

Utilisation de la méthode formelle B pour un système SIL3 : la commande des portes palières sur la ligne 13 du métro Parisien

The B formal method for a SIL3 sensor system: the control system of the platform doors, line 13 in Paris subway

F. PATIN, G. POUZANCRE et D. SABATIER
CLEARSY SYSTEM ENGINEERING

S. HAUVESPRE et P. SAUVAGE
RATP

Résumé

Nous présentons comment l'emploi de la méthode formelle B alliée à l'emploi de calculs probabilistes a permis de concevoir et de qualifier le système de commande des portes palières employé depuis avril 2006 sur la ligne 13 du métro Parisien. Une étude système globale a d'abord été réalisée avec la méthode B ; une architecture basée sur l'emploi de capteurs redondants détectant des séquences longues et recoupées a ensuite été choisie. La sûreté de l'algorithme de détection a été démontrée avec B dans la limite des perturbations tolérées, et une évaluation probabiliste a permis de s'assurer de l'absence de risque des perturbations non tolérées. En particulier, il a ainsi été possible d'évaluer à quel point le principe de détection en lui-même est infalsifiable.

Summary

In this article, we explain how the B formal method coupled with probabilistic calculus was used for the design and safety approval of the control system for platform doors, in operation on Paris subway line 13 since April 2006. A global system study was first conducted with the B method, and then a design was chosen, based on redundant sensors using long detection sequences with cross checking. In the scope of tolerable perturbations, the safety of the chosen algorithm was then formally proven, and a probabilistic evaluation of the perturbation outside this scope was used to guarantee the safety. In particular, we evaluated how difficult to forge this detection principle is.

Présentation du système

60% des retards subis sur les lignes du métro Parisien sont causés par des intrusions sur les voies. Outre le problème de la sécurité des voyageurs, l'absence de barrière entre le quai et les voies cause donc une diminution importante de la disponibilité du réseau. Bien sur, ce problème n'existe plus sur les nouvelles lignes automatiques équipées de portes palières telles que la ligne 14, mais est-il possible de bénéficier de la même amélioration sur l'ensemble du réseau actuel ? Une ligne existante avec conducteurs peut-elle être équipée avec profit de portes palières ?

Pour répondre à cette question, la RATP procède à un test en vraie grandeur sur les stations St Lazare et Invalides de la ligne 13. Trois quais sur ces stations ont été équipés de portes palières. Le système qui les pilote doit coupler leur ouverture et leur fermeture aux ouvertures et fermetures du train, lesquelles sont effectuées par les conducteurs.



Le système de commande des portes palières employé pour ce test en vraie grandeur doit répondre aux objectifs suivants :

- Il doit garantir la sécurité des usagers pendant toute la durée du test (6 mois)
- Sachant qu'il n'y a que 3 quais à équiper, mais que tous les trains de la ligne 13 passent par ces stations, il convient de minimiser l'équipement des trains.

ClearSy a tout d'abord effectué **une étude formelle** (à l'aide de la méthode formelle B) concernant la sécurité du dispositif envisagé dans son ensemble. En tenant compte de ces résultats, ClearSy a

ensuite conçu et réalisé le système de commande des portes palières, incluant l'étude de sécurité propre à ce système.

L'étude système globale

L'étude système globale effectuée par ClearSy répond à la question suivante :

Sous quelles hypothèses peut-on **garantir** que le système envisagé interdit toute communication illicite entre les espaces voie / quai / train ?

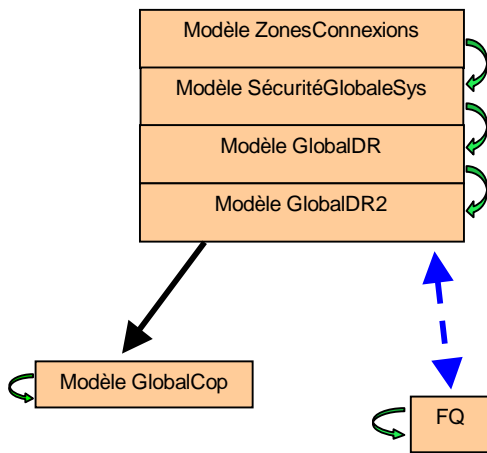
Les hypothèses obtenues portent :

- Sur le comportement de l'équipement « portes palières »
- Sur le comportement du système de commande
- Sur le comportement des conducteurs (et donc des trains)
- Sur les événements particuliers (interventions pompiers, etc.)

Cette étude formelle vient compléter l'étude globale de sûreté effectuée par la RATP, qui détermine les événements redoutés, classe leur gravité et étudie / quantifie les causes possibles. L'étude formelle permet de **se prémunir contre les erreurs de raisonnement** qui pourraient entacher l'étude des causes pouvant mener aux événements redoutés créant des communications illicites entre les espaces voie / quai / train.

Le fait de disposer d'une liste exhaustive des hypothèses nécessaires à la preuve de la garantie citée précédemment est un atout important. Par exemple, comme les trains repartent sur décision du conducteur, lequel s'assure de la fermeture effective des portes palières grâce à un signal sur la voie, nous avons du insérer une hypothèse particulière sur le fait que ces portes palières ne doivent en aucun cas mémoriser un ordre d'ouverture et l'honorer avec retard. Si c'était le cas, alors le conducteur pourrait prendre la décision de partir alors qu'un ordre d'ouverture est latent. La preuve formelle nous donne **la garantie que toutes les hypothèses de ce type ont été formulées**.

L'étude formelle est constituée d'une architecture de modèles B, liés par des liens de raffinement et démontrés suivant les règles de la méthode B, via les outils B (Atelier B et B4Free) :



Dans ce schéma :

- ZonesConnexions est l'énoncé formel de la propriété « pas de communication illicite entre les espaces voie / quai / train »
- GlobalCop est l'énoncé formel des hypothèses prises sur le système de commande des portes palières, que nous retrouverons plus loin,
- FQ (« Façades de Quai ») est l'énoncé des hypothèses prises sur les portes palières
- GlobalDR est le modèle de liaison, qui contient de plus directement les hypothèses prises sur le comportement des trains, des conducteurs et de l'exploitation
- SécuritéGlobaleSys et GlobalDR2 sont des niveaux intermédiaires.

Articulation études formelles / sûreté de fonctionnement

A cette étape de notre exposé, il est utile d'expliquer plus en détails comment une étude formelle telle que la précédente se situe dans une étude de sûreté de fonctionnement.

Précisons tout d'abord qu'aucun système ne peut respecter ses spécifications *quelles que soient les perturbations auxquelles il est soumis*. Autrement dit, il existe toujours un niveau de perturbations qui force le système à faire ce qu'il ne devrait pas. Par perturbations, nous entendons les catégories suivantes :

1. Défauts de conception : bugs informatiques, pièces avec des faiblesses de conception, etc. Il y a deux parades possibles : soit éviter ces défauts (tests, preuves, qualité), soit les tolérer (redondances, mécanisme de détection, mécanismes de tolérance).
2. Pannes matérielles : on admet généralement que tout appareil peut être frappé par des pannes matérielles purement aléatoires, non dues à une mauvaise conception ou à des actions de l'environnement. Parades : redondances, mécanisme de détection, mécanismes de tolérance.
3. Actions de l'environnement : influences électriques, mécaniques ou thermiques non supportées par des éléments du système, actions anormales des systèmes voisins. Parades : soit faire en sorte que le système ne soit pas employé dans des conditions qu'il ne peut supporter, soit augmenter sa résistance (en particulier face aux actions anormales des systèmes voisins).

En toute rigueur, une spécification doit donc être accompagnée du « paysage des perturbations » malgré lesquelles le système doit continuer à la respecter (perturbations simples ou combinaisons de perturbations). On peut alors faire différents niveaux de perturbations associés chacun à une spécification plus ou moins dégradée. Généralement, les niveaux sont les suivants :

1. Aucun défaut de conception, pas de panne matérielle, aucune action anormale de l'environnement : c'est la spécification nominale.
2. Aucun défaut de conception, pas de panne matérielle, mais actions imprévues des systèmes voisins : c'est ce

qu'on appelle souvent la spécification en mode dégradé.

Pour des systèmes non sécuritaires, il n'y a souvent que ces deux niveaux. Pour des systèmes sécuritaires, on inclut généralement un niveau supplémentaire :

3. Spécification : se mettre dans un mode refuge en cas de défaut de conception, de panne matérielle ou d'actions destructrices de l'environnement.

Notons que ce dernier niveau nécessite toujours de bien définir les perturbations supportées, car on peut **toujours** imaginer des perturbations où le système ne pourra pas se mettre en mode refuge ; ce n'est limité que par la vraisemblance des perturbations. Au-delà de ces perturbations supportées, le système n'a généralement plus aucune spécification.

Les activités de sûreté de fonctionnement s'expriment en terme de *fréquences d'événements redoutés*. Ces fréquences sont censées être absolues et ne tenir compte **d'aucune limitation sur les perturbations envisagées**.

Pour garantir la sécurité d'un point de vue sûreté de fonctionnement, il faut donc disposer d'une spécification pour un niveau de perturbation bien choisi, qui permette de garantir que la fréquence absolue des événements redoutés est inférieure aux seuils tolérables. Il suffit par exemple que les 2 conditions suivantes soient vraies :

- cette spécification suffit à interdire les événements redoutés dans le cadre des perturbations tolérées ;
- La fréquence des perturbations **non tolérées dans le niveau choisi** est inférieure aux seuils permis pour les événements redoutés.

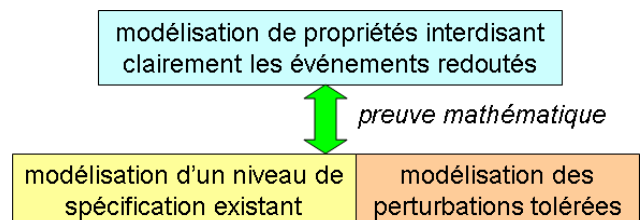
Dans toute cette démarche, un point faible important est que **les erreurs potentielles dans les diverses étapes du raisonnement ci-dessus sont toujours possibles**. Ces problèmes peuvent être :

- La spécification employée peut être ambiguë ou incomplète ;
- Les perturbations tolérées peuvent être pas ou mal définies ;
- Le raisonnement logique montrant que la spécification garantit l'absence d'événements redoutés dans le cadre des perturbations tolérées est peut-être faux ;
- Enfin, la fréquence des perturbations non tolérées peut avoir été mal estimée, ou des sources de perturbations ont été oubliées.

En pratique, ces problèmes risquent d'être prépondérants. Autrement dit,

rien ne sert d'avoir développé un calcul précis de la fréquence d'un événement redouté si à cause d'une faille de raisonnement, l'événement redouté se produit dans des cas non prévus.

C'est pour éviter ce genre d'erreur que Clearsy réalise des études formelles. Nous utilisons ces modélisations formelles suivant le schéma ci-après :



Comment cette activité de modélisation adresse t-il les problèmes cités précédemment ?

- **La spécification employée peut être ambiguë ou incomplète** : la modélisation formelle incite à une

grande rigueur. Après chaque modélisation d'un niveau de spécification, nous détaillons la traçabilité entre la spécification après formalisation ayant permis la preuve, et les sources d'informations dans les documents. Les interprétations que nous avons du faire, les informations non trouvées et les problèmes potentiels sont révélées.

- **Les perturbations tolérées peuvent être pas ou mal définies** : même action que ci-dessus, la modélisation formelle impliquant une définition précise, que nous traçons ensuite dans les spécifications sources.
- **Le raisonnement logique montrant que la spécification garantit l'absence d'événements redoutés dans le cadre des perturbations tolérées est peut-être faux** : le raisonnement qui garantit que les propriétés modélisées sont tenues par les spécifications modélisées est **prouvé mathématiquement**. Attention, l'erreur reste possible dans les raisonnements de liaison avec les documents sources ou avec les événements redoutés.
- Enfin, **la fréquence des perturbations non tolérées peut avoir été mal estimée, ou des sources de perturbations ont été oubliées** : l'activité formelle développée ici n'a pas pour objet de remplacer les calculs de fréquence de perturbations ou d'événements redoutés. Ce calcul reste donc à faire, notons néanmoins que la modélisation des perturbations permet d'imaginer celles-ci d'une manière plus systématique.

En résumé, les études formelles viennent **assurer** les raisonnements faits dans l'étude de sûreté de fonctionnement en garantissant qu'en l'absence des perturbations ou des combinaisons de perturbations intolérables, le système tient parfaitement les propriétés de sécurité.

Solution choisie pour réaliser le système de commande des portes palières

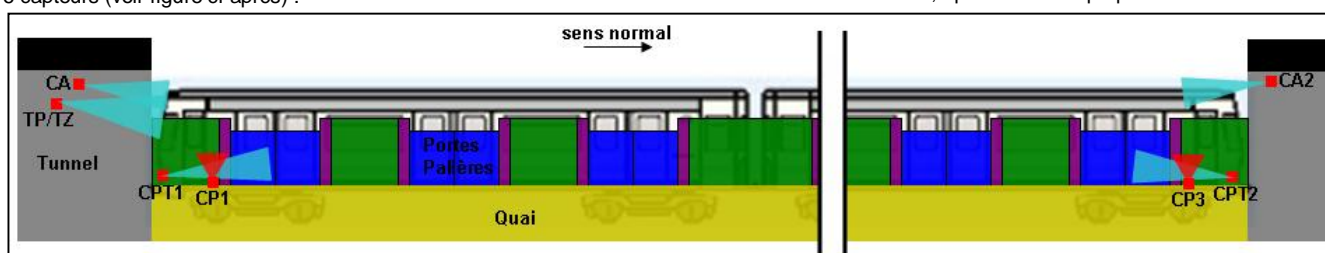
Après cette parenthèse à propos de comment les études formelles s'articulent par rapport à l'analyse de sûreté de fonctionnement, revenons aux portes palières. L'étude système globale a permis de mettre en évidence une propriété fondamentale pour le système de commande des portes palières, baptisé COPPILOT. Cette propriété est la suivante :

COPPILOT ne doit jamais commander l'ouverture des portes palières dans une situation autre que celle où un train est présent et :

- Il ne laisse aucune portion de voie découverte sur une porte palière
- Il est immobile
- L'entrée dans ce train n'est pas dangereuse (c'est un train de voyageur ou un train fermé)

Cette interdiction nous donne donc l'événement redouté pour le système COPPILOT de commande des portes palières, auquel l'analyse de sécurité a affecté un niveau SIL3 suivant la norme 61508 : cet ER doit se produire à une fréquence inférieure à 10^{-7} occurrences / heure. Le système constitué de COPPILOT + portes palières + trains avec conducteurs est sûr si COPPILOT respecte cette condition, les deux autres sous systèmes devant respecter d'autres conditions spécifiques.

Pour réaliser un système de commande capable de donner cette garantie, ClearSy et la RATP ont choisi une conception basée sur 6 capteurs (voir figure ci-après) :



- Deux Capteurs de présence train infra-rouges CP1 et CP3, à chaque extrémité du quai ; toutes les portes palières à commander sont situées dans l'espace entre CP1 et CP3.
- Deux capteurs d'arrêt (CA) qui permettent de détecter l'arrêt du train.
- Un télémètre qui a deux fonctions : il détecte la présence d'un train (TP) et il permet aussi de contrôler que le train est aligné dans une zone précise où les portes palières sont considérées comme utilisables (TZ).
- Deux capteurs de portes à hyperfréquence (CPT1 et CPT2) pour repérer le mouvement de 2 des vantaux des portes du train. Les capteurs mesurent les mouvements sur le flanc du train. Chaque capteur est équipé de 2 sorties, ce qui donne au total 4 signaux : CPT1n, CPT1i, CPT2n, CPT2i. (n détection d'un mouvement dans le sens normal du train, i détection dans le sens inverse au sens normal).

L'idée fondamentale de cette conception est de séparer deux fonctionnalités :

- I. La reconnaissance des conditions nécessaires à la sécurité, c'est-à-dire la présence d'un train **de voyageurs, positionné et arrêté**. Ceci est obtenu en observant sur **tous les capteurs à la fois** la séquence de détection produite lors de l'arrivée et de l'arrêt du train, et une fois les conditions reconnues en surveillant sur **chaque capteur** tout signe indiquant le départ du train.
- II. La reconnaissance de l'ouverture et de la fermeture de deux des portes trains, qui se fait avec les deux CPT.

Ainsi la première condition permet le « déverrouillage » du système d'une manière sécuritaire, tandis que la partie fonctionnelle contenant la détection des mouvements de porte train est séparée. Mais les portes palières ne peuvent s'ouvrir que si le déverrouillage a bien eu lieu.

On se doute que la sécurité est recherchée à la fois par la **redondance** des capteurs et par l'observation de **séquences de mesures recoupées** sur ces capteurs. Nous allons voir comment la démonstration de sécurité d'un tel système a été conduite.

Preuve de l'algorithme dans le paysage de perturbations choisi

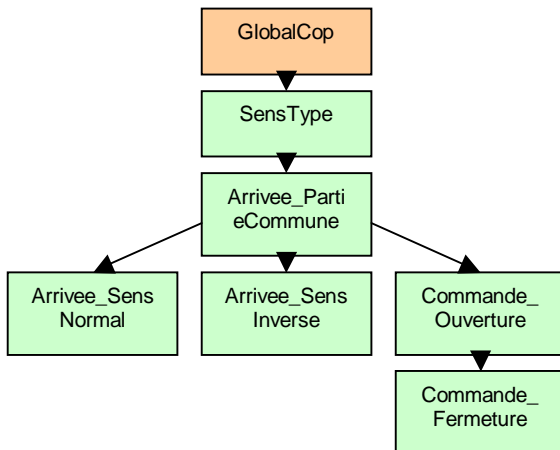
Les 6 capteurs dont nous avons parlé produisent des signaux TOR (tout ou rien) simples qui sont conduits sur un calculateur, lequel prendra la décision d'ouvrir ou de fermer les portes palières. Ce calculateur est le cœur du système, pour COPPILOT nous avons choisi un automate programmable SIEMENS SIMATIC possédant une homologation TÜV compatible avec le niveau SIL3 visé.

Bien entendu, le système ne peut être sécuritaire que si le programme applicatif chargé dans cet automate est exempt d'erreurs. Pour obtenir cette condition nécessaire, la méthode formelle B a été employée. La preuve mathématique effectuée consiste à partir d'une définition précise des séquences de signaux TOR que seuls les trains de voyageurs faisant une arrivée correcte sont censés produire, à démontrer que cet algorithme ne produit l'ordre d'ouverture que pour de tels trains. L'architecture de modèles B est constituée des modèles suivants :

- GlobalCop : c'est le modèle repris de l'architecture de démonstration, qui énonce la propriété « COPPILOT ne

doit ouvrir que pour un train de voyageurs, positionné et arrêté »

- SensType : dans ce modèle apparaissent les différents types de trains (voyageurs, travaux, etc.) caractérisés par leurs propriétés en terme de signaux de détection et de sens d'arrivée
- Arrivee_SensNormal, Arrivee_SensInverse, Commande Ouverture et Commande Fermeture sont les modèles qui décrivent l'algorithme concret, en terme d'automates faisant évoluer des variables d'état du programme
- Arrivee PartieCommune est le modèle de liaison.



Au terme de ce processus, nous obtenons une définition écrite en B de l'algorithme du futur programme, défini comme des automates à états. Autrement dit : une spécification du programme quasi exécutable.

A ce stade, il serait logique de traduire cette « spécification très détaillée » en code par l'action d'un outil automatique. Néanmoins, l'automate programmable employé impose l'emploi d'un langage de programmation graphique issu de LADDER pour la création d'applications sécuritaires, avec saisie manuelle dans la suite de programmation graphique. Il n'est pas facile d'insérer dans ce processus un code traduit à partir des modèles B tout en respectant les préconisations de l'automate. Pour cette raison, la programmation graphique a été effectuée à partir des modèles par un processus non automatisé, tracé par des documents de conception détaillée conformes aux préconisations des normes 61508 et 50128 pour le niveau SIL3. Les procédures classiques de test (validation et vérification) ont été appliquées, conformément à ces normes.

C'est pourquoi nous parlerons de preuve d'algorithme et non de preuve de programme. Cette preuve donne la garantie que si une ouverture à tort se produit, **cela ne peut pas être du à un cas imprévu dans la complexité de l'algorithme** qui se déclencherait sur un paysage de détections par ailleurs prévu.

Analyse et démonstration de sécurité

A cette étape de notre article, nous avons obtenu les éléments suivants :

- La sécurité globale est obtenue si le système COPPILOT ne commande l'ouverture que pour des trains de voyageurs, positionnés et arrêtés.
- L'algorithme chargé dans l'automate est correct, c'est-à-dire qu'il ne commande l'ouverture qu'en présence d'une suite de mesures sur les capteurs qu'on suppose ne pouvoir être produite que par des trains de voyageurs, positionnés et arrêtés.
- L'automate programmable employé est sûr (technique de processeur sécuritaire codé, modules d'entrée sortie TOR sécurisés). Autrement dit, la fréquence d'événements où, à la faveur de perturbations électriques dans le processeur, d'erreurs de compilation ou de défauts électriques dans les E/S TOR, l'automate

aurait un comportement anormal autre que la mise en état refuge, est compatible SIL3.

Il reste néanmoins une question importante à laquelle nous devons répondre :

Est-il possible qu'à cause d'objets divers se déplaçant devant les capteurs, ou à cause d'influences diverses sur ces capteurs, une ouverture soit commandée alors qu'il n'y a pas un train de voyageurs positionné et arrêté ?

Dans la preuve de l'algorithme, nous avons formulé l'hypothèse que *seul un train de voyageurs positionné et arrêté a pu produire une séquence de détection ayant les propriétés voulues*. En fait on peut toujours imaginer des objets simulant le vrai train, mais de telles simulations sont improbables. Il nous faut maintenant **recourir à une évaluation quantifiée** pour savoir à quel point elles sont réellement improbables.

La méthode employée pour faire cette évaluation consiste à considérer chaque source de perturbation possible comme un événement aléatoire, caractérisé par sa fréquence moyenne d'occurrence λ (occurrences / heure). On considérera par exemple que les objets parasites pouvant passer devant un capteur infrarouge constituent une source de sorties à 1 à tort pour ce capteur, se produisant de manière aléatoire en moyenne toutes les $1/\lambda$ heures. Une fois recensées toutes ces sources de perturbations, nous employons un raisonnement combinatoire pour en déduire la fréquence des ouvertures à tort.

Le raisonnement est le suivant : si une ouverture à tort se produit à cause des perturbations sources envisagées, alors cet événement a forcément été précédé d'une séquence de ces perturbations. Si N sources ont été envisagées, la première des perturbations de la séquence ayant conduit à l'ouverture à tort est forcément l'une d'entre elles : nous débutons ainsi N cas. Pour chaque cas, la perturbation suivante doit agir avant que l'effet de la première ait disparu ou ne puisse plus être dangereuse : par exemple, une torsion du support d'un capteur infrarouge qui provoquerait une sortie à 1 en permanence n'agit au maximum que pendant la durée de stationnement d'un train. En effet : une fois le train parti, comme *aucune* séquence d'arrivée normale ne débute par un « 1 » sur l'un des capteurs infrarouges, plus aucune ouverture ne sera jamais produite.

Nous avons alors N possibilités pour poursuivre la branche ainsi débutée, la seconde perturbation pouvant être n'importe laquelle des N sources envisagées. On obtient ainsi « arbre de parcours de séquence » où chaque feuille serait caractérisée par une fréquence d'occurrence de l'ouverture à tort : l'addition des feuilles donnerait la fréquence globale.

En pratique, lors du déroulement de l'arbre des séquences on arrête l'examen d'une branche dès que la fréquence d'occurrence devient trop faible, ou que la branche est clairement négligeable devant une autre branche qui est entièrement visitée. Sachant qu'il y a environ une trentaine de sources de perturbations envisagées, l'arbre aurait sans ces simplifications un bien trop grand nombre de feuilles !

Le calcul employé pour obtenir la fréquence d'occurrence d'une séquence de perturbations est le suivant : si λ_1 est la fréquence d'une première source E_1 , si λ_2 est la fréquence de la seconde perturbation E_2 devant se produire moins de T après E_1 pour être nocive :

- Le rapport entre les périodes de T où E_2 peut agir, comparée à l'écart moyen entre deux événements E_1 égal à $1/\lambda_1$, tend sur une durée infinie vers $T\lambda_1$ (ou plus précisément $\min(1 ; T\lambda_1)$ pour tenir compte du cas où $T > 1/\lambda_1$)

La fréquence cherchée est donc :

$$F = \min(1 ; T\lambda_1) \times \lambda_2 [1]$$

Dans notre cas, T est souvent lié aux paramètres d'exploitation des trains : durée de stationnement, écart entre les trains, etc.

Dans le cas de perturbations fugitives telles que les objets pouvant causer des détections à tort devant les capteurs infrarouges, il est difficile de savoir combien de temps la perturbation va durer. Pour éviter ce problème, nous avons pris un principe conservatif : la perturbation fugitive est toujours considérée comme durant assez longtemps pour que la perturbation suivante puisse être nocive et faire progresser vers l'ouverture à tort.

Une caractéristique intéressante de la formule [1] est que toute perturbation permanente dont la période de nocivité n'est pas négligeable devant son intervalle moyen d'occurrence contribue avec un facteur 1. Autrement dit, un défaut permanent sur un capteur (défaillance d'un composant, désorientation du support...) qui affaiblit le système sans être détecté, doit être considéré dans le calcul comme **se produisant toujours**. Ceci a conduit à l'ajout de fonctions particulières dans le programme applicatif : par exemple, il est extrêmement improbable que tous les capteurs tombent en panne lors du stationnement d'un même train d'une manière qui ferait que l'automate resterait déverrouillé après le départ du train (fréquence meilleure que SIL4). Néanmoins si ceci se produit, alors on pourrait imaginer que l'exploitation reste possible : si les capteurs CPT fonctionnent encore (perturbés seulement au départ du premier train), COPPILOT commanderait les portes palières apparemment normalement, mais en fait en « croyant » traiter indéfiniment le même train ! Ceci est rendu impossible grâce à un « timeout » sur l'état de déverrouillage. Ainsi même pour cette séquence très improbable, une durée de nocivité T finie est obtenue.

L'analyse de l'arbre des séquences ainsi constitué nous a conduit à repérer un nombre très réduit de séquences, qui contribuent aux ouvertures à tort de manière prépondérante. Toutes les autres branches sont négligeables devant ces « pires cas ». Sans surprise, il s'agit de cas où **des perturbations viennent compléter au mauvais moment une séquence presque complète obtenue par un véritable train** : trains de travaux ressemblant à des trains de voyageurs, périodes précédant juste l'arrêt du train ou suivant immédiatement son départ, le train étant encore entre les deux CP. Le système est bien sûr choisi pour que ces cas conduisent à une fréquence d'ouverture à tort compatible SIL3.

Notons que cette évaluation pose le problème de la séparabilité de la qualification des capteurs. Supposons par exemple un capteur infrarouge certifié SIL3. Cela signifie que la fréquence de pannes du capteur conduisant à une détection à tort (en supposant que l'état sécuritaire choisi soit l'absence de détection) est inférieure à 10^{-7} occurrences par heure. De telles informations **ne suffisent en aucun cas** pour l'évaluation précédente, il est toujours nécessaire d'énumérer et de quantifier les perturbations physiques telles que les objets parasites ou la perte d'orientation des capteurs pour calculer la seule fréquence d'occurrence qui importe en définitive : celle des événements redoutés sur le système. Dans le cas de COPPILOT, le niveau SIL3 est obtenu en supposant des fréquences de perturbations physiques élevées : de l'ordre de 10^{-2} pour les perturbations fugitives, 10^{-3} pour les permanentes. Les capteurs sont choisis pour que la contribution de leurs pannes internes soit faible comparée à ces fréquences. En résumé, **l'emploi de capteurs qualifiés ne permettrait pas à lui seul de qualifier un tel système de détection** ; en fait l'influence de la fiabilité des capteurs n'est pas prépondérante devant les perturbations physiques envisagées. C'est bien **en utilisant une redondance de capteurs dont on recoupe les informations, et sans s'appuyer sur la sûreté de ces capteurs qui n'empêche pas la détection d'objets parasites** que nous avons obtenu le niveau de sécurité requis.

Un grand soin doit être apporté à la détermination des sources de perturbation sur lesquelles le calcul est basé. Pour obtenir la meilleure exhaustivité possible, nous avons considéré sur chaque capteur :

- Tout ce qui peut-être causé par l'introduction de matière dans le champ de détection
- Tout ce qui peut-être causé par l'émission d'ondes électromagnétiques
- Tout ce qui peut être causé par une modification des capteurs (pannes, actions mécaniques...)

- Tout ce qui peut provenir des liaisons électriques des capteurs (en particulier : perturbation d'alimentations)

Ces catégories ne sont pas absolues et se recouvrent, mais elles permettent de chercher une certaine exhaustivité. Par exemple, la catégorie « matière dans le champ » permet de ne pas oublier d'envisager ce qui pourrait être causé par du brouillard ou de la fumée dans la zone des capteurs.

En considérant ces sources, il convient également d'isoler les cas où une cause sous jacente pourrait provoquer la perturbation envisagée sur plusieurs capteurs à la fois ou suivant une séquence de détection non aléatoire. Dans l'exemple précédent, la fumée devant les capteurs a beaucoup plus de chances de toucher tous les capteurs à la fois que ne le laisserait présager la formule [1] précédente : imaginez le cas d'un incendie... Pour ces **modes communs**, nous caractérisons la fréquence de la cause commune, qui intervient alors dans le calcul comme une source de perturbation à part entière.

Pour la plupart de ces sources physiques de perturbation, il n'est pas possible de faire une évaluation précise de la fréquence d'occurrence. Par contre, il est possible de choisir un majorant de cette fréquence qui soit suffisamment élevé pour qu'il soit **clairement invraisemblable** que la perturbation se produise plus fréquemment. Ce sont ces majorants qui sont employés dans l'évaluation. Ensuite, on procède à une **vérification sur le terrain** sur une période la plus longue possible, en contrôlant que les perturbations sources enregistrées sont bien celles qui ont été prévues et qu'elles se produisent à des fréquences très inférieures aux majorants choisis.

Sûreté contre disponibilité

A partir des chiffres rassemblés pour le calcul de la fréquence d'ouvertures à tort, il a été possible de faire aussi un calcul de disponibilité (fréquence de non ouvertures, ou de fermetures intempestives). Ce calcul permet de mettre en évidence la nécessité de **s'appuyer sur des séquences de détection suffisamment longues et sur des vérifications de cohérence entre les capteurs** pour obtenir le niveau de sécurité choisi. En s'appuyant uniquement sur la redondance des capteurs, le niveau de disponibilité chuterait trop vite par rapport au gain de sécurité.

Conclusion

Les systèmes automatiques en contact avec le public sont de plus en plus fréquents dans de nombreux domaines. Avec leur développement, savoir obtenir la sûreté nécessaire pour un prix optimal devient un atout majeur. Les défauts de sûreté peuvent provenir soit d'erreurs directes de conception, qui peuvent être parées par des preuves formelles, soit de menaces non prises en compte ou mal évaluées, isolément ou en séquence, ce qui peut être évité par une analyse et un calcul de fréquence des perturbations.

Nous pensons que l'alliance de ces deux parades est souhaitable : un raisonnement formel prouvant le bon fonctionnement dans les limites des perturbations tolérées, suivi d'une évaluation probabiliste des perturbations létales explicitement écartées. Clepsy a appliqué ceci pour le système de détection et de commande qu'est COPPILOT ; à partir d'un calculateur central sécuritaire il est possible d'obtenir un tel système sûr grâce à une redondance des capteurs. L'emploi de séquence de détection longues et de cohérence entre capteurs permet à cette redondance de réaliser le gain en sûreté avant d'atteindre un taux de redondance qui nuirait à la disponibilité.

Remerciements

Les auteurs remercient l'ensemble du personnel d'exploitation de la ligne 13 pour sa collaboration dans cette opération. Nous remercions également la division EST de la RATP, dirigée par M. BENSE qui nous a fait confiance pour ce projet.

Références

J.R. Abrial, The B-Book, assigning programs to meaning,
Cambridge University Press, 1996

