Zeitschrift: Tracés : bulletin technique de la Suisse romande
Herausgeber: Société suisse des ingénieurs et des architectes
Band: 134 (2008)
Heft: 15-16: Montrer le m2

Artikel: Validation par test et simulation
Autor: Joubert, Dominique / Roland, Raoul
DOI: https://doi.org/10.5169/seals-99694

Dominique Joubert et Raoul Roland

Validation par test et simulation

Un système de transport fait partie des systèmes dits « complexes ». Sa complexité vient du fait qu'il se compose de plusieurs sous-systèmes qui s'emboîtent et communiquent entre eux. La sécurité et la disponibilité de l'ensemble reposent non seulement sur celles de chaque élément, mais aussi sur celles de fonctions « transversales » qui sont implémentées par deux ou plusieurs sous-ensembles. Ces sous-systèmes sont fournis par des industriels différents, ce qui ajoute à la complexité technique une complexité contractuelle. Les simulations et les tests jouent un rôle capital pour garantir le fonctionnement final.

Prenons par exemple une fonction simple du m2, l'ouverture sécurisée des portes de quai. Pour obtenir ce résultat, il faut en résumé :

- immobiliser la rame et transmettre cet état une fois l'arrêt assuré,
- contrôler le positionnement de la rame concernée en face des portes et transmettre l'autorisation d'ouverture,
- commander l'ouverture des portes.

Dans le cas présent, ces trois actions doivent être exécutées dans un temps minimum et par des équipements appartenant à trois lots séparés : la rame, les automatismes et les portes palières.

Un rôle central : l'intégrateur

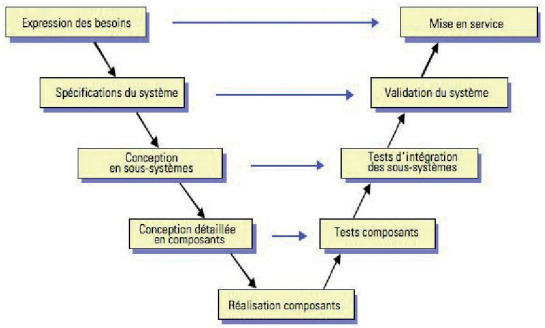
C'est pour cela que dans ce genre de système, le rôle de « l'intégrateur » est fondamental. Dès les premières phases du projet, ce rôle consiste à spécifier, pour chaque pièce du puzzle, les fonctionnalités demandées à cet élément ainsi que les interfaces mécaniques, électriques et informatiques avec les autres pièces avec lesquelles il communique. Ceci afin que chaque sous-élément s'ajuste aux autres. Que ce soit au cours des études, de la fabrication ou des tests d'équipement, l'intégrateur se doit de gérer les interfaces et leurs évolutions. Vers la fin du projet, son rôle consiste à vérifier et à mettre en place l'ensemble des pièces fabriquées pour, au final, valider le fonctionnement global souhaité.

Ce rôle d'intégrateur peut être tenu par le maître d'ouvrage – futur propriétaire du système – ou délégué (partiellement ou totalement) à un maître d'œuvre qui intervient alors comme architecte du système. Dans le cas du m2, le Métro Lausanne-Ouchy (MLO) a conservé la responsabilité de l'intégration du projet, en s'adjoignant l'assistance de bureaux externes afin de trouver les compétences et les ressources nécessaires à ce travail.

Cycle en V

La méthodologie utilisée pour ce genre de projet trouve son origine dans le développement de logiciels. Ce sont les projets informatiques militaires qui, dans les années 70, ont les premiers utilisé la méthodologie dite du « cycle en V » (fig. 1). Son principe est simple : on décrit le système de façon descendante, c'est à dire en précisant progressivement le besoin du général au détail (top - down). Parallèlement, on découpe le système en sous-systèmes, puis en logiciels, puis en modules et enfin en programme. Lorsque les programmes sont codés, le système est intégré progressivement dans l'ordre inverse (bottom - up) en modules, puis en sous-systèmes pour finalement aboutir au système voulu.

Pour assurer la réussite de ces deux phases (descendante, puis montante), le concepteur doit produire, pour chaque étape de la phase descendante, d'une part les spécifications décrivant les éléments de l'étape suivante et, de l'autre, les



1

Fig. 1 : Cycle en V pour le développement d'un système

Fig. 2 : Pyramide des essais pour le m2

Fig. 3 : Planning pour le m2

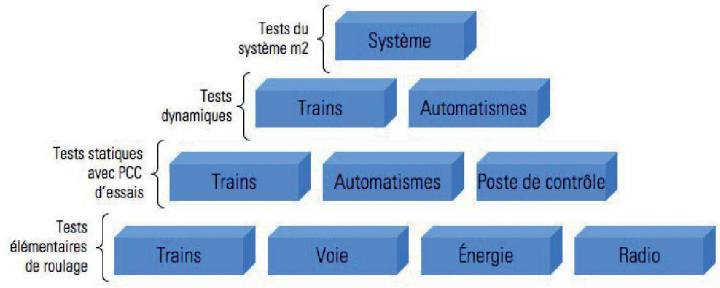
tests à réaliser sur ces éléments lors de la phase montante pour vérifier qu'ils sont conformes.

Phase de tests

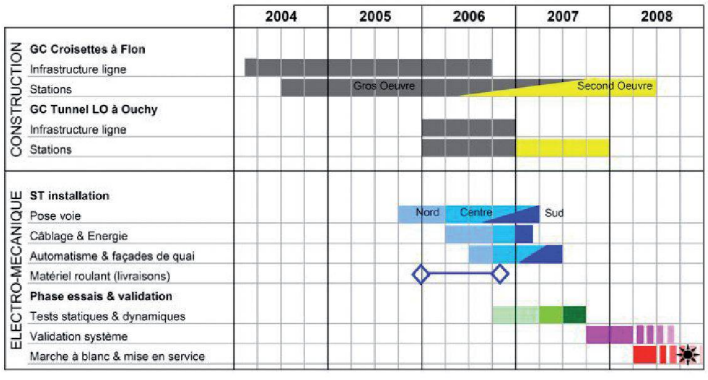
La phase montante du cycle en V correspond donc à une suite de tests, allant du test du module jusqu'au test final du système intégré. Les premières « couches » de tests sont effectuées en usine, alors que les dernières ont lieu sur le site d'exploitation. Comme la ressource « site » est unique et que la durée des tests sur le site est toujours forcément limitée, il est essentiel de porter un effort maximum lors des tests en usine. La règle d'or est donc : « tout ce qui peut être fait en usine ne doit pas être fait sur site ».

Malheureusement, ce précepte n'est pas toujours simple à respecter car le puzzle du système est en quelque sorte pyramidal, c'est-à-dire que certains équipements du système doivent être intégrés et fonctionnels pour que d'autres puissent être intégrés à leur tour (fig. 2). Par exemple, tant que la voie n'est pas posée et l'énergie alimentée, il est impossible de tester le sous-système « rame » *in situ*.

Pour le m2, la durée globale des tests sur site a été d'environ deux ans. Les tests « dynamiques », c'est à dire avec des trains qui circulent, a été de 18 mois. Les tests « système », c'est à dire avec l'ensemble des sous-systèmes installés et en fonction sur le site ont duré neuf mois (fig. 3).La couverture de l'ensemble des spécifications du système a impliqué de passer environ 1000 tests d'une durée de deux à douze heures. L'exécution de tous ces tests a occupé le site 24h/24h et 7j/7j.



2



3

Risques, simulation et tests *in situ*

Depuis la création du modèle en V, beaucoup de théories, livres et méthodologies ont été émis. Mais la réalité reste souvent assez éloignée de la théorie et l'expérience montre que malgré ces méthodes, les risques de dérapage voire d'échec dans la construction des systèmes complexes restent encore importants.

Un projet bien piloté se doit donc de connaître et de maîtriser ces risques, en particulier ceux qui sont générés par sa conception même, à savoir qu'une fois fabriqués, un ou plusieurs éléments ne s'intègrent pas correctement *in situ*. Ces risques existent aussi bien dans le contexte environnemental existant (particularités du lieu, environnement électromagnétique, etc.) que dans celui réalisé par d'autres fournisseurs (construction génie civil, voie, énergie, câblage, interfaces équipements, etc.). En cas d'incompatibilité non ou mal traitée, les besoins souhaités risquent de ne pas être obtenus, selon le principe du maillon faible : la performance de l'ensemble du système n'est pas la moyenne de l'ensemble, mais bien celle de son élément le plus faible ou le moins bien conçu.

Un moyen de diminuer le risque que le projet n'aboutisse pas à un système couvrant les besoins initiaux est d'anticiper sur son résultat. Outre les études « papier », que les concepteurs utilisent pour vérifier intellectuellement leur solution, les outils de simulation permettent de modéliser, par des algorithmes informatiques, l'environnement futur du système ou du sous-système et de valider qu'avec les hypothèses retenues, le système devrait avoir un comportement cohérent avec le besoin.

Le deuxième grand intérêt des simulations est l'énorme gain de temps qu'elles sont à même de générer. En effet lorsqu'il a été possible, par le biais de simulations, de démontrer que le comportement de tel ou tel sous-système est conforme à ses spécifications, les tests sur site peuvent être sensiblement allégés. Les essais se réduisent à la vérification que l'environnement réel est conforme à l'environnement simulé. Si tel est le cas, un gain de temps d'ordre dix ou plus est possible.

Pour le m2, l'efficience de la complémentarité entre tests et

Fig. 4 : Production de fumée pour un test, 6 mars 2008
(Photo M. Schobinger / MLO SA)

4

simulation pour le développement de systèmes complexes peut être diversement illustrée. Nous traitons ici le cas des événements redoutés, la simulation de l'exploitation et la simulation aéraulique étant chacune l'objet d'articles séparés de la part de mandataires spécialisés (voir articles p. 19 et 25).

Simulation des événements redoutés

La validation des logiciels sécuritaires dans un environnement simulé en plateforme informatique n'est pas une particularité du m2 : avec le développement d'équipements informatiques remplaçant l'homme pour des fonctions de sécurité, la validation des logiciels sur plateforme fait partie des règles de l'art. A tel point que les normes internationales définissent, selon le niveau de risque à couvrir, le minimum de tests requis pour obtenir l'assurance du bon fonctionnement de ces logiciels.

Ces tests permettent de vérifier en simulant les scénarios à risque, par exemple les scénarios de collision, que les logiciels sont fiables dans toutes les situations. Ils sont ainsi livrés sur site avec un « safety certificate » garant de leur bon fonctionnement. A noter encore que certains tests – par exemple concernant les mouvements de trains sur des itinéraires incompatibles, l'approche d'un butoir en terminus, etc. – doivent nécessairement être réalisés sur simulateur avant de mettre réellement des rames en mouvement, puisqu'un test sur site s'avérerait dangereux en cas de défaut.

Plateforme de test

La complexité des logiciels induit une quantité de paramètres et de fonctionnalités à tester très importante. Un travail qu'il n'est physiquement pas envisageable de réaliser « à la main », encore moins sur site. A moins d'y consacrer quelques siècles ! Pour réduire les délais et répondre aux exigences de démonstration imposées par les normes de sécurité ferroviaire, les industriels utilisent des « plateformes » de validation en usine. Ces plateformes consistent en un ou plusieurs équipements qui sont soit les équipements ou les logiciels réels du système, soit des équipements qui simulent leur environnement. Une plateforme simple comprend un équipement ou logiciel à tester qui fonctionne « normalement », comme s'il était sur site, à ceci près que son environnement est virtuel : ses entrées sont générées par un simulateur alors que ses sorties sont renvoyées au simulateur ou à un outil d'observation.

Fig. 5 : Frotteur positif de captage du 750 Volts DC (Photo M. Schobinger / MLO SA)

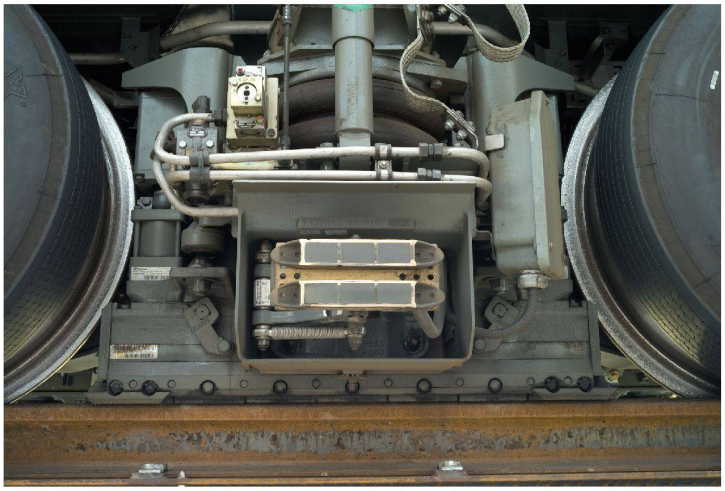
(Sauf mention, tous les documents ont été fournis par les auteurs.)

Pour la validation du m2, la plateforme de test d'*Alstom* à Meudon autorise la mise en œuvre non pas d'un, mais de tous les principaux sous-systèmes des automatismes. Les trains, leurs mouvements ainsi que les équipements *in situ* (signaux, aiguillages) sont quant à eux simulés. On peut ainsi faire des tests « d'intégration » très élaborés qui permettent de valider les interfaces et les fonctions complexes entre les équipements, ceci sans avoir à attendre leurs installations sur site.

Variation des paramètres

L'intérêt du simulateur est qu'il est facilement paramétrable et automatisable. On peut ainsi élaborer un grand nombre de situations de test (scénario) et les dérouler automatiquement. Un scénario est défini par une situation d'origine et une série d'actions pour lesquelles on attend une réaction prédéfinie de l'équipement testé. Le simulateur peut ainsi dérouler des milliers de cas de test en un seul clic : les scénarios s'enchaînent les uns aux autres sans aucune assistance, les résultats étant enregistrés automatiquement.

Par exemple, pour valider les données de cartographie de la ligne – positions des stations, du garage, des aiguillages, des signaux, des fins de voies, des courbes, des pentes, etc. –, on peut tester individuellement chaque élément par un scénario impliquant un ou plusieurs trains virtuels, afin de vérifier que tous les risques potentiels sont correctement traités par les calculateurs de sécurité (collisions face à face, par rattrapage, par conflit d'itinéraires sur un aiguillage, survitesse). Sur simulateur, démarrer un nouveau test avec un train à un nouveau point de départ se réduit à changer une variable dans un scénario ; sur site, c'est un mouvement de train complexe à réaliser. Le gain de temps et de souplesse est évident.



5

De plus, la complexité du système fait qu'il est rare que les équipements et les logiciels fonctionnent sans problème du premier coup. Il faut donc pouvoir rejouer un même test à l'identique pour comparer facilement les résultats et vérifier que l'on corrige bien les « bugs » au fur et à mesure. En laboratoire, on peut répéter le test autant de fois que l'on veut en faisant varier à loisir les paramètres : cela ne « coûte » qu'une simulation. Sur site, on imagine aisément les difficultés et le temps nécessaires pour chaque nouvel essai.

Les outils de test sont de plus en plus perfectionnés et reproduisent de plus en plus fidèlement un environnement qui soit représentatif de la réalité. Ils permettent aussi d'assurer une plus grande exhaustivité des tests nécessaires pour démontrer la sécurité des logiciels critiques. Certains outils vérifient par exemple que toutes les lignes du code d'un logiciel ont été sollicitées par au moins un scénario de test alors que d'autres prouvent par des méthodes mathématiques qu'une règle de sécurité n'est jamais enfreinte.

Etape fondamentale

L'usager d'un métro automatique sans conducteur n'est certainement pas conscient de la complexité des systèmes qui le meuvent. Si le nombre de lignes sans conducteur dans le monde n'est pas négligeable[1], ce n'est pas encore un produit « sur étagère » qu'il suffit d'installer pour qu'il fonctionne. Tant que les vérifications ne sont pas terminées, rien ne prouve que le système va fonctionner.

La phase de test est donc fondamentale pour valider le système, ses performances et sa sécurité. Les outils de simulation anticipent cette phase en environnement informatique. Ils permettent d'une part de réduire l'ampleur et la durée des essais *in situ* et d'autre part d'éviter la découverte tardive d'aléas techniques ou de diminuer leur impact sur le résultat final.

A Lausanne, la maîtrise des risques techniques a contribué à l'atteinte du double objectif de tenir le budget et le délai. Cette réussite est en grande partie due aux équipes de conception qui ont été capables d'anticiper puis de résoudre les problèmes, notamment grâce aux outils de simulations.

Dominique Joubert, ing. ECL
GESTE Engineering SA, Parc scientifique PSE-C
CH – 1015 Lausanne

Raoul Roland, ing. ESIEE Paris
Alstom Schienenfahrzeuge AG
Industrieplatz 1, CH – 8212 Neuhausen am Rheinfall

[1] De l'ordre de 25, liste non exhaustive : Lille (2 lignes), Paris, Rennes, Lyon, Toulouse (2 lignes), Vancouver, Chicago, Nuremberg, Turin, Copenhague (2 lignes), Londres (2 lignes), Japon (plusieurs lignes)