Développement d'une méthode de prédiction des défaillances du couplage équipage-cockpit

Developing a new methodology to predict and assess pilot-cockpit interaction failure for certification purposes

Vincent Gauthereau, Florence Magnin et Jean Pariès
Dédale S.A.
15 Place de la Nation
75011 Paris

Résumé
Ce texte présente un projet de développement d'une méthode de prédiction des défaillances du couplage équipage-cockpit. Cette méthode, appelée PREVIENS pour Prédiction des Vulnérabilités de l'Interaction Equipage-Nouveauté en Situation, a été développée afin d'assister les organismes de conception ainsi que leurs autorités de tutelle dans les processus de certification «FH » des cockpits. La formulation de nouvelles exigences de certification (Règlement EASA CS25-1302) avait en effet crée un besoin que nous avons tenté de combler. PREVIENS se veut une méthode dite de deuxième génération s'inspirant des acquis scientifiques de l'ingénierie des systèmes cognitifs. PREVIENS permet d'identifier quatre grandes familles de risques : les risques associés à la défaillance des fonctions attendues de la nouveauté, les risques associés à l'utilisation de cette nouveauté en dehors de son périmètre d'usage, les risques associés aux dérives d'usage éventuelles, et enfin les différents effets de bord de l'introduction de cette nouveauté dans le cockpit. Suite à plusieurs mises en application de PREVIENS, nous pensons qu'en plus du systématisme qu'elle apporte à la prise en compte des dimensions FH dans les dossiers de sécurité (ou équivalents), le questionnement que la méthode suscite peut permettre une meilleure conception centrée utilisateur.

Summary

This text presents a project aimed at developing a method to predict and assess pilot-cockpit interaction failures. This method, called PREVIENS for « Prédiction des Vulnérabilités de l'Interaction Equipage-Nouveauté en Situation » (Prediction of crew-novelty interface vulnerabilities in situation), has been developed in order to assist design organizations and authorities in the human factors certification process of cockpits. Indeed, the expression of new certification requirements (EASA CS25-1302 Regulation) had created a need to be fulfilled. PREVIENS is a second generation HRA method, based on Cognitive Systems Engineering scientific grounds. PREVIENS allows the exploration of four families of risks: risks associated to the failure of the intended functions of the novelty, risks related to the use of the novelty outside of its scope of use, risks associated with potential drifts of use, and the various side-effects induced by the introduction of the novelty in the cockpit. Following several test implementations of PREVIENS, we believe that in addition to the standardization it brings to the integration of HF issues in safety cases (or equivalents), the questioning that this method raises may also allow a better user-centered design.

1. Introduction

Ce texte présente un projet de développement d'une méthode de prédiction des défaillances du couplage équipage-cockpit. Cette méthode, appelée PREVIENS pour Prédiction des Vulnérabilités de l'Interaction Equipage-Nouveauté en Situation, a été développée afin d'assister les organismes de conception ainsi que leurs autorités de tutelle dans les processus de certification «FH » (Facteurs Humains) des cockpits. Après un rappel du cadre de développement de cette méthode, les principes fondateurs de PREVIENS sont présentés. Ensuite, les grandes étapes d'une analyse PREVIENS sont énoncées. Puis, dans la discussion nous revenons sur ce que la mise en application de PREVIENS peut apporter à un processus de conception.

2. Le développement d'une méthode d'aide à la certification FH des cockpits

2.1. L'évolution du cadre réglementaire

En 1996, un groupe de travail conjoint FAA (Federal Aviation Adminsitration (USA)/ JAA (Joint Aviation Authorities, Europe) publiait un rapport mettant en avant deux besoins relatifs à la certification des avions. Tout d'abord, la nécessité de prendre en compte la réalité des pilotes de ligne dans le processus de certification : l'avion devrait être certifié pour être utilisé par les pilotes de ligne et pas seulement par des pilotes d'essais. Mais aussi, la nécessité d'intégrer plus de connaissances sur les facteurs humains (FH) dans la conception des avions.

Suite à ce rapport, un groupe d'harmonisation s'est vu confier la tâche d'examiner les questions de FH relatives à la certification de postes de pilotage dans le FAR/JAR25. Leurs tâches étaient d'examiner les exigences réglementaires, de rechercher les manques au sein de ces exigences, puis donner des réponses en termes de réglementation, de moyens acceptables de mise en conformité (AMC) ou autres. En Octobre 1999, ce groupe d'harmonisation a publié une liste ordonnée de 33 vulnérabilités. L'étape suivante consistait à créer un règlement qui permettrait de couvrir ces lacunes. Un sous-groupe travaillerait sur le cadre réglementaire (la CS 25-1302), tandis qu'un autre sous-groupe travaillerait sur le développement des AMC couvrant les 33 lacunes identifiées.

Pour comprendre cette nouvelle exigence réglementaire (dite « la 1302 »), nous pensons qu'il est important de prendre note des points suivants :

- Le groupe voulait éviter d'utiliser le jargon « facteurs humains » tels que « feed-back », etc.
- La structure du cadre réglementaire est centrale,
- Ce règlement est applicable à tous les produits soumis à la certification (certification de type, STC, etc.),
- L'AMC se réfère également aux autres paragraphes réglementaires de la CS 25,
- On doit considérer la CS 25-1302 comme étant complémentaire, séparée et distincte de la CS 25-1309: les exigences contenues dans le paragraphe 1302 ne remplacent pas celles qui se rapportent à « l'erreur humaine » telles qu'exprimées dans d'autres paragraphes, notamment le 1309. Les AMC pour ces deux séries d'exigences ne devraient pas être identiques.

Voici les exigences contenues dans la CS 25-1302:

Cette section s'applique aux équipements installés et destinés à une utilisation par des membres d'équipage dans le cadre de leur utilisation opérationnelle de l'avion, depuis leur position normalement assise dans le cockpit. Ce matériel installé, individuellement et en combinaison avec d'autres, doit démontrer qu'il est conçu de manière à ce que les membres d'équipage qualifiés et formés à son utilisation puissent sans danger s'acquitter de leurs tâches relatives à sa fonction attendue en satisfaisant les conditions suivantes :

(a) Les commandes du poste de pilotage doivent être installées pour permettre l'accomplissement de ces tâches et les informations nécessaires pour accomplir ces tâches doivent être fournies.

b) Les commandes du poste de pilotage et les informations destinées à l'emploi de l'équipage doivent :
(1) Etre présentées clairement et sans ambiguïté, avec la résolution et la précision adaptées à la tâche.
(2) Être accessibles et utilisables par l'équipage d'une manière compatible avec l'urgence, la fréquence et la durée de leurs missions.
(3) Permettre la prise de conscience de l'équipage, si celle-ci est nécessaire pour la sécurité des opérations, des effets que les actions de l'équipage ont sur l'appareil ou les systèmes.

(c) Le comportement opérationnellement adéquat des équipements installés doit être:
(1) Prévisible et sans ambiguïté, et
(2) Conçu pour permettre à l'équipage d'intervenir d'une manière appropriée à la tâche.

(d) Dans la mesure du possible, les équipements installés doivent permettre à l'équipage de gérer les erreurs qui résultent du type d'interaction de l'équipage avec le matériel auquel on peut raisonnablement s'attendre pendant le service, en supposant que l'équipage agit de bonne foi. Cet alinéa ne s'applique pas aux erreurs relatives aux aptitudes associées avec le contrôle manuel de l'avion.

2.2. Pourquoi une « méthode » de certification FH ?

Actuellement, une partie importante de la contribution de l'Autorité, que ce soit au stade de la définition des nouveautés ou plus tard quand il s'agit de démontrer l'acceptabilité d'une nouveauté, s'appuie sur l'expertise individuelle d'un nombre limité d'experts de haut niveau. En effet, les compléments et / ou les modifications du plan de certification suggérés par le fabricant sont basés sur la compréhension par l'Autorité des systèmes et des Interfaces Homme Machine (IHM) (construite à partir des présentations, des descriptions, des tests ou des simulations), de sa compréhension du rôle des systèmes / IHM dans la sécurité (construite principalement à partir des Analyses Fonctionnelles de Danger - FHA) et de son expérience et de son expertise (fondées sur les certifications du passé ou sur l'expérience de vol, les connaissances techniques et des FH…). Les scénarios d'essais supplémentaires demandés par l'Autorité, reposent plus sur la solide expertise incarnée par des individus que sur une approche systématique. Il en va de même pour l'acceptation des scénarios ou des cas déjà suggérés par le fabricant. Toutefois, cette ressource très rare et coûteuse est limitée et ne peut garantir une approche exhaustive (pour autant qu'une approche prédictive puisse l'être) de la certification FH. Aujourd'hui, c'est surtout l'expertise qui permet de convaincre que les questions les plus critiques ont été correctement traitées. Cependant les experts de l'Autorité se révèlent être assez dépendants des scénarios développés par le constructeur ou des autres aspects de l'approche (échantillons d'équipage, cadres d'observation/d'entretiens, …) proposés par le fabricant, et dont l'appréciation est principalement basée sur l'avis de spécialistes.

Le but de développer une méthode n'est pas de remplacer les experts du fabriquant ou de l'Autorité. En fait, comme nous le verrons dans une prochaine sous-section, la méthode est fondée sur cette expertise. Toutefois, l'objectif de la méthode est d'appuyer cette expertise. L'utilisation d'une méthode devrait permettre de :

- Générer un examen plus systématique des vulnérabilités potentielles : puisque nous ne pouvons pas éviter la subjectivité des « évaluations des facteurs humains », une méthode d'évaluation plus systématique et structurée devrait réduire cette part de subjectivité à son minimum ou, au moins, devrait augmenter la fiabilité du jugement subjectif.
- Rendre plus explicites les processus de réflexion des experts,et par là-même faciliter la construction de consensus inter-subjectifs raisonnés plutôt que l'affrontement de subjectivités basé sur des rapports de force.
- Améliorer la traçabilité du raisonnement des experts et donc favoriser la capitalisation, et le futur suivi de la certification à partir de l'expérience en service.
- Fournir un argumentaire structuré pour la définition de l'évaluation et les essais de scénarios.

2.3. Le projet de développement méthodologique 'PREVIENS'

Le processus de développement a été itératif et a impliqué les deux avionneurs (Airbus et Dassault Aviation) ainsi que l'expertise de l'Autorité. Après un premier développement de la méthodologie, nous avons utilisé la méthode sur quelques « nouveautés ». Nous avons choisi des nouveautés qui étaient à des stades de développement différents, de manière à disposer de différents types d'équipements, ainsi que de différents niveaux de connaissance sur les risques associés à l'usage de la nouveauté. Après chaque cas, nous avons évalué la méthode selon cinq axes d'analyse. Le travail autour de la méthode a été mené de telle sorte que la « qualité » de la méthode soit améliorée. Puisque cette « qualité » est en fait multidimensionnelle, nous présentons ci-dessous comment cette notion a été précisée, comment les concepts qui devaient être utilisés ont été choisis (validité interne, validité externe, fiabilité, précision, exactitude…) et comment l'évaluation de PREVIENS a été structurée.

Selon Thorngate [1], et son postulat de la complexité proportionnée (postulate of commensurate complexity), « *il est impossible qu'une théorie du comportement social soit à la fois générale, simple ou parcimonieuse, et précise* ». Bien que nous soyons ici concernés par une méthode (et non une théorie), cette affirmation peut aider à définir ce que serait une bonne méthode:

- Un certain niveau de généralité est nécessaire : la méthode devrait être utilisable pour les différents types de nouveautés potentiellement intégrées dans un cockpit.
- La méthode devrait être simple à utiliser : une méthode complexe serait inutilisable, car nécessiterait une durée d'apprentissage et un temps de mise en œuvre excessifs pour ses utilisateurs.
- Enfin, elle devrait être précise: les résultats devraient être « corrects » ainsi qu'utiles. La méthode devrait permettre de discriminer entre les choses acceptables et les choses inacceptables. En fait, nous avons besoin que la précision des résultats soit adaptée à leur utilisation future.

Nous avons donc proposé que la réflexion soit menée autour de cinq dimensions:

1. tout d'abord, **l'utilisabilité de la méthode** ;
2. ensuite, **l'exactitude des résultats** produits ;
3. au cours d'une troisième étape, sa **validité externe** qui renvoie au caractère générique de la méthode (est-elle utilisable au-delà des 'nouveautés' analysées ?).
4. ensuite, les **compromis nécessaires entre les trois dimensions** qui précédentes, en vérifiant qu'ils correspondent aux intentions annoncées au début du projet.

5. Enfin, la **conformité de la méthode à son cadre conceptuel initial** : est-elle vraiment une méthode HRA (Human Reliability Assessment) de deuxième génération? Est-elle conforme aux principes de l'Ingénierie des Systèmes Cognitifs? Etc.

Une telle évaluation a ouvert la voie à une version améliorée de la méthode après chaque essai sur les différentes nouveautés.

3. Les fondamentaux de PREVIENS

3.1. Une extension de l'expertise par le biais de discussions structurées

Comme indiqué ci-dessus, la méthode ne vise pas à remplacer le travail des experts, mais à le soutenir. Une condition requise pour le bon fonctionnement des différentes étapes de la méthode est donc, entre autres, la disponibilité de ces experts. La méthode est développée autour de l'organisation de groupes de travail multidisciplinaires. Ces groupes doivent être composés de différents types d'expertise : une expertise opérationnelle (par exemple des pilotes d'essais), une expertise liée à la conception des systèmes, une expertise dans le domaine des facteurs humains, une expertise en évaluations de sécurité, une expertise de la méthode, et enfin une expertise en formation des pilotes. Les raisons pour l'utilisation de groupes de travail multidisciplinaires sont les suivantes :

- Stimuler « l'imagination requise» de chaque domaine d'expertise,
- Rassembler et faire interagir différentes visions du monde autour d'un même sujet.

En fait, si l'on pense qu'une conception ne sera jamais « parfaite » mais seulement « le meilleur compromis à un certain point dans le temps », alors l'organisation d'un débat entre les différentes parties est certainement une des voies vers une meilleure conception. Nous avons besoin de ces groupes de travail pluridisciplinaires non seulement pour stimuler l'imagination de chaque individu, mais aussi pour que nous puissions structurer les *négociations* entre ces parties.

Il faut toutefois reconnaître que les ressources nécessaires pour appliquer la méthode doivent être maintenues à un niveau raisonnable. Ainsi, pour chaque étape de la méthode, nous identifions clairement ce qui doit être réalisé dans un groupe de travail, et ce qui peut être éventuellement réalisé par l'analyste seul, mais aussi ce qui doit être réalisé en coopération avec l'autorité de certification. Car, en fait, les groupes mentionnés ci-dessus sont essentiellement internes à l'organisme de conception (le bureau d'étude du constructeur). Toutefois, comme mentionné plus haut, PREVIENS est une méthode de certification. Une des parties en présence est l'autorité de certification et ses experts. Il faut souligner que la méthode n'a pas été conçue pour être « utilisée » par les experts de l'autorité en ce sens que l'autorité ne met pas chaque étape de la méthode en pratique. Mais les résultats de la méthode devraient structurer les réunions entre l'organisation de conception et l'autorité. En fait, l'autorité souhaite éviter de n'être impliquée qu'au stade final de l'approbation de la conception tandis que, dans le même temps, elle se doit de ne pas aider l'organisme de conception dans ses travaux de conception. Ainsi, l'autorité n'interviendra que dans certaines phases spécifiques (étapes du processus d'approbation). Au cours de ces étapes, l'autorité doit valider (ou invalider) les travaux antérieurs et, par conséquent, donner son consentement pour la poursuite des travaux par l'organisation de conception. L'identification de plusieurs de ces étapes durant le processus de conception devrait permettre à l'autorité de suivre le processus de conception et lui permettre ainsi de participer par son savoir-faire - mais sans être pris à défaut comme un participant à part entière - dans le processus de conception.

3.2. Une méthode qui s'inscrit au sein de l'ingénierie des systèmes cognitifs

Le cadre conceptuel choisi est celui de l'ingénierie des systèmes cognitifs [2, 3, 4]. Naturellement, ce cadre théorique a des répercussions sur la fondation des méthodes prédictives de fiabilité humaine (Human Reliability Assessment). Les méthodes prédictives ont été tellement touchées par ce cadre théorique que l'on a même parlé d'un changement de génération (des méthodes HRA de première génération, vers les méthodes de deuxième génération). Dans les méthodes HRA de première génération, l'évaluation des risques est une question de contrôle où le «signal» est une «probabilité de l'erreur humaine» et le «bruit» des facteurs de développement de la performance. De telles méthodes visent effectivement à évaluer le niveau de la fiabilité humaine. Les méthodes HRA de deuxième génération reposent, elles, sur quatre postulats :

- La performance nominale et la défaillance sont des phénomènes émergents ;
- Lorsque l'issue des actions diffère de ce qui était prévu (requis), ceci est dû à la variabilité du contexte et des conditions plutôt qu'à un échec de l'action ;
- L'adaptabilité et la flexibilité sont nécessaires pour l'efficacité. Les mécanismes du succès et de la défaillance sont identiques ;
- Nous ne pouvons pas être à la fois précis et efficace.

En d'autres termes, pour les méthodes de seconde génération (Athena, Mermos, etc.), ce n'est pas la fiabilité intrinsèque de la composante humaine qui est importante, c'est celle de la performance, en tant qu'interaction entre l'opérateur ou l'équipe d'opérateurs, et son contexte.

4. Une méthode, cinq questions

PREVIENS s'articule autour de cinq grandes questions ou étapes, dont la première est une question préliminaire apportant des éléments de réponse aux quatre suivantes. Ces quatre dernières ont pour objectif d'identifier les risques associés à quatre « types de défaillance » du couplage homme-machine à l'aide de procédures détaillées. Ces cinq questions sont :

Question 1 - Quelle est la fonction attendue de la nouveauté et quelles sont ses limites d'usage ?

Cette première question, préalable aux quatre autres, a pour objectif principal de définir la ou les fonction(s) attendue(s) de la nouveauté de la part du concepteur ainsi que le périmètre d'utilisation de cette nouveauté. Les éléments issus de cette première étape permettront d'analyser les défaillances possibles par écart vis-à-vis de ces fonctions « de référence » (lors de la question 2) et d'identifier les risques liés à l'utilisation de la nouveauté hors de son périmètre d'usage (lors de la question 3).

Cette étape étudie aussi les limites de la conception de la nouveauté, et notamment les deux autres problématiques suivantes :

- Tout d'abord, l'utilisation normale de la nouveauté peut, dans certaines situations particulières, avoir un impact sur la sécurité : le comportement « produit » par la nouveauté, bien que prévu, peut avoir un impact négatif sur la sécurité par rapport au comportement « naturel » de l'équipage à qui on n'aurait pas fourni la nouveauté.
- Puis, lorsque la nouveauté est destinée à remplacer un équipement existant, les fonctions attendues de la nouveauté pourraient ne pas remplacer entièrement celles qui sont remplies par l'équipement existant. Par exemple, la radio sert à communiquer avec le contrôle aérien (fonction attendue). Dans le cas d'un remplacement de cet équipement par un dispositif de communication électronique (CPDLC – Controler-Pilot Data Link Communication), la fonction attendue de la radio est effectivement remplacée. Néanmoins, la radio remplissait de fait d'autres fonctions : elle permet à l'équipage d'évaluer la densité du trafic environnement (fonction effective), elle permet d'entendre ce que le contrôleur dit aux autres avions, et donc de se faire une idée du trafic et des situations conflictuelles potentielles. Cette étape de PREVIENS permet : d'identifier ces fonctions effectives, et de questionner leur perte éventuelle lors du remplacement de l'équipement.

Cette étape préliminaire permet donc de préciser les fonctions attendues de la nouveauté (fonctions du couple équipage-

nouveauté, et non fonctions techniques), d'expliciter et de questionner le domaine d'utilisation de ces fonctions, mais aussi de préciser le cadre de la démonstration de sécurité.

Question 2 - Quels sont les risques de défaillance de cette fonction attendue ?

Cette deuxième question vise à identifier les défaillances du couplage homme-machine pouvant avoir des conséquences sur la sécurité. Cette étape part du principe que la fiabilité du système (dans sa globalité) est le résultat d'une maîtrise dynamique par l'équipe, et non pas le résultat d'un comportement en tout point infaillible de la part de cet équipage. Cette idée est loin d'être novatrice et a fait l'objet de nombre de publications scientifiques : la performance est le produit d'une maîtrise dynamique et non le produit d'une conformité de l'activité de l'équipage à une tâche prédéfinie. Ainsi, si l'on s'intéresse aux impacts sur la sécurité de l'intégration d'un nouvel équipement au sein d'un cockpit, la question centrale doit être celle de la performance du couple homme machine (du « Joint Cognitive System » ou JCS [4]) : c'est ce que ce couple produit qui nous intéresse, et non comment il le fait.

Sur la base de ce principe, PREVIENS commence par identifier les défaillances fonctionnelles (au niveau du JCS) et leurs impacts sur la sécurité. Ensuite, l'analyse PREVIENS cherche à comprendre les raisons derrière les défaillances fonctionnelles impactant la sécurité. Pour rechercher ces raisons, PREVIENS se base sur le principe suivant : pour que la fonction attendue soit réalisée, il faut que le JCS réalise correctement quatre fonctions cognitives (fonctions d'exécution, de perception/reconnaissance/identification, d'interprétation, et de planification, sans ordre chronologique particulier). Ainsi, on ne cherche pas à évaluer la capacité de l'équipage à réaliser les tâches attendues, mais bien la capacité du couple homme-machine à réaliser, conjointement, ces quatre fonctions cognitives. PREVIENS aide alors les analystes à identifier les caractéristiques de conception pouvant participer aux défaillances de ces fonctions cognitives.

Question 3 - Quels sont les risques d'éventuelles extensions d'usage ?

Cette troisième question étudie un autre type de défaillance : les extensions d'usage. Dans cette partie de la méthode, il s'agit d'étudier les risques liés à l'utilisation de la nouveauté pour la fonction attendue, mais en dehors de son périmètre d'usage (tel que défini dans l'étape préliminaire). Pour chacune des limites du domaine d'utilisation, PREVIENS aide l'analyste à identifier les raisons pouvant amener à de telles extensions d'usage, et ce selon deux axes principaux de questionnement : qu'est-ce qui peut pousser l'équipage à sortir consciemment du domaine d'usage ? quelles caractéristiques de conception peuvent expliquer une sortie involontaire de ce domaine d'usage ? Eventuellement, ce questionnement des risques associés aux extensions d'usage peut aboutir à une redéfinition du périmètre d'usage de l'équipement.

Question 4 - Quels sont les risques de dérives d'usage ?

Une quatrième question permet d'identifier les risques liés aux dérives d'usage. Les dérives d'usage sont des utilisations non prévues de la nouveauté pour réaliser une autre fonction que la fonction attendue définie lors de l'étape préliminaire (en d'autres termes les catachrèses éventuelles). PREVIENS considère que les dérives d'usage ne sont que très rarement le fruit de « mauvais équipages » ou le fruit d'un « manque de professionnalisme ». Ainsi, la base de l'analyse consiste à partir des manques exprimés par les équipages et à identifier la capacité de l'équipement à remplir certains de ces manques. Une fois de plus : seules les dérives d'usage ayant un impact sur la sécurité sont considérées dans l'analyse.

Question 5 - Quels sont les effets de bord liés à l'introduction de cette nouveauté dans le cockpit ?

Enfin, la cinquième question de la méthode a pour objet d'étude les effets de bord induits par une proximité. Il s'agit des effets provoqués par l'utilisation de la nouveauté sur des systèmes « à proximité », mais n'ayant pas de lien fonctionnel. PREVIENS identifie trois types de proximité :

- Physique/ géographique : lorsque la nouveauté est située à proximité physique d'un autre système.
- Temporelle : lorsque l'utilisation de la nouveauté doit se faire simultanément à l'utilisation d'autres systèmes ou dans une séquence/suite d'action déterminée dans le temps.
- Cognitive : lorsque l'utilisation de la nouveauté nécessite un schéma cognitif ou des réflexes mentaux similaires à ceux d'un autre système.

5. Discussion

5.1. Cinq questions interdépendantes

Il nous faut tout d'abord noter que bien que les méthodologies permettant d'analyser chacune des familles de risques identifiées soient différentes, PREVIENS doit être considérée comme une seule et unique méthode. Les questions abordées par PREVIENS sont complémentaires les unes des autres, et aucune ne peut vraiment être laissée de côté. En fait, la réponse à ces questions dépend amplement de la définition des fonctions attendues. Plus les fonctions attendues sont étendues, plus les risques associés à des dérives ou extensions d'usage vont être réduits, mais plus les risques associés aux défaillances des fonctions attendues seront importants (et inversement). Ainsi, pour que la démonstration soit valable, on ne peut pas décider de ne couvrir qu'une partie des problèmes.

5.2. Une application itérative

PREVIENS n'est pas une méthode qu'on applique sur un produit fini pour valider, ou non, les choix de conception. En fait, si PREVIENS est bien une méthode pouvant assister un processus de certification (et donc de validation de choix de conception), elle a été conçue pour permettre les échanges entre l'organisme de conception et ses autorités de tutelle tout au long du processus de conception. En fait, PREVIENS trouve toute sa valeur dans sa capacité à organiser et structurer les échanges entre autorités et organisme de conception tout au long du processus de développement. Au travers des questionnements de PREVIENS, le concepteur est invité à réfléchir autour de certains risques. Ce questionnement lui permet notamment d'identifier clairement le besoin de répondre à certaines exigences de conception contenues dans la réglementation. Ainsi, PREVIENS n'est pas à proprement parler un moyen de répondre aux exigences (« means of compliance »), mais plutôt une méthode permettant de déterminer l'applicabilité de certaines exigences de conception. En d'autres termes, une application itérative de PREVIENS permet à un organisme de conception de construire un dossier de sécurité cohérent et systématique. En forçant le regard des concepteurs sur la qualité du couplage homme-machine, nous pensons que PREVIENS favorise un processus de conception centré utilisateur. Par exemple, le fait de 'forcer' les concepteurs à définir la fonction attendue au niveau du système cognitif conjoint oblige à une réflexion allant au-delà des fonctions techniques de l'équipement. Notre expérience montre que cette étape préliminaire à toute analyse PREVIENS est fortement bénéfique à la prise en compte des utilisateurs finaux dans le processus de conception.

5.3. Une application à d'autres domaines

Nous avons eu l'occasion d'appliquer PREVIENS à d'autres domaines et, notamment, le monde automobile. Sur l'initiative d'un constructeur français, nous avons en effet réfléchi à la possible adaptation de PREVIENS à ce domaine. L'applicabilité de PREVIENS n'était pas évidente : nous passions en effet d'un monde très contraint (aussi bien du point de vue du domaine de fonctionnement que de l'activité de l'opérateur), à un monde présentant une plus grande variabilité. A la suite de notre travail, nous avons pu montrer l'applicabilité de PREVIENS à ce domaine. L'application d'une version légèrement modifiée de PREVIENS sur plusieurs équipements semble montrer que :

- le systématisme apporté par PREVIENS dans la définition des fonctions attendues et de leurs domaines d'utilisation peut permettre de rationaliser certains

choix techniques aujourd'hui réalisés sur le simple fondement de l'habitude ou la répétition d'une conception précédente.
- l'application de PREVIENS peut permettre de systématiser et structurer une approche FH riche mais naturellement peu normalisée.

6. Conclusion

Quel que soit le domaine, les différentes applications de PREVIENS, ont montré l'utilisabilité de la méthode malgré son déroulement parfois fastidieux.

Ces essais ont également confirmé que la méthode permettait d'identifier certains 'pièges' de conception. La question est maintenant de savoir si les pièges décelés sont suffisamment pertinents pour motiver les efforts nécessaires à l'application de la méthode.

Néanmoins, nous savons d'ores et déjà que la méthode peut :
- améliorer la traçabilité des décisions
- favoriser le dialogue entre les différents experts concernés par la conception
- forcer un questionnement systématique

Ainsi, en fonction des motivations de l'analyste, plusieurs utilisations de PREVIENS sont possibles. Elle peut aider à :

- Construire un dossier de sécurité en apportant à la fois la structure du dossier et le fond de l'argumentation.
- Convaincre, donner du poids à l'analyste dans sa démonstration de sécurité.
- Dialoguer avec l'autorité dans un objectif commun.

6.1. Remerciements

Nous tenons à remercier la DGAC.DAST pour avoir subventionné ce projet, Stéphane Deharvengt et Claude Valot pour leurs commentaires constructifs tout au long du projet, ainsi que Airbus et Dassault Aviation (et leurs différents experts qui ont participé à ce projet) sans lesquels les mises en applications de PREVIENS auraient été moins riches d'enseignements.

6.2. Références

|1] Thorngate, W. (1975). "In general" vs. "It Depends": Some comments of the Gergen-Schlenker Debate. Personality & Social Psychology bulletin, 2, 404-410.
[2] Neisser, U. (1976). Cognition and Reality - Principles and Implications of Cognitive Psychology. San Francisco: Freeman.
[3] Reason, J. T. (1998). Broadening the cognitive engineering horizon: more engineering, less cognition and no philosophy of science, please. Ergonomics, 41(2), 150-152.
[4] Woods, D. & Hollnagel, E. (2006). Joint cognitive systems patterns in cognitive systems engineering. CRC Press.

Développement d'une méthode de prédiction des défaillances du couplage équipage-cockpit

Developing a new methodology to predict and assess pilot-cockpit interaction failure for certification purposes

Vincent Gauthereau, Florence Magnin et Jean Pariès
Dédale S.A.
15 Place de la Nation
75011 Paris

Résumé
Ce texte présente un projet de développement d'une méthode de prédiction des défaillances du couplage équipage-cockpit. Cette méthode, appelée PREVIENS pour Prédiction des Vulnérabilités de l'Interaction Equipage-Nouveauté en Situation, a été développée afin d'assister les organismes de conception ainsi que leurs autorités de tutelle dans les processus de certification «FH » des cockpits. La formulation de nouvelles exigences de certification (Règlement EASA CS25-1302) avait en effet crée un besoin que nous avons tenté de combler. PREVIENS se veut une méthode dite de deuxième génération s'inspirant des acquis scientifiques de l'ingénierie des systèmes cognitifs. PREVIENS permet d'identifier quatre grandes familles de risques : les risques associés à la défaillance des fonctions attendues de la nouveauté, les risques associés à l'utilisation de cette nouveauté en dehors de son périmètre d'usage, les risques associés aux dérives d'usage éventuelles, et enfin les différents effets de bord de l'introduction de cette nouveauté dans le cockpit. Suite à plusieurs mises en application de PREVIENS, nous pensons qu'en plus du systématisme qu'elle apporte à la prise en compte des dimensions FH dans les dossiers de sécurité (ou équivalents), le questionnement que la méthode suscite peut permettre une meilleure conception centrée utilisateur.

Summary

This text presents a project aimed at developing a method to predict and assess pilot-cockpit interaction failures. This method, called PREVIENS for « Prédiction des Vulnérabilités de l'Interaction Equipage-Nouveauté en Situation » (Prediction of crew-novelty interface vulnerabilities in situation), has been developed in order to assist design organizations and authorities in the human factors certification process of cockpits. Indeed, the expression of new certification requirements (EASA CS25-1302 Regulation) had created a need to be fulfilled. PREVIENS is a second generation HRA method, based on Cognitive Systems Engineering scientific grounds. PREVIENS allows the exploration of four families of risks: risks associated to the failure of the intended functions of the novelty, risks related to the use of the novelty outside of its scope of use, risks associated with potential drifts of use, and the various side-effects induced by the introduction of the novelty in the cockpit. Following several test implementations of PREVIENS, we believe that in addition to the standardization it brings to the integration of HF issues in safety cases (or equivalents), the questioning that this method raises may also allow a better user-centered design.

Introduction

Ce texte présente un projet de développement d'une méthode de prédiction des défaillances du couplage équipage-cockpit. Cette méthode, appelée PREVIENS pour Prédiction des Vulnérabilités de l'Interaction Equipage-Nouveauté en Situation, a été développée afin d'assister les organismes de conception ainsi que leurs autorités de tutelle dans les processus de certification «FH » (Facteurs Humains) des cockpits. Après un rappel du cadre de développement de cette méthode, les principes fondateurs de PREVIENS sont présentés. Ensuite, les grandes étapes d'une analyse PREVIENS sont énoncées. Puis, dans la discussion nous revenons sur ce que la mise en application de PREVIENS peut apporter à un processus de conception.

Une méthode, cinq questions

PREVIENS s'articule autour de cinq grandes questions ou étapes interdépendantes et complémentaires. La première est une question préliminaire apportant des éléments de réponse aux quatre suivantes. Ces quatre dernières ont pour objectif d'identifier les risques associés à quatre « types de défaillance » du couplage homme-machine à l'aide de procédures détaillées. Ces cinq questions sont :

1 - Quelle est la fonction attendue de la nouveauté et quel est son périmètre d'usage ?
2 - Quels sont les risques de défaillance de cette fonction ?
3 - Quels sont les risques d'éventuelles extensions d'usage ?
4 - Quels sont les risques de dérives d'usage ?
5 - Quels sont les effets de bord liés à l'introduction de cette nouveauté dans le cockpit ?

Au travers des questionnements de PREVIENS, le concepteur est invité à réfléchir autour de certains risques. Ce questionnement lui permet notamment d'identifier clairement le besoin de répondre à certaines exigences de conception contenues dans la réglementation. Ainsi, PREVIENS n'est pas à proprement parler un moyen de répondre aux exigences (« means of compliance »), mais plutôt une méthode permettant de déterminer l'applicabilité de certaines exigences de conception. En d'autres termes, une application itérative de PREVIENS permet à un organisme de conception de construire un dossier de sécurité cohérent et systématique. En forçant le regard des concepteurs sur la qualité du couplage homme-machine, nous pensons que PREVIENS favorise un processus de conception centré utilisateur.

Une application à d'autres domaines

Nous avons eu l'occasion d'appliquer PREVIENS à d'autres domaines et, notamment, au monde automobile sur l'initiative d'un constructeur français. A la suite de notre travail, nous avons pu montrer l'applicabilité de PREVIENS à ce domaine. L'application d'une version légèrement modifiée de PREVIENS sur plusieurs équipements semble montrer que :

- le systématisme apporté par PREVIENS dans la définition des fonctions attendues et de leurs domaines d'utilisation peut permettre de rationaliser certains choix techniques.
- l'application de PREVIENS peut permettre de systématiser et structurer une approche FH riche mais naturellement peu normalisée.