



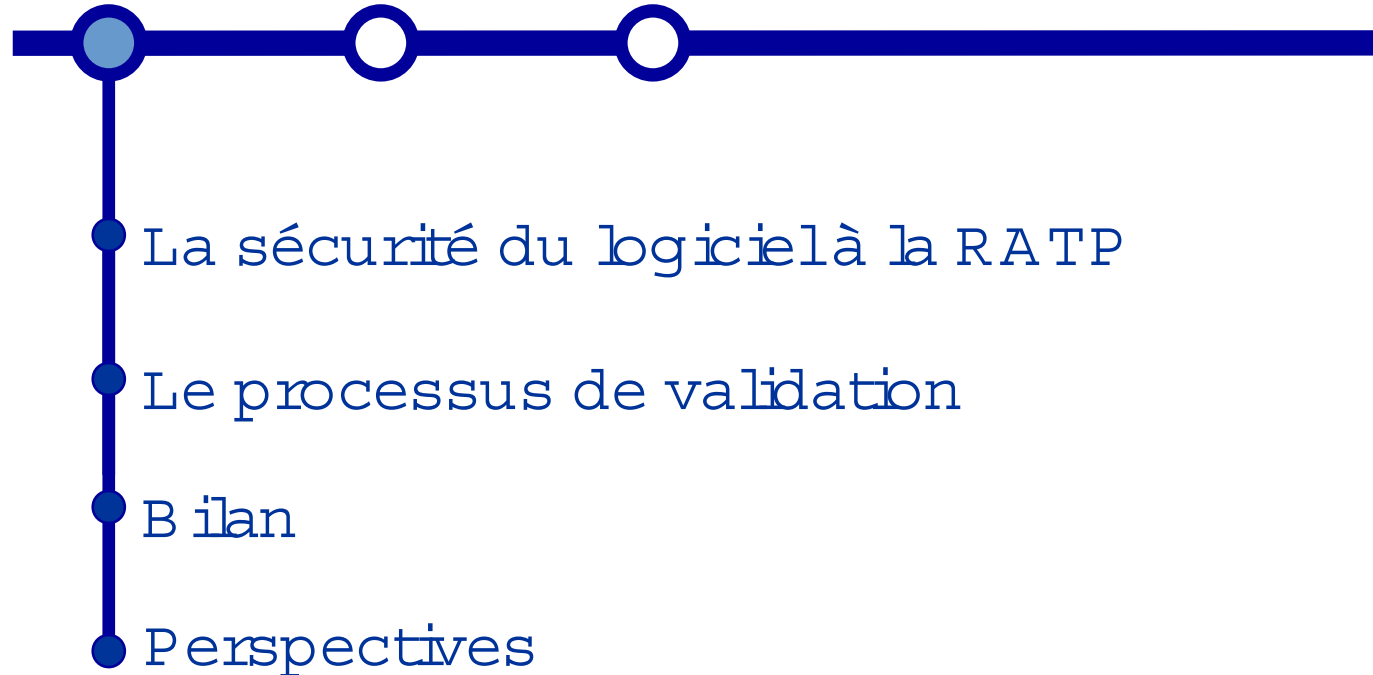
Evaluation de la SdF des logiciels de contrôle-commande à la RATP Bilan et perspectives

Pierre CHARTIER
Atelier de Qualification des Logiciels

17 juin 2003



PLAN



La Sécurité du logiciel à la RATP

Historique

- Années 80 : passage de l'électronique câblée à des architectures informatiques pour réaliser le système de contrôle continu de vitesse SACEM - RER - Ligne **A**
 - Le modèle de sécurité n'est plus celui de la sécurité intrinsèque
 - La RATP se dote alors des moyens et des techniques permettant de vérifier la sécurité d'un système de contrôle-commande ferroviaire incluant du logiciel

La Sécurité du logiciel à la RATP

Le laboratoire AQL

- Le laboratoire AQL a pour mission, dans le domaine des logiciels ferroviaires critiques de sécurité,
 - d'homologuer ces logiciels,
 - et de rendre un avis d'évaluateur indépendant pour le dossier de sécurité final présenté aux tutelles pour la mise en service du système.
- Le laboratoire est accrédité COFRAC sur 6 essais du programme n°152 « Evaluation de la Sûreté de Fonctionnement des systèmes logiciels »

La Sécurité du logiciel à la RATP

Le référentiel normatif applicable

- Norme EN 50128 : Applications ferroviaires. Systèmes de signalisation, de télécommunication et de traitement - Logiciels pour systèmes de commande et de protection ferroviaire
 - Elaborée par les industriels et les opérateurs ferroviaires
 - Applicable depuis juillet 2001
 - Définit, pour les différents niveaux d'intégrité de la sécurité du logiciel, les méthodes et techniques à utiliser pour atteindre le niveau de sécurité spécifié.

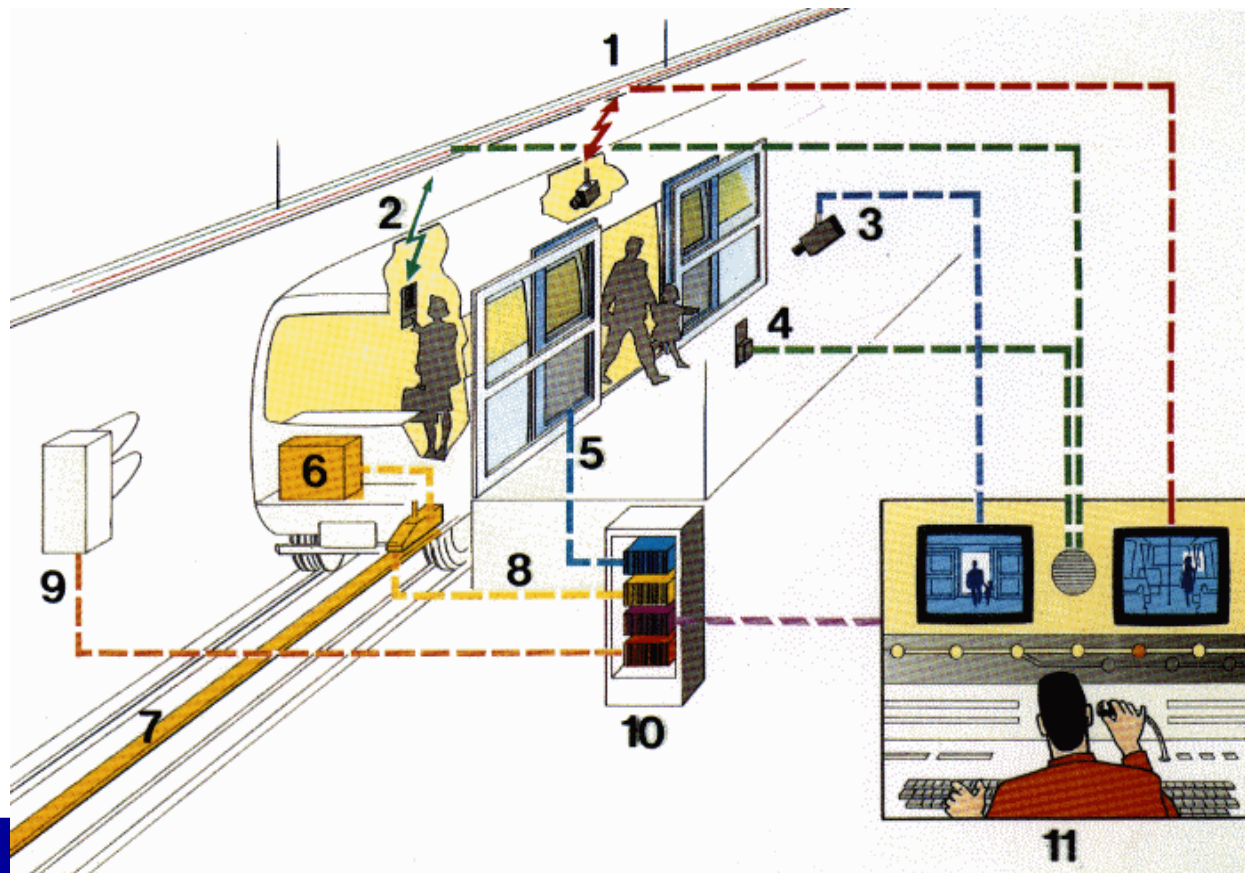
Le processus de validation

Le système SAET Météor

- Un système automatique complexe fortement intégré : matériel roulant, équipements électriques, infrastructures, automatisés, ...
- Six sous-systèmes :
 - Moyens Audio et Vidéo
 - Poste de Commande Centralisée
 - Logique Traction
 - Portes Palières
 - Pilotage Automatique
 - Signalisation

Le processus de validation

Le système SAET Météor



- 1 - vidéo-surveillance train
- 2 - interphonie train
- 3 - vidéo-surveillance quai
- 4 - interphonie quai
- 5 - portes palières
- 6 - pilotage automatique en barqué
- 7 - tapis de transmission
- 8 - transmission sol-bord
- 9 - signalisation
- 10 - pilotage automatique fixe
 - 1 PA de ligne
 - des PA de section
- 11 - poste de commande centralisé

Le processus de validation

Activités RATP (1)

- Validation du calculateur de base DIGSAFE
 - Analyse et modélisation statique des interfaces
 - ✱ logiciels/matériel
 - ✱ logiciels de base / application
 - ✱ logiciel de base / logiciel de base
 - Identification des critères de sécurité applicables aux logiciels de base du calculateur
 - Vérification du respect des critères de sécurité
 - ✱ Lecture critique de code
 - ✱ Analyse statique de code outillée
 - ✱ Injection de fautes en environnement simulé

Le processus de validation

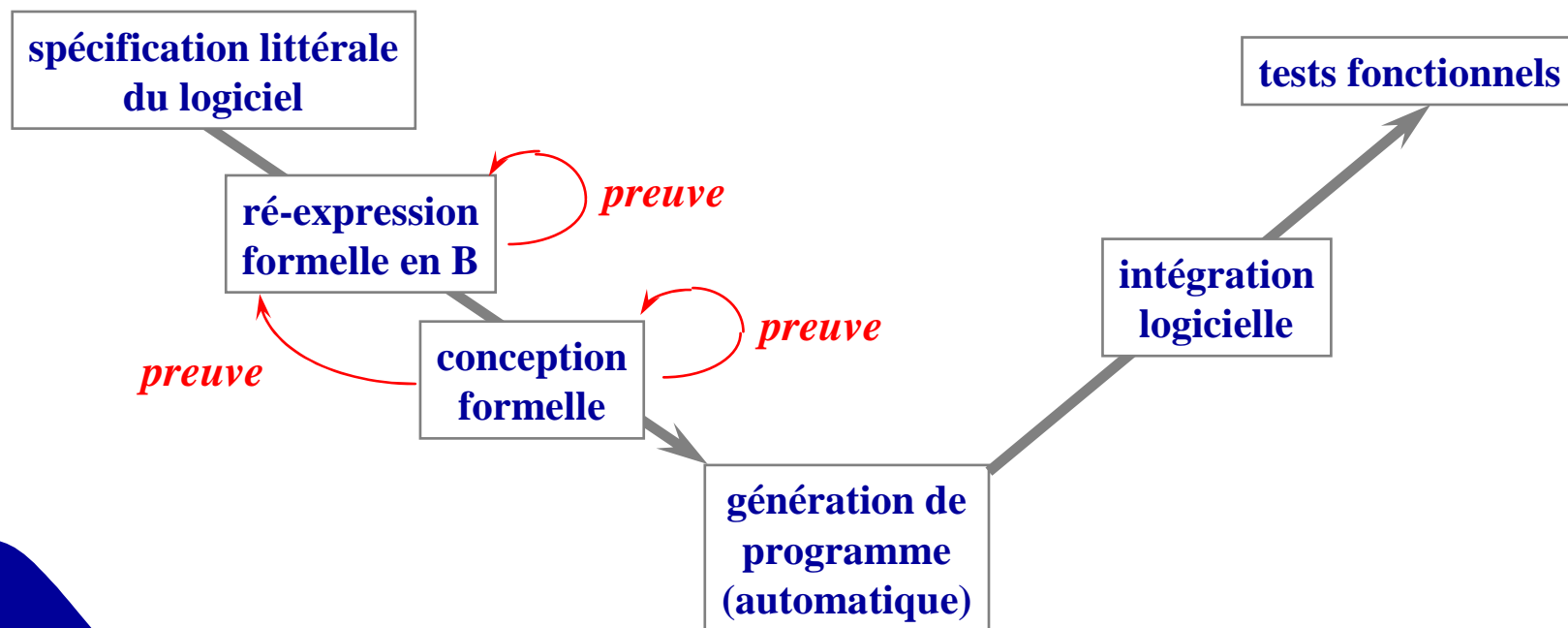
Activités RATP (2)

- Validation fonctionnelle des applications de sécurité indépendante de celle de l'industriel
 - Vérification de la spécification du logiciel
 - ✱ modélisation statique
 - ✱ modélisation dynamique
 - ✱ vérification des exigences du niveau supérieur par simulation

Le processus de validation

Activités RATP (3)

- Validation fonctionnelle des applications de sécurité indépendante de celle de l'industriel
 - Vérification de la conception formelle B



Le processus de validation

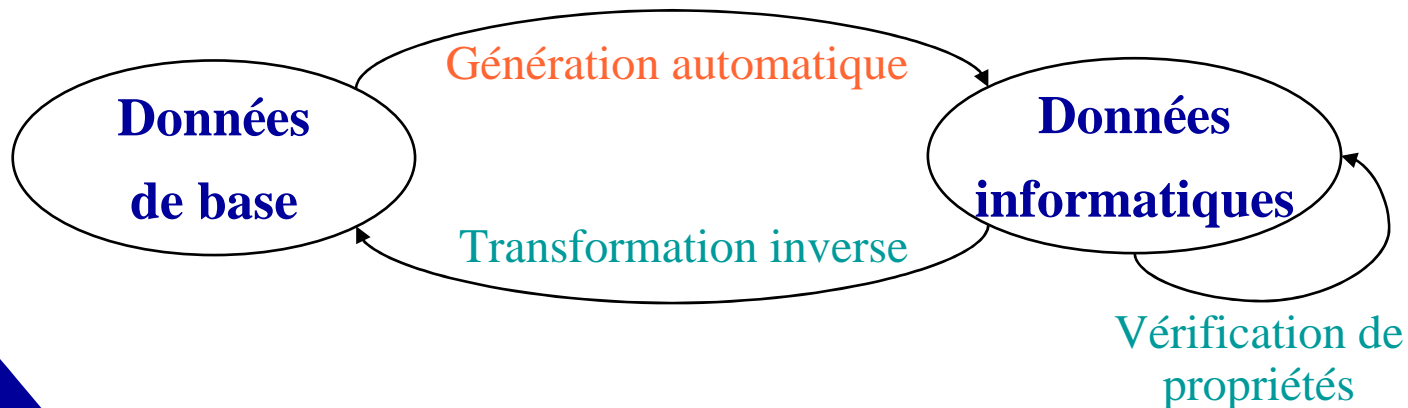
Activités RATP (4)

- Validation fonctionnelle des applications de sécurité indépendante de celle de l'industriel
 - Validation des fonctions critiques
 - ✱ rédaction d'un plan de tests
 - ✱ rédaction de cahiers de tests de validation
 - ✱ exécution des tests sur calculateur cible
 - ✱ mesure du taux de couverture des tests sur cible
 - vis à vis du code
 - vis à vis de la spécification

Le processus de validation

Activités RATP (5)

- Validation fonctionnelle des applications de sécurité indépendante de celle de l'industriel
 - Validation des données automatisée (outil)
 - ✱ transformation inverse des données
 - ✱ vérification de propriétés sur les données





Le processus de validation

Activités RATP (6)

- Contrôle des activités de l'industriel
 - Approbation des plans
 - Audits de processus
 - Analyse des documents produits au cours du cycle de développement pour vérifier la conformité aux plans



Bilan

Éléments quantitatifs des logiciels SAET

- 1150 composants B
- 115000 lignes de code B
- 27 800 obligations de preuve B
- 150 000 lignes de code ADA SIL 4



Bilan

Éléments quantitatifs du processus RATP

- 20 Dossiers de principes
- 23 modèles
- 30 Cahiers de tests
- Plus de 5000 tests en environnement simulé

Bilan

Résultats obtenus

- 400 remarques critiques pour la sécurité au niveau des spécifications
- 110 anomalies détectées sur l'ensemble des versions des logiciels de sécurité
- un système logiciel qui a fonctionné dès sa première installation
- la conviction de la sécurité à l'issue du processus

Bilan

Un processus très efficace, mais :

- coûteux : coût de validation RATP égal à celui de la validation de l'industriel pour le logiciel
- long alors qu'il est sur le chemin critique du planning de mise en service
- qui pourrait ne plus responsabiliser suffisamment l'industriel

Perspectives

Des systèmes de plus en plus nombreux...

- Les systèmes de contrôle continu de vitesse comme SACEM - Ligne **A**
- Le contrôle continu de vitesse de la ligne B KCVP
- L'automatisation intégrale METEOR **M** **14**
- Les Postes de Manœuvre informatisés (PM I)
- Les systèmes de commande contrôle du mouvement des trains OURAGAN :
 - ✱ Ligne **13** : projet en cours
 - ✱ Lignes **3** et **5** : consultation en cours
- Automatisation de la ligne **1**

Perspectives

Une cadence accélérée

- Les 11 autres lignes de métro à équiper avec OURAGAN dans les 15 ans à venir
- 70 postes de manœuvre à informatiser dans les 30 ans à venir
- Prolongement METEOR (M¹⁴) à Saint Lazare en 2003
- Prolongement METEOR (M¹⁴) à Olympiades en 2006
- Apparition de Matériels Roulants intégrant des calculateurs de sécurité (MF2000)

Perspectives

Adaptation du processus d'évaluation SdF

- Nécessaire pour :
 - réduire la durée des évaluations de la Sûreté de fonctionnement afin de faire face à une cadence élevée de renouvellement des systèmes
 - prendre en compte la maturité atteinte par les industriels dans le domaine de l'ingénierie logicielle
 - bénéficier des outils et des techniques innovantes qui sont désormais dans le domaine industriel

Perspectives

Reflexions en cours sur :

- Les outils de traçabilité des exigences (RTM , DOORS , CLEARCASE , etc ...)
- Les méthodes formelles (AtelierB -SCADE)
- Les outils de conception de logiciels permettant la génération automatique de code (SCADE , Rose RT , etc...)
- L'automatisation de la génération de jeux de tests
- L'analyse statique de code outillée
 - L'interprétation abstraite (POLYSPACE , ABSINT , ...)
 - La preuve de programme (CAVEAT , ...)

Perspectives

Axes de progrès identifiés

- Utiliser des techniques nouvelles pour atteindre les mêmes objectifs de vérification avec moins de ressources
- Identifier les activités RATP dont l'apport en terme de sécurité est devenu minimale compte tenu de la maturité des processus et des techniques utilisées par les industriels
- Remplacer les activités ainsi identifiées par des contrôles des fournisseurs de l'industriel