Utilisation d'un modèle d'accident systémique comme référentiel commun à une analyse de risque interdisciplinaire

Fabien Belmonte, Jean-Louis Boulanger, Walter Schön

Utilisation d'un modèle d'accident systémique comme référentiel commun à une analyse de risque interdisciplinaire

Fabien Belmonte, Jean-Louis Boulanger, Walter Schön

Laboratoire Heudiasyc, Génie Informatique
Université de Technologie de Compiègne
Centre de Recherches de Royallieu
BP 20529, 60205 Compiègne cedex, France

fbelmont@utc.fr, boulange@utc.fr, wschon@utc.fr
http://www.hds.utc.fr

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[1] et sur la base de la méthode *Functional Resonance Accident Model* (FRAM) développée par Hollnagel [1], 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.**

Mots-clés— **Sûreté de fonctionnement, sécurité, facteurs humains, FRAM, supervision de trafic ferroviaire.**

I. Introduction

Le management des risques industriels est devenu une discipline incontournable pour notre société. Née du besoin de contrôler les dangers induits par l'évolution croissante des technologies (notamment à partir de la deuxième moitié du XX^{e} siècle), la maîtrise des risques industriels a d'abord été formalisée dans les années 60 grâce à la théorie de la fiabilité et de la maintenabilité [2]. Les concepteurs de systèmes à risques ont ensuite intégré ce formalisme aux techniques usuelles de l'ingénierie des systèmes [3]. Ces techniques ont par la suite été normalisées pour des domaines d'activité particuliers : À titre d'exemple, citons [4] pour l'électronique programmable ou [5], [6], [7] pour le domaine spécifique des équipements de signalisation ferroviaire. La prise en compte du facteur humain et organisationnel n'a pas été associée directement à ce mouvement.

Pourtant, les armées[2] ont rapidement compris la position centrale de l'opérateur humain dans la conduite de systèmes à risque, de nombreux travaux sur la psychologie ergonomique (*Human factor* en Américain) ont été menés. La cybernétique de Norbert Wiener [8], par exemple, est née des observations effectuées sur l'opérateur de canon de défense aérienne et d'un raisonnement par analogie entre les lois qui gouvernent la mécanique du système piloté et l'opérateur. De nombreuses études sur l'amélioration des conditions de travail ont été menées avec succès et ont donc indirectement contribué à réduire les risques. Cependant, il demeure difficile à ce jour d'extraire un lien direct entre management des risques et l'apport des sciences humaines et sociales. Le référentiel méthodologique établi au fil des ans pour le management des risques comprend des outils spécifiques à l'évaluation de la fiabilité humaine et depuis peu celle des organisations. Les premières méthodes créées dans les années 60 à 80 ont utilisé le cadre formel de la fiabilité en réduisant la composante humaine à une machine. Cette approche a été fortement critiquée par la communauté scientifique. [9], [10] résument ces critiques. Cette première génération de méthodes a également initié un débat sur la nature de l'erreur humaine [11]. Une deuxième génération de méthode est née tenant compte des aspects humains et sociaux de façon plus approfondie grâce à l'apport des sciences humaines et sociales [10].

Le présent 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 cet article, nous proposons une démarche d'évaluation des risques industriels tenant compte de ces trois disciplines. L'idée consiste à effectuer l'analyse de risques telle que préconisée par les différents référentiels normatifs et d'appliquer une approche complémentaire 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. Dans une première partie, nous présenterons les différences entre les démarches de l'ingénierie et celle des sciences humaines et sociales. La deuxième partie de l'article s'appuie sur la théorie des modèles d'accidents pour présenter l'intérêt de l'approche systémique pour évaluer les niveaux humain et organisa-

[1]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).

[2]L'aéronavale américaine en tête.

tionnel. La méthode *Functional Resonance Accident Model* (FRAM) développée par Hollnagel pour analyser les accidents utilise une cette approche dans laquelle les trois composantes (technique, humaine et organisationnelle) cohabitent et sont en interactions mutuelles. La méthode est présentée et appliquée au cas d'évaluation de la sécurité d'une procédure de protection de travaux ferroviaires où l'opérateur humain est fortement impliqué. 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.

II. Des démarches scientifiques différentes

La composante technique des systèmes sociotechniques est régie par des modèles et des théories issus des sciences exactes. L'analyse de la composante humaine au travail est l'objet d'étude de la psychologie cognitive [12], [13] et de la psychologie ergonomique cognitive [14], [15], [16]. Enfin la composante organisationnelle repose sur les sciences sociales. Ces trois disciplines n'ont pas les mêmes fondements. Les démarches, les techniques de représentation et de modélisation utilisées sont différentes et quelques fois opposées.

Le statut de la modélisation est différent pour chaque discipline scientifique. Les sciences dites « exactes » (mathématiques, physiques notamment) donnent une position dominante aux modèles mathématiques structurés entièrement formalisés. Les sciences de l'ingénieur privilégient ce type de modèle mais n'excluent pas les modèles semi-formalisés associant une structure formelle à un langage graphique. Ces deux types de modélisation sont validés en priorité par la logique et l'expérimentation.

Les sciences du vivant ainsi que les sciences sociales n'ont généralement pas la possibilité de valider de tels modèles par l'expérimentation. L'observation pourrait permettre de contourner cette difficulté si ce n'est que l'observateur introduit un biais dans le système. Le psychologue ou le sociologue doit alors recourir à la modélisation à partir des informations qu'il a pu recueillir sur le terrain ou dans la littérature.

A. L'approche de l'ingénierie

Le management des risques industriels s'appuie sur les techniques de sûreté de fonctionnement, reprenant le formalisme mathématique de la fiabilité et de la maintenabilité développé par Barlow et Proschan [2]. Ce formalisme contient un modèle de fonctionnement des composantes du système bimodal dans lequel le composant n'a que deux états possibles : le bon fonctionnement ou bien la panne. Le système est alors caractérisé par le vecteur d'état de tous ses composants. La démarche consiste a déterminer l'état du système en fonction de ce vecteur caractéristique. L'analyste utilise un raisonnement rigoureux construit par une logique déductive ou inductive pour arriver à cette fin. La méthode de travail repose sur une logique d'exploration systématique des événements ou des composants potentiellement dangereux.

Les méthodes développées par les ingénieurs de sûreté de fonctionnement apportent les outils nécessaires au raisonnement permettant d'expliquer l'apparition des défaillances à différents niveaux du système jusqu'à l'apparition des accidents. (Voir [3] pour une présentation détaillée de ces méthodes).

B. L'approche des sciences humaines et sociales

Le cadre théorique et la méthodologie utilisées pour l'évaluation des facteurs humains sont ceux de la psychologie cognitive et de la psychologie ergonomique cognitive. 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 opérateur effectuant un travail. Le point de vue de cette discipline conçoit l'opérateur comme un système cognitif, c'est à dire comme un système de traitement de l'information à capacité limitée capable d'acquérir, de stocker, d'utiliser des connaissances déclaratives et procédurales dans un environnement de travail.

L'apport de la psychologie ergonomique cognitive est à la fois conceptuelle et méthodologique. Sur le plan conceptuel deux champs d'étude qui ont été abondamment abordés par cette discipline sont pertinents dans le cadre du management des risques des grands systèmes industriels complexes [17], [13], [15], [18], [16] : la supervision et le contrôle de processus de situations dynamique d'une part, et la coopération opérateur - machine d'autre part. Ces études ont débouché sur l'élaboration de concepts et de modèles permettant d'améliorer les conditions de travail des opérateurs et ainsi que de garantir indirectement plus de sécurité.

Contrairement à l'ingénierie de sûreté de fonctionnement, la psychologie cognitive et la psychologie ergonomique cognitive s'appuient largement sur le raisonnement empirique (basé sur des expériences) et est parfois amenée à utiliser un raisonnement flou et discriminant basé sur une logique d'abduction notamment pour supprimer les solutions improbables (l'abduction s'oppose à une logique d'exploration systématique très largement utilisée en sûreté de fonctionnement).

La psychologie cognitive est l'étude empirique des processus de traitement de l'information qui interviennent dans les conduites humaines (et animales). Basées sur l'observation d'événements sur le terrain ou dans un environnement simulé, les méthodes de la psychologie cognitive visent à établir, par des techniques statistiques, des hypothèses qui permettent de prédire des événements dans des situations analogues. Les méthodes statistiques utilisées sont aussi bien descriptives qu'inférentielles. Citons, parmi les plus utilisées, l'analyse de la variance, les tests statistiques paramétriques et non paramétriques, l'analyse factorielle, *etc.*. Les modèles utilisés sont des modèles de dépendance entre variables expérimentales.

Les résultats de l'étude de psychologie cognitive forment un ensemble d'hypothèses validées ou invalidées par l'expérience, ainsi qu'une description qualitative de l'activité cognitive au travail préconisant des recommandations sur l'environnement de travail.

III. Théorie des modèles d'accidents

La démarche analytique en sûreté de fonctionnement représente les accidents comme une succession d'événements dans laquelle la sécurité apparaît comme une propriété des systèmes. L'ingénierie de la résilience [19], dans un cadre

systémique, définit la sécurité comme un phénomène émergeant du système plutôt que comme une propriété.

A. Modèles d'accident

Pour étayer ce propos, Hollnagel [1] classe les modèles d'accidents en trois catégories : séquentiel, épidémiologique et systémique.

Dans le modèle séquentiel, l'accident est expliqué par une succession d'événements reliés entre eux par une relation de cause à effet. Dans le modèle épidémiologique élaboré par Reason [20], l'accident est le résultat des défaillances passives, introduites par des conditions latentes dont l'effet n'est pas immédiat, mais révélées lors de la sollicitation d'une fonction ou d'un composant du système. Enfin, le modèle systémique, introduit par Woods, Leveson et Hollnagel [21], [22], [1] décrit l'accident par l'émergence d'interactions complexes entre les différentes composantes du système. L'accident est la conséquence de coïncidences d'événements plutôt qu'une succession déterministe d'événements [1].

B. Référentiel méthodologique

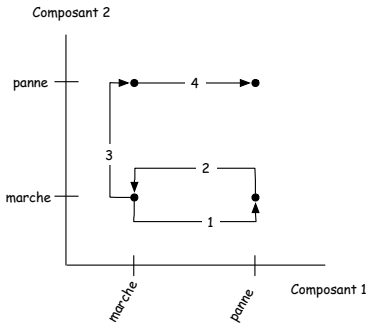

Fig. 1. Représentation séquentielle de la dynamique du système

La sûreté de fonctionnement n'a pas encore développé des méthodes d'évaluations et de scénarisation de la dynamique des accidents relatives aux trois modèles présentés. Dans les faits, seuls les deux premiers modèles d'accident forment un cadre méthodologique en sûreté de fonctionnement. Les principales méthodes sont (voir [3] pour une présentation détaillée) :

- la technique des arbres de défaillance ;
- celle des arbres d'événements ;
- ou encore l'Analyse des Modes de Défaillances, de leurs Effets et de leurs Criticités (AMDEC).

Elles sont largement employées dans l'industrie et préconisées par les référentiels normatifs.

Elles établissent une base de représentation du système à partir de l'état de ses composants. Que ce soit la méthode des arbres de défaillances, celle des arbres d'événements ou bien l'AMDEC, l'état des composants est bimodal : fonctionnement et non-fonctionnement ou multimodal. Ces méthodes permettent d'inférer l'état du système à partir du vecteurs des variables binaires ou multimodales des composants du système et l'on peut suivre l'évolution de l'état du système sur un graphe d'état. À titre d'illustration, la figure 1 représente un système formé de deux composants aux états binaires, cela forme quatre états possibles pour le système, la trajectoire dessinée sur la figure décrit un scénario d'évolution de l'état du système en quatre temps.

Cette représentation des accidents répond entièrement au besoin des systèmes techniques dont la sécurité est basée sur un ensemble de scénarios préétablis contre lesquels le système doit se prémunir. Toutefois elle s'avère trop réductrice lorsqu'il s'agit de traiter des événements impliquant les humains et les organisations. L'assimilation des opérateurs humains à un système bimodal va à l'encontre des modèles de la psychologie cognitive. Pour s'affranchir de cette simplification, les modèles systémiques transfèrent l'étude des composants à l'étude des fonctions du système. L'objectif étant de pouvoir représenter la dynamique du système sociotechnique dans un continuum basé sur des mesures des fonctions exercés par le système. La figure 2 présente une trajectoire continue de l'évolution d'un système effectuant trois fonctions. La difficulté réside dans la recherche d'une mesure efficace des fonctions.

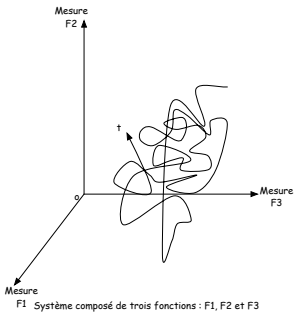

Fig. 2. Représentation de la dynamique du système dans un continuum

C. Un référentiel commun : la systémique

L'avantage immédiat de l'approche systémique est une meilleure intégration des études orientées facteurs humains avec celles de la sécurité, notamment en corrigeant le référentiel de l'étude. Dans la perspective de Woods et d'Hollnagel [23], [24], [25], les systèmes sociotechniques sont des systèmes cognitifs, ils les nomment *Joint Cognitive Systems*. Les auteurs ont développé une nouvelle branche de l'ingénierie des interactions hommes machines appelée *Cognitive Systems Engineering* (CSE) [26], [27]. Les systèmes Humains-Machines ont traditionnellement été analysés séparément et à cela venait s'ajouter l'étude des interactions. Pour les fondateurs de CSE cette décomposition est insuffisante, une représentation du système dans son ensemble est requise unissant les opérateurs et les machines. Le dénominateur commun est donné par la dimension cognitive du système ainsi réuni.

Toutefois, une représentation essentiellement globale du système ne permettra pas de réaliser l'amélioration de la sécurité. En effet, les relations à l'intérieur du système n'ont pas toutes la même intensité et les mêmes conséquences pour la sécurité. [28] énonce un bilan mitigé des représentations systémiques dans les études de sécurité. L'auteur conclut sur le nécessaire rapprochement des spécialistes de l'ingénierie de la sûreté de fonctionnement et des spécialistes des sciences humaines et sociales. La réalisation d'études de sécurité à l'aide d'une méthode systémique demeure, à notre point de vue une démarche complémentaire

aux analyses de sûreté de fonctionnement existantes.

IV. La méthode fram

La méthode FRAM développée par Hollnagel [1] (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 linaire (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 utilisé 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 [1], 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 assimilé à des signaux non linéaires. D'autre part, Hollnagel utilise la superposition des signaux comme modèle de dépendance fonctionnel 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 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 qu'elle 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 trois étapes appliquées à l'étude d'une activité ou d'une fonction du système qu'il faudra préciser.

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 3). Ces attributs servent de connecteurs entre les fonctions ou activités élémentaires :

Inputs (i) : La ou les entrées de la fonction ;

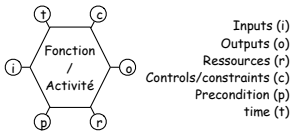

Fig. 3. Codage des fonctions dans FRAM (Hollnagel, 2003)

Outputs (o) : La ou les sorties de la fonction ;

Ressource (r) : La ou les ressources nécessaires au traitement de la fonction ;

Time (t) : Le temps nécessaire à la réalisation de la fonction ;

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 nécessairement être satisfaits pour que la fonction soit opérationnelle.

La deuxième étape consiste à déterminer le potentiel de variabilité de chacune des fonctions. FRAM classe les fonctions en trois catégories : humaines (H), techniques (T) ou organisationnelle (O). Le potentiel de variabilité des fonctions est déterminé par le poids de onze conditions de performance qui agissent comme autant de facteurs de contexte sur la fonction selon sa catégorie. Les facteurs de contexte utilisés dans FRAM sont issus de la méthode d'étude de la fiabilité humaine d'Hollnagel CREAM *Cognitive Reliability and Error Analysis Method* se reporter à [10] pour une présentation détaillée.

Les conditions de performances (ou facteurs de contextes) sont présentées dans le tableau I avec la catégorie de fonction à laquelle elles s'appliquent. L'action de ces facteurs de contexte peut être positive ou négative sur la performance de l'activité ou de la fonction.

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

TABLE I
Facteur de contexte CREAM

La qualité de chacune des conditions de performance est appréciée par trois valeurs possibles : (1) stable ou variable mais adapté ; (2) stable ou variable mais inadapté ; (3) imprévisible. Il s'agit de déterminer pour chacune des

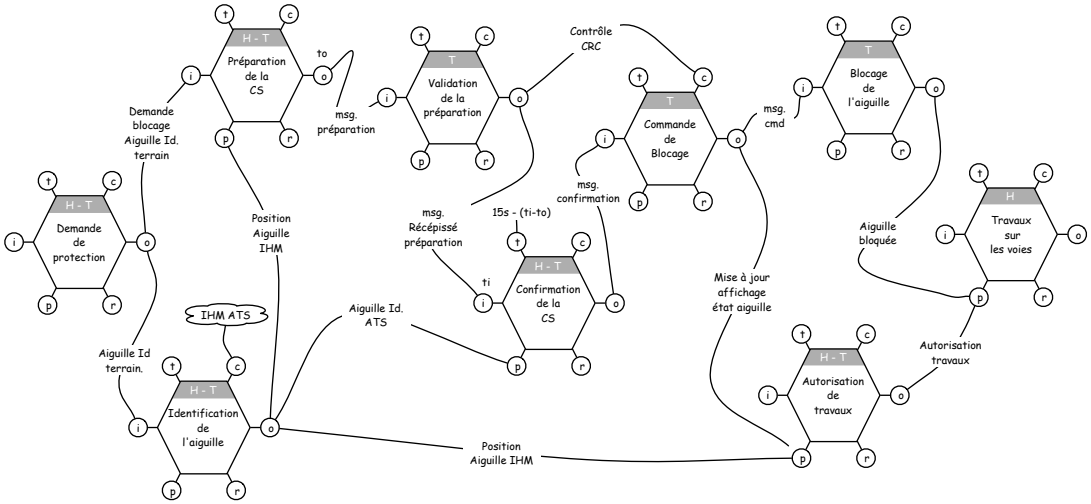

Fig. 4. Réseau FRAM

fonctions les conditions de performance (ou facteurs de contexte) applicables et d'en évaluer la qualité. En général, si une condition de performance est stable ou variable mais adaptée alors la variabilité de performance associée 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.

La troisième étape établit les dépendances entre les fonctions ou activités. Ceci est facilement 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 4 fournit un exemple de réseau FRAM. 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 fonctions. Il s'agit alors de rechercher les résonances fonctionnelles négatives qui affectent le bon déroulement des opérations et de leurs propagations dans le système.

La partie suivante présente un cas d'étude de la méthode FRAM dans le domaine de la sécurité du trafic ferroviaire.

V. Application à la supervision de trafic ferroviaire

A. Contexte de l'étude

Depuis quelques années, la supervision de trafic ferroviaire a été considérablement transformée. Autrefois bâtie sur l'omniprésence de l'opérateur humain dans les activités, l'arrivée des systèmes informatisés de surveillance et de commande ont réduit considérablement le nombre d'opérateurs 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 [29].

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 technique 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[3], 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 [30], [31]. 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 [32]) 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 procédure (juridiquement, l'opérateur demeure responsable de ses actes).

L'objectif de notre démarche 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.

Afin de présenter l'intérêt d'une approche systémique dans cette démarche interdisciplinaire, nous avons appliqué la méthode FRAM en complément des études de sécurité classiques traditionnelles au cas du blocage d'un appareil de voie en vue de la protection d'une équipe de maintenance. Dans cet exemple, les interactions opérateurs - opérateurs et opérateurs - machines ont un impact sur la sécurité.

B. Présentation du cas d'étude

La protection des équipes de travaux nécessite le blocage des appareils de voies (aiguillages) convergeant vers la zone de travaux. La défaillance du blocage des aiguillages peut s'avérer fatale pour les membres des équipes de maintenance en activité sur les voies.

L'opération est menée en collaboration entre le chef de l'équipe de maintenance et l'opérateur ATS. Elle nécessite

[3]Les systèmes d'enclenchements ont depuis été informatisés.

la commande directe des enclenchements « ultra » sécuritaires par l'opérateur ATS et est en cela réellement atypique puisque la majeure partie des opérations exécutables depuis le PCC sont normalement « filtrées » par ces mêmes systèmes d'enclenchements et l'ATP. Ici, la commande est directement passée sur le système de contrôle commande des protections. Les ingénieurs et les spécialistes de la sécurité ont toutefois prévu une procédure sécurisée que nous appellerons « Commande de Sécurité » (CS).

Cette procédure est une séquence de communication sécurisée entre le poste informatique ATS et le système de protection. Un Code de Redondance Cyclique (CRC) permet de protéger l'intégrité des échanges d'informations numériques entre les machines. Un mécanisme de double commande est demandé à l'opérateur pour s'affranchir des commandes non intentionnelles. La séquence de CS de demande de blocage d'une aiguille pour protection de travaux se déroule de la façon suivante (voir figure 5) :

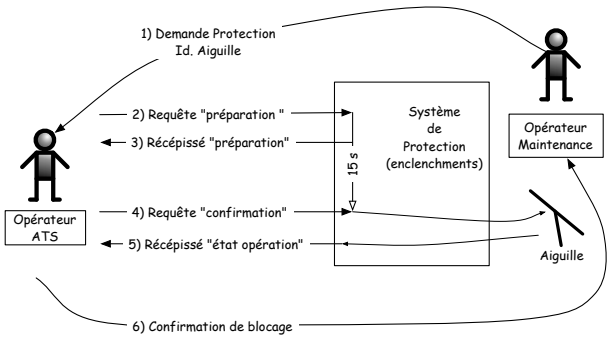

Fig. 5. Procédure CS

1. L'opérateur de maintenance recherche le numéro de l'aiguille à bloquer et demande la protection à l'opérateur ATS ;

2. L'opérateur ATS envoie une requête de préparation au système de protection ;

3. Le système de contrôle commande des enclenchements prépare et envoie un récépissé de la préparation de commande de l'opérateur.

4. L'opérateur ATS valide sa commande en s'assurant que le récépissé est conforme à sa commande et envoie une requête de confirmation ;

5. Le système de contrôle commande des enclenchements s'assure de la validité du message en contrôlant la cohérence du CRC des deux messages reçus par l'ATS, puis réalise le blocage de l'aiguille considérée et envoie un récépissé à l'ATS indiquant le statut de l'opération sur l'aiguille ;

6. Enfin, l'opérateur ATS s'assure du blocage de l'aiguille sur son interface et confirme à l'opérateur de maintenance le blocage de l'aiguille.

C. Étude de sécurité

C.1 Approche analytique classique

La probabilité d'un accident potentiel est liée au temps que l'opérateur ATS met pour détecter une CS non réalisée ou erronée. Sur la base des analyses fonctionnelles, les ingénieurs de sûreté de fonctionnement conçoivent les arbres de défaillances des accidents potentiels après identification

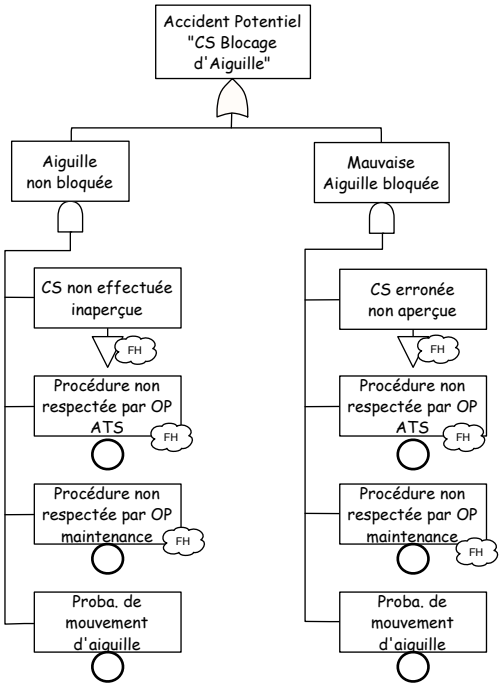

Fig. 6. Arbre de défaillances « Accident sur Blocage d'Aiguille »

au préalable des dangers potentiels. Cette technique, analytique repose sur un modèle d'accident linéaire dans un espace d'état du système discrétisé. L'arbre de défaillance d'un accident potentiel sur défaillance du blocage d'aiguille est présenté dans la figure 6. Les rectangles représentent les événements « défaillances des fonctions ». Les portes logiques indiquent la conjonction ou la disjonction de défaillances des fonctions filles générant la défaillance de la fonction mère. Les cercles signifient que l'événement n'est pas décomposable et qu'il dispose d'une valeur de probabilité propre. Les triangles inversés, à l'inverse des cercles, indiquent que l'événement se décompose en d'autres événements de base représentés dans un autre arbre de défaillance. Pour une meilleure lisibilité, un symbole « FH » est accolé sur les événements de type humain.

Les valeurs de probabilité des équipements techniques sont calibrées sur la base d'études spécifiques du comportement des composants, sur le retour d'expérience et les données du fournisseur. Les probabilités de défaillance des actions des opérateurs sont généralement issues de la littérature dans le domaine de la fiabilité humaine, les travaux de Swain et Rasmussen [33], [34] sont mis à contribution. Par exemple, la probabilité qu'une procédure ne soit pas respectée par un opérateur dépend de facteurs de contexte tels que l'expérience ou l'entraînement. Ainsi, pour un opérateur suffisamment entraîné et pour une procédure habituelle dans l'activité, on considère une probabilité de défaillance de 10^{-3}.

Le résultat de cette méthode appliqué au cas d'une CS de blocage d'aiguille pour protection de travaux montre qu'un accident potentiel peut être généré par la défaillance coordonnée d'au moins quatre fonctions dont les valeurs de probabilité sont inférieures à 10^{-3} chacune.

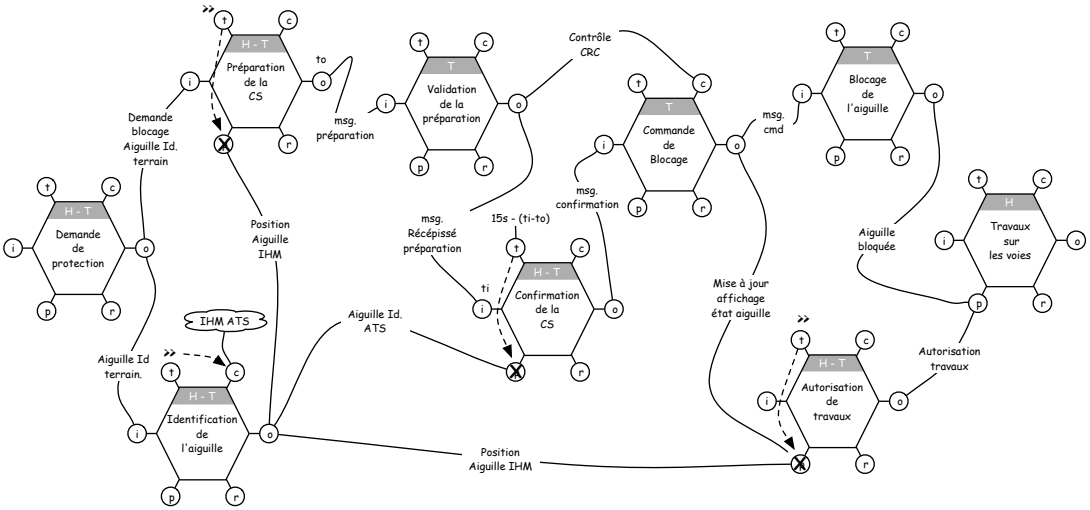

Fig. 7. Modèle FRAM dégradé

C.2 Approche complémentaire avec FRAM

La modélisation de la CS de blocage d'aiguille pour la protection de travaux par la méthode FRAM est synthétisée dans la figure 4. La procédure est initiée par l'opérateur de maintenance qui réalise une demande de protection de sa zone de travaux. Deux informations découlent de cette activité, une demande de blocage et l'identifiant de l'aiguille à bloquer. Ces deux informations sont envoyées à l'opérateur ATS. Sur le schéma, cela se traduit par deux relations de dépendance fonctionnelle entre l'activité de l'opérateur de maintenance et l'activité de l'opérateur ATS qui consiste à identifier l'aiguille sur l'interface de l'ATS d'une part et l'activité de l'opérateur ATS qui consiste à préparer la CS de protection demandée d'autre part.

La procédure requiert en grande partie l'action d'opérateurs humains. Sur cette base il est possible de visualiser un grand nombre de scénarios, simplement en modifiant les conditions de variabilité de performance des fonctions ou des activités réalisées par l'opérateur ATS.

À titre d'exemple, la figure 7 présente un scénario dans lequel la condition de performance de l'opérateur ATS liée au temps disponible est inadaptés ou imprévisible. Sur le schéma, cette pression temporelle est représentée par le signe (») sur l'attribut *time* des actions entreprises par cet opérateur (notation reprise de l'exemple fourni dans [1]). Cette pression peut être expliquée par l'urgence de la situation, ou bien par le trop grand nombre d'objectifs simultanés entrepris par l'opérateur. Ainsi, l'opérateur n'identifie pas correctement l'aiguille à bloquer, La pression temporelle étant trop forte pour exécuté les opérations de contrôle servant à l'identification sur l'IHM de l'ATS. Ceci est représenté par la croix sur les connecteurs des fonctions qui dépendent de l'activité d'identification de l'aiguille. La répercussion négative, associée à la pression temporelle, restreint la précondition de l'activité suivante de l'opérateur qui ne vérifie pas les deux récépissés envoyés par le contrôle commande du système de protection et ne confirme pas le blocage de l'aiguille à l'opérateur de maintenance. En définitive, une CS de blocage d'aiguille a bien été effectuée, mais sur la mauvaise aiguille et les agents de maintenance ne sont pas protégés.

FRAM permet d'analyser de manière plus approfondi les événements de l'arbre de défaillance. L'exemple qui a été présenté a permis d'approfondir l'étude des causes humaines de la porte « Mauvaise aiguille bloquée » de l'arbre de défaillance (figure 6).

D. Étude interdisciplinaire

D'autres scénarios peuvent être décrits sur un même modèle. Ce modèle sert actuellement de support commun entre les spécialistes de la sûreté de fonctionnement et les chercheurs en sciences humaines et sociales spécialistes de la psychologie cognitive. Une plateforme ATS nommée SPICA-RAIL a été installé à Compiègne dans le laboratoire Heudiasyc [35]. SPICA-RAIL sert de support aux études comportementales des opérateurs. Placée dans un environnement simulé de trafic ferroviaire, la plateforme permet de reproduire l'activité d'un PCC. D'une part, le modèle FRAM permet aux expérimentateurs de formuler des hypothèses sur les conditions de performance des opérateurs et leurs répercussions sur la sécurité et, d'autre part, de synthétiser leurs résultats dans un scénario utilisable par les études de sûreté de fonctionnement classique. Une première série d'expériences a été menée, avec pour objectif de valider et de calibrer la faisabilité d'un protocole expérimental, celuici est présenté dans [36]. Les conditions de performance testées dans cette première série d'expériences ont porté sur la pression temporelle. Les temps de détection d'événements anormaux de sujets novices apparentés à des opérateurs en formation ont été mesurés.

Les premiers résultats suggèrent que dans un environnement favorable et simplifié de détection d'événements anormaux, les sujets ont des difficultés à détecter rapidement l'événement anormal. L'étude se poursuit par l'analyse des verbalisations. Replacés dans le contexte du modèle FRAM, ces premiers éléments permettent de donner un ordre de grandeur de la performance de l'opérateur dans un contexte particulier.

D'autres séries d'expériences seront menées sur la plateforme SPICA-RAIL en utilisant le modèle commun présenté dans cet article. Les résultats de ces expériences permet-

tront de préciser les conditions de performance et d'élaborer de nouveaux scénarios d'accidents.

VI. Discussion

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 organisationnel.

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. Une telle entreprise porterait atteinte au raisonnement scientifique des psychologues pour lequel il est impossible de fournir une probabilité d'erreur ou de défaillance de l'activité humaine.

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 que la simple allocation d'une probabilité d'erreur. 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 étudier 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 [1]. 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] E. Hollnagel. *Barrier analysis and accident prevention*. Aldershot, UK : Ashgate, 2004.

[2] Richard E. Barlow et Frank Proschan. *Mathematical theory of reliability*. Wiley, New York, 1965.

[3] A. Villemeur. *Sûreté de fonctionnement des systèmes industriels : fiabilité, facteur humain, informatisation*. Eyrolles, 1988.

[4] IEC. *61508 :1998 and 2000, part 1 to 7. Functional Safety of Electrical, Electronic and Programmable Electronic Systems.*, 2000.

[5] CENELEC. EN-50126 : Application ferroviaires - spécification et démonstration de fiabilité, disponibilité, maintenabilité et sécurité (fmds). Norme, CENELEC, 1999.

[6] CENELEC. EN-50128 : Applications ferroviaires - système de signalisation, de télécommunication et de traitement - logiciels pour systèmes de commande et de protection ferroviaire. Norme, CENELEC, 2001.

[7] CENELEC. EN-50129 : Application ferroviaires - système de signalisation, de télécommunication et de traitement - systèmes électroniques relatifs à la sécurité pour la signalisation. Norme, CENELEC, 2001.

[8] Norbert Wiener. *Cybernetics, Second Edition : or the Control and Communication in the Animal and the Machine*. The MIT Press, 1965.

[9] Ed M. Dougherty. Human reliability analysis - where shouldst thou turn ? *Reliability Engineering & System Safety*, 29(3) :283–299, 1990.

[10] Erik Hollnagel. *Cognitive reliability and error analysis method*. Oxford : Elsevier Science Ltd, 1998.

[11] Ed M. Dougherty. Is human failure a stochastic process ? *Reliability Engineering & System Safety*, 55(3) :209–215, March 1997.

[12] A. Bertrand et P.-H. Garnier. *Psychologie cognitive*. Studyrama, 2005.

[13] R. Amalberti. *La conduite des systèmes à risque*. Paris : PUF., 2001.

[14] F. Darses et M. De Montmollin. *L'ergonomie*. La découverte, 2006.

[15] J-M. Hoc. *La gestion de situation dynamique*. Paris : PUF, 2004.

[16] K.J. Vicente. *Cognitive Work Analysis : Toward Safe, Productive, and Healthy Computer-Based Work*. Mahwah, NJ : Lawrence Erlbaum Associates, 1999.

[17] J-M. Hoc. *Supervision et contrôle de processus : la cognition en situation dynamique*. Grenoble : Presses Universitaires de Grenoble, 1996.

[18] J. Rasmussen. *Mental models and the control of action in complex environments*, chapter 1, pages 41–46. North-Holland : Elsevier Science Publishers, 1990.

[19] E. Hollnagel, D.D. Woods, et Leveson N. *Resilience Engineering*. Ashgate, 2006.

[20] J. Reason. *Human Error*. Cambridge University Press, 1990.

[21] David D. Woods. On taking human performance seriously in risk analysis : Comments on dougherty. *Reliability Engineering & System Safety*, 29(3) :375–381, 1990.

[22] N. Leveson. A new accident model for engineering safer systems. *Safety Science*, 42(4), 2004.

[23] David D. Woods, Emilie M. Roth, et Kevin B. Bennett. Explorations in joint human-machine cognitive systems. *Cognition, computing, and cooperation*, pages 123–158. Ablex Publishing Corp., Norwood, NJ, USA, 1990.

[24] D. Woods et E Hollnagel. *Joint Cognitive Systems*. CRC Press, Inc., Boca Raton, FL, USA, 2006.

[25] E. Hollnagel. Dependability of joint human-computer systems. *SAFECOMP '02 : Proceedings of the 21st International Conference on Computer Safety, Reliability and Security*, pages 4–9, London, UK, 2002. Springer-Verlag.

[26] E. Hollnagel et D. Woods. *Joint Cognitive Systems : Foundations of Cognitive Systems Engineering*. CRC Press, 2005.

[27] Björn Johansson. *Joint control in dynamic situations*. PhD thesis, Linköpings universitet, Institute of Technoloy, 2005.

[28] C. Bieder. *Les facteurs humains dans la gestion des risques, évolution de la pensée et des outils*. Hermes, 2006.

[29] F. Belmonte, K. Berkani, JL. Boulanger, et W. Schön. Safety enhancement of railway traffic by modern supervision systems. WCRR, editor, *Seventh World Congress on Railway Research.*, Montreal (Canada), 4-8 June 2006.

[30] F. Belmonte, K. Berkani, JL. Boulanger, et W. Schön. Taking into account human factors in railway supervision. International Social Security Association (ISSA), editor, *Ninth International Symposium of the ISSA Research Section : Design process and human factors integration : optimising compagny performance.*, Nice (France), 1-3 March 2006.

[31] F. Belmonte, K. Berkani, JL. Boulanger, et W. Schön. Supervision et sécurité : Le projet spica-rail. *Lambda-Mu, 15e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement*, Lille, France, 9-13 octobre 2006. IMDR-Sdf.

[32] Lisianne Bainbridge. Ironies of automation. *Automatica*, vol. 19 :pp. 775–779, 1983.

[33] A-D. Swain et Guttmann H-E. Handbook on human reliability analysis with emphasis on nuclear power plant application. Technical Report NUREG/CR-1278, USNRC, 1983.

[34] J. Rasmussen. Skills, rules, knowledge ; signals, signs, and symbols, and other distinctions in human performance models. *IEEE Transactions on Systems, Man and Cybernetics*, 13 :257–266, 1983.

[35] F. Belmonte, W. Schön, JL. Boulanger, et K. Berkani. Railway traffic supervision research program : Spica rail platform. *EURNEX-ZEL, 14th international symposium "Toward the competitive rail systems in europe"*, Zilina, Rep. Slovaque (EU), 30-31 mai 2006.

[36] F. Belmonte, W. Schön, et JL. Boulanger. Facteur humain et évaluation du risque : Procédure expérimentale spica-rail. *Workshop international : Logique et Transport*, Sousse, Tunisie, 18-20 novembre 2007. IEEE System Man and Cybernetics Society.