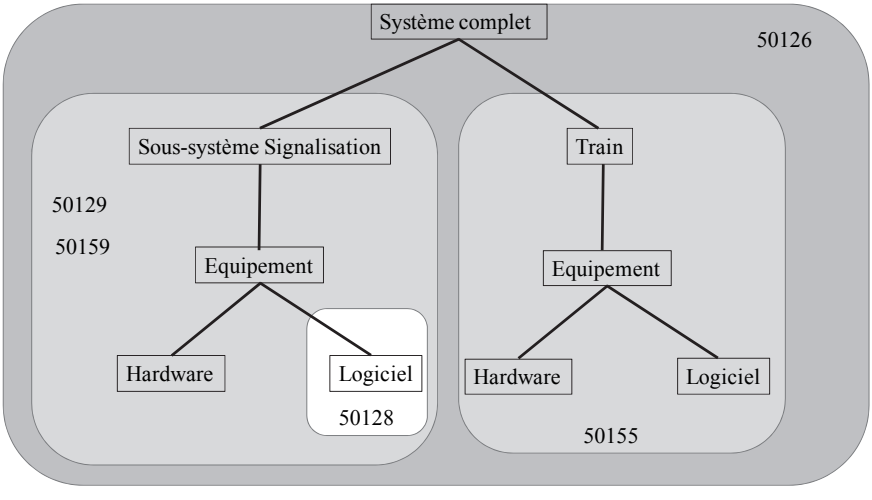

Figure 1.1. *Contexte normatif*

La figure 1.1 montre que le domaine ferroviaire est partitionné en deux parties : les applications liées à la signalisation et les applications embarquées au sein des trains. En fait, il est nécessaire d'ajouter une troisième famille « les autres », il peut s'agir des moyens de gestion de l'énergie, des systèmes de gestion des tapis roulants et des escaliers roulants, des systèmes d'information, les applications de gestion des systèmes annexes (ventilation en tunnel, détection d'incendie, etc.), en fait tout ce qui peut être connecté au système ferroviaire. Les systèmes annexes ne sont pas moins importants. Le système de détection d'incendie et de ventilation en tunnel est un système connexe au domaine qui pourrait enfumer le tunnel lors d'une évacuation, ainsi ce système a un impact sur la sécurité.

Le découpage du référentiel normatif est lié au fait qu'initialement la sécurité des systèmes ferroviaires reposait sur la signalisation (faire évoluer l'état des signaux en fonction de la présence des trains sur la voie) et le fait que le conducteur du train était responsable du respect de la signalisation.

CENELEC	IEC	Commentaires
50126:1999	62278:2002	
50129:2003	62425:2007	
50128:2001	62279:2002	Identique à la première page près
50128:2011	62279:2014-draft	La version en préparation contient des différences notables par rapport à la version CENELEC (contraintes complémentaires pour la qualification des outils, etc.)
50159-1 50159-2	62280-1:2002 62280-2:2002	
50159:2011	62280:2014	
50155	60571	La même chose avec des explications complémentaires

Tableau 1.1. *Traçabilité commentée CENELEC/IEC*

Les premières utilisations des logiciels ont permis de rendre plus souples les principes de signalisation (report en cabine de l'information de signalisation, découpage virtuel de la voie, etc.). La seconde étape a consisté à embarquer du logiciel dans les trains pour gérer les informations non sécuritaires et pour développer des fonctions spécifiques de petite taille. La nécessité de maîtriser le poids et le coût a amené les industriels à remplacer le cuivre et les relais par des logiciels (TCMS par exemple). En complément, le besoin d'évolution rapide (sans remplacement de l'équipement) et les innovations (moteur à aimant permanent) à entraîner l'utilisation

du logiciel pour les équipements classiques comme le manipulateur de conduite, la traction, le freinage, etc.

Concernant les normes CENELEC 50126, 50128, 50129, 50159 et 50155, elles sont applicables au niveau européen mais elles sont de plus en plus utilisées au niveau international. En complément, les normes CENELEC ont une image au niveau international au sein des normes IEC[1] comme le montre le tableau 1.1.

Ce livre présente la version 2011 de la norme CENELEC[2] 50128 [CEN 11] et sa mise en œuvre. Dans le cadre du chapitre 12, nous ferons un bilan des différences entre la CENELEC 50128:2011 et sa version IEC la 62279.

La norme CENELEC 50128:2011 identifie un processus de réalisation d'un logiciel pour les applications ferroviaires et identifie les moyens qui doivent être mis en œuvre afin d'atteindre le niveau d'assurance identifié.

La norme CENELEC 50128:2011 introduit de nouveaux besoins comme la séparation entre le logiciel générique et les données de paramétrage, la qualification des outils, le besoin de documenter et le besoin de maîtriser la maintenance et le déploiement des nouvelles versions du logiciel. Nous allons présenter cette nouvelle version de la norme, mais surtout nous allons fournir les éléments de lecture qui permettent de la mettre en œuvre.

1.2. Rappel

La sécurité des applications ferroviaires reposait sur la maîtrise de la signalisation. Avec des systèmes automatiques comme le métro (voir la ligne 14 du métro parisien[3] et/ou le VAL (pour Véhicule Automatique Léger)[4] de l'aéroport Charles de Gaulle), les logiciels participent à la maîtrise de la sécurité. La norme CENELEC 50128 dans sa version 2001 [CEN 01] a été rédigée pour définir un contexte permettant la

1. IEC pour *International Electrotechnical Commission* pour en savoir plus, voir le site : www.iec.ch/.

2. CENELEC pour Comité Européen de Normalisation ELECtrotechnique, voir le site www.cenelec.eu/.

3. La conception et la validation du SAET-METEOR (développé par MATRA-transport maintenant SIEMENS pour la RATP voir [MAT 98]) mis en service en 1998 a très largement contribué à la rédaction de la version 2001 de la norme CENELEC 50128.

4. Le premier VAL a été inauguré à Lille en 1983. Il équipe aujourd'hui les villes de Taipei et de Toulouse, de Rennes et de Turin (depuis janvier 2006). Concernant le déploiement du VAL, il y a au moins 119 km de ligne qui sont déployés dans le monde et plus de 830 voitures sont en exploitation ou en construction. Le VAL CDG combine la technologie du VAL et des équipements numériques complémentaires basés sur la méthode B [ABR 96].

maîtrise de la sécurité des logiciels. Cette version de la norme a profité de la mise en service de plusieurs systèmes à base de logiciel.

Figure 1.2. *Le VAL de CdG à quai*[5]

Depuis cette version, l'utilisation du logiciel a été généralisée à l'ensemble des parties du domaine ferroviaire (aide à la conduite, manipulateur de conduite, gestion des portes, gestion de la traction, gestion du paramétrage des capteurs, système de gestion de la ventilation en tunnel, etc.) et il était nécessaire de prendre en compte les problématiques nouvelles telles que la maintenance et le déploiement. La maintenance du logiciel ne concernant pas simplement la correction des anomalies mais la maîtrise des évolutions sur un ensemble d'équipements, lesquels étant peut-être déployés chez différents exploitants en version différente. Il faut donc mettre en place une maintenance qui prend en compte les versions déployées et un processus de déploiement qui permettra de garantir le bon fonctionnement des systèmes après déploiement des nouvelles versions.

La réalisation d'une application logicielle est basée sur des personnes et sur l'utilisation d'outils complexes. Concernant le premier point, la nouvelle version de la norme met l'accent sur la gestion des compétences et des responsabilités. Pour le second point, les outils peuvent avoir un impact sur l'exécutable (les générateurs de codes, les compilateurs, etc.) et/ou sur la vérification (environnement de test, outil de vérification des règles de programmation, etc.), c'est pourquoi il est nécessaire de qualifier les outils utilisés. A noter que cette notion de qualification est une notion qui a été introduite dans l'ensemble des standards qui ont été mis à jour (IEC 61508 [IEC 08], ISO 26262 [ISO 11], CENELEC 50128, etc.).

1.3. Synthèse

Nous avons présenté rapidement le contexte de la norme CENELEC 50128 et commencé à introduire les changements qui ont été réalisés dans la version 2011.

5. Photo réalisée par Jean-Louis Boulanger.

Aussi, dans la suite de cet ouvrage, nous présenterons la norme CENELEC 50128 en version 2011 et les principes de sa mise en œuvre.

Les chapitres de ce livre se présentent ainsi :

– chapitre 2 : le logiciel au sein du système ;

– chapitre 3 : l'histoire du référentiel CENELEC et la structure de la norme 50128 ;

– chapitre 4 : définition des niveaux de sécurité du système et allocation aux logiciels ;

– chapitre 5 : l'assurance du logiciel (maîtrise de la qualité, maîtrise de l'organisation, vérification et validation, etc.). Application du chapitre 6 de la norme CENELEC 50128 ;

– chapitre 6 : management des exigences ;

– chapitre 7 : l'application spécifique et le paramétrage par les données. Mise en œuvre du chapitre 8 de la norme CENELEC 50128 ;

– chapitre 8 : le développement de l'application générique. Mise en œuvre du chapitre 7 de la norme CENELEC 50128 ;

– chapitre 9 : modèle, modélisation et formalisation ;

– chapitre 10 : la qualification des outils ;

– chapitre 11 : la maintenance et le déploiement. Mise en œuvre du chapitre 9 de la norme CENELEC 50128 ;

– chapitre 12 : évaluation indépendante ;

– chapitre 13 : conclusion.

1.4. Bibliographie

[ABR 96] ABRIAL J.R., *The B-Book*, Cambridge University Press, Cambridge, 1996.

[AFN 07] AFNOR, EN 50155, Applications ferroviaires. Equipements électroniques utilises sur le matériel roulant, norme française, octobre 2007.

[CEN 00] CENELEC, NF EN 50126, Applications ferroviaires. Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FMDS), janvier 2000.

[CEN 01] CENELEC, EN 50128, Railway applications – Communications, signaling and processing systems – Software for railway control and protection systems, mai 2001.

[CEN 11] CENELEC, EN 50128, Railway applications – Communications, signaling and processing systems – Software for railway control and protection systems, mai 2011.

[IEC 02a] IEC 62279, Railway applications – Communications, signaling and processing systems – Software for railway control and protection systems, 2002.

[IEC 02b] IEC 62278, Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS), 2002.

[IEC 02c] IEC 62280-1, Railway applications – Communication, signaling and processing systems – Part 1: Safety-related communication in closed transmission systems, 2002.

[IEC 02d] IEC 62280-2, Railway applications – Communication, signaling and processing systems – Part 2: Safety-related communication in open transmission systems, 2002.

[IEC 07] IEC 62425, Railway applications – Communication, signaling and processing systems – Safety related electronic systems for signaling, 2007.

[IEC 08] IEC 61508, Sécurité fonctionnelle des systèmes électriques électroniques programmables relatifs à la sécurité, norme internationale, 2008.

[IEC 12] IEC 60571, Railway applications – Electronic equipment used on rolling stock, 2012.

[IEC 14] IEC 62280, Railway applications – Communication, signaling and processing systems – Safety related communication in transmission systems, IEC, 2014.

[ISO 11] ISO, ISO/DIS26262, Road vehicles – Functional safety, 2011.

[MAT 98] MATRA et RATP, « Naissance d'un Métro. Sur la nouvelle ligne 14, les rames METEOR entrent en scène », PARIS découvre son premier métro automatique, n° 1076, Hors-série, *La vie du Rail & des transports*, octobre 1998.