



Certification d'Application Ferroviaire
développée formellement ou non

Boulangier Jean-Louis
CERTIFER



Sommaire

- CERTIFER;
- Historique du ferroviaire;
- Contexte Normatif;
- Certification ferroviaire;
- Impact des méthodes formelles;
- Nouveaux besoins;
- Conclusions.



CERTIFER



Création de CERTIFER

- **CREATION**

- Association à but non lucrative loi du 1er Juillet 1901
- Depuis le 14 Février 1997.

- **MEMBRES**

RATP	
RFF	40 %
SNCF	
UTP	
FIF	40 %
INRETS	20 %



CERTIFER: Organisme de Certification

- CERTIFER est un :
- ORGANISME DE CERTIFICATION (J.O. 7 Août 1997)
- ORGANISME NOTIFIÉ pour la Directive EC/96/48 sur l'interopérabilité du réseau Grande Vitesse pour:
 - les constituants d'interopérabilité
 - les sous-systèmes
 - matériel roulant
 - infrastructure
 - contrôle commande et signalisation
 - énergie
 - exploitation
 - maintenance
- ORGANISME ACCRÉDITÉ par le COFRAC (EN 45011 - 27 Janvier 2000)
- OSTI (Organisme ou Service Technique Indépendant) pour l'application du décret 2000/286 sur la sécurité du RFN



Principales références

- **Systeme**
 - Avis sur la sécurité de la LGV Méditerranée
 - Evaluation des lignes de métro de l'agglomération Toulousaine
 - Evaluation de projets URBAINS (Grenoble, Mulhouse)
- **Infrastructure**
 - Audit de processus du contrôle des infrastructures EOLE
 - Audit de processus sur les Infrastructures METEOR
 - Certification de type de cœurs d'appareils de voie, verrous d'aiguilles, mécanismes d'aiguille, voie tramways



- Energie
 - Audit du processus d'électrification de la ligne PERSAN / BEAUVAIS

- Signalisation
 - Evaluation de la signalisation de la ligne nouvelle L2 (LOUVAINS / LIEGE) en Belgique
 - Certification du sous-système ERTMS (en cours)
 - Certification d'un calculateur embarqué

- Matériel Roulant
 - Evaluation différentes configurations du matériel CITADIS
 - Validation modèle pour Essais de Crash
 - Evaluation interface pupitre Locomotive FRET



Historique



SACEM (1)

- Année 80 (première étude)
- Mise en service 1986
- Système d'Aide à la Conduite, à l'Exploitation et à la Maintenance
- Première introduction:
 - De processeur,
 - De logiciel.
- Architecture:
 - Processeur-Codé
 - Famille : 68000

- Développement:
 - Développement classique
 - Développement ADA 83
- Validation
 - La RATP avait demandé une vérification formelle à postériori du développement
 - => Preuve de Hoare
 - La RATP avait financé les études qui sont à la base de l'environnement ASA
 - => IDEF0+ Automate et Model-checking

- Année 90 (première étude)
- Reconduction et extension de l'architecture sécuritaire processeur-codé.
 - DIGISAFE
- La RATP a décidé d'adopter une méthode formelle pour le développement :
 - la méthode B
 - => Preuve

- La RATP a décidé d'améliorer ASA pour la validation:
 - ASA+ (IDEF0 + Automate communicant étendu)

=> Model-checking
- SIEMENS (Matra Transport International)
- Mis en service en octobre 1998.

- Début étude: 1993
- Première mise en service: 1996

- KVB : Contrôle de vitesse à Balise
- SN : Sol Numérique
- Contrôle de vitesse par balise « sol numérique »
- ALSTOM

- Architecture:
 - FIDARE pour la protection vis à vis des erreurs matériels
- Développement:
 - Méthode B
 - ADA 83
- Déployer sur certaines lignes SNCF



Normalisation

- Le domaine du ferroviaire s'appuie sur 3 normes:
 - EN 50126 : Spécification et démonstration de la FMDS;
 - EN 50129 : Systèmes électroniques de sécurité pour la signalisation;
 - EN 50128 : Aspect **Logiciel** de commande.



Norme NF EN 50128 (1)

- Titre :

Application Ferroviaires, Système de signalisation, de télécommunication et de traitement – Logiciels pour systèmes de commande et de protection ferroviaire.

- Norme dérivée de la CEI 61508 (norme générique pour système de sécurité);



Norme NF EN 50128 (2)

- Caractéristiques:
 - Norme en partie écrite par les acteurs du ferroviaire français;
 - Norme Européenne;
 - Norme CENELEC : Comité Européen de Normalisation Electrotechnique;
 - Première version 1998;
 - Première version officielle Juillet 2001.

- **Domaine:**
 - Exclusivement applicable au logiciel et à l'interaction entre le logiciel et le matériel;
 - 5 niveaux de criticité:
 - Pas critique: SIL0,
 - SIL1, SIL2,
 - Critique : SIL3, SIL4
 - Applicable à:
 - L'application;
 - Le(s) système(s) d'exploitation ;
 - Les outil d'aide au développement;

- Directive d'interopérabilité du réseau grande vitesse
 - Europe 1996;
 - France 2001.
- Indique
 - 5 exigences essentielles à respecter pour réaliser l'interopérabilité:
 - E1: la sécurité
 - E2: la fiabilité / disponibilité
 - E3 : la santé
 - E4 : le respect de l'environnement
 - E5 : la compatibilité technique
 - qu'il faudra écrire des spécifications techniques d'interopérabilité

- Spécifications Techniques d'Interopérabilité:
 - infrastructure,
 - énergie,
 - matériel roulant,
 - contrôle commande,
 - exploitation,
 - maintenance
- Les STI sont des textes réglementaires approuvés par les états membres.
- La STI C/C recommande l'application des normes EN50128, EN50129 et EN50126

- Les méthodes formelles (CCS, ... VDM, Z et B) sont HR en SIL3 et SIL4
- Les méthodes semi-formelles sont HR SIL3 et SIL4
- Les méthodes structurées (SADT, SDL, ..., YOURDON) sont HR de SIL1 a SIL4
- La spécification:
 - Texte en langage naturel
 - Et toutes les notations mathématiques nécessaires

EN 50128: Conception

- Les méthodes formelles (CCS, ... VDM, Z et B) sont HR en SIL3 et SIL4
- Les méthodes semi-formelles sont HR de SIL1 à SIL4
- Les méthodes structurées (SADT, SDL, ..., YOURDON) sont HR de SIL1 à SIL4

- La norme EN 50128 met en avant deux notions :
 - Les exigences;
 - La traçabilité des exigences sur l'ensemble du processus.



Certification



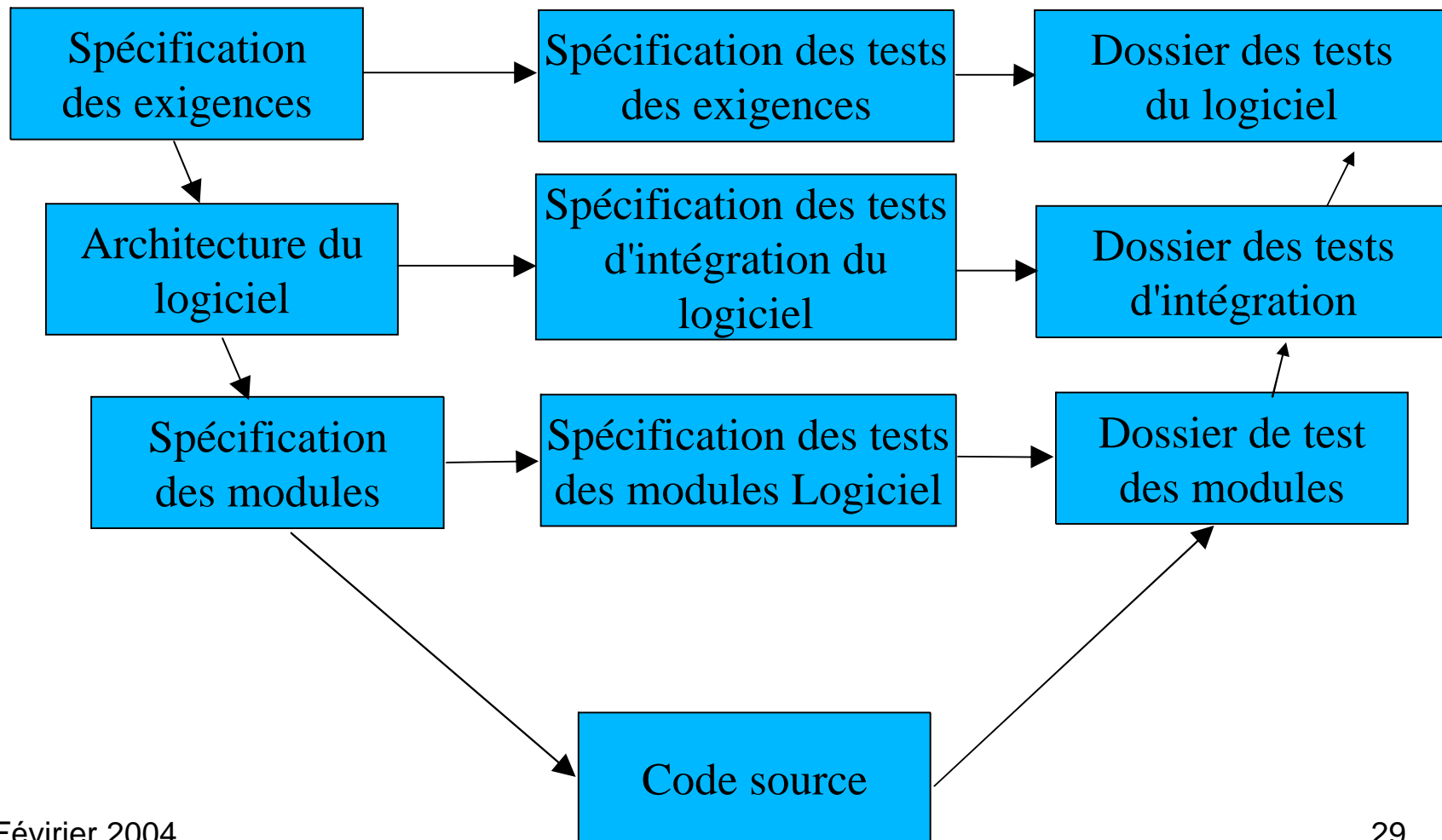
Lien directe avec la norme

- La section 14 de la norme est intitulé
 - « Evaluation du logiciel »
- Son introduction indique:
 - **Evaluer** que les **processus** du cycle de vie et les **produits** résultants sont tels que le logiciel correspond au niveau défini d'intégrité de la sécurité logicielle et qu'il est adapté à l'application prévue.

- 2 phases:
 - Évaluer le processus:
 - Audit du processus de développement et de validation;
 - Évaluation des plans:
 - Existence;
 - Adéquation des méthodes avec le niveau de SIL;
 - Participation à la mise en œuvre des tests.
 - Évaluer les produits:
 - Évaluation des documents produits;
 - Évaluation des composants (test, résultats de test, ...) produits;
 - Évaluation du logiciel.



Impact des méthodes formelles

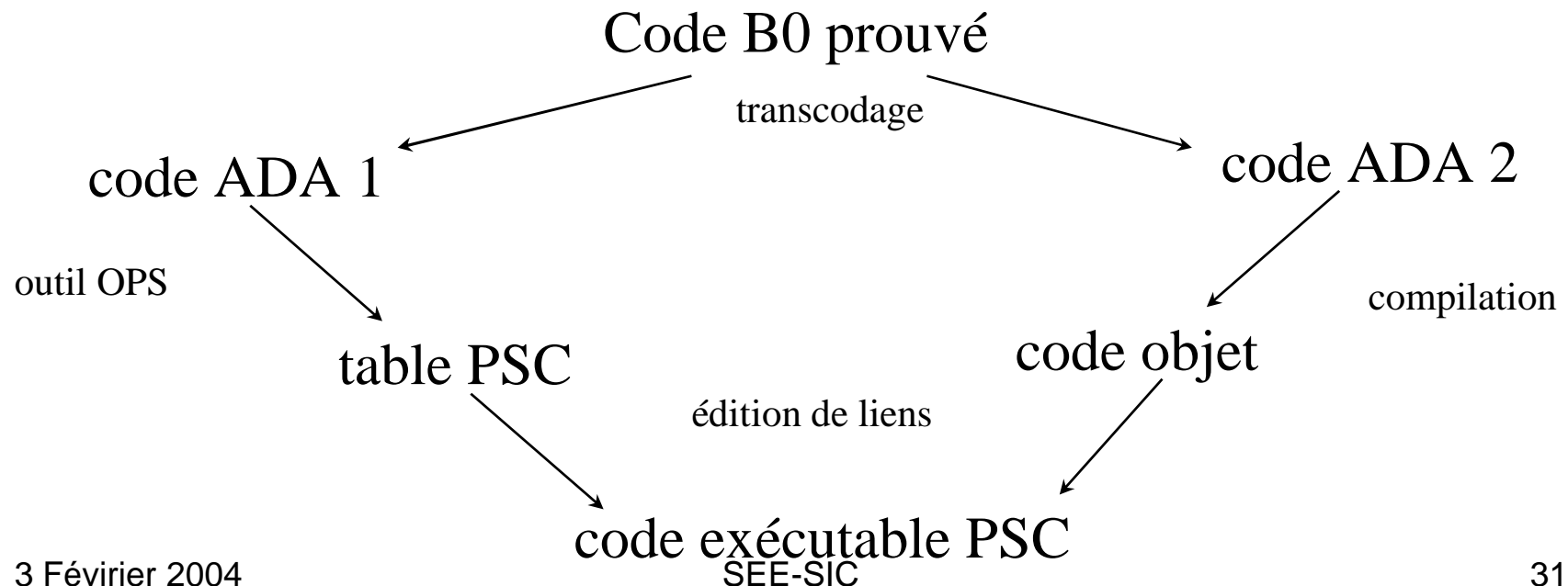




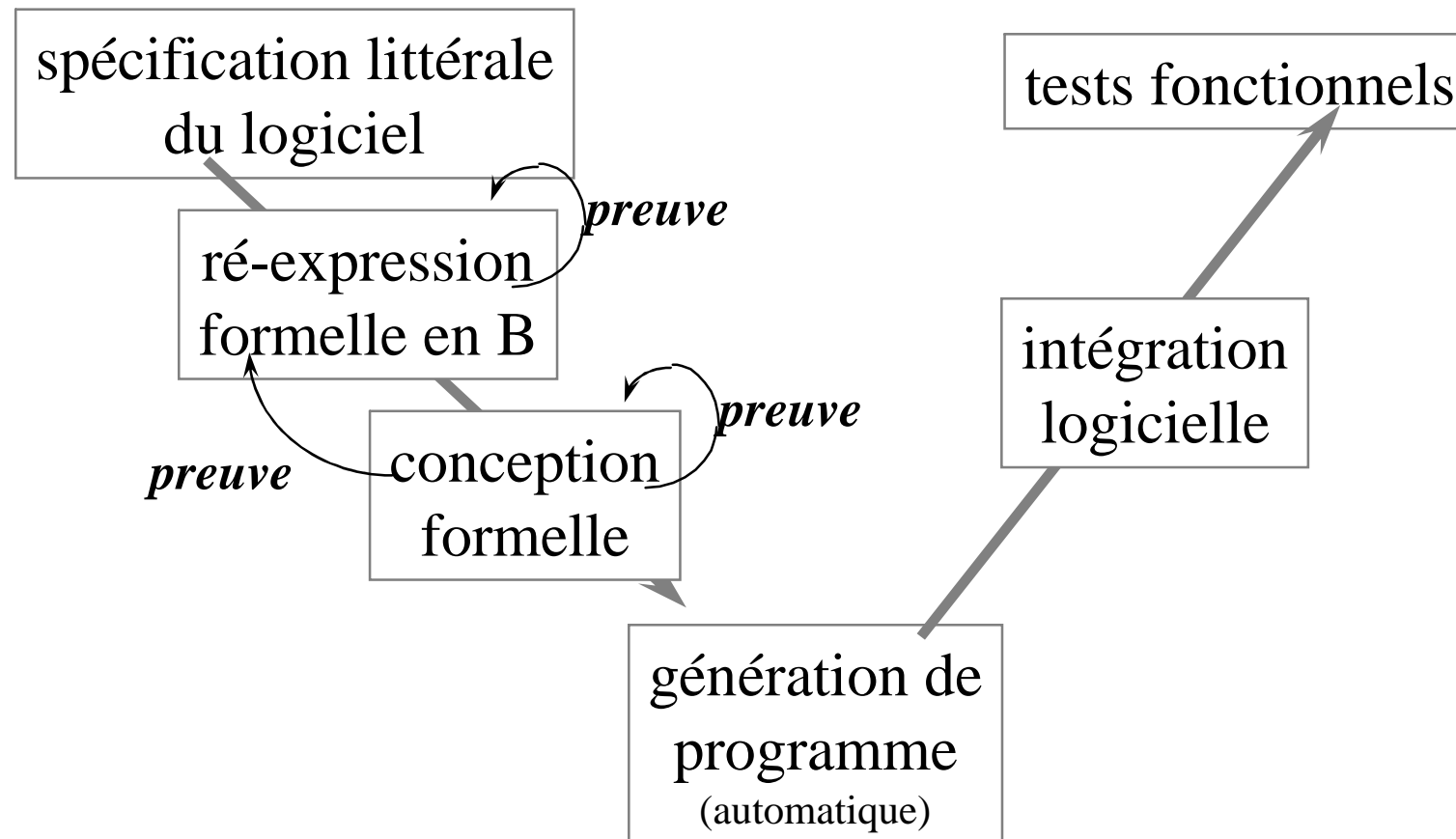
Calculateur METEOR

- Une exigence :
 - le Monoprocasseur codé
- Un nouveau calculateur : DIGISAFE
 - puissance de calcul accrue
 - innovations majeures
 - utilisation d'ASIC pour fonctions de sécurité
 - un coprocesseur (ASIC) dédié aux calculs sur le code

- le transcodage + DIGISAFE permet la sécurisation de l'exécution
- double chaîne de transcodage à partir du B0



Le cycle de vie des logiciels B





Impact des Méthodes Formelles sur la certification



Domaine ferroviaire français

- Types de développement:
 - Développement classique ADA83 ;
 - Développement formel avec B ;
 - Développement formel avec SCADE (Lustre) ;

 - Développement ADA 95 ;
 - Développement UML/C++.



Impact sur la certification

- Identification des langages de spécification et codage;
- Identification des techniques de sécurisation et justification;
- Stratégie de vérification et de validation.

- Impact global:
 - Connaissance du processus de développement B et des exigences associées;
- Relecture des documents de conception:
 - Introduction d'exigence;
- Relecture du code:
 - Connaissance de B;
 - Relecture des lemmes mathématiques;

- Analyse du processus de vérification formelle:
 - Traçabilité spécification textuelle/code B
 - Analyse des résultats
 - nombre de PO,
 - nombre de preuves,
 - nombre de lemmes,
 - ...
 - Analyse des travaux complémentaires (validation des lemmes mathématiques)

Obligation

- Dans le cadre des marchés européens ou internationaux, il n'est plus possible de demander l'utilisation d'une méthode ou d'un outil.
- Il peut y avoir des « recommandations ».



Nouveaux Besoins

- **Spécification : apparition de modélisation UML**
 - UML est une notation;
 - Pb de sémantique;
 - Outillage
- **Conception : Génération de code orienté objet à partir de spécification UML**
 - Processus de génération de code
 - Génération partielle
 - => codage complémentaire

- Spécification :
 - ?
- Conception :
 - Programmation orienté objet R de SIL1 à SIL4
 - Sous-ensemble du langage HR pour SIL3 et SIL4
 - Traducteur validé HR de SIL1 a SIL4
 - Traducteur éprouvé à l'utilisation HR de SIL0 à SIL4
- Vérification
 - Métrique
 - testabilité



Conclusions



A ce jour

- CERTIFER c'est 32 certificats et d'autre analyses.
- Un référentiel normatif prenant en compte l'expérience;
- Plusieurs expériences
 - De développement formel
 - De certification d'application développée formellement
- Un nouveau besoin en cour de maîtrise:
 - L'ingénierie des exigences.

- De nouvelles architectures matérielles:
 - 2 parmi 2
 - 2 parmi 3
- Nouveau processeur
- PC du commerce

- Développement orienté objet (ADA95, C++, JAVA, ...);
- Spécification UML + génération de code;
-



Questions ?