De la modélisation des dysfonctionnements d'un système complexe à la déduction des besoins informationnels des utilisateurs : une transition difficile en IHM

Faouzi Moussa, Christophe Kolski, Meriem Riahi

De la modélisation des dysfonctionnements d'un système complexe à la déduction des besoins informationnels des utilisateurs : une transition difficile en IHM

Faouzi Moussa (*), Christophe Kolski (**), Meriem Riahi (*)

(*) LIPP-Dép. Sciences de l'Informatique- Faculté des Sciences Campus Universitaire
1060 Le Belvédère- Tunis, Tunisie
faouzi@gnet.tn

(**) LAMIH - UMR CNRS 8530
Le Mont Houy
F-59313 Valenciennes cedex 9, France
christophe.kolski@univ-valenciennes.fr

RESUME
Dans de nombreux systèmes industriels complexes, l'analyse et la modélisation des dysfonctionnements est une étape indispensable venant en amont des projets. Elle constitue potentiellement une source précieuse pour s'orienter vers la déduction des besoins informationnels des utilisateurs. Toutefois la transition est considérée depuis longtemps comme difficile en IHM et a d'ailleurs été relativement peu étudiée sur des cas complexes. Cet article vise à apporter une première approche de solution. Celle-ci est illustrée par un cas d'étude représentatif d'une situation industrielle.

MOTS CLES : dysfonctionnements, besoins informationnels des utilisateurs, IHM, systèmes industriels.

ABSTRACT
In industrial processes, the dysfunction modelling step is a must. It is performed in the beginning of the design process. Information carried out in this step offers a great opportunity to deduce the users informational needs. However, going from the dysfunction modelling step to the user's informational needs deduction step still seems to be difficult and is often miss studied on complex cases. In this paper, we present a way of solution. An illustration is given too.

CATEGORIES AND SUBJECT DESCRIPTORS: H.5.2 [User Interfaces]: User-centered design; D.2.2 [Design Tools and Techniques]: User interfaces

GENERAL TERMS: Design

KEYWORDS: dysfunctionings, user informational needs, HCI, industrial systems.

INTRODUCTION

Plusieurs démarches méthodologiques globales pour la conception et l'évaluation de systèmes interactifs ont été proposées [3,14,22...]. On en retrouve également concernant le domaine spécifique des systèmes indus-triels complexes [13,16,18,26]. Dans les systèmes où les risques matériels, écologiques, humains dus aux dys-fonctionnements sont importants, l'opérateur humain demeure indispensable en salle de contrôle. D'une part, l'intelligence humaine fait que celui-ci est à même d'assurer une supervision intelligente sans cesse enrichie par l'expérience. D'autre part, la présence humaine s'avère nécessaire pour réagir face à des situations de dysfonctionnement imprévues [7,12,20,24,25]. Dès lors, la conception des IHM peut en particulier être utilement axée sur deux rôles prépondérants : (1) offrir à l'opérateur le moyen de superviser l'état de fonctionne-ment des principaux constituants du système, (2) prépa-rer les moyens qui permettent (voire assistent) son inter-vention en cas de dysfonctionnement. Le recours indis-pensable à la modélisation du procédé, particulièrement dans les applications industrielles complexes, ne semble pas être complètement assimilé et systématique, même si des recherches actives sont menées dans ce domaine, certaines même depuis plus de 30 ans (voir par ex. pour des approches récentes [10]). Depuis les années 90, nous constatons un engouement progressif autour des appro-ches de conception à base de modèle (Model Based De-sign/Development, [28]), s'accélérant suite à la proposi-tion de l'approche MDA (Model Driven Architecture) par l'OMG. Cette classe d'approche implique forcément le recours aux modèles (procédé, tâche, interaction, etc.) dans le processus de conception. Malgré ceci, soulignons que dans la majorité des approches de conception des IHM étudiées, quand, dans le meilleur des cas, le procé-dé est modélisé, celui-ci n'est dans la plupart des cas pas représenté en état de dysfonctionnement. De ce fait, les interfaces produites ne seront adaptées surtout qu'aux si-tuations de fonctionnement normal. L'occurrence d'un dysfonctionnement ramènera le système à une situation critique imprévisible où l'absence d'informations adéquates au contexte anormal rendra la tâche de l'opérateur plus difficile et son niveau de stress potentiellement plus

important. Le besoin en assistance devient alors indispensable. Cet article se compose de trois parties : nous rappelons d'abord un ensemble de méthodes d'ingénierie largement répandues dans les entreprises (certaines sont orientées vers le fonctionnement normal, d'autres vers le fonctionnement anormal), pouvant venir en amont de l'analyse et la modélisation des tâches. Puis, nous proposons une approche visant à faciliter la transition vers la déduction des besoins informationnels. Enfin, nous validons l'approche proposée sur un cas d'étude représentatif d'une situation industrielle.

METHODES ET OUTILS D'ANALYSE ET MODELISATION DE SYSTEME COMPLEXE

Les méthodes d'analyse et de modélisation de systèmes peuvent venir efficacement en amont de la modélisation des tâches, et permettre de préparer la déduction des besoins informationnels des utilisateurs, qui est le plus souvent difficile à mener à bien. Chaque approche méthodologique de conception des IHM devrait être supportée par un ensemble de méthodes, outils et modèles permettant de l'appliquer. La phase d'analyse du système représente, en effet, un pré-requis nécessaire à la conception des IHM. Plusieurs méthodes peuvent être appliquées à ce sujet. Certaines sont dédiées à l'analyse en mode de fonctionnement normal. D'autres sont destinées à l'analyse en mode de fonctionnement anormal. Nous commençons, dans un premier temps, par synthétiser l'ensemble de ces méthodes, en ne sélectionnant que celles qui sont largement répandues dans les entreprises.

Méthodes et techniques d'analyse des systèmes en mode de fonctionnement normal

La complexité croissante des procédés fait qu'une analyse fonctionnelle et/ou structurelle d'une installation s'avère souvent fastidieuse, voire impossible, sans l'adoption d'une ou de plusieurs méthodes. De nombreuses méthodes d'analyse et de modélisation du système et des tâches sont disponibles dans la littérature en Génie Logiciel ou Génie Automatique. Plusieurs classes de méthodes peuvent être distinguées. Une première classe de méthodes dites cartésiennes s'appuie sur un découpage fonctionnel et hiérarchique du système. Citons à titre d'exemples SA (Structured Analysis), SADT (Structured Analysis and Design Technique) et SART (Structured Analysis for Real Time Systems) ; cette classe présente une carence principale au niveau de la description de la composante dynamique du système. Une deuxième classe de méthodes relève de l'approche systémique ; on y procède généralement en deux modélisations complémentaires ; l'une centrée sur les données et l'autre sur les traitements. Parmi les plus connues, citions MERISE et AXIAL. Elles sont mieux adaptées au domaine de l'informatique de gestion qu'à celui des applications industrielles critiques. Une troisième classe regroupe des méthodes dites d'analyse fonctionnelle ; citons la technique par graphes de fluence [29] consistant à décrire le fonctionnement du système à partir des variables caractéristiques et de leurs interactions ; cette méthode peut aboutir à des schémas très complexes, difficiles à lire et à exploiter. Citons aussi MFM (Multilevel Flow Modelling) ayant pour but d'analyser et de modéliser des systèmes industriels continus et complexes, et se basant principalement sur les concepts de flux, de buts et de fonctions [15] ; cette méthode très prometteuse est encore peu utilisée en entreprise. Une quatrième classe regroupe les méthodes orientées objet, ou plutôt maintenant, suite à l'unification de telles méthodes, UML [8] et les variantes ou extensions d'UML ; rappelons que dans l'approche objet on procède à une structuration du système en termes d'objets (encapsulant données et traitements) et relations entre ces objets. Dans les domaines à risques, soulignons l'utilisation des méthodes d'analyse et spécifications formelles (cinquième classe de méthodes), telles que Z ou B, et dont certaines ont fait l'objet de très intéressantes études ou extensions sous l'angle des IHM et de leur validation (voir par exemple [9]) ; de telles méthodes ne font pas l'objet de cet article.

La problématique ici est de savoir choisir les meilleures méthodes d'analyse et outils de modélisation permettant de satisfaire les besoins pour l'application en cours ; ce choix reste un problème récurrent. Des critères de choix sont disponibles par ex. dans [26] et ne seront pas traités ici. Ainsi, il s'avère que la méthode SADT, bien que développée en fin des années 70, reste parmi les méthodes d'analyse les plus pratiques à utiliser pour de nombreux systèmes industriels, même si elle est maintenant supplantée par UML. SADT est particulièrement adaptée à l'analyse et la conception des systèmes complexes le plus souvent en amont du projet [2]. Elle doit cependant systématiquement être associée à d'autres méthodes adaptées à la prise en compte de la dynamique des applications (les réseaux de Pétri étant considérés comme les plus adaptés à ce sujet et ayant été depuis longtemps exploités pour l'analyse et la spécification d'IHM, cf. par exemple [1,5,21], nous les exploiterons par la suite), et aux situations de dysfonctionnement.

Méthodes et techniques d'analyse des systèmes en mode de fonctionnement anormal

Rappelons qu'une analyse des dysfonctionnements doit déboucher principalement sur l'ensemble des variables pertinentes et significatives de l'ensemble des causes possibles d'un dysfonctionnement donné, afin de pouvoir aider l'opérateur à localiser la cause de la panne et à rétablir une situation de fonctionnement normal. Pour modéliser le système en mode dégradé ou de dysfonctionnement, trois principales classes de méthodes sont à distinguer (Pour une revue quasi-exhaustive, voir [6,30]) ; elles sont successivement décrites.

Méthode d'Analyse Préliminaire des Dangers (APD). La méthode APD (Analyse Préliminaire des Dangers) a été utilisée la première fois vers les années 60 aux Etats Unis, dans le cadre de l'analyse de sécurité de missiles.

Ensuite, elle a été formalisée par l'industrie aéronautique, puis généralisée à de nombreuses industries : chimie, nucléaire, aéronautique, etc. Il est généralement recommandé de l'appliquer dès les premières phases de conception du système à risques.

Méthodes d'analyse et regroupement des pannes. La méthode AMDE (Analyse des Modes de Défaillances et de leurs Effets) fut employée à partir des années 60 dans le domaine de l'aéronautique pour l'analyse de la sécurité des avions. Cette méthode inductive permet de : (1) évaluer les effets de chaque mode de défaillance des composants d'un système sur les différentes fonctions du système, (2) identifier les modes de défaillances ayant des effets sur la disponibilité, la fiabilité, la maintenabilité ou la sécurité du système. L'AMDE constitue une analyse préliminaire qui doit généralement être complétée par l'utilisation d'autres méthodes pour l'identification des combinaisons de défaillances pertinentes. La principale critique faite pour cette approche est sa lourdeur qui vient du principe de son analyse faite pour tous les composants du système quelle que soit leur importance. MCPR (Méthode de Combinaisons des Pannes Résumées) vient compléter l'AMDE, qui ne permet généralement d'étudier que les simples défaillances, par l'étude de combinaisons de ces défaillances. En revanche, sa possible lourdeur invite à ne l'employer qu'à bon escient, selon [30]. MTV (Méthode de la Table de Vérité) consiste à recenser toutes les combinaisons d'états (états de fonctionnement et états de pannes) des composants, les unes après les autres et à en étudier leurs effets ; son principe est fort simple mais il se révèle irréalisable pour l'analyse manuelle de grands systèmes, en raison d'un très grand nombre de combinaisons à considérer.

Méthodes d'analyse détaillée causes/effets d'une panne. Le but essentiel de MDS (Méthode de Diagrammes de Succès) est la représentation de la fonction du système par des diagrammes de blocs. Ses limites sont rapidement apparues au début des années 60. La recherche de voies nouvelles et plus fines d'analyse a conduit aux méthodes AMDE et AdD. La méthode AdD (Arbre des Défaillances), aussi appelée Méthode de l'Arbre des Causes (MAC), est née au début des années 60 dans les bureaux de la société Bell Telephone. Son but est de déterminer les diverses combinaisons possibles d'événements qui entraînent la réalisation d'un événement indésirable unique, puis la représentation graphique de ces combinaisons au moyen d'une structure arborescente. La principale limite de cette méthode, réside dans le fait que l'événement indésirable à analyser doit être défini d'une manière précise. MACQ (Méthode de l'Arbre des Conséquences) fut employée pour la première fois entre 72 et 75 dans l'évaluation du risque lié aux centrales nucléaires aux Etats-Unis. Dérivée de la méthode des arbres de décision, elle fut ensuite appelée "méthode des arbres d'événements" (Event Tree Method). C'est l'outil le plus fréquemment utilisé pour la caractérisation et la détermination des accidents potentiels. Elle permet d'identifier les différentes séquences d'événements possibles (acceptables et inacceptables), les représenter, et les évaluer de manière quantitative et qualitative. MDCC (Méthode du diagramme Causes-Conséquences) a été initialement élaborée par le laboratoire RISO au Danemark (début des années 70). Elle a été utilisée comme aide à l'analyse de fiabilité et de risque des centrales nucléaires dans les pays scandinaves. Elle combine les principes utilisés par la méthode déductive AdD et MACQ qui est inductive. C'est une méthode difficile à utiliser pour l'analyse des systèmes trop complexes. Une fois le système analysé, un document de spécification fonctionnelle peut être établi,précisant la structuration du système, l'ensemble de ses variables "pertinentes", le principe de son fonctionnement normal ainsi que ses différents dysfonctionnements possibles. Pour chacun de ces dysfonctionnements, un diagnostic sera élaboré précisant ses symptômes, ses effets et les procédures de recouvrement possibles.

En synthèse, la figure 1 fait ressortir les relations et complémentarités entre ces méthodes.

APPROCHE PROPOSEE

L'approche proposée pour l'analyse, la modélisation et la déduction des besoins informationnels des opérateurs humains se compose de trois étapes. Une première étape d'analyse préliminaire du procédé et de son système de commande est nécessaire, débouchant sur un document rassemblant les données du procédé et ses différentes contraintes techniques et fonctionnelles. Cette étape est réalisée avec les responsables de l'installation industrielle et implique des spécialités du genre ingénierie des systèmes, génie automatique, etc. La seconde étape consiste à analyser le système homme-machine en termes de procédé, système de commande et tâches opérateur. Il s'agit ici d'identifier et de décrire les tâches en précisant l'enchaînement des actions pour leur accomplissement. Des méthodes classiques d'analyse, telles que SADT, AMDE, AdD, sont proposées à cet effet. Cette étape voit la participation des concepteurs de l'installation industrielle, des futurs utilisateurs de l'interface et des ergonomes. La troisième étape consiste en la modélisation de l'interaction homme-machine, exprimante l'interaction entre l'opérateur et l'interface. Une modélisation formelle de l'IHM, moyennant les RdP Interprétés (pour la modélisation de la dynamique), permet, par la suite, de situer en chaque point d'interaction, l'ensemble des besoins informationnels de l'opérateur (BIO) nécessaires. Les étapes suivantes ont pour objectif de choisir les objets d'interactions les plus adaptés, de concevoir, générer, évaluer et valider le système interactif. Dans l'article, ces étapes « classiques » en IHM ne sont pas traitées ; nous ne nous focaliserons donc que sur les trois premières étapes, source de nom-

breux problèmes en IHM. Celles-ci sont illustrées sur un cas représentatif d'un système industriel réel.

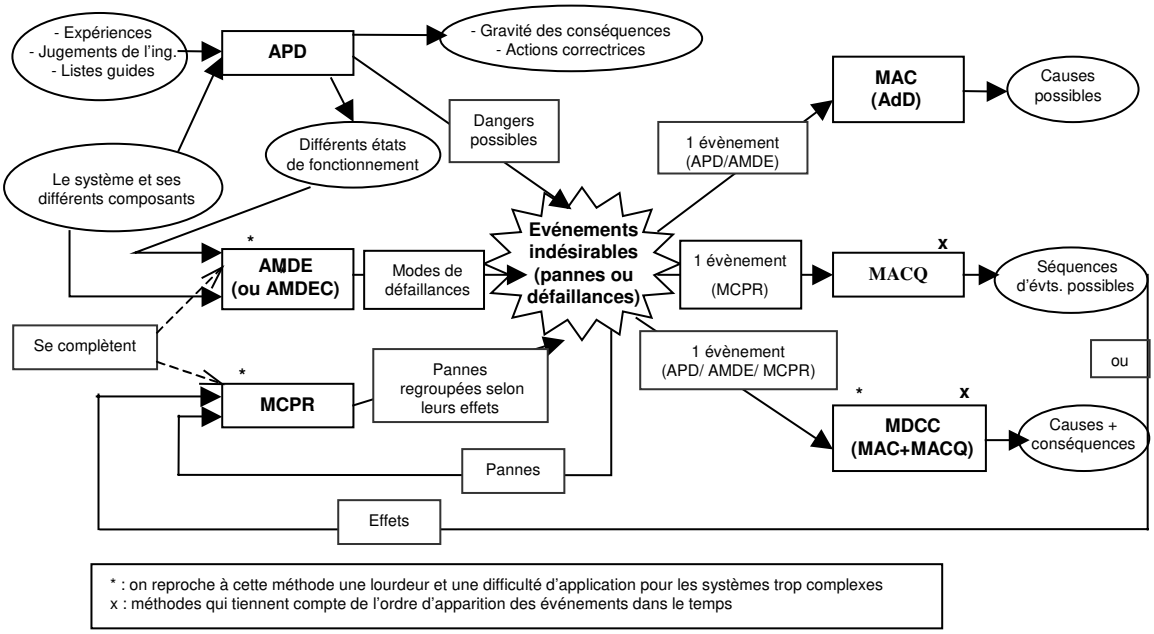

***Figure 1*:** Schéma récapitulatif des principales méthodes pour la sûreté de fonctionnement des systèmes industriels

ETUDE DE CAS

L'application étudiée concerne le cas d'un procédé industriel de fabrication de godets métalliques remplis par une solution chimique préparée préalablement (l'application est détaillée dans [26]), figure 2. Le processus simplifié de préparation comprend deux phases principales : (1) le façonnage des godets par emboutissage de pièces métalliques prédécoupées ; (2) le versement dans les godets d'une dose de solution chimique. La solution est obtenue à partir d'une préparation primaire P et d'un produit S. L'étude a porté sur cette deuxième phase qui met en œuvre deux modules : un module de préparation et un module de remplissage. La fonctionnalité principale de la partie étudiée de ce système consiste à préparer le mélange puis à en remplir les godets.

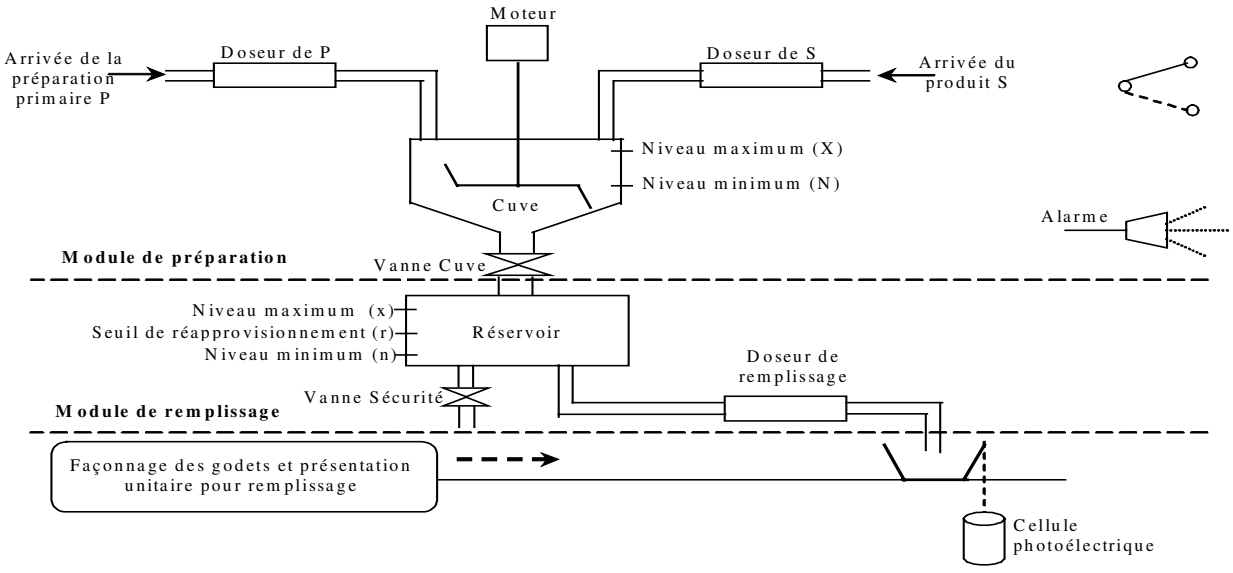

Figure 2: Procédé à superviser en salle de contrôle

Analyse du système homme-machine

Décomposition fonctionnelle du système par SADT. La première étape de la démarche consiste à appliquer une méthode permettant une analyse fonctionnelle, par exemple SADT, pour décomposer le système et déceler les principaux sous-systèmes élémentaires pour les étudier. L'actigramme A0 (figure 3) présente à titre d'exemple la fonctionnalité principale "préparer mélange et remplir godets". Une décomposition de cette fonctionnalité peut révéler, dans l'actigramme A1 (au niveau inférieur), deux sous-fonctionnalités "préparer mélange" et "remplir godets".

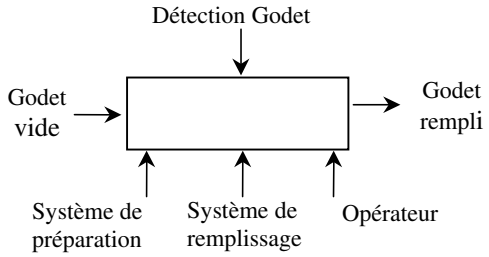

Figure 3 *:* Décomposition du système par SADT (Actigramme A0)

Analyse des dysfonctionnements du système.

- Analyse par la méthode AMDE

Le premier sous-système (S1) est responsable de la fonctionnalité de préparation du mélange. Il est composé de deux doseurs (l'un pour la solution primaire P et l'autre pour le produit S), d'une cuve et d'un moteur pour remuer la solution, d'une vanne-cuve permettant l'écoulement de la solution vers le réservoir et de cinq capteurs (pour mesurer les températures des entrées P et S ainsi que le volume courant dans la cuve et contrôler l'atteinte des niveaux seuil minimum et seuil maximum). Le deuxième sous-système (S2) est responsable de la fonctionnalité de remplissage des godets. Il est composé d'un réservoir, d'une vanne de sécurité permettant l'évacuation du mélange vers l'extérieur, d'un doseur du mélange pour le remplissage et d'un capteur de température de la solution de remplissage.

L'élaboration de l'AMDE consiste donc à considérer ces deux sous-systèmes et étudier pour chacun d'eux, les modes de défaillances de leurs composants, les causes possibles, ainsi que les effets de ces défaillances sur le système, de détection et les éventuelles actions de l'opérateur. Le résultat de cette analyse produit un tableau renseignant sur chaque composant, ses modes de défaillances, les Causes possibles, les effets sur le sous-système concerné, les effets sur tout le système, les moyens de détection et les actions de l'Opérateur.

- Elaboration de l'arbre des défaillances (AdD)

Rappelons que la méthode de l'arbre des défaillances (AdD) suppose les événements indésirables du système à étudier comme étant connus, et procède à une analyse plus fine de ces événements en précisant leurs causes éventuelles et ce, en se référant aux résultats de l'analyse AMDE menée précédemment. Dans le cas de notre application, l'événement redouté principal du système est "l'arrêt de son fonctionnement". Cet événement peut être dû soit à l'arrêt du sous-système de préparation (S1), soit à l'arrêt du sous-système de remplissage (S2). Il faut donc d'analyser de près chacun de ces deux événements indésirables : (E1) : arrêt du sous-système de préparation (S1) et (E2) : arrêt du sous-système de remplissage (S2). L'AdD permet d'identifier les combinaisons possibles d'événements élémentaires qui causent ces dysfonctionnements. Ces événements élémentaires reviennent, en fait, à des défaillances des composants matériels du système. Les principales défaillances discernées par l'AdD sont les suivantes : problème de dosage de la solution primaire P, problème de dosage du produit S, perturbation du niveau du réservoir, perturbation du niveau de la cuve, problème d'évacuation de la solution du réservoir, problème de remplissage du godet, arrêt du moteur, défaillances des capteurs (de température et de volume), problèmes au niveau des vannes (vanne cuve et vanne sécurité).

Analyse de la tâche opérateur

Une fois le fonctionnement du système étudié, les dysfonctionnements possibles analysés, l'étape qui suit consiste à analyser la tâche de l'opérateur humain face à ces différents états de fonctionnement du système (fonctionnement normal et fonctionnements anormaux). En cas de fonctionnement normal, l'opérateur a besoin de savoir que tout marche bien et de surveiller les dérives éventuelles. Cet état de bon fonctionnement peut être reflété au niveau de l'interface par une représentation d'un ensemble de variables pertinentes synthétisant l'état courant du système. Pour notre exemple d'application on considère que, l'état de fonctionnement normal peut être représenté par l'ensemble des informations suivantes :

- le volume courant dans la cuve avec les niveaux min et max (Out.VolCuve, Cs.MinCuve, Cs.MaxCuve),
- l'état du moteur (Out.Moteur),
- le volume courant dans le réservoir avec les niveaux min et max (Out.VolRes, Cs.MinRes, Cs.MaxRes),
- la température de la solution mélange dans le réservoir (Out.TempMel).

Cet ensemble de variables constitue les besoins informationnels de l'opérateur (BIO) en cas de fonctionnement normal. En cas de dysfonctionnement, il doit être averti du mauvais fonctionnement par des signaux d'alarme et un ensemble d'informations en termes de variables représentatives au niveau de l'interface résumant la situation en cours. L'opérateur doit alors réagir le plus rapidement possible et intervenir sur un certain nombre de variables de commande, exécutant sa tâche de correction pour ramener le système en état de fonctionnement normal. Cet ensemble de signaux d'alarme, d'information et

de commande constitue les BIO pour la situation courante et dépendra du cas du dysfonctionnement en question et de la tâche de correction de l'opérateur. L'ensemble de BIO, pour le cas d'une telle situation, ne pourra donc être défini qu'après avoir mené une analyse détaillée de la tâche opérateur. Une analyse préliminaire pour notre cas d'application révèle deux tâches humaines principales : une tâche de surveillance en cas de fonctionnement normal, et une tâche d'analyse et de reprise en cas de dysfonctionnement du système. Cette dernière doit être détaillée relativement à chaque événement 'élémentaire' mis en évidence par l'arbre des défaillances produit par l'AdD. Pour chacun de ces événements élémentaires, l'opérateur doit accomplir une suite d'actions sur les composantes matérielles du système afin de restituer son bon état de fonctionnement. Cette étude a pour objectif de construire un modèle de la tâche opérateur en termes d'actions élémentaires (différents modèles de tâche bien connus en IHM sont décrits dans [4]). Les actions de l'opérateur sont déduites à partir du tableau AMDE et de l'arbre AdD. La manière de déduire la modélisation de l'interaction homme-machine à partir de cette analyse est expliquée dans le paragraphe suivant.

Modélisation de l'interaction homme-machine par RdP

Une fois l'analyse des dysfonctionnements possibles du système effectuée, l'arbre des défaillances élaboré et les tâches opérateur d'intervention analysées, l'étape suivante de la démarche consiste à élaborer un modèle de l'interaction homme-machine en fonction de l'évolution de l'état du système et des interventions de l'opérateur humain afin de pouvoir déduire par la suite l'ensemble des BIO relatifs à chaque état. Cette modélisation peut être basée sur une composition de structures élémentaires de RdP [11,19,23,27]. Les RdP proposés ici sont les RdPI (Réseaux de Petri interprétés) [17] ; ils ont été choisis dans la mesure où ils permettent une validation formelle, non traitée ici. Ce type de réseaux introduit les notions d'événements et de conditions ainsi que la notion d'actions. En effet, une condition de passage (Cj), un événement de déclenchement (Evj) et une action éventuelle (Aj) sont associés à chaque transition Tj d'un RdPI. Pour modéliser l'interaction homme-machine moyennant les RdPI, nous avons convenu d'utiliser les places pour représenter « l'état du comportement de l'opérateur » vis-à-vis de l'évolution du système [11]. Nous considérons qu'une tâche opérateur est composée d'un ensemble organisé d'actions élémentaires. La structure modélisant une action élémentaire (par ex. une action de régulation de température) est donnée en figure 4. La construction du modèle global d'une tâche utilisateur s'effectue à partir de structures de base modélisant les différentes actions élémentaires de l'opérateur. Elle se base sur l'application de différentes opérations de composition. Son principe réside dans le fait que la construction du modèle de la tâche n'utilise que des structures et des règles de composition définies. Cela est important pour assurer par avance de bonnes propriétés au modèle obtenu. Toutes les actions de l'opérateur (élémentaires ou non) sont ordonnées selon des compositions typiques : séquentielle, parallèle, alternative, de choix, itérative ou de fermeture [11]. Cette technique de modélisation, que nous ne détaillerons pas ici, nous permet de déduire les BIO en fonction des changements de contexte de fonctionnement du système industriel.

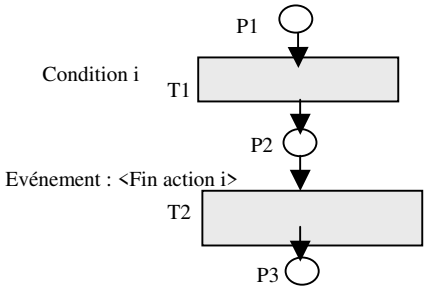

Figure 4 : Structure modélisant l'état d'un opérateur face à une action élémentaire

L'algorithme de passage de l'AdD et du modèle de la tâche opérateur au modèle RdP, est décrit ci-dessous.

Algorithme *Déduire-modèle-RdP* : /* pour un dysfonctionnement donné */

Début :

Etape 1 : parcourir l'arbre AdD jusqu'à localiser le nœud $n_{i,j}$ correspondant à l'événement redouté relatif à cet état de dysfonctionnement

Etape 2 : Traduire la sous-arborescence ayant pour racine le nœud $n_{i,j}$ en un RdP conformément aux règles suivantes :

1- une branche OU est traduite par une composition choix inclusive de RdP *(Composition ou inclusif)*
2- une branche ET est traduite par une composition parallèle de RdP
3- une branche OU exclusif est traduite par une composition alternative de RdP

Etape 3 : Formuler les conditions au niveau des différentes transitions du RdP, en fonction des formules de détection associées aux feuilles de la sous-arborescence (nous faisant ici appel à la fonction formuler-conditions(nœud $n_{i,j}$) que nous ne détaillerons pas ici).

Fin

Le modèle de l'interaction homme-machine déduit pour le cas de cette application est présenté dans la figure 5. La place P0 modélise un état de supervision du système en état de fonctionnement normal. P1 modélise l'état de dysfonctionnement : "atteinte du seuil max du réservoir" et P2 modélise l'état de dysfonctionnement "température non conforme". Les transitions T1 et T2 modélisent donc la détection de ces dysfonctionnements moyennant les conditions qui leur sont affectées (c01 et c02) : (1) "atteinte du seuil max du réservoir" (la condition c01 est

"CS.maxRes =1"), (2) "température non conforme" (la condition c02 est "Out.tempMel > 35°C"). Le bloc SRP2 représente le sous réseau qui modélise l'interaction homme-machine face au dysfonctionnement 2. L'autre partie du réseau développée à partir de T3 modélise l'interaction pour le cas du dysfonctionnement 1. Ce bloc est déduit de l'AdD conformément à l'algorithme de passage expliqué ci-dessus. Il est construit à partir d'une composition "ou inclusive" de trois sous réseaux, chacun d'eux modélisant l'interaction face à l'une des causes possibles de cet état de dysfonctionnement.

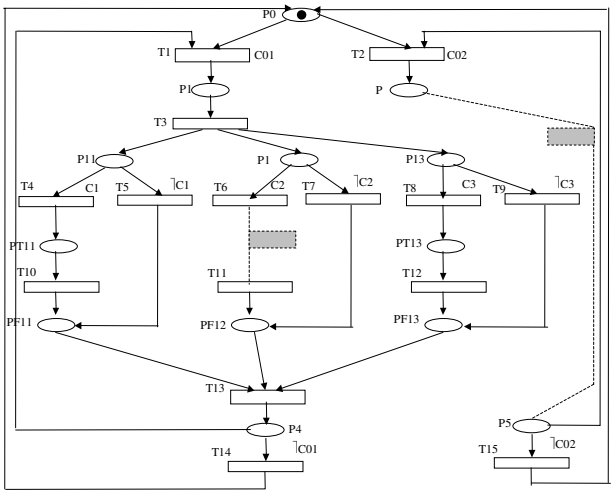

Figure 5 : modèle de l'interaction homme-machine déduit de l'AdD

A partir de l'AdD, nous pouvons distinguer trois causes possibles du dysfonctionnement "atteinte seuil max du réservoir" : une défaillance du capteur de mesure, un problème d'évacuation, et un problème de bouchage de conduites du réservoir. Ces trois causes possibles sont modélisées respectivement par les places P11, P12 et P13. Pour les première et troisième causes, les analyses effectuées par l'AdD renvoient à des événements élémentaires et par la suite à des actions élémentaires de l'opérateur pour changer le capteur défectueux ou réparer les conduites bouchées. Chacune des ces actions est modélisée par une structure élémentaire (bloc [T4, PT11 et T10] pour la première action et bloc [T8, PT13 et T12] pour la deuxième). Pour la cause "problème d'évacuation" modélisée par P12, c'est un événement composé dû à une défaillance du doseur du mélange avec un blocage de la vanne sécurité en état fermée, ou un bouchage de la conduite réservoir-doseur mélange avec un blocage de la vanne sécurité en état fermée, ou un blocage de la vanne cuve en état ouverte avec un blocage de la vanne sécurité en état fermée. Le sous réseau SRP12 (figure 6) modélise cette éventualité. Pour chacun de ces trois cas possibles, une action élémentaire de l'opérateur est nécessaire. Elle consisterait à débloquer la vanne de sécurité de l'état fermée et changer le doseur, ou déboucher la conduite réservoir-doseur ou la changer ou alors débloquer la vanne cuve de l'état ouverte.

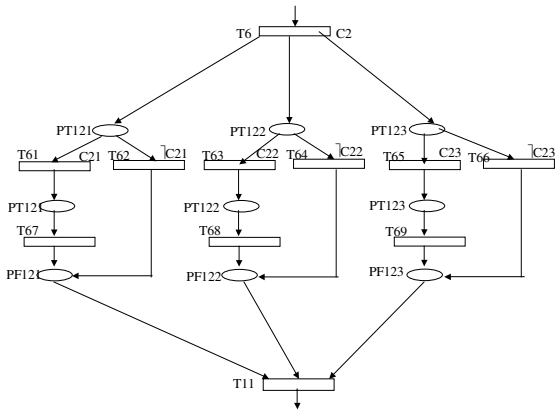

Figure 6 : le sous réseau SRP12

Déduction des BIO

L'étape de déduction des BIO consiste à associer au niveau de chaque état les variables d'informations nécessaires pour les représenter à l'opérateur, et éventuellement les variables de commande avec lesquelles il pourrait accomplir ses tâches de correction. Considérons donc principalement les places PT11, PT13, PT121, PT122 et PT123, qui représentent des états relatifs à la présence des événements particuliers en attente de l'accomplissement de ses tâches de correction. La liste des BIO associés à chacun de ces états est :

- Pour la place PT11, l'opérateur a besoin de savoir les seuils min et max et le volume actuel ; ceci est décrit par l'ensemble des variables : x, n, Cs.MaxRes, Out.VolRes.
- Pour PT13, il a besoin de savoir les seuils min et max, le volume actuel et les états des vannes. Ceci est décrit par : x, n, Cs.MaxRes, Out.VolRes.
- Pour la PT121, il a besoin de savoir les seuils min et max et le volume actuel, mais aussi les états des vannes et la quantité dosée et il aura à agir sur les variables de commande de dosage et d'ouverture de la vanne réservoir. Ceci est décrit par : x, n, Cs.MaxRes, Out.VolRes, Out.VanSecurite, Out.VanCuve, Out.QteMel, Cd.DebDosMel, Cd.OuvVanRes.
- Pour PT123, l'ensemble des BIO est décrit par : x, n, Cs.MaxRes, Out.VolRes, Out.VanSecurite, Cd.OuvVanRes.
- Pour PT122, l'ensemble des BIO est décrit par : x, n, Cs.MaxRes, Out.VolRes, Out.VanSecurite,Cd.OuvVanRes, Cd.OuvVanCuve.

CONCLUSION

Dans les méthodes de conception d'IHM, l'analyse et la modélisation des dysfonctionnements ne sont pas systématiquement mises en avant. Pourtant, elle s'avère indispensable dans certains domaines, en particulier dans les systèmes industriels complexes. Une difficulté en IHM consiste, à partir de l'analyse et la modélisation du système, à déduire les besoins informationnels des opé-

rateurs. Cet article a mis en avant des pistes à ce sujet, tout en illustrant l'approche proposée à partir d'une étude de cas représentative d'un système industriel réel. Les perspectives de recherche concernent l'outillage d'une telle approche. Il s'agirait aussi de faire le lien avec d'autres méthodes provenant de la sûreté de fonctionnement, telles que les méthodes stochastiques.

REMERCIEMENTS

Les auteurs remercient vivement le Prof. M. Moalla pour ses remarques pertinentes relatives à l'étude de cas.

BIBLIOGRAPHIE

1. Abed, M. *Contribution à la modélisation de la tâche par outils de spécification exploitant les mouvements oculaires: application à la conception et à l'évaluation des interfaces homme-machine*. Thèse de doctorat, Valenciennes, France, 1990.
2. Abed, M. *Méthodes et modèles formels et semi-formels pour la conception et l'évaluation des systèmes homme-machine*. Mémoire d'HDR, Valenciennes, 2001.
3. Bodart, F., Hennebert, A.-M., Leheureux, J.-M., Vanderdonckt, J. *A model-based approach to presentation: a continuum from task analysis to prototype*, In Interactive Systems: Design, Specification and Verification, Springer-Verlag, Berlin, p. 77-94, 1995.
4. Diaper, D., Stanton, N. (Eds.) *The handbook of task analysis for human-computer interaction*. Lawrence Erlbaum Associates, 2003.
5. Ezzedine, H., Kolski, C. *Démarche d'évaluation d'IHM dans les systèmes complexes, application à un poste de supervision du trafic ferroviaire*. Revue d'Interaction Homme-Machine, 5, pp. 91-122, 2004.
6. Fadier, E. *Fiabilité humaine : méthodes d'analyse et domaines d'application*. In J.Leplat et G. De Terssac (Eds.), Les facteurs humains de la fiabilité dans les systèmes complexes, Octarés, Marseille, 1990.
7. Gilmore, W.E., Gertman, D.I., Blackman, H.S. *User-computer interface in process control, a Human Factors Engineering Handbook*. Academic Press, 1989.
8. Jacobson I., Booch G., Rumbaugh I, *Le processus unifié de développement logiciel*. Eyrolles, 2000.
9. Jambon, F., Ait-Ameur, Y., Breholée, B., Girard, P., Guittet, L. Formal Verification and Validation of Interactive Systems Specifications. In Johnson, C., Palanque, P. (Eds.). *Human Error, Safety and Systems Development 2004. Proceedings of HESSD 2004*.
10. Johnson, C., Palanque, P. (Eds.). *Human Error, Safety and Systems Development 2004. Proceedings of HESSD 200*4. ISBN 1-4030-8152-9.
11. Khelil, N. *Modélisation sûre des interactions dans les interfaces homme-machine*. Mémoire de DEA, Faculté des Sciences de Tunis, octobre, 2001.
12. Kolski, C. *Interfaces homme-machine, application aux systèmes industriels complexes* (2ème édition). Éditions Hermès, Paris, 1997.
13. Lepreux, S., Abed, M., Kolski, C. A human-centred methodology applied to decision support system design and evaluation in a railway network context. *Cognition Technology and Work*, 5, pp. 248-271, 2003.
14. Lim, K.Y., Long, J. *The Muse Method for Usability Engineering*, Cambridge University Press, Cambridge, 1994.
15. Lind, M. *Representing goals and fonctions of complex systems : an introduction to Multilevel Flow Modelling*. RISO Laboratory, Denmark, Ref: 90-D-381. ISBN 87-87950-52-9, november, 1990.
16. Millot, P, Debernard, S. Men-machines cooperative organizations: methodological and practical attempts in air traffic control. *Proceedings IEEE SMC*, Le Touquet, France, October 17-20, 1993.
17. Moalla, M. Réseaux *de Petri interprétés et Grafcet*. TSI, 4 (1), 1985.
18. Moussa, F., Kolski, C., Riahi, M. *A model based approach to semi-automated user interface generation for process control interactive applications*. Interacting with Computers, 12, pp. 279-292, 2000.
19. Moussa, F., Riahi, M., Kolski, C., Moalla, M. *Interpreted Petri Nets used for Human-Machine Dialogue Specification in Process Control: principles and application to the Ergo-Conceptor+ tool*. ICAE, 9, 87-98, 2002.
20. Moray, J. *Human factors in process control*. In Handbook of human factors and ergonomics, G. Salvendy (Ed.), John Wiley & Sons, pp. 1944-1971, 1997.
21. Palanque, Ph. *Modélisation par objets coopératifs interactifs d'interfaces homme-machines dirigées par l'utilisateur*. Thèse de l'Université Toulouse 1, Septembre 1992.
22. Palanque Ph, Bastide R. A design life-cycle for the formal design of interactive systems BCS-FACS Workshop on the Formal Aspects of the Human-Computer Interface, *Proceedings FAHCI'96*, Shefield, U.K., September 1996.
23. Palanque, Ph, Bastide, R. *Synergistic modeling of tasks, system and users using formal specification techniques.* Interacting With Computers, 9, 12, pp. 129-153, 1997.
24. Rasmussen, J. *Information processing and human-machine interaction, an approach to cognitive engineering*. Elsevier Science Publishing, 1986.
25. Reason, J. *Human error*. Cambridge University Press, Cambridge, 1990.
26. Riahi, M. *Contribution à l'élaboration d'une méthodologie de spécification, de vérification et de génération semi-automatique d'interfaces homme-machine : application à l'outil Ergo-Conceptor+*. Thèse de Doctorat, Valenciennes, septembre 2004.
27. Riahi, M., Moussa, F., Kolski, C., Moalla, M. Use of interpreted Petri nets for human-machine dialogue specification in process control. *Proceedings ACIDCA'2000*, 22-24 March, Monastir, Tunisia, 2000.
28. Szekely, P. Retrospective and Challenges for Model-Based Interface Development, in: Bodart, F., Vanderdonckt, J. (eds.), *Proc. of the Eurographics Workshop, Design, Specification and Verification of Interactive Systems '96*, pp. 1–27, Springer, 1996.
29. Sinclair, I.A.C., Sell, R.G., Beishon, R.J., Bainbridge L. *Ergonomic study of L.D. Waste-heat boiler control room*. Journal Iron and steel inst., 204, pp. 434-442, 1965.
30. Villemeur, A. *Reliability, availability, maintainability and safety assessment (vol.1 & 2).* John Wiley & Sons, 1992.