



**HAL**  
open science

## Évaluation du facteur humain dans le domaine de la supervision de trafic ferroviaire: le projet SPICA-Rail

Fabien Belmonte, Walter Schön, Jean-Louis Boulanger, Robert Capel

### ► To cite this version:

Fabien Belmonte, Walter Schön, Jean-Louis Boulanger, Robert Capel. Évaluation du facteur humain dans le domaine de la supervision de trafic ferroviaire: le projet SPICA-Rail. Lambda-Mu, Oct 2008, Avignon, France. pp.session 7A. hal-00335053

**HAL Id: hal-00335053**

**<https://hal.science/hal-00335053v1>**

Submitted on 28 Oct 2008

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# ÉVALUATION DU FACTEUR HUMAIN DANS LE DOMAINE DE LA SUPERVISION DE TRAFIC FERROVIAIRE : LE PROJET SPICA-RAIL

## HUMAN RELIABILITY ASSESSMENT IN THE RAILWAY TRAFFIC SUPERVISION DOMAIN: SPICA-RAIL PROJECT

Belmonte F., Schön W. et Boulanger JL.  
Université de Technologie de Compiègne  
60200 Compiègne  
☎+33 3 44 23 79 93  
✉{fbelmont,wschon,boulange}@hds.utc.fr

Capel R.  
ALSTOM  
23 rue Morane Saulnier  
92360 Meudon la forêt  
✉robert.capel@transport.alstom.com

### Résumé

Les études de sécurité issues de la sûreté de fonctionnement sont difficilement conciliables avec les études liées aux facteurs humains. Dans le cadre du projet SPICA-RAIL<sup>1</sup> et sur la base de la méthode *Functional Resonance Accident Model* (FRAM) développée par Hollnagel [12], l'article démontre qu'il est possible d'utiliser cette technique en complément des techniques classiques de sécurité afin d'établir un référentiel commun entre ces deux spécialités. Un exemple pratique est proposé dans le domaine de la supervision de trafic ferroviaire.

### Summary

Safety studies in dependability modelling are hardly compatible with human factor. Under the project SPICA-RAIL and on the basis of the method *Functional Resonance Accident Model* (FRAM) developed by Hollnagel [12], this article argues that it is possible to use this technique in addition to traditional safety techniques in order to establish a common reference between human factors and dependability specialities. A practical example is proposed in the field of train traffic supervision.

## 1. Session recherche-industrie : Présentation de la thèse

### 1.1. Contexte industriel

La thèse a pour objet d'étude le transport ferroviaire, plus particulièrement les systèmes de supervision du trafic.

Depuis quelques années, la supervision de trafic ferroviaire a été considérablement transformée. Autrefois bâtie sur l'omniprésence de l'opérateur humain dans les activités ferroviaires depuis le terrain jusqu'au poste de régulation, l'arrivée des systèmes informatisés de surveillance et de commande a réduit considérablement le nombre d'opérateurs ferroviaires et notamment dans la boucle de supervision. En effet, les systèmes modernes de supervision de trafic ferroviaire appelés Automatic Train Supervision (ATS) ont tendance à centraliser toute la commande ferroviaire dans un seul poste appelé « Poste Centralisé de Commandement » ou PCC [3].

Autrefois garant de la sécurité, l'opérateur de trafic ferroviaire est de plus en plus mis à l'écart au profit de systèmes de sécurité techniques de plus en plus autonomes. Au delà des systèmes d'enclenchements garantissant la sécurité des circulations sur les voies depuis le début du siècle dernier, des systèmes de protection appelés Automatic Train Protection (ATP) ont vu le jour et offrent un niveau de sécurité tel que l'ATS n'est plus considéré comme un acteur majeur de la sécurité [5, 4]. Les opérateurs de l'ATS sont confinés à des tâches de surveillance dans la majeure partie de leur activité. De fait, les « surprises de l'automatisation » (voir [2]) ne sont pas en reste, puisque l'ATS en raison de sa position centrale dans le système demeure le centre névralgique des opérations lorsque la situation se dégrade ou exige l'exécution de procédures.

La société ALSTOM, intervenant majeur de l'industrie ferroviaire internationale produit des systèmes de signalisation et de contrôle automatique de trains appelés Automatic Train Control (ATC). Au sommet du système ATC, le système ATS est intégré dans le PCC et offre de nombreuses fonctionnalités rendues possibles par la généralisation des nouvelles technologies de l'information.

Dans l'objectif de renforcer la sécurité de ses systèmes, ALSTOM a souhaité, dans le cadre d'une démarche de recherche partenariale université-industrie, que puisse être évalué le niveau de sécurité qui pourrait être attribué au système ATS en tenant compte du facteur humain. Le projet Spica-rail, « Supervision Picarde de transport par Rail » financé par l'État et la région Picardie dans le cadre de l'axe mobilisateur « Hommes Technologies et Systèmes Complexes » associe donc ALSTOM, l'Université de Technologie de Compiègne (UTC, référent dans le domaine de la sécurité ferroviaire), l'Université de Picardie Jules Verne (UPJV, référent de l'aspect facteur humain) la société Sigma-Conseil (pour l'expertise en matière d'exploitation ferroviaire) et Veritas pour l'évaluation indépendante du dossier de sécurité. L'objectif de ce projet consiste à intégrer une évaluation de l'interaction entre opérateurs humains et l'ATS dans les études de sécurité des systèmes ferroviaires. La thèse s'inscrit dans ce projet et vise à synthétiser cette collaboration dans une démarche interdisciplinaire.

### 1.2. Contexte méthodologique

Le management des risques industriels est devenu une discipline incontournable dans notre société. Née du besoin de contrôler les dangers induits par l'évolution croissante des technologies (notamment à partir de la deuxième moitié du 20<sup>e</sup> siècle), la maîtrise des risques industriels a d'abord été formalisée dans les années 60 grâce à la théorie mathématique de la fiabilité initiée par Barlow et Proschan. Les concepteurs de systèmes à risques ont ensuite intégré ce formalisme aux techniques de l'ingénierie des systèmes, techniques qui, par la suite, ont été normalisées permettant aux industriels et aux organismes de régulation et de contrôle de la sécurité de disposer d'un référentiel méthodologique commun pour bâtir des systèmes de haut niveau de sécurité. Dans le domaine des systèmes à électronique programmable, la norme IEC 61508 [15] établit une procédure d'évaluation et de mise en œuvre de la sûreté de fonctionnement tout au long du cycle de vie du système. La procédure consiste à évaluer la criticité des fonctions exécutées par le système en allouant un niveau d'intégrité de la sécurité (Safety Integrity Level ou SIL) définissant le niveau de risque accepté pour cette fonction. Quatre niveaux de SIL sont définis. Pour chaque niveau, la norme propose un ensemble de méthodes et de bonnes pratiques permettant de garantir le niveau de sécurité accepté. Les normes sont également contextualisées pour différents domaines industriels, la norme IEC 61508 par exemple est déclinée en trois normes pour les équipements de contrôle-commande et de signalisation ferroviaire : EN 50126 [7], EN 50128 [8], EN 50129 [9].

<sup>1</sup> Le projet SPICA-RAIL « Supervision PICARde de transport par RAIL » est soutenu par l'État et la région Picardie dans le cadre du programme « Hommes Technologies et Systèmes Complexes » (HTSC).

La prise en compte des facteurs humains n'a pas été associée à ce mouvement normatif. En effet, les normes présentées ci-avant, auxquelles sont soumis les systèmes ATS, ne font aucune référence directe à une méthodologie de prise en compte des facteurs humains dans les études de sécurité, bien que mentionnant l'importance d'une telle démarche. Les normes fournissent une liste non exhaustive des facteurs humains susceptibles d'avoir un impact sur la sécurité [7]. Récemment, des travaux effectués au Health & Safety Executive au Royaume-Uni [18] ont identifié les limitations de la norme IEC61508 pour adresser un niveau d'intégrité de la sécurité aux fonctions effectuées par l'opérateur humain en interaction avec un système de supervision. Le rapport de ces travaux propose une démarche visant à pallier ce manque en considérant l'opérateur comme partie intégrante du système et en considérant les fonctions de sécurité exécutées par l'opérateur humain de la même façon que les fonctions de sécurité exécutées par des équipements techniques. Cependant, il existe de nombreuses particularités liées à l'activité humaine de sorte qu'il est impossible d'établir une définition non équivoque du niveau de SIL avec un niveau de sécurité de l'opérateur humain. Le concept de SIL est normalement appliqué à un système de protection qui permet de réduire les risques. Or, l'opérateur humain est à la fois source et récupérateur de dangers et de ce fait, les fonctions exécutées par l'opérateur humain ne sont pas couvertes par le concept de réduction de risque considéré par la norme. Cette démarche est encore soumise à discussions et n'a pas été introduite dans la norme.

Dans la pratique, les études de sûreté de fonctionnement réalisent des analyses sur le facteur humain sur la base d'un référentiel méthodologique établi au fil des ans et qui comprend des outils spécifiques pour l'évaluation de la fiabilité humaine (Human Reliability Analysis HRA, ou Étude Probabiliste du Facteur Humain en français) et depuis peu pour l'évaluation de l'organisation dans le travail. Les premières méthodes créées dans les années 60 à 80 ont utilisé le cadre formel de la fiabilité en modélisant le fonctionnement de la composante humaine de la même façon qu'un système technique, à savoir par un modèle bimodal (marche ou panne). Cette approche a été fortement critiquée par la communauté scientifique, [10] et [13] résumant ces critiques. Cette première génération de méthodes a également initié un débat sur la nature de l'erreur humaine [16, 1]. Une deuxième génération de méthodes est née tenant compte des aspects humains et sociaux de façon plus approfondie grâce à l'apport des sciences humaines et sociales [13].

### **1.3. Objectifs de la thèse**

La thèse consiste à évaluer l'impact des systèmes ATS sur la sécurité. Les composantes technologiques ayant atteint un niveau élevé de sécurité, l'étude doit se focaliser sur l'évaluation de l'interaction opérateurs - machines et son impact sur la sécurité. Cette démarche nécessite la coopération de spécialistes de l'ingénierie ferroviaire (composante technique), des sciences humaines et sociales (composante humaine et organisationnelle) et de la sûreté de fonctionnement pour la synthèse et l'évaluation de la sécurité.

Pour ALSTOM, cette démarche apporte un point de vue extérieur et nouveau concernant les ATS. Les études existantes de sûreté de fonctionnement des systèmes ferroviaires utilisent la méthode des arbres de défaillances pour évaluer la probabilité d'occurrence de catastrophes ou d'accidents. La thèse a permis l'élaboration d'une méthode d'évaluation de l'interaction opérateurs humains-ATS permettant d'approfondir l'étude des événements relatifs à l'activité humaine en situation de supervision de trafic ferroviaire.

L'objet de l'étude s'inscrit dans le cadre des systèmes sociotechniques complexes composés d'un niveau technique (les machines et les logiciels), d'un niveau humain (les opérateurs et les concepteurs) et d'un niveau organisationnel (l'ensemble des règles et des interactions qui gouvernent le travail). Chacune de ces composantes est l'objet d'études de différentes disciplines scientifiques. La composante technique est régie par des modèles et des théories issus des sciences de l'ingénieur. La composante humaine au travail est l'objet d'études de la psychologie cognitive et de l'ergonomie cognitive. Enfin, la composante organisationnelle repose sur les sciences sociales. Ces disciplines ont des approches différentes et quelques fois opposées, la thèse vise à établir un pont entre ces différentes disciplines dans un objectif commun de l'évaluation de la sécurité.

Une démarche d'évaluation des risques industriels interdisciplinaire a donc été élaborée. L'idée consiste à compléter l'analyse de risques telle que préconisée par le référentiel normatif par une approche complémentaire permettant d'approfondir l'étude des événements humains et organisationnels insuffisamment traités dans l'approche classique.

Des études spécifiques du facteur humain ont donc été réalisées sur la plateforme SPICA-RAIL. Installée dans les locaux de l'UTC, cette plateforme comprend un système ATS couplé à un simulateur de trafic permettant de recréer en laboratoire les conditions de travail d'un opérateur de supervision de trafic ferroviaire. L'objectif des expérimentations est d'obtenir des informations sur les processus cognitifs généraux impliqués dans la gestion d'un environnement dynamique de circulation de mobiles et de contribuer ainsi à l'évaluation du système ATS en situation d'utilisation par des opérateurs confrontés à la gestion d'une situation nominale, normale et dégradée.

La difficulté d'une telle démarche demeure l'intégration des résultats obtenus par l'observation et les techniques de la psychologie ergonomique cognitive dans l'étude de sécurité.

Une approche interdisciplinaire s'appuyant sur un référentiel commun aux trois disciplines a été proposé afin de disposer d'un modèle commun entre spécialistes des sciences humaines et sociales et spécialistes de la sûreté de fonctionnement. Ce référentiel a été puisé dans une perspective systémique de l'étude de la sécurité. Dans cette perspective, Hollnagel [12] a développé une méthode d'étude systémique des accidents appelée Functional Resonance Accident Model (FRAM) que nous avons appliquée au cas du système de supervision de trafic ferroviaire.

## **2. Introduction**

Dans une précédente communication [4] nous avons présenté un état de l'art industriel approfondi de la supervision des installations à risques. L'accent a été mis sur le rôle de celle-ci vis à vis de la sécurité. Quel que soit le domaine industriel visité, la supervision demeure le centre névralgique des opérations bien que les systèmes de haut niveau d'intégrité de sécurité remplacent de plus en plus l'activité humaine. En effet, l'automatisation des opérations de contrôles et de commandes devient la règle et l'opérateur humain est relégué dans un rôle passif, d'attendant que l'on nomme superviseur. Cependant, il existe toujours des modes d'exploitations dans lesquels, l'opérateur humain doit reprendre le contrôle des opérations. L'objet de cette communication est de présenter l'approche interdisciplinaire qui a été utilisée durant cette thèse. La première partie de cette communication présente l'étude spécifique du facteur humain qui a été réalisée sur la plateforme SPICA-RAIL en collaboration avec les spécialistes de la psychologie cognitive et de la psychologie ergonomique cognitive. La deuxième partie présente l'approche interdisciplinaire utilisée dans la démarche de la thèse afin d'intégrer les résultats des expériences dans les études de sécurité.

### 3. Expérimentations

Le cadre théorique et la méthodologie utilisés dans cette partie du projet sont ceux de la psychologie cognitive et de la psychologie ergonomique cognitive. La réalisation des procédures expérimentales ainsi que les expériences ont été réalisées en collaboration avec les chercheurs de l'Université de Picardie Jules Verne, membres du laboratoire ECCHAT.

#### 3.1. Préambule

L'apport de la psychologie cognitive se situe essentiellement sur le plan théorique en fournissant des outils conceptuels permettant de comprendre le fonctionnement cognitif d'un agent de circulation assurant une tâche de supervision et de contrôle de trafic ferroviaire. L'opérateur est ici conçu exclusivement d'un point de vue cognitif, c'est à dire comme un système de traitement de l'information à capacité limitée capable d'acquiescer, de stocker, d'utiliser des connaissances déclaratives et procédurales dans un environnement de travail.

L'apport de la psychologie ergonomique cognitive se situe quant à lui sur un plan à la fois conceptuel et méthodologique. Sur le plan conceptuel deux champs d'études qui ont été abondamment abordés par cette discipline sont pertinents dans le cadre de l'évaluation de l'agent circulation : la supervision et le contrôle de processus en situations dynamiques d'une part, et la coopération homme-machine d'autre part.

L'adoption de cette double approche nous conduit, *a priori*, à considérer le couple HOMME - MACHINE comme un système à part entière et non de manière séparée. Ainsi l'objectif général de l'étude psychologique et ergonomique est de caractériser l'adaptation du système OPÉRATEUR - ATS à son environnement et aux tâches qu'il est censé assurer [11]. Plus précisément l'objectif est de déterminer, à l'aide d'expérimentations dans un environnement de simulation réalisées à partir d'un ATS existant, en l'occurrence la plateforme SPICA-RAIL, dans quelle mesure le système formé par le couple OPÉRATEUR - ATS permet d'assurer la supervision et le contrôle efficace vis à vis de la sécurité d'une situation de trafic ferroviaire.

#### 3.2. La plateforme SPICA-RAIL

Le produit choisi pour l'environnement de simulation est un produit du commerce développé par ALSTOM sous le nom d'ICONIS. Celui-ci appartient à la classe de systèmes nommée *Automatic Train Supervision* ou ATS. Les ATS représentent la nouvelle génération de système intégré de gestion de trafic ferroviaire, voir [4] pour une présentation détaillée.

Une photographie de la plateforme est présentée dans la figure 1. Le Tableau de Contrôle Optique (TCO) est l'IHM principale et commune à l'ensemble du personnel du poste. Sur la plateforme, le TCO est rétroprojeté sur deux écrans, permettant d'afficher deux vues différentes de l'ATS. Cette fonctionnalité permet de visualiser à la fois la vue générale de la ligne et de focaliser l'attention sur une zone en particulier (vue « zoomée ») sur l'autre écran. Les postes de supervision sont des postes informatisés munis d'un écran, d'un système de pointage (la souris) et d'un clavier. Les postes se répartissent selon la zone géographique dont ils ont le contrôle. Enfin, les deux postes informatiques au premier plan de l'image permettent de simuler le trafic pour l'un et les communications entre le simulateur de trafic et l'ATS pour l'autre. L'image de droite de la figure 1 représente une copie d'écran de l'IHM global de l'ATS et qui est reprise en partie sur les postes de supervision. Les zones hachurées correspondent aux parties non opérationnelles ou débranchées pendant les expérimentations.

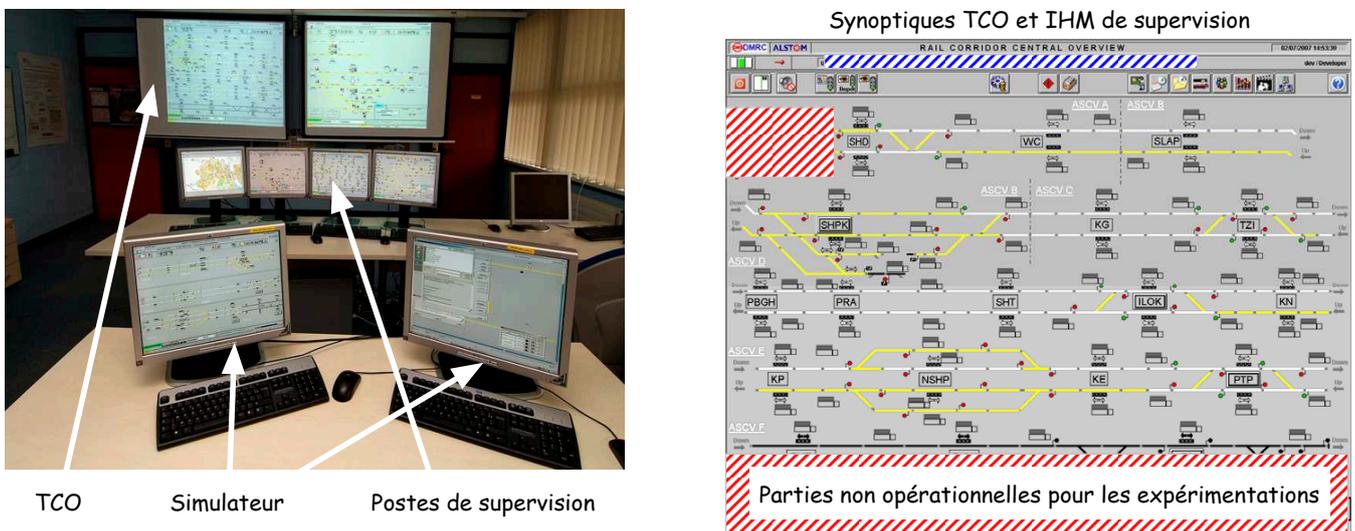


FIG. 1 – La plateforme SPICA-RAIL

Les principales fonctions fournies par l'ATS sont la gestion des équipements de signalisation, la surveillance des équipements, le suivi des trains et le routage des trains.

Les opérateurs disposent directement de toutes ces informations via le TCO et leur poste de supervision, ils passent leurs commandes via ce dernier.

Le simulateur de trafic permet de créer les scénarios d'exploitation de la ligne à l'aide d'un langage de scripts. Il est également possible à partir du poste informatique du simulateur de trafic d'injecter une anomalie sur n'importe quel équipement supervisé par l'ATS et ainsi créer les situations d'exploitation dégradées.

### 3.3. Protocole expérimental

D'un point de vue cognitif, l'interface de l'ATS peut être vue comme un stimulus complexe présentant des éléments statiques (ex : les voies, les gares, etc.) et des éléments dynamiques (les éléments représentant la position des aiguilles, l'occupation successive des circuits de voies, l'état des signaux, etc.). À partir de ce stimulus (Tableau de Contrôle Optique ou TCO, écran du poste informatique) destiné à représenter une situation distante, l'opérateur de supervision est censé détecter le plus rapidement possible les anomalies susceptibles de perturber plus ou moins gravement la circulation des trains sur une ligne ferroviaire et d'en affecter la sécurité.

L'expérience qui a été menée sur la plateforme SPICA-RAIL (Supervision PICARde de transport par RAIL) avait pour objectif de mesurer le degré d'efficacité et d'efficacités de l'interface de l'ATS. La conception de l'interface graphique devrait faciliter la détection des événements survenant de manière imprévue qui pourraient nuire à la sécurité. Pour assurer la sécurité des circulations, les agents de circulation doivent être capables d'extraire toute anomalie dans l'état des aiguilles et des signaux manifestant un incident potentiel ou actuel. L'interface graphique est un des moyens par lequel cette information leur est délivrée, encore faut-il que l'opérateur en prenne connaissance clairement et rapidement afin d'actualiser sa représentation de la situation. Le système d'alarme a volontairement été débranché afin d'évaluer les éléments graphiques du TCO et de l'IHM.

Pour tester l'efficacité de l'interface, il semble approprié d'avoir recours à des agents de circulation novices qui s'appuient fortement sur l'interface graphique pour se construire une représentation de la situation. Si l'interface est efficace, les opérateurs novices seront capables de détecter l'apparition d'un incident.

L'intérêt de recourir à des sujets non experts se situe au moins à deux niveaux. Le premier est que ces sujets, compte tenu de leur inexpérience, peuvent être assimilés dans une certaine mesure à des agents en formation. Le second est que des sujets non experts peuvent s'avérer plus adaptés pour révéler les insuffisances d'un dispositif d'aide que des sujets ayant une grande expertise. Les premiers sont plus dépendants dudit dispositif tandis que les seconds sont capables de pallier les manques par leur expérience et ainsi occulter involontairement les défauts éventuels.

Trois sujets ont participé volontairement à l'expérience, l'un âgé de 22 ans et étudiant en dernière année du cycle d'ingénieur, le deuxième âgé de 30 ans et docteur en informatique et le troisième âgé de 34 ans lui aussi docteur en informatique.

Après avoir été formés individuellement pendant trois demi-journées à la gestion de trafic ferroviaire au moyen de cette interface les sujets ont été soumis à une évaluation des connaissances acquises sous forme de questionnaire à choix multiples. Les trois sujets ont obtenu 99% de bonnes réponses, une question ayant été jugée ambiguë lors du dépouillement.

La tâche des sujets consiste à surveiller le trafic et détecter les dysfonctionnements éventuels ainsi que tout écart par rapport à la situation nominale (situation dégradée). Trois types de dysfonctionnement ont été introduits aléatoirement dans les scénarios correspondants aux situations dégradées :

- Une aiguille qui ne contrôle plus. Ce type d'anomalie n'est pas contraire à la sécurité, il correspond au fait que le système de contrôle de l'aiguille ne parvient pas à détecter la position de l'aiguille, en conséquence, la signalisation interdit le franchissement de cette aiguille. Toutefois, ce type d'incident perturbe le trafic et génère donc une mise en tension du système ;
- Un raté d'ouverture d'un signal. Ce type d'anomalie n'est pas contraire à la sécurité, il s'agit d'un dysfonctionnement d'un signal dans lequel le signal reste fermé (n'autorise pas la circulation) alors qu'il devrait être ouvert (autorise la circulation). Ce type d'incident perturbe le trafic et génère donc une mise en tension du système ;
- Un raté de fermeture d'un signal. Ce type d'anomalie est contraire à la sécurité. En effet, un signal qui aurait dû se fermer reste ouvert et autorise la circulation sur une voie non libre. Ce type d'incident est potentiellement générateur d'accidents.

Quatre variables indépendantes ont été testées vis à vis de la variable dépendante « temps de détection ». La première variable indépendante est le type d'anomalie présentant deux modalités : dérangement d'aiguille et dérangement de signal. Comme les dérangements d'aiguilles se manifestent généralement par davantage d'indices que les dérangements de signal, nous avons fait l'hypothèse que les temps de détection devraient être moins élevés pour les scénarios impliquant un dérangement d'aiguille que pour ceux impliquant un dérangement de signal. La seconde variable indépendante est « le moment de l'incident ». Dans notre expérience la durée maximale d'un scénario est fixée à 30 minutes. Toutefois on peut s'attendre à ce que le moment d'apparition d'un accident ait un effet sur la vitesse de détection des anomalies. La troisième variable indépendante testée est « la proximité des mobiles ». Les scénarios ont été établis de façon à ce que 6 trains soient présents sur le TCO au moment de la survenue des incidents. Ces trains constituent des éléments mobiles qui peuvent se situer à distance ou à proximité des anomalies à détecter. L'incident peut provoquer une modification du comportement du train. En outre, on peut penser que des sujets novices auront tendance à focaliser leur attention sur les installations à proximité des trains en mouvement. Nous avons fait l'hypothèse que le temps de détection des anomalies devrait être moins élevé dans les scénarios où les anomalies surviennent lorsqu'un train se situe à proximité que lorsque les anomalies surviennent dans une zone dans laquelle ne se trouve aucun train. De plus, le temps de détection devrait être moins élevé lorsque l'incident provoque l'arrêt de train que dans le cas où il n'affecte par le comportement de ce dernier. Enfin la quatrième variable indépendante relève du « type d'itinéraire » qui peut prendre deux modalités :

- les itinéraires permanents qui, comme leur nom l'indique, existent avant l'arrivée d'un train et se reforment automatiquement après le passage d'un train. Ce type d'itinéraire est utilisé sur des zones où les circulations empruntent toujours le même itinéraire (la pleine voie) ;
- les itinéraires en destruction automatique qui se forment au moment où un train arrive et se détruisent au fur et à mesure du passage du train sur l'itinéraire. Ce type d'itinéraire est utilisé sur des zones où les circulations peuvent aller vers plusieurs destinations.

D'une manière générale, le nombre d'anomalies visibles est plus élevé dans le premier cas que dans le second. De fait, les temps de détection devraient être moins élevés lorsque les deux voies sont en itinéraires permanents que lorsqu'au moins une voie est en destruction automatique.

En faisant varier les variables indépendantes, cette procédure a permis d'évaluer la capacité de l'interface à représenter efficacement de manière externe les situations dégradées. Vingt scénarios définis ont été élaborés à partir du plan d'expérience à mesure répété constitué des quatre variables indépendantes. Dix scénarios distrayeurs ont également été introduits de manière à empêcher les sujets de développer des attentes à propos des variables étudiées et des hypothèses testées. Chaque passation s'est déroulée de manière individuelle et chaque opérateur novice a vu des scénarios variés. Nous avons demandé à chaque sujet de détecter les éventuels écarts au nominal mais également de diagnostiquer les raisons de ces écarts ainsi que de pronostiquer l'évolution de la situation. Les données recueillies sont les temps de latence entre la survenue d'un événement et sa détection, le diagnostic et le pronostic. Le nombre de détections correctes de problèmes, de fausses alarmes, de manqués, constitue une mesure importante de cette étude.

### 3.4. Statistiques descriptives

Les passations ont permis de recueillir environ 10 heures d'enregistrements vidéo par sujet, soit au total une trentaine d'heures pour les trois sujets.

Dans la quasi totalité des cas, les anomalies ont été correctement détectées dans un délai de 5 minutes. Les taux d'anomalie non détectées et de fausses alarmes sur l'ensemble des scénarios sont très faibles, ces taux sont de 1/30 pour chacun des trois sujets.

Ces résultats confirment d'une part que la formation initiale a parfaitement rempli son rôle et indiquent, d'autre part que les anomalies simulées dans la présente expérience sont parfaitement détectables en mode hors alarme par des sujets peu expérimentés.

L'analyse des temps de détection des anomalies a nécessité une numérisation préalable des enregistrements vidéos puis une analyse image par image à l'aide du logiciel Adobe™Premiere®Pro 1.5 pour Windows®.

En raison d'une forte variabilité intra et inter sujets et de l'existence de temps de détection extrêmes, les moyennes et variances ont peu de significativité. En conséquence, les analyses ont été réalisées sur les médianes et les étendues.

Le temps de détection (noté  $T_D$ ) médian est de 11,96 pour une étendue de 299. L'analyse des temps de détection sur les scénarios tests révèle une forte variabilité entre les sujets. Les temps de détection médians et les étendues pour les 3 sujets sont indiqués dans le tableau 1.

Sujet	$T_D$ médian (sec.)	Étendue
1	5,48	299
2	22,42	160,9
3	11,57	298,96

TAB. 1 – Temps de détection médians et étendues

Ces premières analyses permettent d'établir que les temps de détection sont relativement élevés si l'on considère que la présente expérience met les sujets dans les conditions les plus favorables pour détecter rapidement les anomalies :

- Les sujets sont informés que chaque scénario comporte une anomalie à détecter (ce qui n'est pas le cas dans un vrai poste ATS) ;
- Les incidents sont réduits à deux types d'incidents, aiguilles et signaux, dans un vrai poste ATS, la nature des incidents peuvent être beaucoup plus variée ;
- La durée des scénarios est très courte (30 mn) comparée à un quart réel de 6 heures dans un poste ATS ;
- Les sujets n'ont que la tâche de détection à accomplir alors que dans un vrai poste ATS, les opérateurs sont amenés à accomplir plusieurs activités en parallèle ;
- Toute la ligne n'a pas été implémentée sur le TCO. De fait la zone à superviser est relativement réduite ;
- Enfin, la ligne a été simplifiée, elle ne comporte que deux gares commerciales et une seule bifurcation.

Par ailleurs, on note que le sujet 2 est moins rapide que les autres sujets pour détecter les anomalies. En effet, alors que chez ce sujet 60% des temps de détection sont supérieurs à 20 sec., ce taux n'est plus que de 20% chez les sujets 1 et 3. Ce résultat suggère que le temps de détection dépend des stratégies employées par les sujets pour explorer le TCO et que les anomalies ne sont pas suffisamment saillantes pour être perçues de la même manière par tous les sujets.

### 3.5. Comparaison des sujets

Une analyse de normalité réalisée sur les données disponibles indique que les distributions ne satisfont pas aux conditions de normalité et d'homogénéité. En conséquence, la significativité statistique des effets pour toutes les comparaisons portant sur des mesures répétées a été testée à l'aide de tests non paramétriques pour échantillons appariés. Le seuil de significativité est fixé *a priori* à  $\alpha = 0.05$  pour toutes les comparaisons.

L'objectif de notre démarche consiste à comparer de façon non paramétrique deux échantillons. Pour comparer les performances des sujets deux à deux, la statistique de Mann et Witney a été utilisée, elle représente le nombre de fois où une observation du premier sujet est plus grande qu'une observation du second sujet.

Chaque sujet a effectué  $n = 20$  scénarios tests. Les valeurs des probabilités de rejeter à tort les hypothèses que les distributions des deux sujets comparés soient identiques (noté  $p$ ) sont données dans le tableau 2.

Paire	$p$	$H_0$ « $T_D^1 = T_D^2$ »
Sujet 1 - Sujet 2	0,00041	Rejeté
Sujet 1 - Sujet 3	0,21	Accepté
Sujet 2 - Sujet 3	0,03	Rejeté

TAB. 2 – Comparaisons des données des trois sujets. Test de Mann et Witney,  $\alpha = 0.05$

Ce résultat confirme le résultat des statistiques descriptives, les analyses indiquent que les temps de détections du sujet 2 diffèrent significativement de ceux du sujet 1 et de ceux du sujet 3.

### 3.6. Effets des variables

Pour tester l'effet des variables indépendantes sur les temps de détection, les données ont été soumises à la statistique de Wilcoxon pour échantillons appariés qui consiste à sommer les rangs signés des différences entre paires d'observation de chaque échantillon.

Ce type de test est utile lorsque l'on veut établir si deux traitements sont différents ou si un traitement est « meilleur » qu'un autre. Dans tous les cas, le groupe qui a subi le traitement est comparé à celui qui n'en a pas subi, ou qui a subi un traitement différent. Ce cas se présente, par exemple, quand on compare deux méthodes de mesure en soumettant à ces deux méthodes les mêmes individus, choisis dans une population donnée. Ici nous avons soumis plusieurs scénarios avec la même modalité d'une variable à plusieurs sujets et un nombre identique de scénarios avec l'autre modalité. Nos hypothèses à tester consistent à vérifier si une modalité donne des temps de détection plus grands ou plus petits que l'autre modalité.

Les résultats des tests statistiques ne sont pas significatifs, il est donc impossible d'inférer des conclusions concernant l'effet des variables sur la base des tests statistiques non paramétriques. La taille des échantillons est sans doute responsable du manque de significativité de ces résultats. Pourtant, les tests non paramétriques de rang signé pour échantillons appariés tels que le test de Wilcoxon sont tout à fait applicables à notre expérience. Le nombre de paires dans chaque test est toujours supérieures à  $n = 8$ , or, l'étude des rangs signés donne des résultats pour des valeurs de  $n$  petites [17]. Pour  $n > 30$  nous aurions pu utiliser l'approximation normale puisque la statistique de Wilcoxon converge vers la loi normale lorsque  $n \rightarrow \infty$ .

On observe que l'effet de la variable « Contexte mobile » a fourni un résultat significatif. Les temps de détection d'anomalies se sont avérés significativement plus élevés dans le cas où un train se trouve dans la zone où l'incident se produit que dans le cas où aucun train ne circule sur cette zone. Et ce, contrairement à ce qui avait été prédit. Ce résultat semble surprenant, en effet, il paraissait raisonnable de supposer que la stratégie du sujet pour balayer le TCO soit sensible à la présence d'une circulation et que celui-ci s'attache à poser son regard périodiquement sur les circuits de voies occupés. Or, l'analyse statistique montre que cette supposition n'est pas valable. La performance des sujets n'est vraisemblablement pas améliorée par une telle stratégie.

L'ensemble des résultats statistiques indique qu'il serait souhaitable de prolonger l'analyse sur la stratégie de balayage du TCO par l'opérateur. Nous avons constaté des différences significatives d'un sujet par rapport aux deux autres. Cet écart pourrait donc provenir de la stratégie utilisée par les sujets pour balayer le TCO, toutefois il faudrait néanmoins vérifier que cette différence n'est pas liée à la variabilité normale inter-sujets, chose que nous n'avons pu analyser dans notre expérience, il aurait fallu un nombre plus important de sujets pour conclure sur la variabilité inter-sujets. De même la contradiction avec l'hypothèse qui a été émise concernant le contexte mobile de l'incident est un indice supplémentaire pour continuer les recherches dans cette voie. S'il s'avérait possible d'identifier plusieurs stratégies de surveillance et de les classer par ordre de performance, il serait alors possible de proposer des spécifications pour l'amélioration des IHM qui orienteraient l'opérateur dans sa tâche de surveillance.

Ces observations dans un environnement simulé avait pour objectif de déterminer les mécanismes généraux de la cognition d'un opérateur humain en situation de supervision de trafic ferroviaire afin d'améliorer les études de sécurité par l'intégration des travaux des spécialistes du domaine de la cognition. Cette démarche, nécessite d'être intégrée dans le processus d'évaluation de la sécurité du système ferroviaire. À ce jour, exclusivement basées sur des techniques issues des sciences de l'ingénieur, les études de sécurité doivent intégrer d'autres techniques et plus particulièrement celle des sciences humaines et sociales [6].

## **4. Étude de sécurité interdisciplinaire**

### **4.1. Motivation**

Cet article traite des systèmes sociotechniques complexes composés d'un niveau technique (les machines, les logiciels), d'un niveau humain (les opérateurs, les concepteurs) et d'un niveau organisationnel (l'ensemble des règles et des interactions qui gouvernent le travail accompli par le système.) Chacune de ces composantes correspond à une discipline scientifique.

Dans cette partie de l'article, nous proposons une démarche d'évaluation des risques industriels permettant d'associer ces trois disciplines. L'idée consiste à appliquer une approche complémentaire à l'analyse de risque classique permettant d'approfondir les niveaux humain et organisationnel insuffisamment traités dans l'approche classique de sûreté de fonctionnement.

Cette approche complémentaire doit disposer d'un référentiel commun aux trois disciplines impliquées dans les systèmes sociotechniques complexes. La méthode *Functional Resonance Accident Model* (FRAM) développée par Hollnagel pour analyser les accidents utilise une approche dans laquelle les trois composantes (technique, humaine et organisationnelle) cohabitent et sont en interactions mutuelles. Utilisée en complément de l'approche classique, la méthode FRAM permet de « zoomer » sur les événements humains et organisationnels afin d'affiner le résultat qualitatif de l'étude.

### **4.2. La méthode FRAM**

La méthode FRAM développée par Hollnagel [12] (chapitre 5) permet de décrire le système sociotechnique par ses fonctions et ses activités plutôt que par sa structure. L'objectif de FRAM est de représenter la dynamique du système par la modélisation des dépendances non linéaires qu'elle contient et par une représentation originale de la performance des fonctions et des activités. Le modèle de dépendance repose sur le concept de résonance fonctionnelle emprunté à la physique ondulatoire, métaphore de la résonance stochastique. Le principe de résonance stochastique consiste à la surimposition d'un signal non linéaire (bruit) sur un signal périodique de faible amplitude difficilement détectable. L'addition du bruit permet alors d'établir une résonance avec le signal de faible amplitude et de le rendre ainsi détectable.

Normalement utilisée pour expliquer l'émergence d'ordre dans un système, Hollnagel l'applique ici pour expliquer l'apparition des accidents. Il réalise ce transfert vers l'étude de sécurité en s'appuyant sur la variabilité de performance des fonctions ou des activités d'un système sociotechnique.

Selon [12], la variabilité de performance dans les systèmes techniques est relative aux imperfections en conception et en production, aux spécifications non exhaustives des conditions de travail (effets de l'environnement et des entrées non prévues). La variabilité de performance des humains et des organisations vient de leur capacité à s'adapter aux conditions de travail et à l'absence de régularité dans les activités (perception, cognition, action, communication).

Le parallèle avec la résonance stochastique s'explique par le caractère stochastique de la variabilité de performance des fonctions et des activités du système assimilés à des signaux non linéaires. D'autre part, Hollnagel utilise la superposition des signaux comme modèle de dépendance fonctionnelle entre les fonctions et les activités du système.

Le signal faible correspond à la variabilité de performance de chaque fonction exercée par les différents sous-systèmes. Cette variabilité de performance est faible dans le sens où les écarts de performance des fonctions n'ont pas ou peu d'impact sur la performance globale du système et sur la sécurité. Le signal non linéaire permettant d'établir la résonance correspond à la variabilité de performance du reste du système lorsqu'on considère une fonction ou une activité prise à part. Le signal faible peut être la variabilité de performance de n'importe quelle fonction ou activité du système et le bruit correspond à l'agrégation des variabilités de performance du reste du système (environnement compris). Hollnagel appelle ce phénomène la « résonance fonctionnelle »

L'étude des potentialités d'accident avec la méthode FRAM se résume en quatre étapes appliquées à l'étude d'une activité ou d'une fonction du système.

1. Identifier et caractériser les fonctions essentielles. L'étude fonctionnelle des activités et des fonctions est basée sur une représentation hexagonale munie de six connecteurs ;
2. Déterminer le potentiel de variabilité à l'aide d'une liste de contrôle ;
3. Appliquer le principe de résonance fonctionnelle sur les dépendances entre les activités et les fonctions ;
4. Identifier les barrières contre la variabilité et spécifier les nécessaires mesures de surveillance de la performance.

Seules les trois premières étapes sont utilisées dans notre démarche.

La première étape récrit l'analyse fonctionnelle ou l'analyse de la tâche dans un formalisme constitué de tâches ou de fonctions élémentaires auxquelles sont attachés six attributs (voir figure 2). Ces attributs servent de connecteurs entre les fonctions ou activités élémentaires :

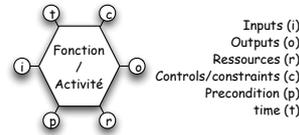


FIG. 2 – Codage des fonctions dans FRAM (Hollnagel, 2003)

**Inputs (i)** Représente ce qui sera traité ou transformé par la fonction ;

**Outputs (o)** Représente le ou les produits de la fonction ;

**Ressource (r)** Représente ce qui sera consommé ou utilisé par la fonction ;

**Time (t)** Représente le temps nécessaire à la réalisation de la fonction et tout ce qui concerne les pressions temporelles ;

**Control (c)** Représente le ou les contrôles et contraintes qui gouvernent l'exécution de la fonction (boucle de rattrapage, procédures, méthodes, etc.) ;

**Precondition (p)** Les préconditions représentent les éléments qui doivent être satisfaits avant que la fonction soit exécutée.

La deuxième étape consiste à déterminer la variabilité de performance du contexte général de l'activité dans lequel s'exécute toutes les fonctions. La variabilité de performance du contexte général est déterminée par onze conditions communes de performance (CCP). Toutes les fonctions ne sont pas affectées de la même façon par les CCP. FRAM classe les fonctions en trois catégories : humaines (H), techniques (T) ou organisationnelles (O) selon la nature des acteurs exécutant les fonctions. De plus, chaque CCP ne s'applique que sur une catégorie de fonction. Le tableau 3 présente les onze CCP proposées par Hollnagel [14] et la catégorie de fonction à laquelle elles s'appliquent.

Les conditions communes de performance utilisées dans FRAM sont issues de la méthode d'étude de la fiabilité humaine d'Hollnagel CREAM *Cognitive Reliability and Error Analysis Method* se reporter à [13] pour une présentation détaillée.

Numéro	Conditions de performance	Catégorie
C <sub>1</sub>	Disponibilité des ressources	H - T
C <sub>2</sub>	Entraînement et expérience	H
C <sub>3</sub>	Qualité des communications	H - T
C <sub>4</sub>	Qualité des interfaces opérateurs - machines	H
C <sub>5</sub>	Accessibilité et disponibilité des méthodes et des procédures	H
C <sub>6</sub>	Conditions de travail	H - T
C <sub>7</sub>	Nombre d'objectifs simultanés	H - O
C <sub>8</sub>	Temps disponible	H
C <sub>9</sub>	Rythme circadien	H
C <sub>10</sub>	Qualité de collaboration en équipe	H
C <sub>11</sub>	Qualité et support de l'organisation	O

TAB. 3 – Nomenclature des conditions communes de performance

La qualité des CCP est appréciée par trois valeurs possibles : stable ou variable mais adapté ; stable ou variable mais inadapté ; imprévisible. Il s'agit de déterminer pour chaque scénario d'étude la qualité des onze CCP. Hollnagel [12] (page 193) établit une relation entre la qualité d'une condition de performance et la variabilité de performance. Si une condition de performance est stable ou variable mais adaptée alors la variabilité de performance associée à la fonction est faible. Dans le cas stable ou variable mais inadapté, la variabilité de performance est élevée. Enfin, si une condition de performance est imprévisible, la variabilité associée est très élevée.

Les CCP déterminent donc la contrainte de variabilité commune ou propre aux fonctions de l'activité étudiée. L'évaluation des effets des CCP sur les fonctions doit être précisé à l'aide d'un modèle causal, issu d'une expertise interdisciplinaire et indiquant le potentiel de variabilité de la performance d'une fonction à partir des CCP et ce pour chaque fonction. Hollnagel, utilise le modèle ETTO [12] acronyme de *Efficiency Thoroughness Trade Off* (compromis efficacité minutie) qui permet d'inférer le comportement potentiel d'un opérateur humain à partir du contexte de la fonction et des pressions auquel il est soumis. Le cas d'étude présenté ci-après utilise en partie les résultats des expérimentations présentées précédemment à cette fin.

La troisième étape établit les dépendances entre les fonctions ou activités. Ceci est effectué par la mise en correspondance des attributs assignés à la première étape. Graphiquement cela revient à connecter les entrées et les sorties des fonctions représentées par leur hexagone, la figure 3 fournit un exemple de réseau FRAM appliqué à la surveillance et au diagnostic d'anomalie en situation de supervision de trafic ferroviaire. Le réseau ainsi créé permet de visualiser le flux des informations et des matières lors de l'exécution normale de l'activité étudiée. Les mentions H, T ou O dans l'en-tête des fonctions indique la catégorie des entités participants à la fonction. Il s'agit alors de rechercher les résonances fonctionnelles issues de la variabilité de performance des fonctions et propagées par les interrelations complexes entre les fonctions. De même, un raisonnement causal doit être utilisé pour déterminer l'effet de la variabilité d'une fonction connectée à un attribut

d'une autre fonction sur la performance de cette dernière. Seul le contexte de l'étude et une expertise interdisciplinaire permet d'élaborer un tel raisonnement.

La méthode FRAM est actuellement utilisée dans le domaine du contrôle de trafic aérien [19]. Elle sert de support à une étude prospective des risques dans le cadre de l'introduction d'automatismes dans le système de management du trafic aérien. Un modèle de gestion des conflits aériens par le contrôleur aérien a été développé. Ce modèle FRAM a permis de relever des questions sur les risques lors de l'utilisation du futur système automatisé.

## 5. Cas d'étude

### 5.1. Modélisation

Le cas d'étude reprend l'activité des opérateurs de supervision de trafic ferroviaire qui a été expérimentée sur la plateforme SPICA-RAIL à savoir la surveillance du TCO et la mise en place de mesures correctives suite à un incident. Le modèle élaboré est synthétisé sur la figure 3.

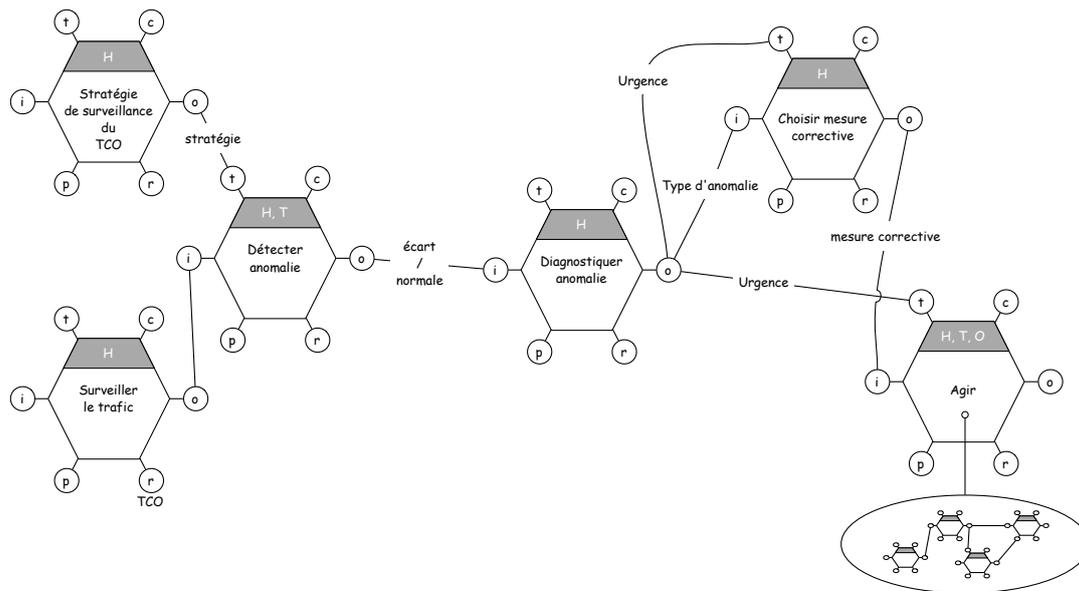


FIG. 3 – Modèle de l'activité de surveillance du trafic

Six fonctions ont été identifiées. La première fonction a été identifiée grâce à l'expérimentation sur SPICA-RAIL. En effet, les résultats des expériences suggèrent que la stratégie de surveillance du TCO influe sur le temps de détection des anomalies. Le choix de cette stratégie constitue la première fonction du modèle. Elle dépend uniquement de la condition de performance relative à l'entraînement et l'expérience de l'opérateur. Dans le cas où cette condition de performance est évaluée adaptée et donc dans le cas d'un opérateur expérimenté, on peut considérer que la stratégie choisie a une faible variabilité de performance. Dans le cas où cette condition de performance est jugée stable ou variable mais inadaptée, ceci se traduit pour notre exemple par un opérateur novice qui a suivi une formation initiale mais qui ne dispose pas d'expérience. En conséquence, nous considérerons que la variabilité de performance de la stratégie choisie est élevée. Enfin, un opérateur inexpérimenté (la condition de performance est jugée « imprévisible ») produit des heuristiques de surveillance aléatoires, de fait, la variabilité de performance de la stratégie choisie est très élevée.

La deuxième fonction consiste à surveiller le trafic, elle est exécutée par le couple opérateur humain - système ATS. Cette fonction utilise comme ressource le TCO et l'IHM du poste de supervision. Les conditions de performance de cette fonction sont : la qualité des communications entre le terrain et l'ATS, la qualité de l'IHM et le nombre d'objectifs simultanés suivis par l'opérateur humain. La qualité des communications est jugée à partir de l'étude de sûreté de fonctionnement, et notamment par la disponibilité et la fiabilité, du système de communication entre le terrain et l'ATS, nous considérons pour cet exemple que celui-ci a été développé avec un haut niveau de fiabilité et de disponibilité. La qualité de l'IHM peut être appréciée grâce aux expériences menées sur la plateforme SPICA-RAIL. L'expérimentation sur SPICA-RAIL montre que les taux de fausses alarmes et de non détection sont faibles, ceci nous amène à juger la qualité de l'IHM adaptée à la tâche de surveillance et de détection, en conséquence la fonction de surveillance du trafic n'est vraisemblablement pas soumise à la variabilité de performance de l'IHM. Par contre, le nombre d'objectifs simultanés suivis par l'opérateur n'a pas été testé lors des expériences. Si ce nombre est adapté à l'activité, l'opérateur dispose du temps nécessaire pour suivre l'évolution du trafic et donc la variabilité de performance du produit de la fonction de surveillance reste stable et peu élevée. Par contre, si le nombre d'objectifs suivis par l'opérateur humain est trop élevé, ce dernier peut être amené à ne pas suivre l'évolution du trafic et donc la variabilité de performance de la fonction est très élevée.

La troisième fonction est relative à l'activité de détection d'une anomalie. Elle est assurée par le couple opérateur - système ATS. Le temps de détection dépend de la stratégie de détection qui a été choisie par l'opérateur. Il s'agit pour l'opérateur de détecter un écart par rapport à la situation normale. Cette fonction dépend des conditions de performance relatives à l'entraînement et l'expérience des opérateurs, de la qualité de l'IHM et de la qualité des communications entre le terrain et l'ATS. Ces deux dernières ont été traitées dans la deuxième fonction. Les expériences ont montré que dans un environnement favorable et pour des sujets novices formés, ceux-ci avaient une variabilité de réponse assez élevée. En conséquence, si l'entraînement et l'expérience est jugé inadapté (opérateur novice manquant d'expérience) la variabilité de performance de la détection d'un écart par rapport à la normale est élevée. Nous considérons que cette variabilité se stabilise lorsque l'entraînement et l'expérience est jugé adapté (opérateur expérimenté), cette hypothèse doit être confirmée par l'expérience. La variabilité de performance sera très élevée lorsque l'opérateur n'a pas été formé à ce métier. Les expériences ont également émis l'hypothèse que la tâche de détection dépendait de la stratégie de surveillance du TCO (variabilité inter sujets) et qu'elle influait sur le temps de détection.

Nous supposons que si la variabilité de performance de la stratégie utilisée par l'opérateur est faible, alors le temps de détection est faible. Inversement, plus la variabilité de performance de la stratégie utilisée est élevée, plus le temps de détection sera long.

La quatrième fonction identifiée représente la tâche de diagnostic. L'opérateur ayant détecté un écart de fonctionnement, il doit alors déterminer la nature du dysfonctionnement. Deux éléments sont produits par cette fonction. Le résultat du diagnostic révèle le type d'anomalie et l'urgence avec laquelle la situation doit être traitée. Cette fonction dépend des deux conditions de performance : « entraînement et expérience » ainsi que « temps disponible ». La variabilité de performance de la fonction est d'autant plus faible que ces deux conditions de performance sont adaptées.

La cinquième fonction consiste pour l'opérateur à choisir la mesure corrective adaptée. Elle dépend du type d'anomalie et est contrainte dans le temps par l'urgence de la situation. De la même façon que la fonction précédente, le choix de la mesure corrective dépend des deux conditions de performance : « entraînement et expérience » et « temps disponible ». Cette dernière condition dépend du résultat du diagnostic, en effet le diagnostic permet d'établir le niveau d'urgence de la situation et induit nécessairement une contrainte temporelle sur la tâche du choix de la mesure corrective. Une forte variabilité dans les résultats du diagnostic peut provoquer une erreur de diagnostic et/ou une erreur d'appréciation du niveau d'urgence de la situation. En conséquence, une forte variabilité de performance au niveau de la tâche de diagnostic implique nécessairement une variabilité de performance imprévisible au niveau du choix de la mesure corrective. Le cas où la variabilité de performance du diagnostic est faible n'est pas non plus sans conséquence sur cette fonction. Un diagnostic correct peut conduire à un type d'anomalie nécessitant un traitement d'urgence, dans ce cas le choix de la mesure corrective est contraint par la pression temporelle relative à l'urgence de la situation.

La sixième fonction, nommée « agir » consiste à mettre en œuvre les mesures correctives. Cette fonction est initiée par l'opérateur de supervision de trafic, puis exécutée par un système technique (dans le cas d'une commande) ou bien par une organisation (dans le cas d'intervention d'une équipe de maintenance). Cette fonction peut se décliner en plusieurs sous fonctions et donc constituer un autre modèle FRAM.

## 5.2. Instanciation du modèle

Le terme instanciation est issu de l'informatique, il indique le remplacement d'une variable par une constante. En programmation orientée objet, on appelle instance d'une classe un objet avec un comportement et un état, tous deux définis par la classe. Dans ce contexte, instance est un anglicisme, qui signifie « cas », « exemple ». Ce terme a été utilisé dans FRAM par [19] et reflète bien l'utilisation qui est faite du modèle. En effet, le modèle initial permet de visualiser le comportement normal d'une activité et offre ainsi une approche complémentaire aux techniques classiques de sûreté de fonctionnement (arbres de défaillance ou arbres d'événement) qui représentent seulement la vue des défaillances du système. La vue « défaillante » de l'activité dans FRAM est donnée par l'instanciation du modèle.

L'instanciation du modèle FRAM consiste à initialiser les fonctions à partir de l'évaluation des conditions de performance, à déterminer à partir des raisonnements causaux de chaque fonction la propagation de la variabilité de performance au travers du modèle et à identifier les accidents potentiels lorsque la variabilité de performance d'une ou plusieurs fonctions atteint le seuil critique d'accident du système.

Une instance possible, parmi de nombreuses autres, consiste à supposer que l'opérateur est novice, qu'il n'effectue que la tâche de surveillance (nombre d'objectifs simultanés compatible) et qu'un incident de type « raté de fermeture » apparaît sur la ligne ferroviaire. L'instance du modèle est présentée sur la figure 4.

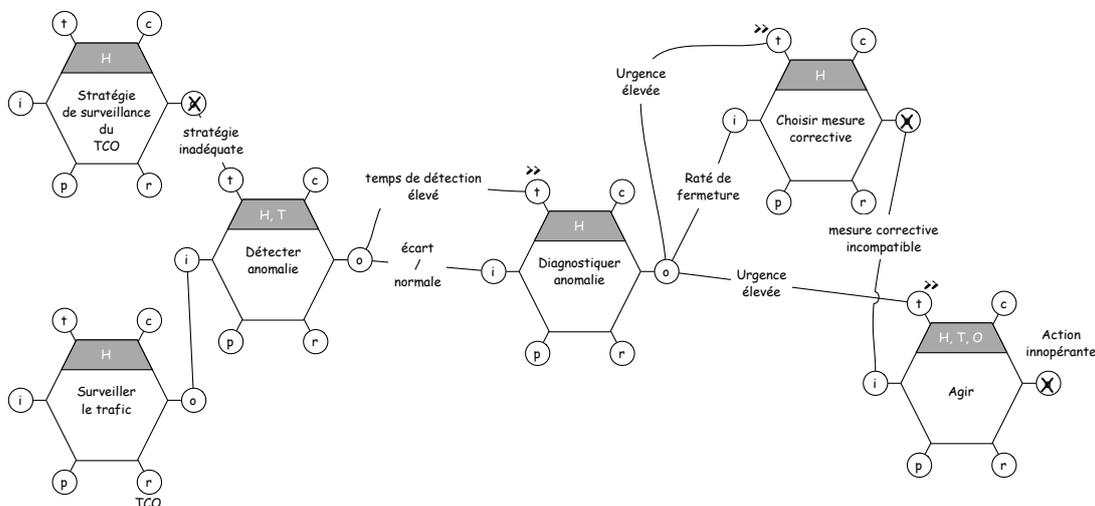


FIG. 4 – Instance du modèle

Le manque d'expérience de l'opérateur le conduit à utiliser une stratégie de surveillance inadaptée, une croix sur l'attribut *output* de la fonction symbolise cette forte variabilité de performance. En conséquence, lorsque l'anomalie apparaît sur l'IHM celui la détecte tardivement. De fait, il ne lui reste que peu de temps pour accomplir le diagnostic, choisir la mesure corrective et agir. La pression temporelle est symbolisée sur le modèle par la mention « sur l'attribut *time* de la fonction. L'écart par rapport à la normale est suffisamment explicite pour diagnostiquer un raté de fermeture et inférer un niveau d'urgence de la situation très élevé. Le choix de la mesure corrective contraint par le temps précipite la décision de l'opérateur (novice) et le conduit à faire un mauvais choix et qui l'amène à exécuter une mesure incompatible avec la situation « raté de fermeture » et donc inopérante. La conséquence immédiate d'une telle instanciation est un accident par collision de deux trains lorsque le raté de fermeture intervient en présence de mobiles à l'abord du signal défaillant.

## 5.3. Discussion

Ce ne sont pas tant les résultats de la méthodes qui sont enrichissants, mais comme toute modélisation systémique, la construction du modèle apporte des éléments de connaissance du système dans son fonctionnement et notamment en ce qui concerne les interrelations complexes

qu'il renferme. En effet, l'analyse systémique requiert de nombreuses informations et nécessite de comprendre en détail les différents contextes d'exécution des fonctions et leurs effets sur l'activité. Cette démarche constructive propose à l'ingénieur de sécurité une méthode dirigée qui lui permet de comprendre les phénomènes complexes intervenant dans le système avec un regard interdisciplinaire nécessaire.

Le besoin d'une expertise interdisciplinaire approfondie de chaque fonction afin de déterminer son modèle causal demeure la principale difficulté de cette approche. Cependant, c'est le coût nécessaire à investir pour dépasser les limitations des modèles basés sur un raisonnement causal plus simple tel que celui de la méthode THERP (méthode inductive basée sur les arbres d'événements). Les systèmes ferroviaires ont atteint un niveau élevé de complexité, le rapport entre activité humaine et sécurité ayant évolué avec l'introduction de systèmes fortement automatisés, il est donc important de prendre en compte cette nouvelle relation, plus complexe, avec les outils méthodologiques adaptés. La possibilité de modéliser les interrelations complexes dans FRAM répond à cette attente.

La méthode FRAM reste toutefois limitée à une approche qualitative de la sécurité. C'est pourquoi, elle demeure une approche complémentaire de l'étude de sécurité classique par arbres de défaillance ou d'événement. L'apport de cette méthode permet d'identifier de nouveaux événements de base pour les arbres de défaillance et d'événement à partir de l'instanciation du modèle FRAM. Subsiste cependant, l'épineux problème de leur quantification. De nouvelles expériences sont nécessaires pour pallier ce manque, l'objectif de quantifier ces événements nécessite de nombreuses passations sur le scénario identifié dans l'instance du modèle FRAM afin d'obtenir un échantillon inter sujets suffisamment représentatif pour obtenir des statistiques paramétriques fiables.

## 6. Conclusion

L'intérêt d'une approche systémique complémentaire offre un support d'échange entre le management des risques et les disciplines spécialisées des facteurs humains et organisationnels.

La méthode FRAM a permis d'intégrer dans un même formalisme les résultats d'expériences de psychologie cognitive du comportement des opérateurs de supervision de trafic ferroviaire avec les analyses de sûreté de fonctionnement.

Les résultats des expériences ne sont pas directement intégrables par une méthode définie à partir d'un modèle d'accident séquentiel du type arbres de défaillance ou arbres d'événement. Une telle entreprise porterait atteinte au raisonnement scientifique des psychologues pour lequel il est impossible de fournir une liste exhaustive des défaillances ou des modes de défaillance d'un opérateurs humains autrement que par l'observation en situation ou l'expérience.

La méthode FRAM utilisée en complément des techniques usuelles de sûreté de fonctionnement permet de s'intéresser plus avant à l'impact des facteurs humains et sociaux. De plus, la représentation de la dynamique du système à l'aide de mesures qualitatives permet d'imaginer de nouveaux scénarios incidentels ou accidentels et de les étudier par la formulation de nouvelles hypothèses à tester sur le terrain ou en environnement simulé.

« Alors que les méthodes classiques de sûreté de fonctionnement permettent de visualiser comment les choses vont mal, FRAM modélise l'exécution d'une activité ou d'une fonction qui fonctionne bien » [12]. C'est en quoi ces deux méthodes sont complémentaires pour l'étude de risque et vont dans le sens des études de psychologie et d'ergonomie qui elles visent à comprendre l'activité réelle des opérateurs.

## Références

- [1] R. AMALBERTI – *La conduite des systèmes à risque*, Paris : PUF., 2001.
- [2] L. BAINBRIDGE – « Ironies of automation », *Automatica* vol. 19 (1983), p. pp. 775–779.
- [3] F. BELMONTE, K. BERKANI, J. BOULANGER et W. SCHÖN – « Safety enhancement of railway traffic by modern supervision systems », *Seventh World Congress on Railway Research*. (Montreal (Canada)) (WCRR, éd.), 4-8 June 2006.
- [4] — , « Supervision et sécurité : Le projet spica-rail », *Lambda-Mu, 15e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement* (Lille, France), IMDR-Sdf, 9-13 octobre 2006.
- [5] — , « Taking into account human factors in railway supervision », *Ninth International Symposium of the ISSA Research Section : Design process and human factors integration : optimising compagny performance*. (Nice (France)) (I. S. S. A. (ISSA), éd.), 1-3 March 2006.
- [6] C. BIEDER – *Les facteurs humains dans la gestion des risques, évolution de la pensée et des outils*, Hermes, 2006.
- [7] CENELEC – « EN-50126 : Application ferroviaires - spécification et démonstration de fiabilité, disponibilité, maintenabilité et sécurité (fmds) », Norme, CENELEC, 1999.
- [8] — , « EN-50128 : Applications ferroviaires - système de signalisation, de télécommunication et de traitement - logiciels pour systèmes de commande et de protection ferroviaire », Norme, CENELEC, 2001.
- [9] — , « EN-50129 : Application ferroviaires - système de signalisation, de télécommunication et de traitement - systèmes électroniques relatifs à la sécurité pour la signalisation », Norme, CENELEC, 2001.
- [10] E. M. DOUGHERTY – « Human reliability analysis - where shouldst thou turn ? », *Reliability Engineering & System Safety* 29 (1990), no. 3, p. 283–299.
- [11] J.-M. HOC, R. AMALBERTI, J.-M. CELLIER et V. GROSJEAN – « Psychologie ergonomique : tendances actuelles », ch. Adaptation et gestion des risques en situation dynamique, p. 15–48, Paris : PUF, 2004.
- [12] E. HOLLNAGEL – *Barrier analysis and accident prevention*, Aldershot, UK : Ashgate, 2003.
- [13] E. HOLLNAGEL – *Cognitive reliability and error analysis method*, Oxford : Elsevier Science Ltd, 1998.
- [14] J. HOLY – « Some insights from recent applications of hra methods in psa effort and plant operation feedback in czech republic », *Reliability Engineering & System Safety* 83 (2004), no. 2, p. 169–177.
- [15] IEC – 61508 :1998 and 2000, part 1 to 7. *functional safety of electrical, electronic and programmable electronic systems.*, 2000.
- [16] J. REASON – *Human error*, Cambridge University Press, 1990.
- [17] S. SIEGEL et N. CASTELLAN – *Nonparametric statistics for the behavioral sciences*, McGraw-Hill, New York, 1988.
- [18] A. VECTRA – « Proposed framework for adressing human factors in iec-61508 », Tech. report, Health & Safety Executive, 2001.
- [19] R. WOLTJER et E. HOLLNAGEL – « Modelling and evaluation of air traffic management automation using the functional resonance analysis method », *Proceedings of the 8th International Symposium of the Australian Aviation Psychology Association*, April 2008.