L'atelier de qualification des logiciels

SECURITE
L'ATELIER DE QUALIFICATION DES LOGICIELS

Le laboratoire Atelier de Qualification des Logiciels (AQL) est le premier laboratoire français accrédité par le COmité FRançais d'ACcréditation (COFRAC) pour mener des essais dans le cadre du programme 152 intitulé "Evaluation en sûreté de fonctionnement des systèmes logiciels". Son accréditation porte sur le processus de vérification et de validation qui a été mis en place à la suite des travaux menés sur le SAET-METEOR et le SACEM. Ce processus de vérification et de validation est construit sur un référentiel de qualité et des procédures métiers.

SECURITY
THE SOFTWARE QUALIFICATION WORKSHOP

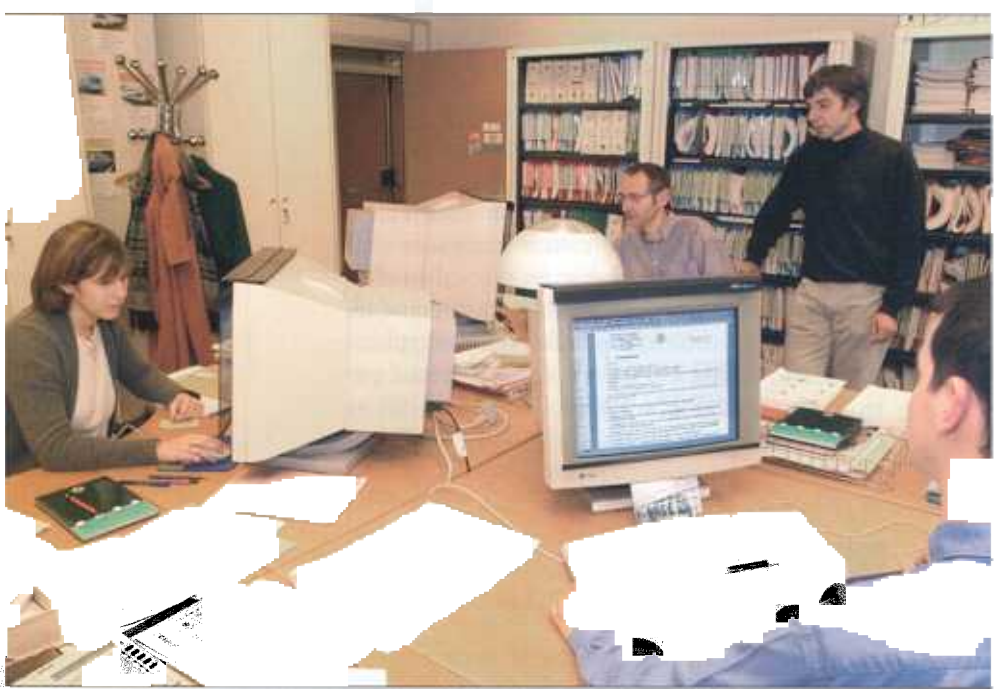
The Atelier de Qualification de Logiciels (AQL) - Software Qualification Workshop - is the first French laboratory to be accredited by the "COmité FRançais d'Accréditation" (COFRAC) – French Accreditation Committee – to perform tests as part of programme 152 entitled "Software system operational security evaluation". Its accreditation concerns the verification and validation process implemented following the work done on the SAET-METEOR and SACEM. This verification and validation process is based on a professional quality baseline and procedures

SICHERHEIT
DIE WERKSTATT FUR DIE SOFTWARE-QUALIFIKATION

Das Labor für die Software-Qualifikation (Laboratoire Atelier de Qualification des Logiciels - AQL) ist das erste frz. Labor, das von dem französischen Ausschuss COmité FRançais d'ACcréditation (COFRAC) eine Zulassung erhalten hat um im Rahmen des Projekts 152 "Bewertung der Funktionssicherheit von Programmsystemen" Tests durchzuführen. Die Zulassung betrifft das Verfahren zur Prüfung und Validierung, das infolge der Arbeiten für die rechnergestützten Betriebsleitungssysteme SAET-METEOR und SACEM eingerichtet worden war. Das Prüf- und Validierungsverfahren basiert auf einem Bezugssystem für Qualitäts- und Fachverfahren.

SEGURIDAD
EL TALLER DE CUALIFICACION DE LOS SOFTWARES

El laboratorio Taller de Cualificación de los Softwares (Atelier de Qualification des Logiciels, AQL) es el primer laboratorio francés acreditado por el COmité FRancés de ACreditación (COFRAC) para llevar a cabo ensayos dentro del marco del programa 152 titulado "Evaluación en seguridad de funcionamiento de los sistemas softwares". Su acreditación se refiere al proceso de verificación y de validación que ha sido implementado tras los trabajos realizados en el SAET-METEOR y el SACEM. Este proceso de verificación y de validación está elaborado en base a un referencial de calidad y de procedimientos de actividades.



Un bureau de l'atelier de qualification des logiciels.

par Jean-Louis Boulanger,
département Equipements
Systèmes du Transport

Depuis les années 80, l'informatisation des systèmes ferroviaires n'a fait que croître. En effet, le contrôle commande des systèmes de transport ferroviaire est passé d'une technologie électronique cablée à une technologie fondée sur des logiciels installés dans des architectures informatiques. Ce changement s'est fait à travers la mise en place de plusieurs systèmes ferroviaires tels que le Système d'Aide à la Conduite, à l'Exploitation et à la Maintenance (SACEM), le TGV, le Système d'Automatisation de l'Exploitation des Trains (SAET) de METEOR en service sur la ligne 14. Lors de la mise en place du SACEM, la RATP a dû se doter de moyens et de techniques qui lui permettent de vérifier le bon fonctionnement du

COFRAC

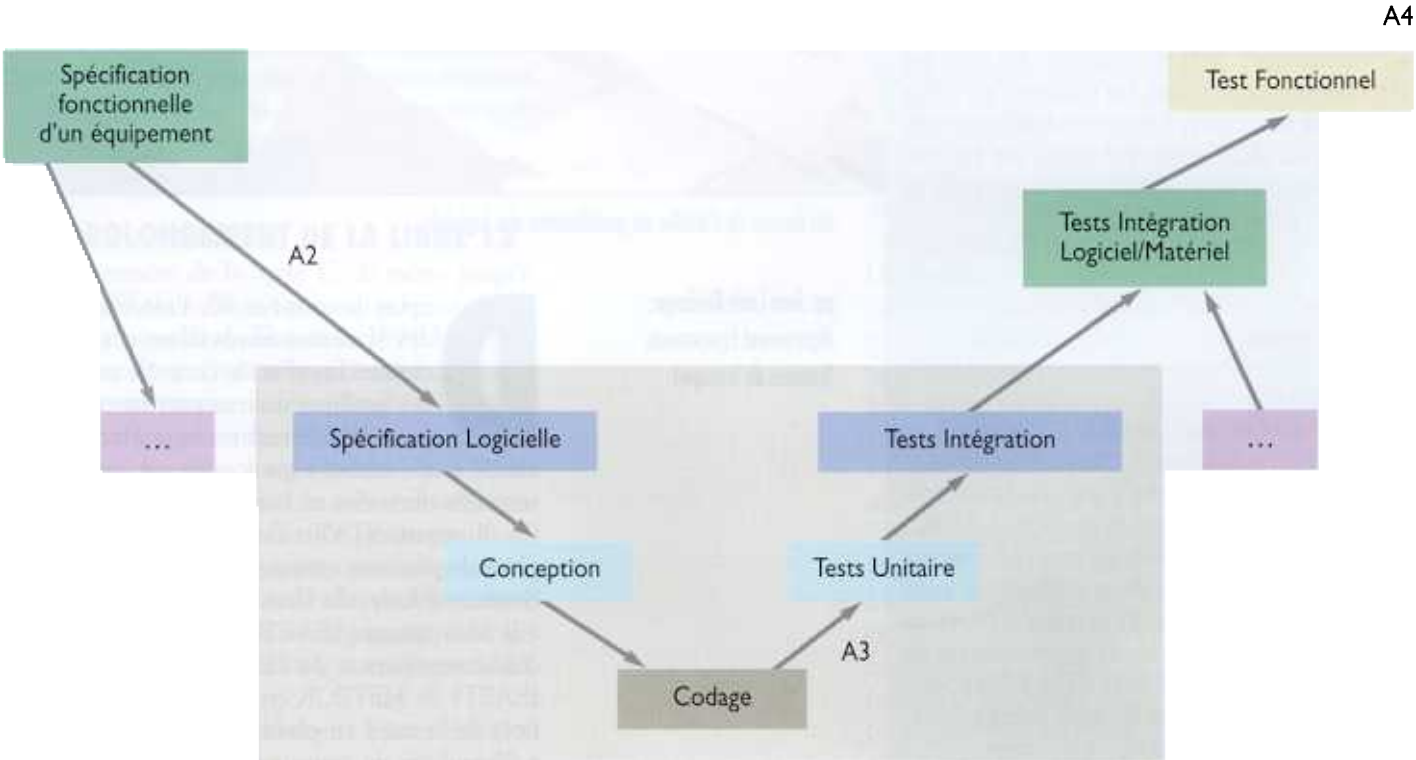
Le COmité FRançais d'ACcréditation (www.cofrac.fr), créé en 1994, permet aux laboratoires et aux organismes qu'il accrédite d'apporter la preuve de leur compétence et de leur impartialité. La section "Laboratoire" procède à l'accréditation des laboratoires d'essais et d'analyses selon la norme ISO/CEI 17025 précisée par des programmes d'accréditation. Le COFRAC constitue un élément essentiel de la promotion de la qualité et gère aujourd'hui plus de 1500 accréditations.
Le laboratoire AQL a demandé une accréditation dans le cadre du programme 152 intitulé "Evaluation en sûreté de fonctionnement des systèmes logiciels". Ce programme traite de la contribution de la composante logicielle à la sûreté de fonctionnement d'un système informatique. La sûreté de fonctionnement des logiciels est présente dans de nombreux domaines et les essais contenus dans le présent programme peuvent s'appliquer aux logiciels de tous les domaines.

contrôle commande d'un système ferroviaire contenant du logiciel. Le monde ferroviaire s'est investi largement dans la mise en place d'un référentiel normatif adapté au développement de systèmes de contrôle commande pour des applications ferroviaires. Ce travail s'est concrétisé par trois normes NF EN 50126, NF EN 50128 et NF EN 50129.

Comme dans tout système complexe, les différents éléments constitutifs peuvent être classés en différentes catégories en fonction de leur criticité qui dépend de l'impact d'une anomalie sur le fonctionnement du système. La norme NF EN 50126 qui traite des activités de sûreté de fonctionnement, définit la notion de niveau d'intégrité de la sécurité logicielle à atteindre (NISL). La norme NF EN 50128 concerne des méthodes qu'il est nécessaire d'utiliser pour fournir des logiciels répondant aux exigences d'intégrité de la sécurité imposées par le niveau de sécurité logicielle à atteindre pour la fonction concernée.

■ LES PROCESSUS DE VERIFICATION

Avant de mettre en service un nouvel équipement ou un nouveau système contenant des logiciels de sécurité (NISL3 ou 4), la RATP doit réaliser des contrôles. Ces contrôles peuvent être de qualification et/ou d'aptitude à l'emploi. Dans le cadre de la qualification des logiciels de sécurité, le laboratoire AQL réalise trois types d'opérations : un contrôle des travaux de l'industriel, une double vérification, des audits de contrôle du processus.
Le développement d'un équipement commence par la mise en place d'une spécification fonctionnelle. Elle est alors découpée en "n" composants matériels ou logiciels, sécuritaires ou non. Chaque composant est ensuite détaillé avant d'être testé. La figure ci-dessous place le développement logiciel au sein du cycle de développement en V. Quatre audits de contrôle sont prévus. Le premier



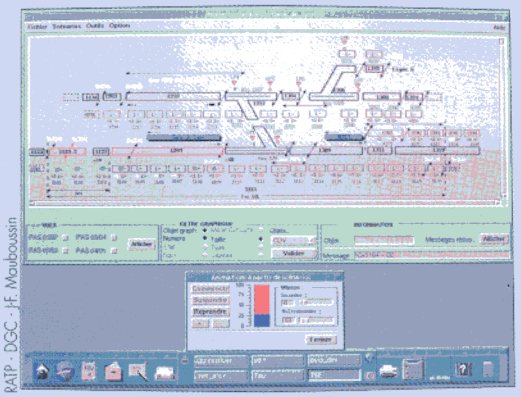
Le cycle de développement d'un équipement.

audit est lié à la mise en place, chez l'industriel, d'une organisation idoine et à l'approbation des plans de développement, de validation et de sécurité... Le second audit a pour but de contrôler la bonne application des plans pour réaliser la spécification fonctionnelle de l'équipement étudié et du logiciel. Le troisième audit permet de contrôler l'application des plans de développement et de validation. Une fois l'ensemble des tests réalisés, unitaire, intégration et fonctionnel, il est possible de réaliser le quatrième et dernier audit.
Après le déroulement complet du processus par l'industriel, tous les éléments, documents et logiciels sont fournis à la RATP pour que le laboratoire puisse réaliser une évaluation approfondie de la sûreté de fonctionnement du logiciel. Le processus d'évaluation du laboratoire est fondé sur la mise en place d'une vérification réalisée par une équipe indépendante avec des méthodes différentes de celles mises en place par le constructeur. Cette vérification porte autant sur la conception fonctionnelle que sur la vérification de la réalisation finale. La vérification est découpée en deux tâches : un contrôle de l'industriel et une vérification indépendante.
Le contrôle de l'industriel consiste à vérifier l'application de l'ensemble des plans et les productions associées. Ce contrôle s'applique donc aux documents, aux sources et aux tests. Chaque écart par rapport aux spécifications initiales doit être justifié par l'industriel.
Comme dans le cas de la validation du système Maggaly pour le métro de Lyon, le processus de vérification mis en place par le laboratoire AQL est basé sur la notion de propriété de sécurité. Des analyses critiques permettent l'édition d'un document définissant l'ensemble des propriétés formelles, fondées sur la logique mathématique, que les logiciels de sécurité de l'équipement doivent vérifier. L'ensemble des propriétés formelles permet de décrire le comportement du logiciel dans sa capacité à vérifier de manière précise, non ambiguë et démontrable.
Les fonctions de sécurité complexes, complexe signifie dans ce cas que l'ensemble de leur comportement ne peut être appréhendé de manière sûre par un opérateur humain, sont ensuite modélisées en relation avec la spécification. Les propriétés formelles sont implantées au sein de ce modèle qui doit lui-même être implanté dans un outil informatique qui permette de raisonner et d'effectuer des simulations de scénarios de tests.

L'ACCREDITATION COFRAC

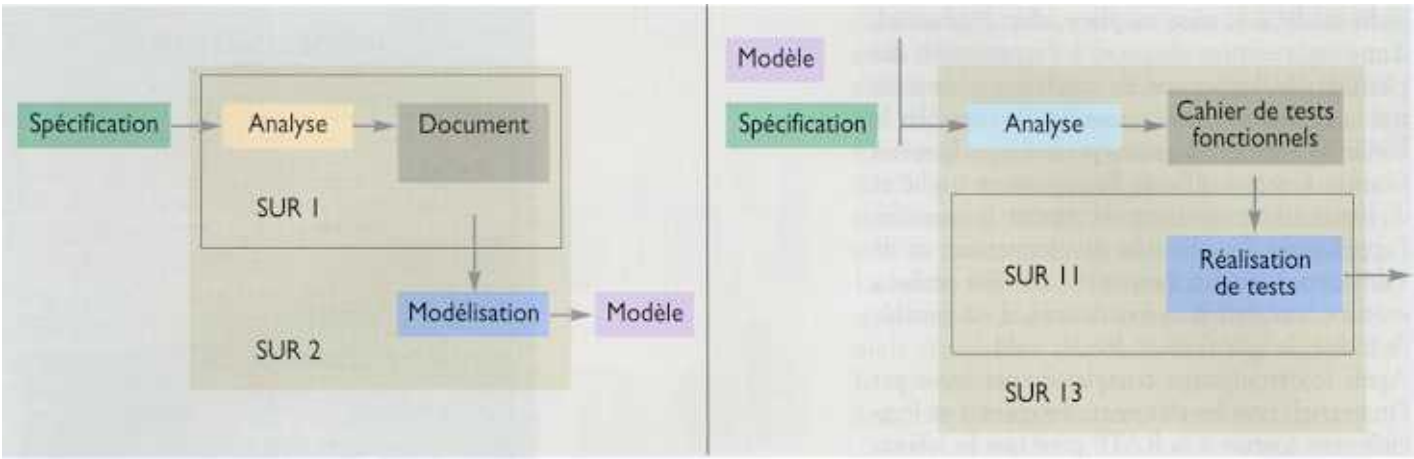
La mise en place d'un référentiel de qualité basé sur des procédures métiers : vérification de spécifications, validation de fonctions critiques, analyse d'impacts... a permis au laboratoire AQL de présenter au COFRAC certains des essais qu'il réalise dans le cadre du programme 152 intitulé "Evaluation en sûreté de fonctionnement des systèmes logiciels". L'accréditation du laboratoire AQL a porté sur le processus de vérification et de validation qui a été mis en place à la suite des travaux menés sur le SAET-METEOR. En 1999, année de l'accréditation du laboratoire AQL, le fonctionnement des laboratoires d'essais était défini par la norme française NF EN 45001. Depuis octobre 2001, le COFRAC prend pour référence la norme ISO/IEC 17025.
Courant mai 1999, le laboratoire AQL a obtenu l'accréditation COFRAC pour les cinq essais

MODELISATION



Dans le cadre d'un système qu'un être humain n'est pas capable d'appréhender dans son ensemble, il est recommandé d'en réaliser la modélisation. Elle consiste à construire une abstraction du problème puis à l'implanter dans un outil informatique qui permette de raisonner et d'effectuer des simulations de scénarios de tests.

Ecran de modélisation avec agent.



La vérification de spécification et la validation du logiciel.

qu'il a présentés : SUR 1, SUR 2, SUR 11, SUR 13 et SUR 14 dans le programme 152. Le laboratoire AQL a été le premier laboratoire français et à ce jour le seul à présenter et à obtenir une accréditation sur ce programme. Dans ce cadre, le laboratoire AQL a réalisé une matrice de traçabilité entre les essais et les éléments du référentiel de qualité qui décrit les processus du laboratoire. Courant juin 2000, l'accréditation COFRAC a donné lieu à un audit de surveillance. Cet audit a été l'occasion pour le laboratoire de présenter un essai complémentaire : SUR 5 intitulé "Vérification orientée sûreté de fonctionnement de la documentation de conception du logiciel". Le laboratoire a mis au point cet essai dans le cadre d'un développement selon la méthode B.

AUTOMATES PROGRAMMABLES

Les systèmes annexes tels que les escaliers mécaniques, les ventilations et autres qui participent à la sécurité du système ont été équipés d'un contrôle commande programmé et géré par un automate programmable. Dans le cadre du renouvellement des escaliers mécaniques de Passy, le laboratoire AQL s'est vu confier la mission de vérifier la spécification fonctionnelle (SUR 2). Cette spécification fonctionnelle fait partie du cahier des charges qui a été envoyé aux fournisseurs lors de l'appel d'offre.

Celle-ci, développée par Jean-Raymond Abrial, a été utilisée par *Siemens Transportation System* dans le cadre du développement du SAET-METEOR. L'accréditation COFRAC du laboratoire AQL a été reconduite pour les cinq premiers essais et étendue à ce sixième essai.

Afin d'étoffer son catalogue de prestations et de couvrir au mieux le processus de qualification précédemment défini, le laboratoire devrait, à terme, présenter au moins deux nouveaux essais : SUR 10 intitulé "Vérification orientée sûreté de fonctionnement du code. Inspection, analyse statique" et SUR 12 intitulé "Vérification orientée sûreté de fonctionnement de la documentation des tests du logiciel (plan, cas de test et résultat)". L'essai SUR 10 couvre l'analyse du code et l'essai SUR 12 est un contrôle du processus de test de l'industriel.

Il est indispensable de rappeler que les résultats de ces essais sur les logiciels ne sont que des éléments à utiliser pour se prononcer sur la sûreté de fonctionnement des systèmes informatiques qui incluent ces logiciels. Ils sont limités à un logiciel évalué dans un contexte d'essais précis, matériel et environnement. Les résultats obtenus ne peuvent pas être généralisés automatiquement à des contextes opérationnels différents.

LA DESCRIPTION DES ESSAIS

L'essai SUR 1 intitulé "Vérification orientée sûreté de fonctionnement de la documentation de la spécification logicielle" consiste en une analyse précise de la documentation avec traçabilité des exigences de sécurité. L'essai SUR 2 intitulé "Modélisation orientée sûreté de fonctionnement de la spécification logicielle" inclut l'essai SUR 1 et poursuit donc l'analyse jusqu'à l'obtention d'un modèle de la spécification. Ce modèle doit prendre en compte les exigences issues de l'analyse et permet de vérifier l'aspect fonctionnel de la spécification. L'essai SUR 11 intitulé "Mesure de la couverture des exigences de sûreté de fonctionnement par les tests" a pour but de réaliser les tests décrits dans le cahier de tests du client. L'essai

SUR 13 intitulé "Tests de validation orientée de sûreté de fonctionnement" est découpé en deux phases : définition des tests et réalisation des tests (SUR 11). L'essai SUR 14 intitulé "Analyse orientée sûreté de fonctionnement de l'impact des modifications du logiciel" permet d'étudier l'impact d'une évolution sur le logiciel.

■ LES APPLICATIONS

Les essais SUR 1, SUR 2, SUR 13 et SUR 14 sont appliqués à chaque évolution des systèmes SACEM et SAET-METEOR. Dans le cadre du SAET-METEOR, l'essai SUR 5 est nécessaire pour vérifier la conception formelle.
Pour les nouveaux systèmes de transport ferroviaire mis en service à la RATP, les essais SUR 1, SUR 2, SUR 5 et SUR 14 seront réalisés.
L'accréditation COFRAC donne au laboratoire AQL la possibilité de réaliser ces essais pour des clients externes (SNCF, Systra, CERTIFER ou EURAILTEST) ou pour des clients internes sur d'autres types de systèmes.
Depuis plusieurs années, les systèmes à base de contrôle commande de toutes natures ont été équipés de systèmes programmés. Les installations fixes telles que les escaliers mécaniques, les ventilations et les autres équipements électro-mécaniques qui participent à la sécurité du système de transport ne font pas exception. Ils se sont vu équiper d'un contrôle commande programmé et géré par un automate programmable. Etant donné leur implication dans la sécurité et la disponibilité, ces systèmes doivent faire l'objet d'une évaluation adaptée de leur sûreté de fonctionnement.
Le laboratoire travaille actuellement sur la vérification des spécifications fonctionnelles (SUR 2) d'un escalier mécanique, d'une ventilation et d'un poste de redressement et la validation fonctionnelle (SUR 13) du poste de redressement. Ces travaux ont permis de démontrer la robustesse des processus du laboratoire et leur caractère générique.

■ LES PERSPECTIVES

Le référentiel qualité du laboratoire AQL est fondé sur un ensemble de procédures métiers qui ont été élaborées à l'occasion de la vérification et de la validation des logiciels critiques du SAET-METEOR et du SACEM. Ces procédures métiers ont donc été testées en réel sur des projets de taille importante et reconduites sur l'ensemble des nouveaux projets. Le laboratoire AQL est actuellement le seul laboratoire accrédité par le COFRAC pour mener des essais dans le cadre du programme 152. La forte implication des acteurs métiers dans la mise en place de ce référentiel de qualité a permis au laboratoire de savoir intégrer les coûts de la qualité dans ces travaux.
Le laboratoire AQL peut réaliser des prestations en interne, département EST, et en commercialiser d'autres en externe, SNCF, Systra, CERTIFER, EURAILTEST et autres. Il participe ainsi au développement de la RATP ■

LE SYSTEME D'AUTOMATISATION DE L'EXPLOITATION DES TRAINS (SAET)

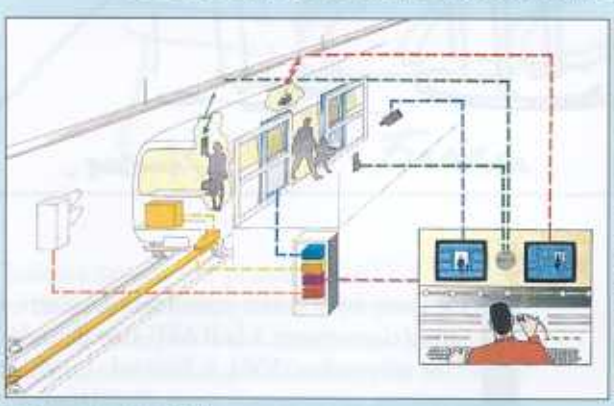


Schéma général du SAET.

Un MP89 sur fosse.

Les équipements embarqués du SAET.

Le système METEOR installé sur la ligne 14 est géré par le Système d'Automatisation de l'Exploitation des Trains (SAET) qui est un système temps réel réparti complexe dont la principale fonction est d'assurer le transport des voyageurs tout en leur garantissant un niveau de sécurité très élevé.

La ligne 14 permet la circulation de trains non équipés de poste de conduite et de trains équipés, avec ou sans conducteur, pouvant utiliser la conduite automatique. Dans le cas des trains équipés, il existe deux modes de conduite : la conduite manuelle et la conduite automatique intégrale. La ligne 14 a été mise en service le 15 octobre 1998. Elle est composée de sept stations réparties sur une distance de 7,2 km. La vitesse commerciale est de 40 km/h et l'intervalle entre deux trains est de 85 secondes pour les trains équipés en conduite automatique intégrale.