VERS UNE INTEGRATION DES FACTEURS HUMAINS DANS LE FORMALISME SAFE-SADT : APPLICATION AU FREINAGE FERROVIAIRE

BENARD V.
INRETS/ESTAS
20 Rue Elisée Reclus BP317
F-59666, Villeneuve d'Ascq

CAUFFRIEZ L., RENAUX D, VANDERHAEGEN F.
LAMIH UMR CNRS 8530 / UVHC
Le mont Houy
F-59313, Valenciennes Cedex 9

Résumé

En accidentologie ferroviaire, le retour d'expérience a montré que les causes majeures d'accidents font une large part à l'erreur humaine et plus généralement aux facteurs humains. Globalement, les analyses de sécurité se focalisent sur un critère quantifiable souvent sans tenir compte des aspects organisationnels, sociaux ou humains pouvant affecter le système. Face à ce constat, nous proposons dans cet article une approche reposant sur le formalisme SAFE-SADT, qui est suffisamment souple et adaptable pour associer fiabilité humaine et sûreté de fonctionnement.

Summary

In rail accident, the feedback has shown that the main causes of accidents are for a large part linked to human error and, more generally, human factors. Overall, safety analysis focus on quantifiable criterion often without taking into account organizational, social or human aspects which can affect the system. Faced with this fact, we propose, in this paper, an approach based on the SAFE-SADT formalism, which is sufficiently flexible and adaptable to associate human reliability and dependability.

Introduction

Les progrès technologiques et scientifiques ont grandement contribué à la réalisation de systèmes industriels compétitifs. En règle générale, ces systèmes sont devenus si complexes qu'il est aujourd'hui difficile d'évaluer leur comportement et les risques qu'ils pourraient engendrer, lorsque ces derniers sont le siège de perturbations. Le modèle d'Embrey met en évidence que les causes d'accidents sont principalement liées aux défaillances techniques et aux erreurs humaines [1]. De nombreux exemples, tels l'accident d'Ariane 5 en 1996 ou la collision ferroviaire de Zoufftgen en 2006 ont montré que ces perturbations pouvaient mener le système dans un état défaillant, non sécuritaire et avoir un impact non négligeable sur certains enjeux socio-économiques essentiellement liés : à la sécurité des hommes et des matériels, à la protection de l'environnement et aux gains de productivité.

Les prévisions et préventions de tels événements font l'objet de préoccupations non seulement de la part des industriels, quel que soit leur domaine (aéronautique, ferroviaire, nucléaire,….) mais également des pouvoirs publics. Dans ce contexte, la sûreté de fonctionnement se révèle cruciale pour maîtriser les risques induits par la défaillance d'un système ou encore par l'erreur d'un opérateur et son évaluation est devenue un critère de référence pour certifier le système et autoriser sa mise en service.

Il apparaît toutefois, que la majorité des travaux de recherche relatifs à la sûreté de fonctionnement se consacre soit à la modélisation du système en écartant volontairement les aspects humains, soit à la fiabilité humaine et à l'étude du comportement de l'opérateur.

Aujourd'hui, il devient impératif de combiner ces deux approches complémentaires pour l'évaluation de la sûreté « homme-machine ».

Cet article se décline en quatre parties. Dans la première, nous rappelons les principes du formalisme SAFE-SADT. Puis, nous proposons quelques pistes pour la modélisation d'un opérateur intégré à ce formalisme, tout en mettant en avant les difficultés liées à la quantification du modèle (hétérogénéité des données « humaines et techniques »). Nous illustrons notre proposition à l'aide d'un système ferroviaire de freinage électropneumatique supervisé par un agent de conduite. La dernière partie conclut l'article, en présentant quelques idées d'extension de notre modèle et prospectives de recherche.

Le formalisme SAFE-SADT

Finalités du modèle SAFE-SADT

Les premières raisons qui ont motivé au développement du formalisme SAFE-SADT visaient à la caractérisation de l'architecture opérationnelle d'un système automatisé et l'évaluation de ses paramètres de sûreté de fonctionnement dès la phase de conception. Ce formalisme s'inspire de la représentation SADT pour l'analyse et la conception des systèmes [2].

Aspects qualitatifs [3, 4]

Un modèle SAFE-SADT est constitué de plusieurs blocs hiérarchiques. Au niveau le plus haut, le bloc A_0 représente le système dans sa globalité. Ce bloc peut être décomposé en plusieurs blocs A_k (où k est le niveau de décomposition) afin de décrire les sous-systèmes et entités qui constituent le système (cf. figure 1).

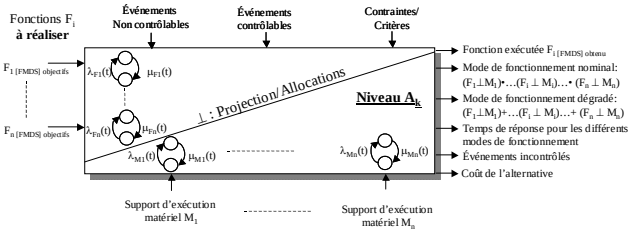

Fig. 1. Formalisme SAFE-SADT

Les paragraphes, qui suivent, listent brièvement les données d'entrées, de sortie et les données utiles à un bloc SAFE-SADT :

- Les données d'entrée d'un bloc A_k correspondent aux différentes fonctions (mission, macro fonctions ou services élémentaires selon le niveau de décomposition) que doit accomplir un système (par exemple : contrôle de vitesse, supervision de la climatisation, etc…). Ces services sont souvent définis dans le cahier des charges du système et leurs performances sont corrélées aux objectifs de sûreté de fonctionnement du système.
- Sous le bloc SAFE-SADT sont spécifiés les différents composants matériels dont les caractérisiques de sûreté de fonctionnement sont intrinsèquement connues (soit fournies par le constructeur, soit obtenues par retour d'expérience ou essais).
- Au dessus du bloc sont placées les contraintes relatives au système étudié (par exemple : contraintes de sécurité, contraintes de performance) et une liste d'événement contrôlables (actions correctives) ou non contrôlables (défaillances aléatoires des matériels ou logiciels), qui peuvent affecter le système durant sa mission.
- L'opérateur de projection, défini par le symbole "⊥", permet de spécifier clairement l'allocation d'un service logiciel sur un composant matériel pour l'exécution d'une fonction et la

caractérisation de l'architecture opérationnelle en termes de chemin de succès 'matériel/fonctionnel'.

- Les données de sorties d'un bloc SAFE-SADT résultent de la projection de la fonction exécutée sur le matériel. Les différents modes de fonctionnement (nominaux et dégradés) sont clairement identifiés par le formalisme SAFE-SADT. Cela permet notamment :
- de calculer les temps de réponse pour les differentes entités opérationnelles, ainsi que les coûts d'une solution alternative,
- d'identifier les événements non contrôlables après la projection. La propagation d'événements non contrôlable pouvant faire obstacle aux objectifs de sûreté de fonctionnement d'autres fonctions, il est intéressant de pouvoir confiner de tels événements dans les blocs SAFE-SADT de niveaux immédiatement supérieurs.

L'utilisation d'une décomposition de type top-down rend possible la modélisation de l'architecture opérationnelle du système et l'identification de ses dépendances (tels que les défaillances de mode commun).

Une fois le niveau le plus bas atteint, il est possible d'évaluer les paramètres FMDS du système global par le biais d'une agrégation des blocs selon une approche bottom-up. Lors de cette étape, le concepteur peut vérifier que les spécifications et les contraintes imposées au système sont satisfaites. Il est également capable de choisir selon plusieurs critères l'architecture opérationnelle la mieux adaptée à ses besoins. A cette étape précise de la modélisation, le formalisme SAFE-SADT met en évidence les ensembles fonctionnels et structurels qui seront implémentés dans la simulation de Monte Carlo.

Aspects quantitatifs

Pour des raisons de coûts et de temps, les paramètres FMDS doivent être évalués au plus tôt durant la phase de conception du système. Une étude bibliographique [5] a montré que les méthodes classiques et déterministes d'évaluation de la sûreté de fonctionnement étaient souvent limitées face à la complexité des systèmes. En conséquence, la quantification des paramètres FMDS par simulation s'imposait et plus particulièrement par simulation de Monte Carlo basée sur une approche système [6], [7], [8]. Cet algorithme de simulation basée sur une approche système requiert en réalité deux simulations (cf. figure 2) :

- une simulation dans l'espace temporel en utilisant le noyau de libre parcours T qui définit la densité de probabilité qu'un système subisse un changement d'état à l'instant t, sachant qu'il était dans l'état B' à l'instant t'.
- une simulation dans l'espace d'état en utilisant le noyau de collision C qui est défini comme la probabilité que le système étant dans l'état B' atteigne l'état B si un événement se produit à l'instant t.

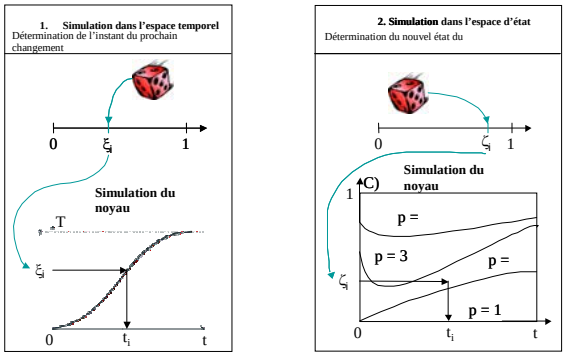

Fig. 2. Simulations temporelle et dans l'espace d'état par approche système

Ces simulations sont exécutées pour un certain nombre d'histoires. Une analyse statistique réalisée sur cet ensemble d'histoire permet d'évaluer les paramètres FMDS [9]. Cet algorithme de simulation de Monte Carlo basée sur une approche système (figure 3), est implémenté dans la méthode SAFE-SADT, et facilite l'évaluation quantitative des paramètres FMDS de l'architecture opérationnelle.

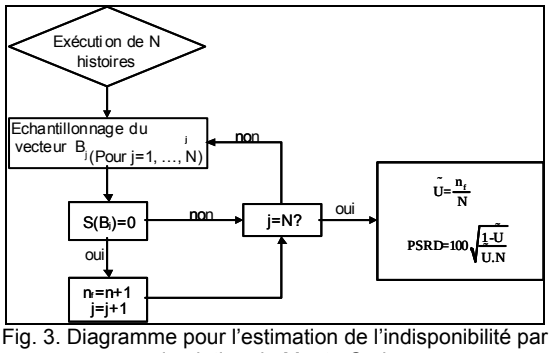

Fig. 3. Diagramme pour l'estimation de l'indisponibilité par simulation de Monte Carlo

Intégration d'un modèle d'opérateur dans le formalisme SAFE-SADT

La fiabilité humaine est aux facteurs humains ce que la sûreté de fonctionnement est aux facteurs techniques. Toutefois, plusieurs divergences existent quant à la définition et la mise en application de ces concepts.

Une analyse de sûreté de fonctionnement se focalise en général sur un critère tel que la sécurité, la maintenabilité, la disponibilité ou la fiabilité sans considérer l'impact de l'affectation d'un critère sur un autre. Lorsque le système de transport est en phase de maturité d'exploitation, le taux d'occurrence de défaillance des composants techniques est supposé faible et constant. Cette hypothèse est difficilement vérifiable et mérite d'être affinée en prenant en compte différentes étapes de fonctionnement telles que la préparation, le démarrage et le déplacement du système de transport en fonction des sollicitations . De plus, ce calcul est souvent simplifié en considérant les occurrences des défaillances comme indépendantes alors que parfois l'usage de probabilités conditionnelles est nécessaire.

Une analyse de la fiabilité humaine peut être effectuée sur deux plans : une analyse hors-ligne et une analyse en ligne :

- La première peut être réalisée par les responsables hiérarchiques ou les concepteurs d'un système de transport. Les normes actuelles n'obligent pas ces derniers à la mettre en œuvre mais leur imposent de démontrer la sûreté de fonctionnement technique. Les études qui en découlent se focalisent surtout sur la sécurité et ne sont pas remises en cause lorsqu'elle est validée par les autorités de tutelle.
- la seconde est gérée par les opérateurs qui utilisent cet outil. Elle intègre plusieurs critères liés aux facteurs techniques, humains et organisationnels. Ses résultats sont variables et dynamiques puisqu'ils dépendent des différences interindividuelles et intra-individuelles des opérateurs humains.

Lorsqu'un composant technique ne réalise pas ce pour quoi il a été conçu, il est considéré comme défaillant et il faut le réparer ou le remplacer. Lorsqu'un opérateur humain ne fait pas les tâches qui lui sont allouées, différents cas de figures peuvent se présenter : il en fait plus que prévu, il en fait moins que prévu, il le fait différemment. Dans la plupart des cas, on ne le répare pas ni le change car il est capable de détecter ses propres erreurs et de les récupérer du fait de ses capacités intrinsèques. De plus, ses erreurs peuvent être involontaires ou volontaires, ce qui met la défaillance humaine en relation avec l'intention. Celle-ci n'est en aucun cas une des caractéristiques des composants techniques ! Enfin, lorsqu'un opérateur décide de ne pas respecter telle ou telle procédure, il peut s'agir d'une erreur de prescription, d'une procédure inadaptée au vue des évolutions technologiques ou de violations permettant d'optimiser d'autres critères que la sécurité par exemple. La défaillance humaine peut

être alors un précurseur de dysfonctionnement dans les règles d'exploitation d'un système.

Une mesure de disponibilité technique peut être la probabilité pour un composant donné d'être prêt à réaliser ses fonctions requises et ce dans des conditions données et à un instant donné. Celle de la fiabilité technique est la probabilité pour un composant donné de réaliser ses fonctions requises, et ce dans des conditions données et sur un intervalle de temps donné. Le concept de disponibilité technique est relatif à un comportement courant ou instantané alors que celui de la fiabilité technique intègre une continuité dans le comportement. La fiabilité humaine rassemble l'ensemble des concepts de la sûreté de fonctionnement technique. Sa mesure peut être définie comme la probabilité, pour un opérateur humain donné, de réaliser ses tâches prescrites dans des conditions données, sur un intervalle de temps donné ou à un instant donné et de ne pas réaliser de tâche supplémentaire nuisible au bon fonctionnement du système. Les conditions dans lesquelles ces probabilités ont été calculées sont rarement explicitées. Il est alors difficile de comparer des probabilités pour lesquelles les unités de mesure peuvent être différentes. Par exemple, un calcul du nombre d'échecs sur le nombre total de sollicitations n'est pas comparable avec le ratio défini par le nombre d'échecs par unité de temps !

Différentes approches permettent d'étudier la fiabilité humaine [10]. Toutefois, plusieurs études comparatives ont montré que les résultats engendrés par les méthodes d'analyse de la fiabilité humaine restent hétérogènes. Les points sensibles semblent être le calcul de la probabilité d'erreur humaine et la définition d'un modèle comportemental suffisamment représentatif de la réalité. De plus, la plupart des méthodes n'intègrent pas le fait que les opérateurs humains peuvent décider de ne pas respecter une prescription donnée.

L'opérateur Humain est facilement intégrable dans le formalisme SAFE-SADT dans l'hypothèse où ce dernier est modélisé par une entité devant réaliser une ou plusieurs tâches dans des conditions données. Cette entité peut défaillir physiquement, être remplacée, faillir à remplir la tâche qui lui a été confiée, recouvrir une erreur lorsqu'elle est détectée.

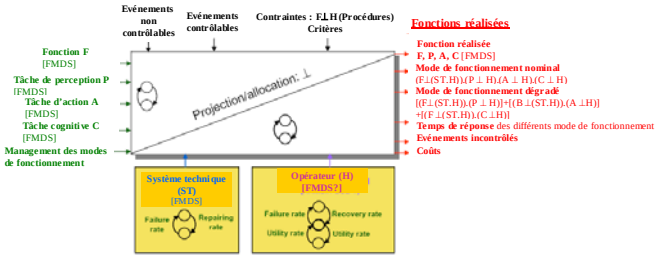

Fig.4. Introduction du facteur humain dans le formalisme SAFE-SADT

La figure 4 introduit l'Homme dans le formalisme SAFE-SADT et propose une modélisation systémique d'un système Homme-Machine où l'opérateur humain se voit attribuer 3 fonctions à exécuter : percevoir, décider, agir en suivant les procédures et moyens prescrits. L'avantage de cette modélisation est de mettre en évidence les interactions entre l'Homme et le système technique par le biais de fonctions techniques telles qu' interfaces, pupitres de commande, alarme….

Naturellement, cette première approche est réductrice, mais elle présente l'intérêt sur le plan qualitatif de déterminer l'importance du rôle de l'opérateur dans un système automatisé (tels certains systèmes de transports guidés) et de définir plus aisément dès la conception du système des systèmes d'aide et des barrières adaptées à l'utilisation du système.

Application du formalisme à un système de freinage électropneumatique ferroviaire type TGV Thalys

Description du système [11]

Le système de freinage des rames Thalys est conçu pour permettre l'exploitation à grande vitesse sur les LGV (Lignes Grande Vitesse). Il a été réalisé de manière à pouvoir assurer un service sans restriction dans certains cas de modes dégradés : la rame peut circuler à vitesse maximale sur les LGV avec un bogie moteur isolé électriquement et un bogie porteur isolé. L'installation de systèmes informatiques embarqués sur la rame a permis d'automatiser certaines fonctions et d'installer un dispositif d'aide à la conduite et à la maintenance.
La rame Thalys est équipée :

- d'un frein pneumatique à air comprimé,
- d'une commande de secours pneumatique,
- d'un frein électrique,
- d'un dispositif de frein de stationnement,
- de commandes d'urgence pneumatique,
- d'une commande du frein électropneumatique.

Pour simplifier l'étude, nous nous sommes intéressé au freinage électropneumatique sur un bogie moteur et un bogie porteur, dont le synoptique est présenté par la figure 5.

Fonctionnement du système de freinage [12, 13]

D'une manière générale, le frein électropneumatique distingue deux modes de fonctionnement : un mode de service et un mode de secours (freinage d'urgence). Il correspond à une architecture dans laquelle :

- la commande du freinage est réalisée de manière purement électrique,
- l'énergie d'actuation est pneumatique.

Mode de fonctionnement normal : le freinage de service

La commande du freinage de service est déclenchée par l'agent de conduite au moyen du manipulateur de conduite MP_CO. Le manipulateur gère les commandes de freinage et de traction. Il intègre des potentiomètres qui délivrent une tension proportionnelle à la position du manipulateur ainsi que des contacts sécuritaires permettant de déterminer des incohérences de consigne en cas de panne d'un des potentiomètres. La tension délivrée par les potentiomètres et l'état des contacts de position sont fournis par l'émetteur de consigne, qui se charge de coder la consigne d'effort sous forme d'un signal PWM. Sur chaque véhicule moteur, une baie électronique de commande traction/freinage reçoit les ordres de traction et freinage (signal PWM). Ces signaux sont décodés par cette baie électronique, et sont traduits en un effort à réaliser en traction ou freinage. De même, sur chaque véhicule remorqué, il existe également une baie électronique de commande freinage qui reçoit les ordres de freinage (signal PWM). Ces baies électroniques commandent ensuite un transducteur électropneumatique afin de transformer la consigne d'effort en une pression pneumatique. La pression en sortie du transducteur est délivrée à un relais de débit à travers un sélecteur de circuit (qui laisse passer la plus grande des deux pressions qu'il reçoit en entrée), lequel relais de débit alimente les cylindres de frein du véhicule.

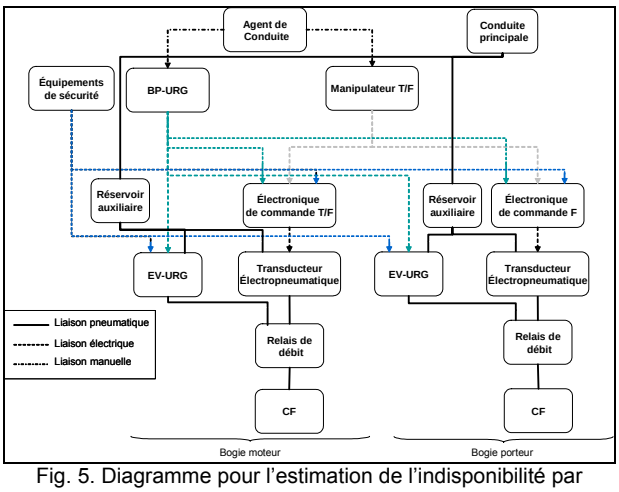

Fig. 5. Diagramme pour l'estimation de l'indisponibilité par simulation de Monte Carlo

Mode de secours : le freinage d'urgence

Le freinage d'urgence est totalement découplé du freinage de service, de manière à garantir un niveau de sécurité élevé. La commande d'urgence est, dans la très grande majorité des cas, réalisée par le biais d'une boucle d'urgence qui parcourt toute la longueur du train, et est bouclée dans le dernier véhicule pour revenir en tête. Pour déclencher le freinage d'urgence, il suffit d'ouvrir l'un des contacts installés en série sur cette boucle pour que celle-ci soit au potentiel nul, indiquant la commande d'un freinage d'urgence. Chacun des contacts installés sur la boucle est actionné par un équipement donné : coup-de-poing d'urgence (BP_URG) ou équipement de sécurité (VACMA, contrôle de vitesse, etc...). Au niveau de chaque véhicule, une électrovalve d'urgence est connectée sur la boucle d'urgence Lorsque la boucle d'urgence est ouverte, chaque électrovalve d'urgence est désexcitée, et délivre une pression prédéfinie correspondant à l'effort de freinage d'urgence. La pression de sortie de l'électrovalve d'urgence est délivrée au relais de débit via le sélecteur de circuit, le relais de débit alimentant les cylindres de frein du véhicule.
En parallèle, chaque baie électronique reçoit l'information de freinage d'urgence par lecture de l'état de la boucle, et force en sortie du transducteur électropneumatique une pression correspondant à l'effort de freinage d'urgence: cette disposition garantit qu'en cas de défaillance de l'électrovalve d'urgence, l'effort de freinage d'urgence sera bien commandé.

<u>Caractérisation de l'architecture opérationnelle</u>

Le système de freinage électropneumatique se caractérise par deux principales macro fonctions : FS : « Freiner en mode de service » et FU : « Freiner en mode d'urgence ». Chacune de ces macro fonctions se déclinera en services élémentaires. Dans le cas d'étude présent, on supposera que pour que le freinage électropneumatique soit réussi, il est nécessaire que les cylindres de frein soient actionnés sur le bogie porteur et sur le bogie moteur.

Description des architectures fonctionnelles, matérielles et opérationnelles

Dans le cadre de l'étude menée, un recensement des différents services et moyens matériels ou humains a été réalisé afin de définir les architectures matérielles et fonctionnelles (l'ensemble des abréviations employées est décrit dans le glossaire fourni en annexe 1).

<u>Définition des services élémentaires pour chaque fonction F_i</u>

Les notations adoptées sont :

- A_F est l'ensemble des fonctions élémentaires, $A_F = \{F_1, F_2 \ldots, F_n\}$,
- A_M est l'ensemble des matériels nécessaires à la réalisation de l'architecture opérationnelle, $A_M = \{M_1, M_2 \ldots, M_k\}$,
- $G(A_F)=\{g_1, g_2, \cdots, g_l\}$ est l'ensemble des parties de A_F projeté sur l'ensemble $P(A_M)=\{p_1, p_2, \cdots, p_k\}$ des parties de A_M.

L'architecture fonctionnelle A_F du système est décrite par l'ensemble des services élémentaires :

A_F={Déclencher_FU, Activer_BP_URG, Gérer_T/F, Délivrer_Air_Comprimé, Déclencher_FS, Respecter_Procédure, Convertir_EE_EP, Ouvir_EV_URGM, Fermer_EV_URGM, Ouvir_EV_URGP, Fermer_EV_URGP, Traiter_Signal_Entrée, Délivrer_Signal_Sortie, Comparer_Pressions, Commander_CF, Gérer_mode_utilisation, Stocker_Air_Comprimé}

Par exemple, l'activation du Freinage de Service Fs peut être décomposée par les services élémentaires suivants :

«Percevoir_Environnement», «Déclencher_F»,
« Gérer_T/F», «Traiter_Signal_Entrée»,
« Délivrer_Signal_Sortie», «Convertir_EE_PE»,
«Comparer_Pressions», «Commander_CF ».

Le tableau 1 désigne l'ensemble des éléments employés dans la décomposition du modèle présenté.

Tableau 1 : désignation des différents éléments

Entité	Désignation	Nom
1	AC	Agent de Conduite
2	EQ_SEC	Equipements de sécurité
3	BP_URG	Bouton poussoir d'urgence
4	MPCO	Manipulateur T/F
5	CP	Conduite Principale
6	EC_T/FM	Electronique de Commande T/F bogie moteur
7	EC_FP	Electronique de commande F bogie porteur
8	RAM	Réservoir auxiliaire bogie moteur
9	RAP	Réservoir auxiliaire bogie porteur
10	EV_URGM	Electrovalve d'urgence bogie moteur
11	EV_URGP	Electrovalve d'urgence bogie porteur
12	TR_EPM	Transducteur électropneumatique bogie moteur
13	TR_EPP	Transducteur électropneumatique bogie porteur
14	RDM	Relais de débit bogie moteur
15	RDP	Relais de débit bogie porteur
16	CFM	Cylindres de frein bogie moteur
17	CFP	Cylindres de frein bogie porteur
18	D_FU	Déclencher Freinage d'urgence
19	D_FS	Déclencher Freinage de service
20	A_BP_URG	Activer bouton poussoir d'urgence
21	G_T/F	Gérer Traction/Freinage
22	D_A_C	Délivrer de l'air comprimé
23	R_PROC	Respecter la procédure
24	CV_EE_EP	Convertir l'énergie électrique en énergie pneumatique
25	O_EV_URG	Ouvrir EV_URG
26	F_EV_URG	Fermer EV_URG
27	TSE	Traiter signal d'entrée
28	DTS	Délivrer tension en sortie
29	CP_P	Comparer les pressions
30	C_CF	Commander le serrage des cylindres de freins
31	ST_A_C	Stocker de l'air comprimé
32	G_MU	Gérer les modes d'utilisation

<u>Description de l'architecture matérielle</u>

L'architecture matérielle A_M du système correspond à l'ensemble des matériels :

A_M={AC, MPCO, BP_URG, EC_TFM, EC_FP, EV_URGM, EV_URGP, TR_EPM, TR_EPP, RDM, RDP, CFM, CFP, RAM, RAP, CP, EQ_SEC}

<u>Choix de l'architecture opérationnelle pour le système global</u>

L'architecture opérationnelle se déduit en projetant l'ensemble $G(A_F)$ des parties de A_F sur l'ensemble $P(A_M)$ des parties de A_M. Cette projection a été réalisée de manière arbitraire pour l'exemple traité.

$$G(A_F) \perp P(A_M)=\{g_1 \perp p_1, g_2 \perp p_2, g_3 \perp p_3, g_4 \perp p_4, g_5 \perp p_5, g_6 \perp p_6, g_7 \perp p_7, g_8 \perp p_8, g_9 \perp p_9, g_{10} \perp p_{10}, g_{11} \perp p_{11}, \quad g_{12} \perp p_{12}\}$$

avec : $G(A_F)=\{g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8, g_9, g_{10}, g_{11}, g_{12}\}$ et $P(A_M)=\{p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9, p_{10}, p_{11}, p_{12}\}$.

L'ensemble des parties $G(A_F)$ et $P(A_M)$ sont précisées dans le tableau 2

Tableau 2 : Description de l'ensemble des parties $G(A_F)$ et $P(A_M)$

i	$G(A_F)$	$P(A_M)$	$G(A_F) \perp P(A_M)$	$g_i \perp p_i$
1	g_1=Déclencher_FU	p_1=EQ_SEC	$g_1 \perp p_1$	Déclencher_FU⊥EQ_SEC
2	g_2=Activer_BP_URG	p_2=BP_URG	$g_2 \perp p_2$	Activer_BP_URG⊥BP_URG
3	g_3=Gérer_T/F	p_3=MPCO	$g_3 \perp p_3$	Gérer_T/F⊥MPCO
4	g_4=Délivrer_Air_Comprimé	p_4=CP	$g_4 \perp p_4$	Délivrer_Air_Comprimé⊥CP
5	g_5=(Respecter_Procédure, Déclencher_F, Déclencher_FU)	p_5=AC	$g_5 \perp p_5$	Percevoir_environnement⊥AC Déclencher_F⊥AC Déclencher_FU⊥AC
6	g_6=Convertir_EE_PE	p_6=TR_EP	$g_6 \perp p_6$	Convertir_EE_PE⊥TR_EP
7	g_7=(Ouvrir_EV_URG,Fermer_EV_URG)	p_7=EV_URG	$g_7 \perp p_7$	Ouvrir_EV_URG⊥EV_URG Fermer_EV_URG⊥EV_URG
8	g_8=(Traiter_Signal_Entrée, Délivrer_Signal_Sortie)	p_8=EC_F	$g_8 \perp p_8$	Traiter_Signal_Entrée⊥EC_F Délivrer_Signal_Sortie⊥EC_F
9	g_9=Comparer_Pressions	p_9=RD	$g_9 \perp p_9$	Comparer_Pressions⊥RD
10	g_{10}=Commander_CF	p_{10}=CF	$g_{10} \perp p_{10}$	Commander_CF⊥CF
11	g_{11}=Stocker_Air_Comprimé	p_{11}=RA	Néant	Néant
12	g_{12}=Gérer_Mode_Utilisation	p_{20}=(EC_F,EC_T/F)	$g_{12} \perp p_{12}$	Gérer_MU⊥EC_F Gérer_MU⊥EC_T/F

Le modèle SAFE-SADT

Le comportement du système global est modélisé au niveau 0 par le bloc SAFE-SADT A_0 (cf. figure 6). La fonction du système global «Assurer le freinage électropneumatique» et ses modes d'utilisation sont présentés avec les objectifs de sûreté de fonctionnement spécifiés dans le cahier des charges.

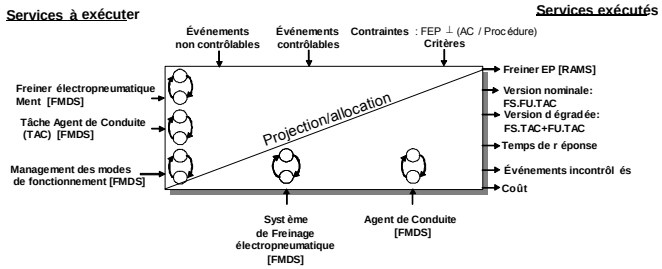

Fig. 6 : Diagramme SAFE-SADT de niveau 0 pour la représentation du système FEP Thalys

La figure 7 illustre une décomposition du modèle SAFE-SADT du système de freinage électropneumatique Thalys.

Les taux de défaillance et réparation associés aux éléments du système sont extraits de divers ouvrages qui tentent de se rapprocher le plus possible de valeurs réelles. Le tableau 3 les temps moyens de fonctionnement (MTTF) et de réparation (MTTR) de chaque élément du système.

Globalement, les taux utilisés s'inspirent d'ouvrages existants [10, 11] et des temps d'exploitation d'un TGV entre deux entrées en Etablissement Industriel de Maintenance du Matériel Roulant pour opérations de maintenance corrective et préventive.

Nous avons dans un premier temps estimé la disponibilité globale du système. La simulation de Monte Carlo a été réalisée pour 2000 histoires et un temps de mission du système de 500 heures à partir de la fonction de structure du système. La figure 9 montre que la disponibilité du système converge vers une valeur asymptotique de 0,7 à partir de 80 heures d'exploitation.

Tableau 3 : Données de fonctionnement et de réparation

Entité	MTTF (h)	MTTR (h)
1	4	2
2	5000	36
3	200	2
4	500	4
5	84	12
6	5000	24
7	5000	24
8	80	12
9	80	12
10	80	6
11	80	6
12	1500	14
13	1500	14
14	1800	6
15	1800	6
16	80	10
17	80	10
18	1300	25
19	150	20
20	350	12
21	250	24
22	240	12
23	2000	2
24	500	24
25	290	12
26	310	12
27	450	24
28	560	24
29	1500	36
30	2400	48
31	350	12
32	850	8

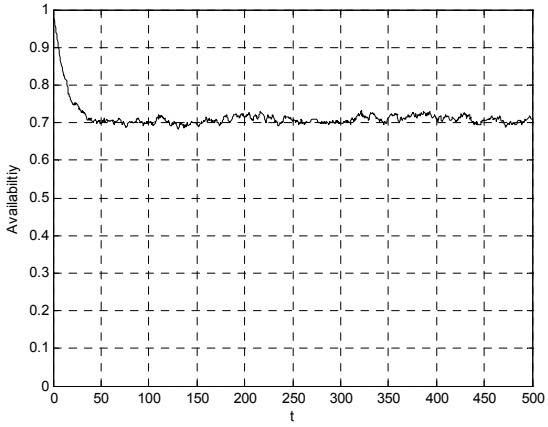

Fig.8. : Disponibilité du système

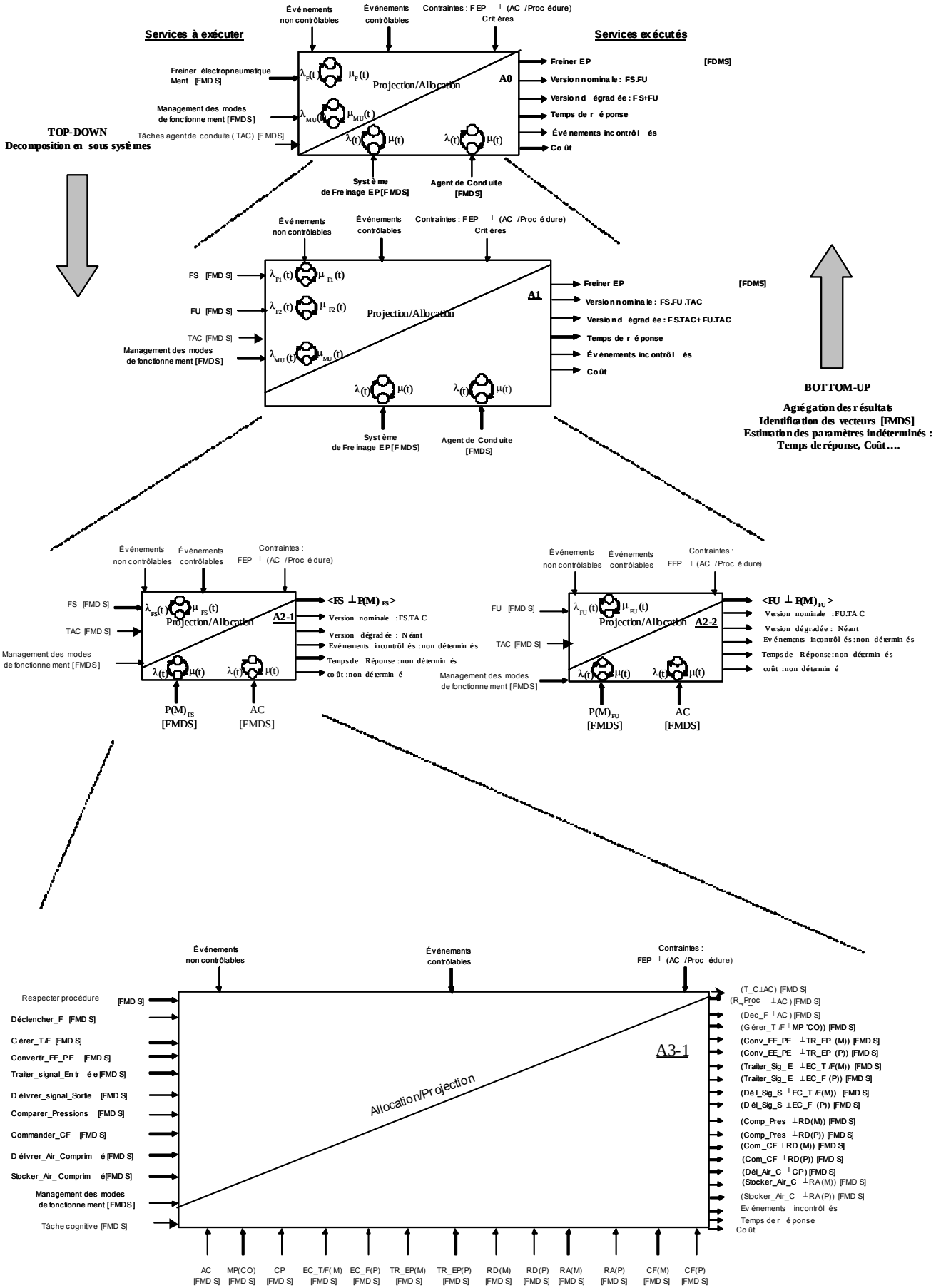

Fig. 7 : Décomposition du système de freinage électropneumatique selon le formalisme SAFE-SADT

La figure 9 présente le facteur de sensibilité S du système global pour le paramètre disponibilité.

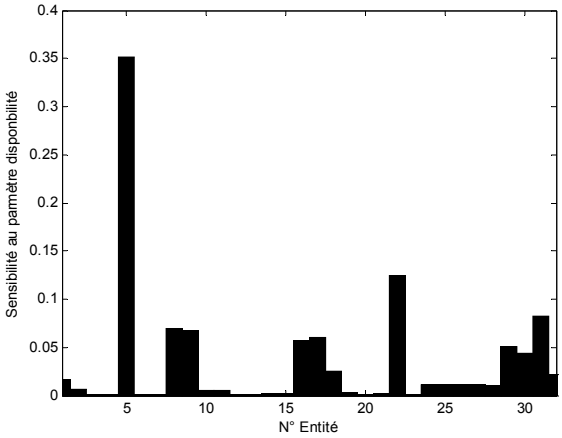

Fig. 9. : Sensibilité des éléments du système

Cet histogramme met en évidence la faiblesse dans la structure du système des éléments 5, 8, 9, 16, 17, 22, 29, 30, 31. Ces éléments présentent des défaillances de mode commun (conduite principale, Cylindres de freins et les services associés) puisque la défaillance de l'un d'entre eux entraîne inévitablement la perte de la mission du système de freinage.

L'agent de conduite n'apparaît pas comme un maillon essentiel pour la fonction de freinage puisqu'il peut être relayé par les équipements de sécurité qui sont très disponibles en exploitation normale. Naturellement il est évident que des perturbations extérieures ne pouvant être détectées par le système de contrôle commande du train (objets abandonnés sur la voie par exemple) peuvent être repérées par l'agent de conduite, dont la présence est essentielle pour la supervision de la conduite.

Conclusion et perspectives

Une méthode unifiée d'analyse de la sûreté homme-machine d'un système donné intégrant les facteurs humain, techniques et organisationnels semble nécessaire à l'évaluation d'un système complexe. Elle doit, d'une part, permettre d'étudier différentes configurations homme-machine et d'en déterminer les conséquences potentielles associées. D'autre part, elle doit identifier les séquences critiques combinant les différents facteurs pouvant générer des situations dangereuses. Cet article se décline en 4 grandes parties. La première partie rappelle les concepts du formalisme SAFE-SADT, la seconde propose une première approche de l'intégration de l'opérateur dans ce formalisme qui est illustré sur un exemple simplifié de système de freinage electropneumatique ferroviaire. Cet exemple permet de mettre en évidence la souplesse du formalisme SAFE-SADT et sur le plan qualitatif l'importance des différents éléments et en particulier le rôle de l'opérateur et ses interactions vis à vis des différentes fonctions du système.

Il semble intéressant de se pencher sur l'aspect quantitatif du modèle unifié présenté. Il conviendrait d'affiner le modèle de l'opérateur humain en s'appuyant sur le modèle BCD pour mener à bien les objectifs cités précédemment [14]. Ce modèle intègre les bénéfices, les coûts et les dangers ou déficits poteniels associés à un comportement donné, et ce par rapport à un comportement de référence. Il permettraitt en outre le calcul de l'utilité d'un comportement donné, l'élaboration de deux modes normaux de contrôle à savoir le contrôle monotone et non-monotone, l'intégration des modes dégradés lors de l'occurrence d'erreurs humaines volontaires ou involontaires et l'intégration des modes de contrôle post-accident pour la gestion des accidents ou sur-accidents. Le contrôle monotone serait identifié à partir de paramètres BCD stables alors que le contrôle non-monotone les déstabiliserait. Par exemple, le contrôle monotone pourrait être relatif aux tâches de surveillance continues, nécessitant une planification sans contraintes d'urgence, et le contrôle non-monotone pourrait être rattaché à des tâches de gestion de crises pour faire face à l'occurrence d'événements particuliers à un instant donné.

Les points sensibles pour cette approche semblent être le calcul de la probabilité d'erreur humaine et la définition d'un modèle comportemental suffisamment représentatif de la réalité.

Remerciements

Ces travaux sont réalisés dans le cadre du projet national SECUGUIDE du PREDIT GO3 et du projet européen MODURBAN du 6e PCRD.

Références

[1] KUMAMOTO H, HENLEY EJ, "Probabilistic Risk Assessment and Management for Engineers and Scientists", 2nd edition, IEEE Press, ISBN : 0-7803-1004-7, 1996

[2] IGL Technology, « SADT, un langage pour communiquer », Eyrolles, Paris, 1989.

[3] Benard, V. 2004. « Evaluation de la sûreté de fonctionnement des systèmes complexes basée sur un modèle fonctionnel dynamique : la méthode SAFE-SADT », Thèse de l'Université de Valenciennes, LAMIH, 2004.

[4] Benard, V. & Cauffriez, L. & Renaux, D. "The Safe-SADT method for aiding designers to choose and improve dependable architectures for complex automated systems", Journal of Reliability Engineering and System Safety, (pp. 179-196). Vol 93/2, February. Elsevier. ISSN 0951-8320, 2008.

[5] Benard, V. , « Evaluation de la sûreté de fonctionnement des systèmes complexes basée sur un modèle fonctionnel dynamique : la. méthode SAFE-SADT », Thèse, Université de Valenciennes, 2004.

[6] A. Dubi, « Monte Carlo applications in systems engineering », Wiley, 2000.

[7] PE. Labeau, E. Zio, « Procedures of monte Carlo transport simulation for applications in system engineering », Reliability Engineering & system safety, pp 217-228, 2002.

[8] B.Bertsche, A. Fritz, « Algorithms for the Monte Carlo simulation of the reliability and availability of mechanical systems, ESREL'01, Turin, 2001.

[9] S PASQUET, « Analyses de sûreté de fonctionnement de systèmes dynamiques à l'aide de diagramme de flux et réseaux de neurones », thèse, Université Technologique de Troyes, 1999.

[10] F. Vanderhaegen, «Analyse et contrôle de l'erreur humaine », Hermès Science Publication - Lavoisier. Cachan, 2003

[11] GEC ALSTHOM Transport SA, "Système de freinage PBKA", FPA 5473 745, 1996.

[12] DJ. Smith, KGL Simpson, "Functional Safety" 2nd edition, Elsevier science, ISBN 0-7506-6269-7, 2004.

[13] Brisou, F, Le frein électro-pneumatique, France,http://pagesperso-orange.fr/florent.brisou, 2008.

[14] Vanderhaegen, F. "The Benefit-Cost-Deficit (BCD) model for human analysis and control". Proceedings of the 9th IFAC/IFORS/IEA symposium on Analysis, Design, and Evaluation of Human-Machine Systems, Atlanta, GA, USA, 7-9 September 2004.

Vers une prise en compte des facteurs humains dans le formalisme SAFE-SADT : Application à un système de freinage ferroviaire

Les progrès technologiques et scientifiques ont grandement contribué à la réalisation de systèmes industriels compétitifs. En règle générale, ces systèmes sont devenus si complexes qu'il est aujourd'hui difficile d'évaluer leur comportement et les risques qu'ils pourraient engendrer, lorsque ces derniers sont le siège de perturbations. Le modèle d'Embrey met en évidence que les causes d'accidents sont principalement liées aux défaillances techniques et aux erreurs humaines. De nombreux exemples, tels l'accident d'Ariane 5 en 1996 ou la collision ferroviaire de Zoufftgen en 2006 ont montré que ces perturbations pouvaient mener le système dans un état défaillant, non sécuritaire et avoir un impact non négligeable sur certains enjeux socio-économiques essentiellement liés : à la sécurité des hommes et des matériels, à la protection de l'environnement et aux gains de productivité.

Les prévisions et préventions de tels événements sont l'objet de préoccupations non seulement de la part des industriels, quel que soit leur domaine (aéronautique, ferroviaire, nucléaire,….) mais également des pouvoirs publics. Dans ce contexte, la sûreté de fonctionnement se révèle cruciale pour maîtriser les risques induits par la défaillance d'un système ou encore par l'erreur d'un opérateur et son évaluation est devenue un critère de référence pour certifier le système et autoriser sa mise en service.

Il apparaît toutefois, que la majorité des travaux de recherche relatifs à la sûreté de fonctionnement se consacre soit à la modélisation du système en écartant volontairement les aspects humains, soit à la fiabilité humaine et à l'étude du comportement de l'opérateur.

Aujourd'hui, il devient impératif de combiner ces deux approches complémentaires pour l'évaluation de la sûreté « homme-machine ». Un nouvel état de l'art est naturellement requis afin d'identifier les méthodologies et les modèles, capables de tenir compte à la fois des aspects techniques et humains. L'objectif de cet article est de proposer, sur la base du formalisme SAFE-SADT, une méthodologie d'évaluation de la sûreté tenant compte du facteur humain.

Les méthodes courantes d'évaluation de la sûreté de fonctionnement sont très délicates à mettre en pratique face à la complexité des systèmes industriels actuels. Du point de vue du concepteur d'un système complexe intégrant des opérateurs humains, les analyses de sécurité et de disponibilité ou de fiabilité sont souvent réalisées séparément et ce de manière indépendante. Par contre, sur le terrain, la gestion des risques effectuée par les opérateurs humains peut prendre en compte différents critères de performance et de sécurité simultanément et ce de manière dépendante. Les capacités humaines d'appropriation du système permettent aux opérateurs de modifier certaines procédures ou d'en créer de nouvelles : ces comportements ne sont en général pas pris en compte dans les méthodes d'analyse de la fiabilité humaine. D'autre part, du point de vue de la sûreté de fonctionnement technique, ces comportements humains sont des comportements défaillants qui nécessitent une réparation ou un changement des composants incriminés. D'une manière générale, dans le cas des opérateurs humains, cette règle ne s'applique pas. Enfin, en phase de croisière d'exploitation d'un système, l'hypothèse de la constance du taux de défaillance technique peut dans certains cas être est reconsidérée.

Ces constats nous ont amené à développer le formalisme SAFE-SADT qui se veut à la fois qualitatif et quantitatif. L'aspect qualitatif vise à caractériser l'architecture opérationnelle du système étudié et la détailler du niveau global au niveau le plus détaillé selon une décomposition multi-niveau. Cela permet notamment de recenser l'ensemble des services élémentaires et ressources nécessaires à leur réalisation à partir des spécifications fournies par le cahier des charges, mais également d'identifier les modes de fonctionnement du système (nominaux ou dégradés). Sur le plan quantitatif, la méthode s'applique à estimer les paramètres FMDS de l'architecture opérationnelle et caractériser d'autres paramètres tels que les temps de réponse des services et fonctions ou encore les coûts moyens de conception et d'exploitation. Le formalisme présenté est suffisamment souple pour permettre l'intégration d'un modèle de comportement d'un ou plusieurs opérateurs agissant selon une procédure ou dans un cadre spécifique. C'est pourquoi, l'article propose une nouvelle démarche d'analyse de la sûreté de fonctionnement d'un système homme-machine. A partir d'une synthèse de modèles de l'opérateur humain et de l'erreur humaine, il discutera de la faisabilité d'intégration de facteurs humains et de leur évaluation dans le formalisme SAFE-SADT

Pour illustrer la méthodologie proposée, une étude est menée qualitativement sur un système de freinage électropneumatique ferroviaire. L'opérateur humain a dans cet exemple un rôle de superviseur du système. Il peut anticiper certaines perturbations extérieures au système et interagir avec le système. Les premiers résultats exploitables mettent en évidence la position de l'homme dans le système au même titre qu'un élément technique. Cela permet rapidement de corriger ou d'optimiser les procédures (ou les règles d'exploitation dans le domaine ferroviaire) pour lesquelles l'homme intervient et de concevoir des barrières de sécurité dès la conception du système.

Cet article se décline en quatre parties. Dans la première, nous rappelons les principes du formalisme SAFE-SADT. Puis, nous proposons quelques pistes pour la modélisation d'un opérateur intégré à ce formalisme, tout en mettant en avant les difficultés liées à la quantification du modèle (hétérogénéité des données « humaines et techniques »). Nous illustrons notre proposition au travers un système ferroviaire de freinage électropneumatique supervisé par un agent de conduite. La dernière partie conclue l'article, en présentant quelques idées d'extension de notre modèle et prospectives de recherche.