L'approche probabiliste des risques ne met pas à l'abri des catastrophes. A quand la généralisation des méthodes formelles dans le ferroviaire ?

(Marc Antoni)

Constats

Les accidents nucléaires survenus sur le site de Fukushima posent encore une fois la question des postulats qui organisent la défense en profondeur des installations industrielles. Considérant que la perte de la source froide et des sources électriques avait une probabilité de survenance très faible dans une région qui subit 20% des séismes et des tsunamis de la planète, rien n'a été prévu pour y faire face. Il n'a pas été imaginé qu'un tsunami puisse engendrer une vague de plus de 10 mètres dans une région qu'une vague de 23 mètres avait submergée en 1923… Ceci fait ressortir l'état des déficits de prise en compte des conséquences d'un accident réputé ne jamais pouvoir survenir.

Si cet accident est devenu une catastrophe, c'est parce que de l'énergie et de l'eau traitée n'auront pas été apportés dans des délais compatibles avec le rétablissement d'un état sûr, et cela parce que personne n'avait imaginé qu'il faudrait y faire face un jour et assumer les conséquences des choix. Dit autrement dit, plusieurs dizaines de milliards d'€ d'actifs ont été perdus, plusieurs centaines de milliers de personnes déplacées et contaminés… pour ne pas avoir dépensé quelques millions d'€ ?

A noter que les responsables de la maintenance sont particulièrement concernés par les accidents car ils sont les premiers intervenants dans ces situations de crise et ils connaissent le mieux les déficits techniques découlant de budgets insuffisants alloués à la maintenance par les actionnaires ou autres gestionnaires d'infrastructures.

Ce constat nous concerne-t-il dans le ferroviaire ? Nous n'y sommes pas à l'abri d'une catastrophe analogue dans ce monde où s'impose l'informatique critiques et où nous considérons généralement qu'une probabilité de survenance très faible nous délivre d'étudier les conséquences d'un accident et de mettre en place les parades qui éviteraient que l'accident ne finisse en catastrophe.

Ainsi le système européen de contrôle d'espacement et gestion des trains ERTMS a été développé en vue d'assurer l'interopérabilité technique des trains à travers l'Europe et de plus améliorer le niveau de sécurité du transport ferroviaire européen. Or, plusieurs incidents majeurs ont touché des installations homologuées et, pour certaines d'entre elles, mises en service :

- Ligne du Lötschberg (Suisse) en fin 2007 : reprise d'itinéraire sur voie occupée avec déraillement d'un train de fret. Les essais fonctionnels croisés requis par l'Office fédéral des Transports (OFT) suite aux « événements » du Lötschberg devaient révéler, sur les logiciels en exploitation, plusieurs centaines de défauts fonctionnels.
- HSL Zuid (Pays-Bas) en 2009 : Autorisation de mouvement au-delà du point de danger lors d'une marche d'essai Thalys entraînant le report de la mise en service et en exploitation de la ligne jusqu'à la correction des anomalies.
- LGV EE (France) en 2010 : Autorisation de mouvement au-delà du point de danger lors d'une marche d'essai avec une rame d'essais POS. La mise en service de l'ERTMS sur cette ligne a été reportée à fin 2013 afin de corriger en profondeur les anomalies révélées. Les RBC espagnols de même conception ont vu leur homologation retirée.

- Concession Perpignan-Figueras (France –Espagne) en 2010 : non affichage en cabine d'une limitation temporaire de vitesse lors d'une marche d'essai avec une rame DASYE. Anomalie bord qui sera corrigée dans la prochaine version du logiciel bord fin 2011. Les TGV DASYE ont néanmoins conservé leur autorisation de mise en service en ERTMS et sont acceptés sur cette ligne avec la contrainte pour le gestionnaire d'infrastructure de ne pas utiliser ERTMS pour les limitations temporaires de vitesse…

Ces incidents extraits d'une litanie d'événements connus des seuls spécialistes prouvent que la démonstration de sécurité du système ERTMS peut être prise en défaut. Tout acteur responsable de la sécurité proposerait de revoir ces principes que l'expérience montre comme inadaptés à la dangerosité de certaines de nos installations industrielles modernes.

Des dogmes à remettre en cause ?

Dans le cas de la centrale de Fukushima, le premier est celui de la perte des sources électriques consécutive à la submersion des installations. Le second dogme est celui de l'impossibilité de perte de la source froide. Dans les deux cas, qu'aurait coûté de prévoir à la conception des installations de secours, des accès souterrains permettant le repli et la relève des exploitants dans des lieux protégés…, si peu en regard des conséquences actuelles et à venir.

Dans les cas des systèmes informatiques critiques, le premier est celui de la perte d'un fonctionnement déterministe prévu des installations consécutive à la survenue d'une séquence particulière d'entrée. Admettre l'occurrence d'un fonctionnement non envisagé des installations c'est admettre la perte de l'exhaustivité des fonctions de sécurité de l'installation. Le deuxième dogme est celui de la définition d'un système indépendamment du sur-système dans lequel le système va devoir fonctionner. Admettre cette dépendance c'est s'imposer d'étudier comment définir et disposer les interfaces entre système de signalisation et sur-système ferroviaire, c'est reconnaître que les industriels ne disposent pas des compétences requises pour assurer ces analyses. Le troisième dogme est celui de la vision probabiliste des défaillances des logiciels ou qu'ils soient spécifiquement fonctionnels. Admettre cet état de fait, c'est accepter l'absence potentielle de barrières fonctionnelles de sécurité, c'est assumer les conséquences d'un tel manquement ?

Qu'en est-il de l'analyse de ces défauts de sécurité pour les installations ERTMS ? Par rapport aux systèmes informatiques critiques en service actuellement tels que les systèmes de Transmission Voie-Machine (TVM) ou les postes d'aiguillage informatisés, ERTMS a atteint un niveau de complexité jamais vu dans le domaine de la signalisation ferroviaire et a été définis avec une distance inégalée des exploitants et des gestionnaires d'infrastructure historiques. Le code de sécurité dépasse le million de lignes de code pour certains équipements. Les spécifications du système sont morcelées dans un grand nombre de documents, peuvent être ambiguës, lacunaires et parfois même contradictoires ou divergentes. Les spécifications ne sont pas rédigées de façon fonctionnelle : ce n'est qu'une suite d'exigences élémentaires manquant de précision sur l'ordre chronologique de traitement des évènements. Les normes de développement informatique apportent peu de garanties car si elles instaurent des obligations de moyens pour les industriels, elles n'imposent aucune obligation de résultat en matière de sécurité réalisé par le logiciel. Aussi les méthodes de développement utilisées ne permettent pas de garantir que le système informatique sera absolument sûr.

De plus, les équipements ERTMS sont produits par plusieurs industriels en compétition. De ce fait nous sommes passés de systèmes (TVM ou KVB par exemple) qui étaient des boîtes blanches fonctionnelles à une boite noire pour ERTMS. Le gestionnaire d'infrastructure n'en maîtrise plus la description fonctionnelle exhaustive mais on a pu constater que les industriels ne la maîtrisaient pas mieux. Une des causes est la prééminence des informaticiens sur les experts

ferroviaires. La transformation des spécifications du système en code informatique demanderait une étape préalable de raffinement et mise en forme des spécifications du système. Cette étape est réalisée par les informaticiens alors qu'elle n'entre pas dans leur champ d'expertise. Pour finir, la complexité du système ERTMS est devenue telle que le logiciel ne peut être testé de manière exhaustive. Les méthodes de vérification sont lacunaires, ce qui conduit à une approche non maîtrisée de la sécurité.

Qu'aurait coûté la réalisation d'une étude d'ingénierie système capable de lever toutes ces ambigüités fonctionnelles qui minent les systèmes actuellement sur le marché ? Mais qu'aurait coûté de prévoir à la conception des interfaces temporelles, physiques et fonctionnelles claires permettant la validation formelle des fonctions de sécurité des sous-systèmes de signalisation ? Et si la survenue d'un incident contraire avait été admise, qu'aurait coûté la conception d'un jeu de fonctions externes capables de contenir les dangers pour les circulations sans les mettre en danger et risquer de tuer des passagers ou de contaminer l'eau ou dans l'air ?

Il est plus que temps de revoir l'approche probabiliste des risques, notamment pour ce qui est du logiciel, car elle ne nous met pas à l'abri des catastrophes.

Faut-il donc attendre que sombre un Titanic informatique pour redevenir raisonnable?

Le Titanic fut le fruit d'une ère de progrès industriels, la confiance dans un avenir ou les hommes maitriseraient la nature. Ce fut le premier bateau insubmersible, l'armateur et le capitaine étaient confiants. La probabilité de heurter "mal" le Titanic est de le couler étaient jugées négligeables... L'expérience a montré que si faible qu'elle soit, la probabilité a permis l'accident, la vision économique a, par l'absence de canots, tué nombre de personnes... Et pourtant, il, n'est pas question de dire qu'il ne faut pas construire de Paquebot, mais qu'il faut rester raisonnable, pragmatique, ne pas assujettir la sécurité à l'économique. Il a fallu des morts médiatisés pour que le monde change.

L'informatique est omniprésente dans les systèmes de la vie courante, les systèmes vitaux... La confiance est telle aujourd'hui que les tailles des systèmes sont croissantes, sans limites, sans se poser la question de comment valider ses fonctionnalités ? Déjà faire une vérification est une inconnue (sûr que « ce qui est fait » égale « ce qui spécifié »), alors une validation (sûr que « ce qui est fait » égale « ce qui est nécessaire in situ », y c. les modes dégradés) l'est davantage encore. L'expérience montre les limitations du système : automobile, aéronautique, ferroviaire… Quand les problèmes sont identifiés, le constructeur dit qu'il ne sait (pas ou plus) corriger le défaut... qu'il faut vivre avec. Faut-il attendre un Titanic informatique pour réagir ? Ne peut-on pas, malgré la concurrence, redevenir raisonnable ? Oublier un moment le leitmotiv tant rabâché par nos industriels, « la sécurité est l'argument des protectionnistes » ?

La maîtrise des systèmes informatiques de signalisation, critiques et complexes, est un challenge d'aujourd'hui et de demain pour les gestionnaires d'infrastructure. L'expérience montre en effet que près des ¾ des accidents ou incidents techniquement contraires à la sécurité sont dus aux spécifications du fonctionnel, à la définition incomplète des interfaces, du domaine des entrées. L'expérience montre que les méthodes classiques, le commissioning des systèmes critiques avec les « doubles regards » et les « experts AEOQA », les essais avant mise en service etc. ont montrés leurs limites, leur efficacité limité devant la complexité croissante des systèmes informatiques modernes et de leurs interfaces avec le sur système ferroviaire.

Un défit s'offre aux signalisateurs : la recherche et la mise en œuvre de méthodes de validation exhaustive du fonctionnel d'un nouveau système dans le cadre du futur sur système devant

l'accueillir, de ses propriétés de sécurité devant être garanties quelques soient les combinaisons possibles des entrées. En effet, s'il existe une possibilité de mettre en défaut un système ferroviaire, le fait est que tôt ou tard, celle-ci va apparaître (les systèmes sont nombreux et fonctionnent 24/h sur 24 pendant de nombreuses années sans interruption)

L'évolution des méthodes et processus de démonstration de la sécurité inhérente aux nouvelles technologies est un enjeu majeur pour les systèmes de signalisation. Le recours aux **méthodes formelles**, comme c'était le cas déjà avec les postes mécaniques, apparaît comme une piste attrayante. Si le monde de l'aéronautique s'y est d'ores et déjà orienté (DO178C), les industriels du monde du ferroviaire s'y refusent toujours, voyant là un surcroit onéreux d'efforts inutiles.

Est-il, possible de faire plus sur et pas plus cher ? La réponse est oui ! Ceci qui rend l'entêtement actuel encore plus criminel. Oui mais en revenant à des principes d'ingénierie système, d'architecture et de spécification qui ont sait leurs preuves :

- subsidiarité / non centralisme des fonctions viables ;
- moyens de communication dédiés fiables et déterministes ;
- isolation avec le monde extérieur / pour espérer faire une preuve de sécurité ;
- systèmes discret à nombre d'états dénombrables ;
- des interfaces physiques et informationnelles claires en sous systèmes ;
- éviter de modifier en même temps, le quoi, le pourquoi et le comment ;
- prise en compte des modes dégradés, des gestions de crise, de la maintenance à la conception…

Une question de fond se pose à nous autres chargés de la signalisation et des systèmes d'exploitation : quelles seront les modes d'exploitation et de maintenance de la signalisation dans 10 ans ou davantage (le futur) ?

- Par mode d'exploitation nous entendons, autant en modes nominaux, peut être différents selon la typologie des lignes et avec différents niveaux d'ERTMS, qu'en modes dégradés la gestion de situations qui vont nécessairement se produire. Les difficultés procèdent de la centralisation des acteurs, de la disparition des acteurs sur le terrain, de l'accroissement des répercussions consécutives à certaines pannes, notamment celles considérées comme suffisamment improbables (ou trop onéreuses) pour ne soit pas pris en compte des conséquences d'un accident réputé ne jamais pouvoir survenir ;

- Par maintenance nous entendons notamment la gestion de la pérennité des différentes couches d'installations (les travaux d'infrastructure ne peuvent se réduire à remplacer les installations de sécurité tous les 15 ou 20ans), la démonstration de la sécurité des systèmes informatiques (démonstration initiale et suite à des modifications; ne vaut-il pas mieux assurer une démonstration logique plutôt qu'un exposé probabiliste ?), la gestion des compétences métier (en cas d'intervention sur les installations de sécurité en service) et l'intégration des installations de sécurité dans un contexte culturel et technique existant.

En soit rien de méchant, rien de compliqué, bien au contraire. Il s'agit juste de ne pas jouer aux apprentis sorciers quand il s'agit de la vie des autres, d'autant que la responsabilité reste aux gestionnaires d'infrastructures, impuissants. Mais peut être est-ce trop demander.

C'est dans le dialogue entre les gestionnaires d'infrastructures et les fournisseurs que ces questions pourront être réglées, avantageusement pour le système ferroviaire et, par là, pour la société et les clients. Une chose est sure, la solution n'est ni uniquement technique, ni uniquement organisationnelle ; la question de la démonstration de la sécurité des systèmes informatiques sera un point important. Et certaines dérives ont déjà pu être observées, tant sur des systèmes en exploitation qu'en essais avant mise en service…

Le Chemin de fer a toujours jusqu'ici fait la preuve de sa capacité à intégrer l'évolution technologique. Il s'agit néanmoins de gérer avec professionnalisme le passage à l'informatique (changement simultané de quoi, pourquoi et de comment) car il présente un écart significatif tant dans le maintien des compétences, de la pérennité des systèmes, de leur niveau effectif de sécurité, des conséquences aux défaillances de fait. Le « juste niveau » de centralisation des équipements est aussi un point important à prendre en compte lors de la spécification que de la réalisation des nouveaux systèmes informatiques, y compris vis à vis des pannes de mode commun (essentiellement liées aux réseaux numériques et aux alimentations en énergie des réseaux), des défaillances systématiques ainsi que de la nouvelle menace avérée du « terrorisme informatique ».

Nous sommes à l'ère des grands Paquebots de l'informatique ferroviaire. N'attendons pas l'accident du Titanic pour prendre les bonnes postures et mettre en œuvre les bonnes solutions !

A quand la généralisation des méthodes formelles pour les nouveaux systèmes dans le ferroviaire ?

Les voies de progrès

Si l'on poursuit dans la voie actuelle, nous perdrons la maîtrise technique du système. Une nouvelle approche est nécessaire afin de poursuivre les développements d'ERTMS en maîtrisant la sécurité, en réduisant les coûts et les délais d'homologation.
Deux actions sont proposées :

- Raffiner les spécifications
- Cadrer la méthode de développement des logiciels (méthodes formelles)

Ces deux actions sont complémentaires car vu la taille du système il ne serait pas possible de faire une seule preuve de sécurité. Il faudra faire une ségrégation des fonctionnalités avec des indépendances fortes afin de tester et prouver le système par morceaux.

Raffiner les spécifications

A partir des spécifications européennes du système, rédiger une spécification raffinée, fonctionnelle avec des indépendances fortes entre les fonctions.
D'un point de vue méthodologique il faudrait réécrire les spécifications pour les rendre exhaustives, cohérentes, non ambigües, testables et prouvables. C'est la spécification formelle rédigée en langage formel et compréhensible par les experts en signalisation, en exploitation ferroviaire et en conduite de trains. Ces spécifications sont alors testées et validées formellement Une première preuve de sécurité pourrait être apportée à cette étape.
Cette spécification formelle ou formalisée serait interprétable par un automate programmable qui la traduirait directement en code informatique.

Utiliser les méthodes formelles

A l'étape suivante, l'industriel pourra utiliser des méthodes de conception formelle qui permettraient de développer le système informatique tout en garantissant in fine le fonctionnel.
L'utilisation de méthodes formelles aboutissant à une preuve formelle du logiciel semble se heurter néanmoins à deux obstacles :

- Le coût très important de mise en œuvre. Ce coût pourrait croître de façon exponentielle avec la taille du système.
- La taille elle-même du système. Pour l'instant il n'y a pas d'exemple de développement formel de plus de 10.000 lignes de code. Or la taille d'ERTMS est de l'ordre du million de lignes de code

Il faudrait alors réserver l'application de méthodes formelles à un noyau critique du code. Pour cela le système aura été à l'étape précédente architecturé et décomposé pour isoler ce noyau critique.

L'application de méthodes formelles sur un système critique de signalisation ne peut se faire sans prise en compte de cet objectif très en amont dans sa conception. Il n'y a en effet pas de génération spontanée de propriétés de sécurité, de postulats ad hoc, d'interfaces judicieuses avec le sur système ferroviaire. Ce fut le cas des postes d'aiguillages mécaniques, conçu pour pouvoir être prouvés formellement selon la méthode Descubes (1896). Reprenant ces mêmes principes, l'ingénierie SNCF a développé il y a maintenant 15 ans le SYMEL (Système modulaire d'équipement des lignes) et le PIPC (poste informatique à base de PC) afin que ceux-ci puissent être prouvés formellement.

Les postes d'aiguillage

Un poste d'aiguillage est une infrastructure permettant de commander les différents appareils de voie et signaux de protection. Sa mission est la gestion des circulations ferroviaires à l'intérieur d'un espace de voies géographiquement délimité. La gestion de ces circulations consiste à former et établir les itinéraires que les circulations ferroviaires peuvent emprunter (c.-à-d. solliciter les ressources utiles, les immobiliser, autoriser le passage d'une circulation, etc.), donner à chaque train des instructions de mouvement en tenant compte de l'état des itinéraires formés et des positions des autres trains. Ces actions se décomposent en opérations élémentaires qui doivent être effectuées « en sécurité », c'est-à-dire dans la certitude d'éviter les collisions et les déraillements. Le poste d'aiguillage permet à un opérateur d'effectuer l'ensemble de ces opérations. L'étape de commande peut être centralisée et réalisée par un sous-système non sécuritaire. Les autres étapes relèvent du niveau de sécurité le plus haut. C'est le rôle du module d'enclenchement informatique du PIPC par exemple. Les installations de signalisation assurent des fonctions de nature combinatoire et séquentielle. Toute perte de fonction suite à une défaillance implique, si le contexte de l'environnement au moment de la défaillance n'est pas mémorisé, la prise de mesure restrictive dont la levée par application de procédures règlementaires a un impact négatif sur le niveau de sécurité et de disponibilité de l'installation.

Le module informatique critique du PIPC

L'application de méthodes formelles repose sur l'expression complète par les experts métier des fonctionnalités attendues, des conditions d'usage et d'environnement, des propriétés de sécurité, le tout en lien avec les fondements du passé. Afin d'anticiper les renouvellements de composant et/ou unités informatiques il est nécessaire de définir exhaustivement les interfaces techniques et fonctionnelles (Figure 1) de nature à permettre le remplacement aisé des constituants à plus faible durée de vie :

- **interface I1** entre les installations de signalisation en technologie informatique et celles à la voie ou en campagne permet des régénérations de l'un ou de l'autre indépendamment. Ces interfaces retenues aujourd'hui sont celles du NS1 ;
- **interface I2** entre les plates-formes physiques (architectures informatiques) et les fonctionnalités requises par le plan de voie et les exigences d'exploitation.

Valorisons les enseignements du passé : les installations les plus sûres, les plus fiables, les plus durables sont les plus simples quant elles sont conçues en adéquation avec leur environnement et

leurs conditions d'usage. Pour le développement d'un système ferroviaire, les frontières doivent être définies fonctionnellement, règlementairement et physiquement. Le fonctionnel reste alors compliqué et non complexe, les états accessibles sont finis déterministes et le système est décidable.

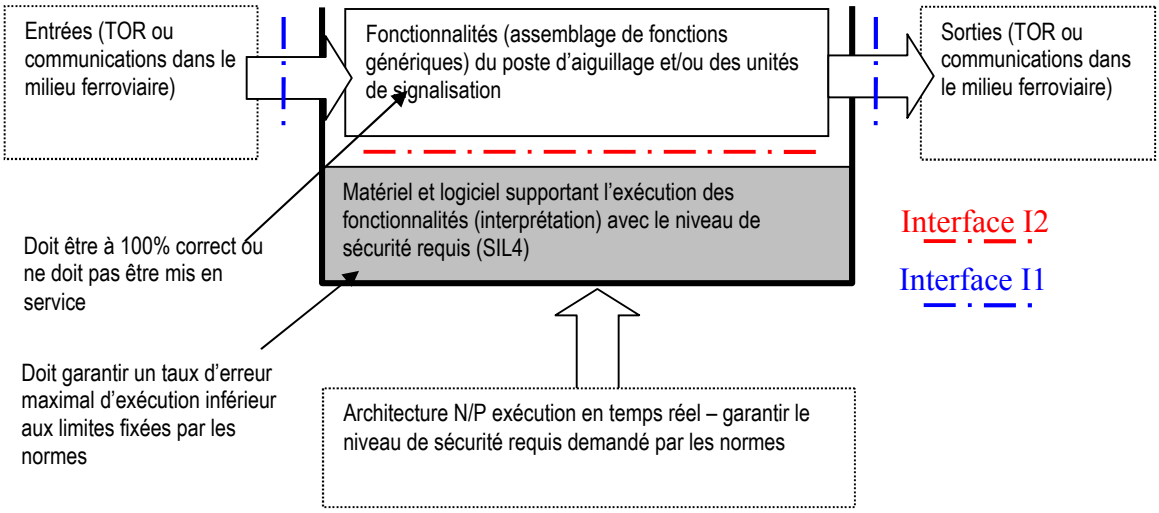


Figure 1 : Architecture d'un système informatique – Interfaces I1 et I2

L'idée principale consiste à développer un automate industriel, de sécurité disposant d'une chaîne de développement réutilisable. Cet automate se comporte comme une machine abstraite (un « automate concurrentiel à contraintes » à temps de transition nul) dont les propriétés rendent possible une validation formelle ultérieure. L'architecture du logiciel du MEI repose sur :

- un ensemble d'automates à états finis les spécifications fonctionnelles pour les trois modes de fonctionnement (initial, nominal et dégradé). L'exécution des fonctionnalités est assurée par la structure d'accueil. Une preuve formelle est apportée sur les spécifications afin de garantir la conservation des propriétés de sécurité et l'absence de conditions surabondantes ;
- une structure d'accueil assurant la gestion des ressources en sécurité et offrant à l'application des services sécurisés. Cette structure d'accueil est indépendante de l'application ;
- un fichier de paramétrage système décrivant l'affectation physique des entrées et des sorties du système selon la configuration du site.

Les fonctions du logiciel de base et du logiciel fonctionnel sont illustrées par la Figure 2 :

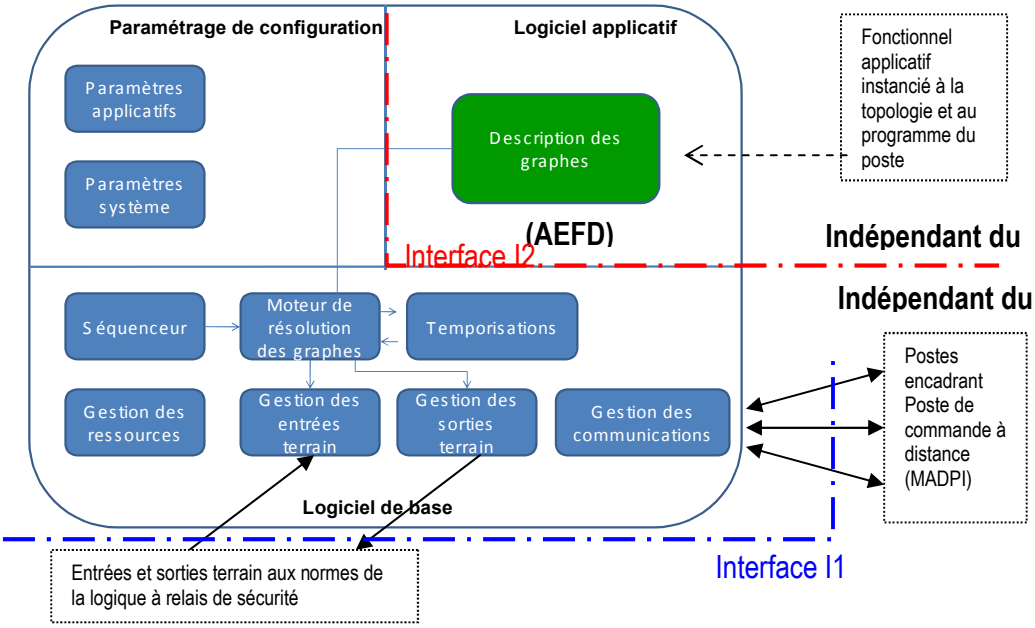
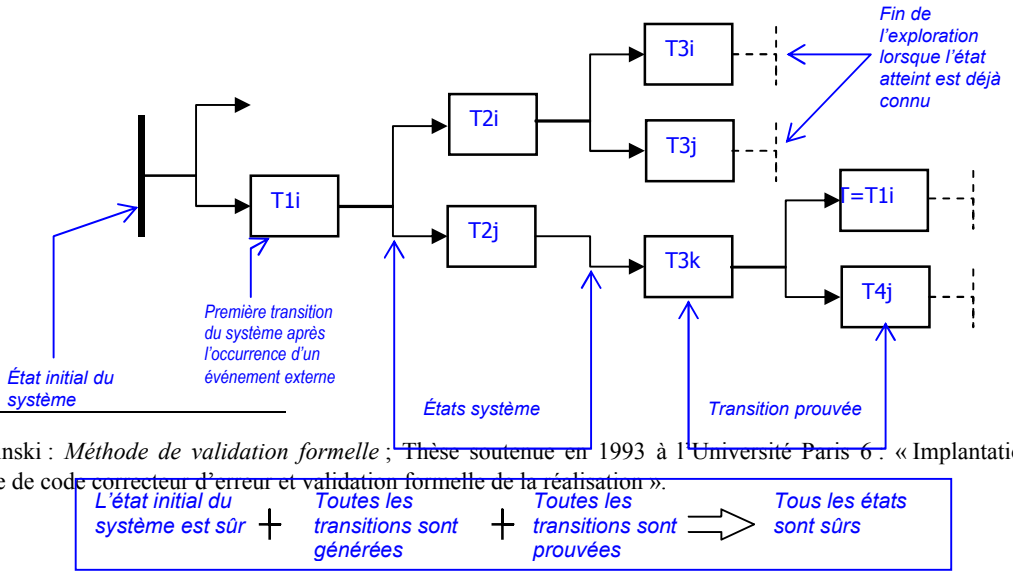


Figure 2 : Architecture logicielle du MEI

Méthode de validation formelle

Il s'agit de valider formellement le fonctionnel conçu humainement à partir de règles fruits de l'expérience : c'est une méthode de validation formelle des propriétés de sécurité. Celle-ci doit garantir que les fonctions et états du module d'enclenchement restent toujours compatibles avec son fonctionnement sûr et de celui de son sur-système. La méthode de validation formelle est issue de travaux universitaires[1] [7]. Utilisé avec le MEI, elle couvre l'ensemble du cycle de la spécification à la validation en passant par l'exécution et elle repose sur une preuve mathématique. Elle s'applique non pas sur un « *modèle* » mais sur le code cible, vérifié que le système suit toutes les propriétés de sécurité et les propriétés fonctionnelles attendues.

La méthode utilise le fait que le module d'enclenchement informatique est strictement déterministe et que le fonctionnel est interprété en temps réel à partir des graphes fonctionnels : le nombre d'états du système est fini. Son application est possible sans besoin de connaissances spécialisées en mathématiques. L'écriture des propriétés de sécurité est directe sous forme de graphes ; elle peut être réalisée par exemple par des signalisateurs. Les principes de la méthode sont simples : « S*i une propriété est vraie dans un état marqué et si la conservation de cette propriété pendant la transition qui suit cet état est garantie la propriété sera vraie dans le nouvel état occupé. La démonstration peut être continuée aussi longtemps que la propriété est préservée* ». (Figure 3)



[1] P. Bielinski : *Méthode de validation formelle* ; Thèse soutenue en 1993 à l'Université Paris 6 : « Implantation VLSI d'un algorithme de code correcteur d'erreur et validation formelle de la réalisation ».

Figure 3 : Principe de la preuve formelle

L'outillage associé à la Méthode

L'application industrielle de la méthode exige le développement d'outils afin de définir les propriétés de sécurité, évaluer leur conservation pour chaque transition entre états du système, définir un état initial où toutes les propriétés de sécurité sont vraies et, enfin, évaluer les propriétés de sécurité à chaque transition entre états de système.

L'ingénierie SNCF a développé un ensemble d'outils permettant de réaliser industriellement les traitements nécessaires à la réalisation de la démarche décrite précédente permettant la réalisation des essais utiles avant mise en exploitation.

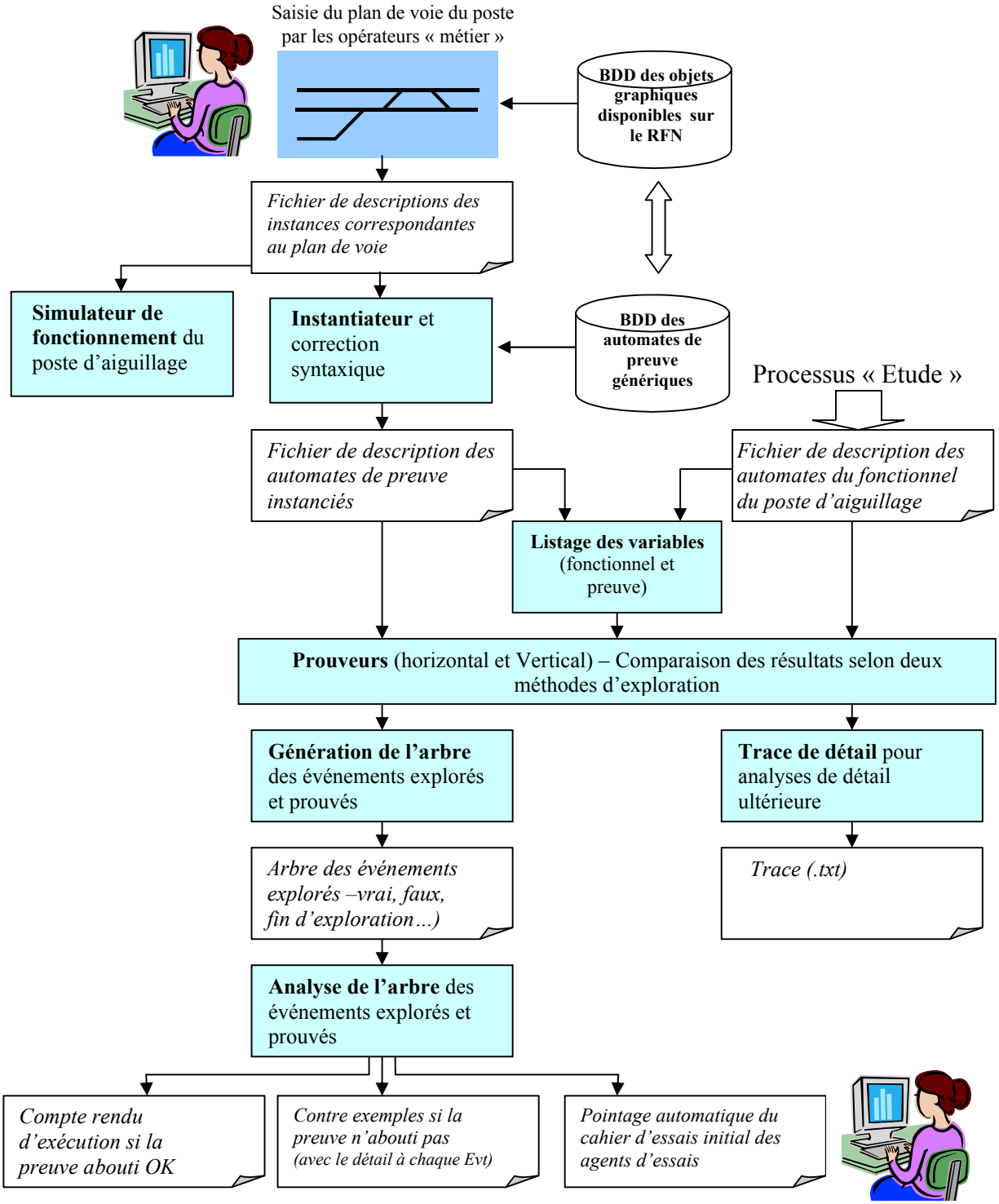


Figure 4 : Processus de validation formelle

En guise de Conclusion

Dans le ferroviaire, notamment dans la signalisation ferroviaire, ce qui s'est passé au Japon montre qu'il n'est plus admissible cautionner l'état criant des déficits de prise en compte des conséquences d'accidents réputés ne jamais pouvoir survenir[2]. Ces accidents peuvent devenir des catastrophes quand les conditions du rétablissement d'un état sûr n'ont pas été anticipées, et cela parce que personne n'avait imaginé[3] qu'il faudrait y faire face un jour. Autrement dit, le ferroviaire peu perdre des centaines de millions d'€ d'actifs et une crédibilité pour ne pas avoir dépensé quelques de millions d'€ ? Il est plus que temps de revoir l'approche probabiliste des risques car elle ne nous met pas à l'abri des catastrophes. Il est plus que temps de réagir sans attendre un nouveau Titanic industriel, un Titanic ferroviaire en particulier.

Les principales difficultés de développement d'un système informatique de signalisation à haut niveau de sécurité concernent la prise en compte à la conception de son intégration dans son futur sur système ferroviaire. Cette étape est primordiale pour que les apports des systèmes informatiques et des communications numériques afférentes soient valorisés et leurs faiblesses minimisées. Il s'avère ainsi que lors de la définition de tout nouveau système informatisé de signalisation, le gestionnaire de l'infrastructure et le mainteneur doivent être associés dès le lancement du projet, notamment pour définir le niveau de maîtrise technique souhaité au vu de leurs objectifs stratégiques et le mode de spécification fonctionnelle garantisse le niveau de maîtrise souhaité au regard des options techniques requises pour une intégration dans le sur système ferroviaire. A l'évidence les spécifications purement fonctionnelles ne sont pas suffisantes pour obtenir un système validable formellement et maintenable sur toute la durée de vie du système. Notre développement a montré qu'il est possible de réaliser des automatismes de sécurité à coûts maîtrisés, pérennes et validables. Il a notamment été possible de montrer que l'utilisation d'une méthode formelle en lieu et place des essais traditionnels permettait de réduire d'un facteur 5 les coûts, tout en donnant évitant de prendre un risque que l'on ne saurait raisonnablement assumer.

\- - - - - - -

[2] Même si certains se sont déjà produits sans victimes humaines…

[3] Ou parce qu'une analyse coûts-bénéfices (CBA) n'avait jugé économiquement opportun de mettre en œuvre les mesures palliatives ou de réduction de l'effet des conséquences. Les exemples dans le ferroviaire sont nombreux, rappelons-nous Echegen : le risque était connu au point que la SNCF s'est toujours refusé de mettre en œuvre le type d'essieu incriminé, la DB a pris le risque et l'on connaît la suite pour 101 passagers…

Encadré :

Accident survenu sur ETCS niveau 2 sur la ligne du tunnel du Lötschberg - Traduction de l'Allemand par l'auteur – Encadré de l'article de décembre 2007 de la revue « Eisenbahn Revue »

Un système de signalisation conçu de manière non sure ?

Le système de signalisation ferroviaire reflète l'histoire des accidents ferroviaires. Les principes qui sont à la base du haut niveau de sécurité des postes d'aiguillage et des installations de signalisation classiques en général devraient être aussi valables pour les nouveaux systèmes. Mais les stratèges du système ETCS et les programmeurs ont évidemment violé ces principes de base de la philosophie de la sécurité ferroviaire.

- *Comment est-il possible qu'un ordinateur sol ETCS (RBC) reçoive des commandes et les perd ensuite au lieu de les transmettre aux mobiles ;*
- *Comment est-il possible qu'un itinéraire tracé puisse être détruit et remplacé par un itinéraire incompatible sans qu'il y ait eu une vérification du fait que la commande d'arrêt d'urgence a bien été reçue par le train déjà engagé (à l'approche) et qu'il est encore possible de l'exécuter ;*
- *Comment est-il possible que lors des essais avant mise en service cette erreur de principe[4] n'ait pas pu être découverte ?*

Accusé de réception de la commande d'arrêt d'urgence

Le système ETCS vérifie par lui-même si une commande d'arrêt d'urgence ou un raccourcissement de la longueur de « l'autorisation de voie libre » initialement générés par lui-même a bien été reçu : le train envoie un accusé de réception vers le RBC via la liaison GSM-R.

Qu'est-ce qui se passe si l'accusé de réception n'arrive pas ? D'après les dires du responsable de la sécurité du tunnel, l'interface entre le RBC et le poste d'aiguillage électronique (informatique) n'est pas spécifié dans ETCS niveau 2, chaque concepteur (industriel ou gestionnaire de l'infrastructure ?) décide lui-même comment il conçoit et tient compte de cette problématique. Pour cette raison il existe des différences entre les installations sur la ligne nouvelle Matstetten-Rashirst (conçu par Alstom) et sur la ligne du Lötschberg (LBS – conçu par Thalès).

Sur la ligne nouvelle, l'interface est ***unidirectionnelle****. Elle transmet uniquement des informations d'un poste d'aiguillage vers le RBC. Rien ne se passe que l'accusé réception arrive ou non. L'accusé réception de la commande d'arrêt d'urgence va ainsi dans le vide.*

Sur la LBS l'interface fonctionne dans les deux sens : le RBC transmet l'accusé réception vers le poste d'aiguillage permettant le cas échéant de raccourcir le délai de 4 minutes pour la destruction de l'itinéraire. Si l'accusé réception de la part du train manque, le RBC ne peut pas le répercuter sur le poste d'aiguillage. Au poste si rien ne se passe, le délai de 4 minutes est respecté après, les itinéraires incompatibles peuvent être détruits.

La différence entre ces systèmes est donc faible, dans les deux cas, après au plus 4 minutes, le poste d'aiguillage peut tracer un itinéraire incompatible avec l'itinéraire initial. La chaîne de sécurité poste-train d'ETCS niveau 2 n'est pas meilleure qu'avec des systèmes de signalisation classiques. L'erreur lors de la définition de l'interface entre le RBC et le poste est une lacune presque incompréhensible des spécifications d'ETCS qui doit être corrigée au niveau européen.

Disparition d'une commande d'arrêt d'urgence

4

La perte d'un ordre d'arrêt d'urgence lors de l'incident de Frutzen est la suite d'une erreur dans le logiciel de sécurité du RBC de la société Thalès, erreur qui devrait être corrigée à la fin novembre 2007.

Certification

Le BAV exprime qu'ils ont vérifié le résultat du rapport de l'audit de sécurité et qu'ils ont également vérifié si les processus suivis par le fournisseur étaient adaptés pour éviter les « trous » de sécurité[5].

Les conséquences possibles

Il est également intéressant d'imaginer ce qui aurait pu avoir lieu dans des circonstances légèrement différentes. Si le conducteur de la locomotive RoLa n'avait pas eu des doutes et s'il ne s'était pas arrêté de lui-même, son train aurait pu atteindre l'aiguille 34 plus tôt, l'aurait vraisemblablement engagée (prise en talon) avant qu'elle ne change de position et en aurait ainsi interdit sa manœuvre. Par ailleurs, il est difficile d'estimer ce qui se serait passé si la locomotive RoLa avait atteint l'aiguille en mauvaise position avec une vitesse plus élevée[6]*. Dans tous les cas, on ne doit pas imaginer ce qui se serait passé si le train postal évoluant en direction inverse avait également atteint l'aiguille 34, prenant en écharpe la locomotive RoLa.*

Cette fois, toutes les intervenants impliqués ont eu de la chance. L'incident s'est terminé sans catastrophe et il a permis de détecter des trous de sécurité que la phase d'essai qui a durée plusieurs mois n'avait pu mettre à jour, ce avant que des incidents plus graves d'arrivent après la montée en charge de la ligne.

---

[5] NB : vérifications « papier » que les procédures qualité prescrites par les normes ont été respectées par les fournisseurs – les essais réalisés avant mise en service ont été réalisés par le fournisseur sous la forme de « scenarii » préétablis générés automatiquement (10000 tests) afin de vérifié les fonctions internes du RBC.

[6] NB : vitesse maximale de 200km/h en voie directe, 120km/h en voie déviée, appareil de voie avec pointe de cœur mobile et lame mobile de 80m.