Erreur humaine, modèles de tâches et description formelle pour la conception et l'évaluation des systèmes critiques et tolérant aux erreurs

Sandra Basnyat

LIIHS – IRIT. 118, route de Narbonne, 31062, Toulouse, France
basnyat@irit.fr

RESUME
Cet article présente une façon d'apporter de la cohérence entre le modèle de tâche et le modèle du système en tenant compte de l'erreur humaine de façon à atténuer la possibilité de cas d'erreur dans les systèmes critiques interactifs. Nous proposons d'étendre un modèle de tâche classique en incorporant l'analyse des erreurs humaine. En raison de la complexité que cela introduit, nous présentons des « task patterns » réutilisables dans l'intention de réduire la quantité du travail. Le modèle de tâche étendu peut alors être systématiquement exploité sur le modèle du système correspondant pour déterminer toutes les fautes du système. Si nécessaire, le modèle du système peut être itérativement révisé pour assurer à la fois la conformité du système aux tâches des utilisateurs, et la tolérance du système aux erreurs des utilisateurs.

MOTS CLES Méthodes Formelles, Système Critique Interactif, Modèles de Tâches, Modèles de Système, Erreur Humaine.

ABSTRACT
This paper presents a way of bringing coherence between the task model and system model while taking into account human error in order to mitigate the occurrence of erroneous events in safety-critical interactive systems. We propose to extend a standard task model by incorporating human error analysis. Due to its complexity, we present re-usable task patterns as a means of reducing workload. The extended task model can then be systematically exploited on its corresponding system model to determine any system flaws. If necessary, the system model can be iteratively redesigned to ensure both system compliance to user tasks and system tolerance to user errors.

KEYWORDS Formal Methods, Interactive Safety-Critical Systems, Task & System Models, Human Error.

INTRODUCTION
Le contexte de ces travaux est à l'intersection de l'analyse, de la conception et de la validation des systèmes critiques interactifs et tolérants à l'erreur. Ceci est accompli en utilisant des techniques issues des méthodes formelles telles que la modélisation des tâches, du système et de l'erreur humaine. En conception, on utilise plusieurs types de modèles basés sur des besoins donnés, qui contribuent à la conception globale (ex. le modèle de tâche, le modèle de l'utilisateur, le modèle de l'environnent, le modèle de la plateforme, le modèle du système, la modèle de présentation et le modèle de conception).

Nos travaux se concentrent principalement sur la modélisation des tâches et du système, en raison de l'orientation de notre équipe et de notre capacité à contribuer à ce domaine. La modélisation des tâches et du système est souvent accomplie par des experts de ces domaines. Il est improbable qu'un spécialiste en facteurs humains conçoive le modèle de tâche puis le modèle du système. Il peut ainsi exister des incohérences entre les deux. Par exemple, une tâche aurait pu être incorporée dans un modèle de tâche qui ne peut pas être accomplie avec le modèle du système. C'est pourquoi nous croyons qu'il est essentiel de garantir la cohérence entre les deux modèles, afin de tester la complétude du système et sa capacité à prendre en charge toutes les tâches de l'utilisateur (nécessaires pour atteindre un but donné) et pour réduire l'occurrence d'accident ou d'incident. Cependant, non seulement les tâches standard de l'utilisateur devraient être prises en compte, mais aussi, les cas erronés. La modélisation des tâches est normalement accomplie sans tenir compte des erreurs des utilisateurs. C'est seulement plus tard pendant le déroulement du cycle de vie, durant les phases essais, que les cas erronés sont découverts. Cette approche préventive permet de réduire la probabilité des cas erronés en concevant un système qui supporte de tels cas. Ceci peut être obtenu en concevant un système qui retournera dans un état sûr après qu'un cas problématique ait eu lieu. Les erreurs humaines jouent un rôle primordial dans l'occurrence d'accidents dans les systèmes critiques tels que l'aviation, les systèmes ferroviaires ou les centrales nucléaires [17]. Ces travaux sont donc nécessaires pour diminuer la possibilité et les effets d'un comportement erroné dans de tels environnements.

VUE D'ENSEMBLE DES TRAVAUX
Dans ce papier et en partie dans la thèse, nous proposons de rendre cohérent le modèle de tâche et le modèle du système, tout en introduisant l'erreur humaine. Jusqu'à présent, nous avons proposé une façon de prendre systématiquement en considération le comportement erroné de l'utilisateur. Ces travaux sont basés sur des résultats précédents dans les domaines de l'analyse de tâche, de la modélisation de tâche et de l'analyse et de l'identification des erreurs humaines.

Nous proposons de définir et d'utiliser les « task patterns » pour traiter la complexité et les répétitions qui apparaissent fréquemment lors de la modélisation des comportements erronés des utilisateurs. Le modèle de tâche peut ensuite être joué sur le modèle du système pour vérifier tous les scenarii possibles et, si nécessaire, dans un processus itératif, de re-concevoir le modèle du système. La Figure 1 montre une version modifiée du processus de maintien de cohérence du modèle du système et du modèle de tâche [10], destiné à démontrer nos idées et l'état d'avancement de nos travaux. La modification est l'addition de l'analyse de la tâche et de l'erreur humaine, ainsi qu'une partie fusion, illustrée par la ligne pointillée. Les quatre phases de modélisation peuvent être identifiées par les flèches circulaires contenant des processus itératifs. Pour plus d'information voir [10].

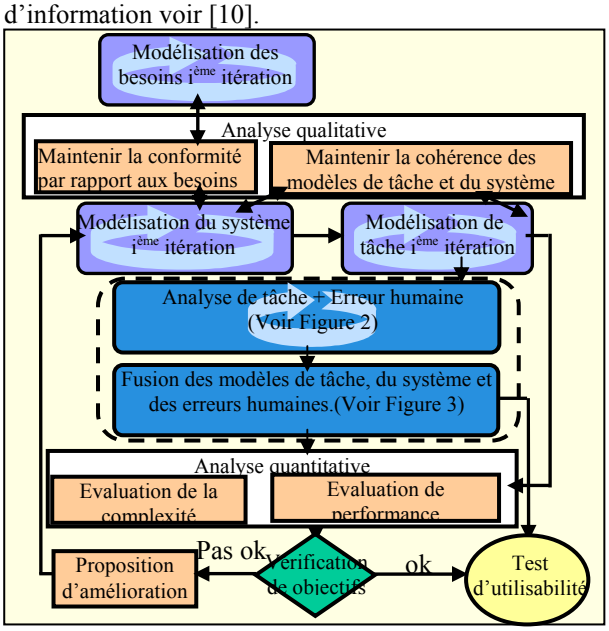

***Figure 1**: Cohérence diagramme*

Dans les sections suivantes, nous fournissons plus de détails sur le diagramme ci-dessus et de ses modifications concernant la modélisation des tâches, l'analyse d'erreur, les « task patterns » et la modélisation du système. Ensuite, nous examinons la fusion de l'information mentionnée auparavant.

LA MODELISATION DES TACHES

L'analyse des tâches et leur modélisation sont largement acceptées en tant qu'élément central pour les approches de conception centrée utilisateur. Le modèle de tâche et la représentation des tâches utilisateur impliquent une forme d'interaction avec un système influencé par son contexte. Un résumé des techniques reconnues d'analyse de tâche est présentées dans le Tableau 1. Les utilisateurs accomplissent des tâches et ils sont structurés en groupe d'activités [15] de façon à obtenir des buts de plus haut niveau.

Acronym	Full Name
HTA	Hierarchical Task Analysis [1]
TKS	Task Knowledge Structure [8]
MAD	Méthode Analytique de Description de tâches [18]
UAN	User Action Notation [5]
GTA	GroupWare Task Analysis [19]
CTT	ConcurTaskTrees [14]
GOMS	Goals, Operators, Methods and Selection rules [3]

***Tableau 1:** Techniques d'analyse de tâche*

Des tâches peuvent être décomposées davantage, correspondant au sous buts de bas niveau. De cette notion de décomposition résulte naturellement un structure en forme d'arbre et ainsi en une représentation hiérarchique du modèle. Cependant jusqu'à présent, la modélisation des tâches ne permet pas la description, la représentation et l'analyse des éventualités inattendues qui pourraient arriver, comprenant l'erreur humaine. Comme le modèle de tâche influence la conception du system, il est important de comprendre comment gérer et maîtriser les événements erronés possibles.

CTT

Au sein de ce travail, nous considérons que ConcurrentTaskTree de F. Paternò [14] est la notation la plus appropriée grâce à son apparence graphique et l'outil associé. CTT est une notation graphique utilisée pour spécifier les modèles de tâche pour des applications coopératives par une structure hiérarchique en indiquant les relations temporelles par des opérateurs. Les modèles de tâche peuvent ensuite être simulés pour étudier les différents chemins d'interaction possibles. La notation est basée sur quatre types de tâche (les tâches abstraites, les tâches utilisateur, les tâches système et les tâches d'interaction), ainsi que sur plusieurs opérateurs temporels (voir [14] pour des détails supplémentaires). Cependant, CTT ne permet pas de prendre en compte le contexte et les conditions d'environnent, les circonstances qui peuvent affecter le procédé, les artefacts manipulés pendant la tâche, la charge de travail cognitive et l'état actuel des utilisateurs (i.e. stress, fatigue), le détail du type d'interaction de bas niveau ou le changement de point d'intérêt de l'utilisateur.

TASK PATTERNS

Les « task patterns » pour la conception des systèmes interactifs est un concept relativement nouveau dont le but est de résoudre les problèmes de conception en utilisant les « task patterns » identifiés auparavant. Introduits à la origine par Paternò [4] et [14] en tant que structures réutilisables pour les modèles de tâche, les « patterns » sont décrits comme des fragment de tâches structurés et hiérarchiques qui peuvent être réutilisés pour construire le modèle de tâche. Nous introduisons ici l'utilisation des « task patterns » comme moyens d'incorporer les comportements erronés dans les modèles de tâche standard et comme méthode pour expliciter les erreurs.

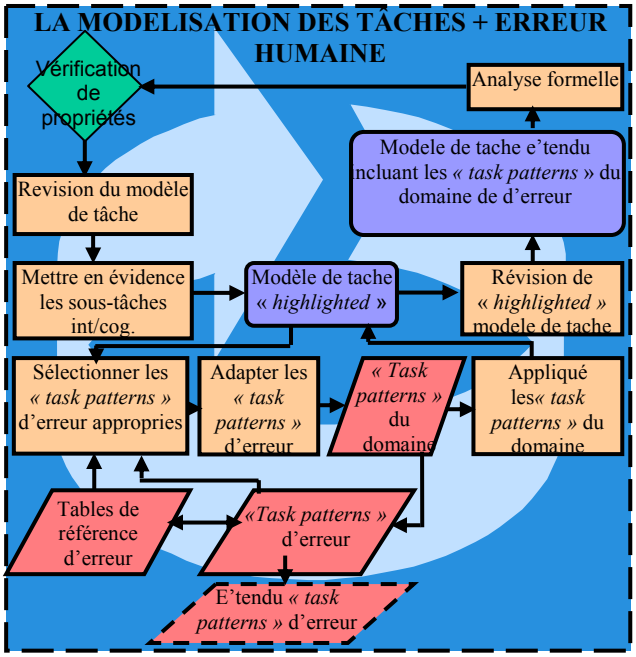

Figure 2: *Modélisation Des Tâches + Erreur Humaine*

ERREUR HUMAINE

80% de tous les accidents d'aviation sont attribués à « l'erreur humaine » [7]. Les systèmes interactifs, et en particulier les systèmes critiques, ont besoin d'être produits dans l'éventualité d'une erreur humaine, pour éviter les catastrophes. Ceci signifie que cela doit être pris en compte au début du processus de conception ainsi que durant la phase de test. Bien que le terme « erreur humaine » apparaisse très discutable, les théories sur les erreurs humaine telles que Rasmussen's [16] SRK, Hollnagel's [6] Phénotypes et Génotypes et Norman's [11] la classification des « slips » peuvent être considérées comme largement acceptables. En utilisant les classifications mentionnées ci-dessus, basées sur la théorie SRK [16], nous avons produit des tables de référence de l'erreur humaine pour l'analyse de l'erreur humaine potentielle dans les modèles de tâche. L'avantage de produire de tels tableaux de référence permet l'identification exacte de type d'erreur très précis durant l'analyse du comportement humain associé à des tâches particulières du modèle de tâche.

LA MODELISATION DES TÂCHES + ERREUR HUMAINE: EXTENSION DU PROCESSUS

La Figure 2 montre en détails le processus interne de la phase optionnelle de « Modélisation des tâches + erreur humaine » ajoutée au diagramme de la Figure 1. En se basant sur le processus existant, le processus étendu commence avec une analyse formelle, la vérification des propriétés et une révision du modèle de tâches. A ce moment, les sous tâches interactives et cognitives sont identifiées à partir du modèle de tâches (puisque ce sont les étapes durant lesquelles les erreurs humaines peuvent être faites) créant un modèle de tâche « highlighted ».

En fonction des nœuds retenus, les « tasks patterns » d'erreur explicite possible peuvent être choisis. En employant les tables de référence de l'erreur humaine (et les « tasks patterns » existants), l'interaction choisie ou les sous-tâches cognitives du modèle de tâche original sont analysées. Par élimination, ces erreurs applicables peuvent être analysées davantage, afin de déterminer les effets de l'erreur sur la tâche. Par ex, si un utilisateur, face un distributeur de billets, entre un code différent de celui attendu, le système va juger que le code est incorrect. Une fois le « task pattern » adapté au domaine, celui-ci venir enrichir la base des « task patterns » déjà existants. Les « task patterns » d'erreur explicite adaptés au modèle de tâche peuvent être connectés aux endroitsmis en avant du modèle de tâche original. Ceci permet une amélioration plus importante du modèle résultant en un modèle de tâches étendu qui inclut les événements à la fois standard et erronés en employant les « tasks patterns ».

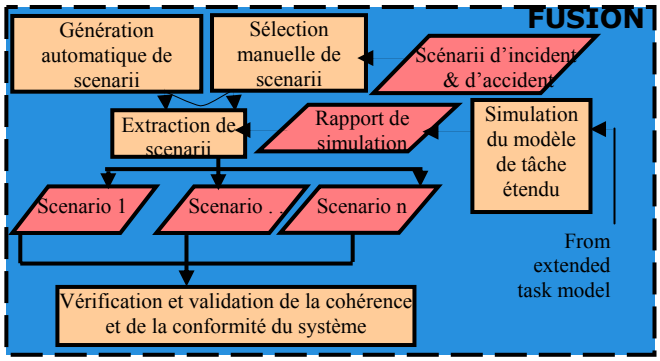

Figure 3:*La phase de fusion*

LA MODELISATION DU SYSTEME

Pour la modélisation du système, nous utilisons l'environnent « PetShop » [10] et la technique de description formelle ICO [2]. Les Objets Coopératifs Interactifs sont un formalisme orienté objet consacré à la modélisation des systèmes interactifs. Ce formalisme est dédié à la construction des applications réparties hautement interactives. Il doit être utilisé par des programmeurs spécialisés, qualifiés en techniques de description formelles, en approches orientées objet et systèmes interactifs répartis [13].

LA FUSION DU MODELE DE TACHE, DE L'ERREUR HUMAINE, DES « TASKS PATTERNS » ET DU MODELE DE SYSTEME

Une fois que le modèle de tâche étendu été créé, celui-ci peut être simulé pour obtenir des scénarii au sein de l'environnement support de CTT (CTTE). Les scénarii extraits peuvent ensuite être appliqués et testés dans l'environnement PetShop sur le modèle du système décrit en réseau de Petri. Si à cette étape du processus il existe déjà un système, celui-ci devra être pris en compte Ce processus assure que lors de la modélisation du système, ou future système, le modèle de tâches peut être testé sur le modèle du système produit en incluant les erreurs humaines déjà identifiées. Ceci limite la

découverte de problèmes durant les phases de test ultérieures au cours du cycle de vie du système. Si nécessaire, le modèle du système peut être re-conçu pour supporter les événements erronés identifiés. Une étude de cas détail décrivant le procède de l'analyse de l'erreur humaine peut être trouvée dans [12].

TRAVAIL EN COURS : VERS DES SYSTEMES CRITIQUES TOLERANTS A L'ERREUR

Nous étudions actuellement les méthodes pour combiner l'erreur humaine et l'analyse de tâches. Ceci implique d'envisager soit d'englober les erreurs au sein du modèle de tâches (comme exposé dans ce papier), soit de les analyser en dehors, en les séparant du modèle de tâches et en les appliquant indépendamment sur le modèle du système. Le processus modifié peut devenir plus utile distinguant les divers groupes de flèches. L'idéal serait que la simulation et l'extraction de tous les scénarii éventuels comprenant toutes les erreurs pour la validation systématique du système soient rendues automatique ; c'est pourquoi nous dirigeons nos travaux dans cette direction. L'analyse de l'erreur ne devrait pas être retreinte à des erreurs basées sur la compétence mais elle devrait incorporer les erreurs basées sur la connaissance et les règles.

BIBLIOGRAPHIE

1. Annett, J. and Duncan, K. *Task Analysis and Training Design, Occupational Psychology*. 41, 1967, pp.211-227.
2. Bastide R. and Palanque P. A Visual and Formal Glue between Application and Interaction. International Journal of Visual Language and Computing, Academic Press Vol. 10, No. 5, pp. 481-507. 1999.
3. Baumeister, L.K., John, B.E., Byrne, M.D.*A Comparison of Tools for Building GOMS Models Tools for Design.* In: Proc. of ACM Conf. on Human Factors in Computing Systems CHI'2000, ACM Press, New York, 502–509 2000.
4. Breedvelt, I., Paternò, F., Sereriins, C. *Reusable Structures in Task Models, Proceedings Design, Specification, Verification of Interactive Systems*. Springer Verlag, pp.251-265 1997.
5. Hix, D. and Hartson, H. R. *Developing User Interfaces*. 1993
6. Hollnagel, E., *The Phenotype of Erroneous Actions: Implications for HCI Design*. In: Weir, G.R.S. and Alty, J.L., (Eds.), Human-Computer Interaction and Complex Systems, Academic Press. 1991
7. Johnson C.W. Failure in Safety-Critical Systems: A Handbook of Accident and Incident Reporting. University of Glasgow Press, Glasgow, Scotland, October 2003. ISBN 0-85261-784-4. 2003
8. Johnson, P., and Johnson, H. *Knowledge Analysis of Task: Task Analysis and Specification for Human-Computer Systems*. In Downton, A. (ed.): Engineering the Human Computer Interface. McGraw-Hill, Maidenhead 1989 119–144
9. Navarre, D., Palanque, P., Bastide, R. *Notations en Interaction Homme-Machine pour une Modélisation Synergique des Tâches et du Système.* Chapitre du livre Ingénierie cognitive: IHM et cognition (Traité des Sciences Cognitives). Editeur Guy Boy. Hermès éditions, 2003. ISBN 2-7462-0571-8
10. Navarre, D, Palanque, P, Bastide, R, & Sy, O A Model-Based Tool for Interactive Prototyping of Highly Interactive Applications. 12th IEEE, International Workshop on Rapid System Prototyping ; Monterey (USA). IEEE ; 2001.
11. Norman D.A. *The design of everyday things*. New York: Currency-Doubleday, 1988.
12. Palanque, P and Basnyat. S. *Task Patterns for Taking into account in an* efficient and systematic way both standard and erroneous user behaviours. HESSD 2004. 6th International Working Conference on Human Error, Safety and System Development, 22-27 August 2004, Toulouse, France (within the IFIP World Computing Congress WCC 04).
13. Palanque, P and Bastide, R. UAHCI 2003. *User-Centered Point of View to End-User Development. Universal Access for Human-Computer Interaction* Heracklion, Crete, June 2003.
14. Paternò, F. *Model Based Design and Evaluation of Interactive Applications.* Springer Verlag, Berlin 1999
15. Preece, J., Rogers, Y., Sharp, H., Benyon, D., Holland, S. & Carey, T. (1994) *Human-Computer Interaction*. Wokingham, UK: Addison-Wesley.
16. Rasmussen, J. *Skills, rules, knowledge: Signals, signs, and symbols and other distinctions in human performance models*. IEEE Transactions on Systems, Man, and Cybernetics, 13(3):257-267 1983
17. Reason, J. *Human Error*. Cambridge University Press, 1990.
18. Scapin, D., Pierret-Golbreich, C. *Towards a Method for Task Description: MAD.* In Berlinguet, L., Berthelette, D. (eds.): Proc. of Conf. Work with Display Units WWU'89, Elsevier Science Publishers, Amsterdam (189) 27–34
19. van der Veer, G.C., ad van der Lenting, B.F., Bergevoet, *B.A.J.: GTA: Groupware Task Analysis - Modeling Complexity*. Acta Psychologica 91 1996 297–322.