Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

Le facteur humain aux différentes étapes de conception, réalisation, exploitation d'un système

Human factor at milestones of design, release, operational use of a system

FAURE BEAULIEU Guillaume
CS GROUP
Le Plessis-Robinson
guillaume.faure-beaulieu@cs-soprasteria.com

***Résumé* —** L'emploi de solutions techniques, notamment de processus automatisés, permet de soulager la charge de travail d'opérateurs devant conduire un système complexe (on pense notamment à l'équipage d'un avion de ligne, aidé par le pilote automatique). Cependant, en situations réelles l'intervention humaine est susceptible d'éviter une catastrophe, là où les automatismes n'ont pas été prévus pour agir. A contrario, une solution technique verrouillée, en ne laissant pas l'humain intervenir, a pu provoquer une catastrophe.

Il faut revenir sur un constat : les solutions techniques sont le fruit d'actions humaines tout au long de leur cycle de vie, depuis la phase la plus amont jusqu'à leur utilisation : étapes de conception, de réalisation, de mise en service, qui conduit à l'exploitation opérationnelle.

La présente étude se propose d'analyser, à chaque étape d'élaboration d'une solution technique, les différents intervenants, leur rôle et les types d'erreurs et d'insuffisances susceptibles d'advenir, de façon pas toujours manifeste, et dont les conséquences surgissent en phase d'exploitation ; mais aussi, les actions positives de l'opérateur dans cette même phase d'exploitation.

Il émerge une notion de facteur humain prospectif (conception, réalisation), et de facteur humain actualisé (exploitation) qui vont se compléter. Et certaines qualités sont propices aux actions positives : connaissance étendue du système, intérêt pour le système.

La conclusion amène à considérer la nécessité, dans la conception d'un système, d'assurer, à l'opérateur, un accès pour rétablir une situation non prévue (par une solution de contournement, par exemple), et comment former l'opérateur pour y parvenir.

Mots-clefs — Facteur humain, solution technique, conception, sécurité, rétablissement de situation

***Abstract* —** *Technical solutions as* automatic processes are well known to make human tasks easier on complex systems driving. But on real situations, it happens that human action can save from catastrophic situation, as automatism is not designed to. On opposite way, such a technical solution can create catastrophic situation when operator is not allowed to act.

Just notice a point: technical solutions are human made products as designed, built, performed.

Following work aims to show how any actor, at each step of a project, contributes to the building effort, and which type of failure can happen, with consequences on operational phase, but also positive actions from human actor on operational phase.

So just consider a concept with (i) forward human factor (design, build), and (ii) actual human factor (run), that are complementary. And some human qualities facilitate positive actions: wide knowledge of the system, care to the system.

On conclusion, it is necessary to design a system with possibility to operator to act, when unknown situation occurs, and train him to this kind of action.

Keywords — Human factor, technical solution, design, safety, situation recovery

I. INTRODUCTION

Le facteur humain est un point de vigilance dans la sécurité d'utilisation d'un système complexe. Il est souvent considéré comme source d'erreurs, dues souvent à des méconnaissances, ou à des surcharges de travail, et pouvant conduire à une situation accidentelle.

Cette considération a amené à concevoir des solutions techniques à base de systèmes automatisés capables de se substituer à l'action humaine, soit en déchargeant l'opérateur, soit en le remplaçant totalement, notamment dès qu'il s'agit d'assurer des tâches très répétitives. La fiabilité de la solution technologique apportée devient alors un argument de confiance.

Cependant, les limites d'une solution technique ont pu se montrer flagrantes, notamment dans le cas des accidents du 737 MAX, où l'opérateur humain (pilote et copilote) n'avait aucun accès pour corriger la situation. A contrario, l'amerrissage d'un avion dans l'Hudson, à l'initiative du pilote, suite à une panne des moteurs, montre la capacité humaine à sauver une situation, là où le système n'était pas implémenté pour apporter une solution.

Ces événements parlants, par leur dimension tragique, nous mettent devant une réalité incontournable : un système, tout au long de son existence, prend en compte le facteur humain, et cela depuis sa phase de conception initiale jusqu'à son retrait de service. Il y a, de ce fait, deux volets du facteur humain à considérer :

- Le facteur humain qu'on pourrait appeler « prospectif », c'est-à-dire relatif à la conception, réalisation, intégration validation d'un système, qui va avoir un rôle important dans la capacité de ce système à tenir les exigences de sécurité, par sa fiabilité intrinsèque et par la façon dont il va être mis en œuvre ; ce volet est actuellement peu étudié,
- Le facteur humain en utilisation, déjà abondamment étudié, et qu'on pourrait désigner par le mot « actualisé », puisqu'il correspond à la mise en œuvre au quotidien du système, avec toutes les réactions humaines en toutes situations.

Il y a donc un enjeu d'équilibre entre facteurs humains « prospectif » et « actualisé ». On va se focaliser ici sur un cas concret pour montrer comment évaluer le facteur humain « prospectif », avec les erreurs humaines potentielles, mais aussi les actions humaines positives, cela dans un domaine à fort enjeu de sécurité : celui du contrôle de la circulation aérienne.

Dans ce domaine, où CS GROUP conduit des projets majeurs, on se propose de présenter l'analyse de certaines étapes d'un projet type, utilisant un cadre normatif, pour respecter les exigences de ce qu'on désigne par « Safety of Air Traffic Management » (SATM). A partir de cette analyse, quelques éléments émergents se dégagent sur les points forts et points faibles du facteur humain à différents étapes.

II. PRESENTATION DU TYPE DE SYSTEME ETUDIE

Le système considéré est la radio, qui permet à un contrôleur aérien, situé en un point géographique donné, d'avoir une communication vocale avec le pilote d'un aéronef, situé dans une zone géographique proche ou éloignée de celle où se trouve le contrôleur, comme représenté en Figure 1.

Cette fonction a un rôle majeur dans la sécurité aérienne, puisqu'elle permet de coordonner le trafic aérien en évitant les rapprochements dangereux entre aéronefs dans le déroulement de leurs missions nominales respectives, mais également d'assurer la réception d'appels d'urgence ou de détresse de la part d'un pilote et de gérer la situation en conséquence.

En termes de solution, le message vocal du contrôleur est capté par des moyens audio (micro) et adressé, via un commutateur radio, à un centre radio comportant un émetteur qui le transmet à l'aéronef par l'intermédiaire d'une antenne, sur la fréquence spécifiée. En retour, les messages vocaux émis par l'aéronefs sont reçus, sur la même fréquence, dans le centre radio, par un récepteur, par l'intermédiaire d'une antenne, et adressés au contrôleur par le commutateur radio.

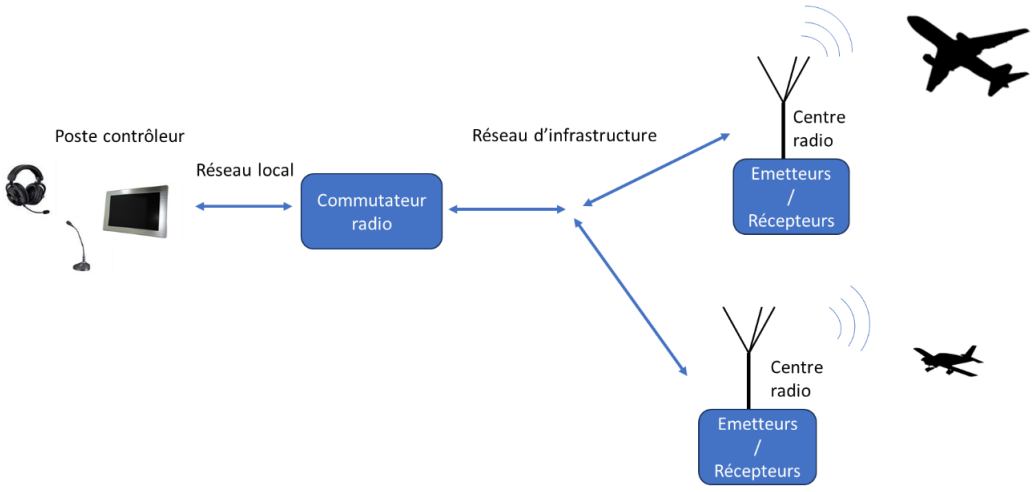

Figure 1 : Système radio du contrôle aérien

Le système optimise la réception du message émis par l'aéronef, en sélectionnant le meilleur centre radio, par comparaison des signaux reçus par les différents centres pour ce même message (a priori, c'est le centre le plus proche de l'avion qui devrait recevoir le meilleur signal). Cependant, le contrôleur a la possibilité de sélectionner manuellement un centre s'il estime en recevoir une meilleure réception.

Le périmètre de la solution CS GROUP porte généralement sur le poste du contrôleur, le commutateur radio, le réseau local de communication, les ressources du centre radio. La liaison entre le centre de contrôle et le centre radio est généralement assurée par un réseau d'infrastructure géré par l'organisme client. La solution CS GROUP prend donc en compte l'accès à ce réseau et le protocole de transport (IP, RNIS, …) concerné. Elle inclut également différents services, comme l'allocation de ressources, la supervision technique, l'enregistrement/restitution.

Le système radio peut être le système nominal ou le système secours. Le système nominal est celui qui assure le service opérationnel en temps normal. Le système secours permet d'assurer le maintien des communications à un niveau minimum requis en cas de panne du système nominal. Il reprend une architecture semblable à celle du système nominal, mais avec des ressources matérielles distinctes et une solution logicielle indépendante. Généralement, d'un point de vue contractuel, l'organisme client désigne deux fournisseurs différents pour implémenter les deux systèmes, de façon à éviter les modes communs.

III. LOGIQUE D'IMPLEMENTATION DU SYSTEME

A. Cycle en V

Le développement du système considéré, décrit en section II, reprend la logique classique du cycle en V, pour répondre au besoin en termes de services rendus, répondant à une mission opérationnelle. Les étapes types sont représentées par la Figure 2. Ces étapes devront prendre les exigences de sécurité de manière spécifique.

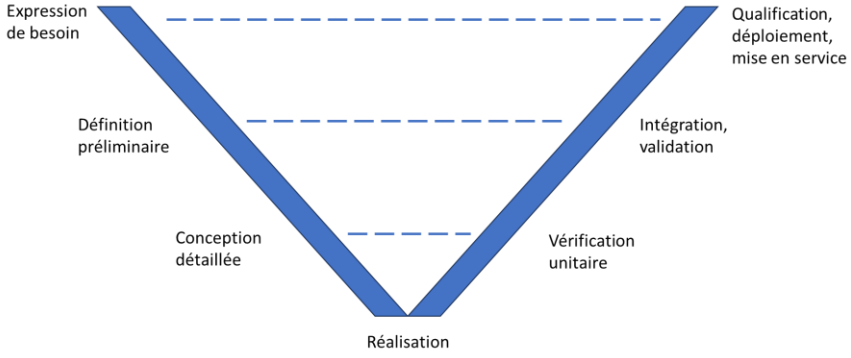

Figure 2 : Cycle en V

B. Impact de la sécurité dans la démarche

Les exigences de la SATM, auxquelles répondent les systèmes radio développés, découlent de directives réglementaires énoncées dans le cadre du Ciel Unique Européen (règlement (CE) n°549/2004), pour assurer le transport de passagers en toute sécurité. Ces directives sont déclinées auprès des différents prestataires de la navigation aérienne, qu'ils soient directement impliqués (organismes de contrôle aérien de l'aviation civile des différentes nations), ou en partage de l'espace aérien (contrôle aérien des forces aériennes).

Vu concrètement de l'industriel qui développe des systèmes radio, il s'agit de prendre en compte les risques liés à la perte de communication radio avec un aéronef. Ça peut être : perte d'une voie radio (une fréquence et une couverture géographique données), perte d'un poste de contrôleur aérien, perte de toutes les voies radio, dégradation de la communication radio. Ces risques sont déclinés en exigences de conception, de réalisation et de mise en œuvre du système.

L'industriel répond donc non seulement au cahier des charges pour que le système assure les services spécifiés, mais aussi à des exigences pour sécuriser son système et le rendre apte à différentes actions de secours.

Il est aidé pour cela par un cadre méthodologique qui va impliquer non seulement ses équipes d'ingénierie, mais également les futurs utilisateurs du système.

La méthodologie couramment utilisée est la Safety Assessment Methodology (SAM) d'EUROCONTROL, qui structure la démarche tout au long du cycle de développement du système. Elle est conduite en cohérence avec les phases d'implémentation du système, et s'applique de façon itérative lorsque des besoins de retour sur la conception ou sur le concept d'emploi du système sont identifiés.

Cette méthodologie est schématisée par la Figure 3.

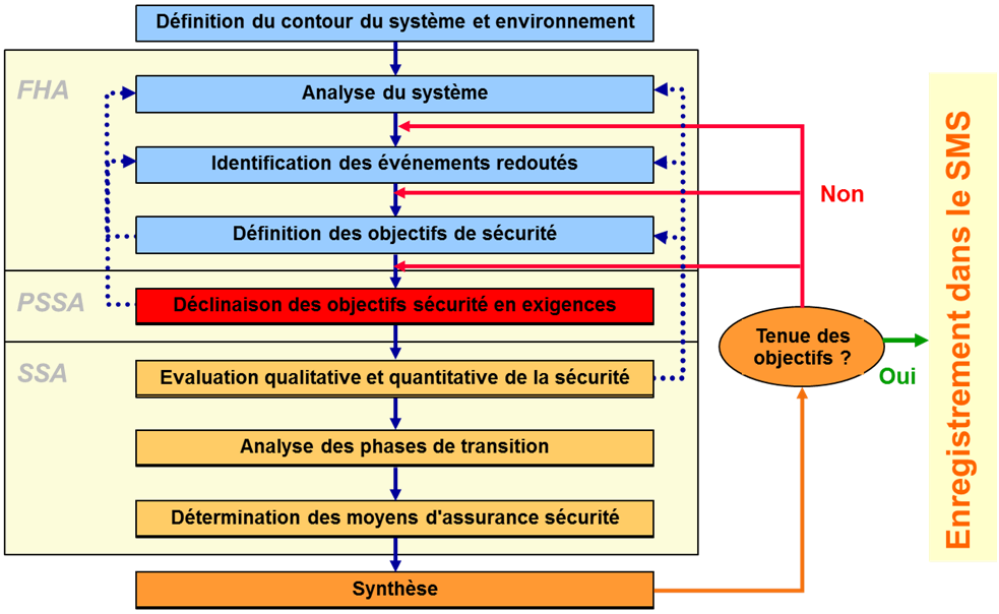

Figure 3 : Démarche de sécurité

La phase FHA (Functional Hazard Assessment) porte, en amont de la définition du système, sur l'analyse des services attendus et des conséquences de leurs dysfonctionnements, synthétisées sous forme d'événements redoutés (ER), qui vont générer des objectifs de sécurité en fonction de leur gravité et des moyens de réduction de risque (MRR) qui leur sont associés.

La phase PSSA (Preliminary System Safety Assessment) porte sur l'analyse de l'architecture du système en regard des objectifs associés aux ER. Cette analyse décline les objectifs de sécurité en exigences relatives :

- A la résilience de l'architecture, c'est-à-dire sa capacité à assurer au minimum un niveau de service en cas d'apparition de pannes (recours à des redondances efficaces, élimination des points de défaillance unique),
- A la fiabilité des matériels,
- A la fiabilité des logiciels,
- A des procédures de mise en œuvre pour réduire les risques, avec les formations associées.

La phase SSA (System Safety Assessment) porte sur l'analyse de la tenue du système aux exigences de sécurité issues de la PSSA et aux éventuelles limites d'utilisation du système, et définit des indicateurs de maintien dans le temps de cette tenue aux exigences. Elle décrit également les phases de transition, c'est-à-dire la montée en puissance de l'exploitation opérationnelle du nouveau système, sa substitution au système existant et le maintien du niveau de sécurité à assurer. Ce dernier aspect n'est pas développé dans la présente étude, car très spécifique à chaque contexte.

C. Articulation des analyses de sécurité sur le développement du système

La méthode résumée ci-dessus est déroulée en cohérence avec le développement du système, comme le montre la Figure 4.

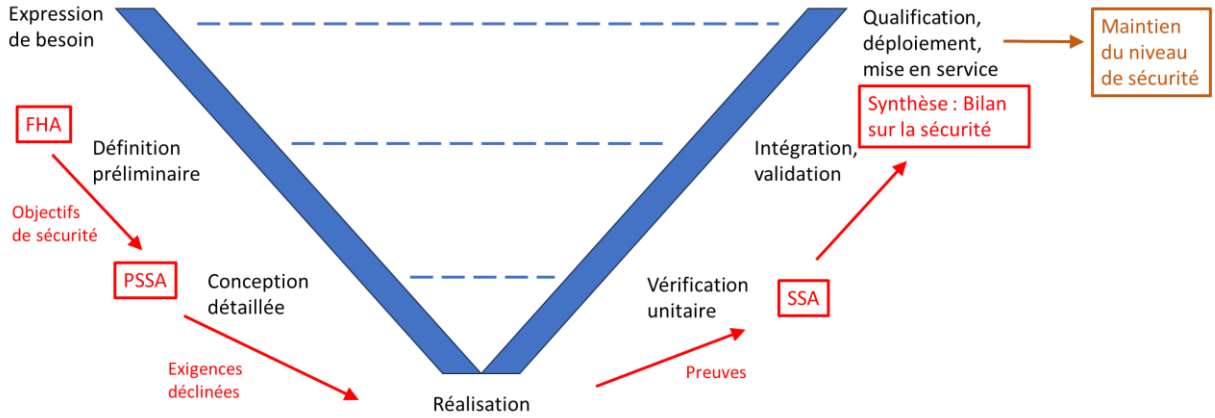

Figure 4 : Articulation de la démarche de sécurité sur le cycle en V

Il convient maintenant de détailler les 3 phases, FHA, PSSA et SSA en montrant comment elles impliquent le facteur humain.

IV. PHASE FHA

Cette phase se déroule dans le cadre d'un groupe de travail qui réunit, côté client, différents profils d'utilisateurs du système : contrôleurs aériens, spécialistes de la supervision technique du système, référents métier, référents en méthodologie et réglementation SATM.

Cette équipe est assistée, côté industriel, d'un architecte apportant une expertise sur le système développé, et de différents référents en analyse de risque et en réglementation SATM.

Une analyse de risque est conduite au niveau des services de base (désignés services élémentaires ou services unitaires) que le système doit assurer. Pour chaque service, des scénarios dysfonctionnels sont déroulés. De façon classique, les dysfonctionnements analysés sont :

- Absence du service,
- Perte du service,
- Fonctionnement intempestif du service,
- Fonctionnement erroné du service,
- Service dégradé.

L'équipe côté client analyse les différents scénarios dysfonctionnels et les ER auxquels ils sont susceptibles de conduire. Les ER sont classés par gravité, selon les critères présentés par le Tableau 1. Dans le cadre de la SATM appliquée au système radio, une perte de communication radio correspond à une gravité pouvant atteindre le niveau 2. On considère, en effet, que cet événement ne conduit pas directement à une situation de catastrophe, mais amène à une forte exposition à l'accident (rapprochement dangereux de deux aéronefs).

Niveau de gravité		**Conséquence**		
		Sur les personnes	**Sur les équipements**	**Sur la mission**
1	Accident	Nombreux morts	Destruction équipement(s)	Échec de la mission.
2	Grave	Un mort et/ou de nombreux blessés	Équipement(s) gravement endommagé(s)	Conditions d'exécution de la mission significativement dégradées pouvant entrainer son annulation et/ou le résultat est très insuffisant au regard de l'effet recherché.
3	Majeure	Quelques blessés graves	Dommages majeurs sur plusieurs sous-ensembles	La mission peut se poursuivre grâce à la mise en œuvre de moyens palliatifs lourds et/ou le résultat est décevant au regard de l'effet recherché.
4	Mineure	Un blessé grave et/ou des blessés légers	Dommages mineurs sur un ou plusieurs sous-ensemble(s)	La mission peut se dérouler grâce à des adaptations de circonstance. L'effet recherché est globalement atteint.
5	Négligeable	Eventuellement un blessé léger	Eventuelles vérifications de bon fonctionnement	La mission ne s'est pas vraiment déroulée dans les conditions prévues mais est un succès.

Tableau 1 : Matrice des gravités

L'équipe côté industriel recueille l'analyse et présente les différentes dispositions inhérentes au système développé et à sa mise en œuvre, pour réduire le risque. Ce sont les moyens de réduction de risque (MRR), répartis en 2 catégories :

- MRR de prévention : tout ce qui annule ou réduit la probabilité d'occurrence de l'ER. Ce type de MRR implique beaucoup l'architecture du système, avec tous les éléments de définition qui constituent des causes potentielles de l'ER. Il est donc, en principe, reporté dans la phase suivante du projet : la PSSA.
- MRR de protection : tout ce qui permet de réduire la gravité de l'ER en agissant sur ses effets, indépendamment de ses causes. C'est un des principaux axes de convergence en phase de FHA entre le client et l'industriel, et qui est développé ci-après.

Les MRR peuvent être d'ordre :

- Technique : une solution permet d'assurer certaines fonctions en cas de survenance d'une panne. Cette solution peut faire partie de la conception du système ou d'un système de secours, mais peut aussi correspondre à la façon dont le système est installé et paramétré.
- Procédural : actions spécifiées aux opérationnels pour appliquer des mesures de précautions ou mettre en œuvre des solutions de secours.

Dans le cas étudié, le principal recours du MRR de protection est l'orientation vers une solution de secours. Par exemple :

- La communication radio est perdue sur un poste de contrôleur aérien : le contrôleur doit avoir la possibilité de changer de poste ou de faire reprendre la communication par un autre opérateur.
- L'ensemble du système radio est en panne : un système de secours doit pouvoir être mis en œuvre.

Il en ressort les principales exigences techniques et FH pour mettre en œuvre la solution de secours :

- Présence du moyen secours : postes de contrôleur en surnombre, système radio secours → Exigence technique.
- Définir des procédures de mise en œuvre du moyen secours → Exigence FH.
- Former les opérateurs à appliquer les procédures → Exigence FH.
- Apporter un moyen d'information pour détecter les situations de panne et pouvoir déclencher les procédures de mise en œuvre du moyen secours → Exigence technique.

Cette dernière exigence est primordiale pour que le MRR soit efficace (déclenchement de la procédure dès que nécessaire et à bon escient). Par exemple, en cas de perte de la réception radio, on ne saura pas qu'un pilote cherche à appeler, puisque c'est une action indépendante du contrôleur. (A contrario, si le contrôleur appelle en premier et qu'il n'obtient pas de réponse, il peut avoir la présomption d'une situation de panne). Il faut donc spécifier des tests à différents niveaux pour alerter le contrôleur et la supervision technique du système.

Cette exigence est contraignante, mais elle permet de réduire la gravité de l'ER grâce aux MRR, et donc la sévérité des exigences pesant sur l'ensemble du système, comme on le verra dans le chapitre consacré à la PSSA.

Un point important est à souligner : pour mettre en œuvre un système radio secours, on spécifie des procédures, donc de l'action humaine. On aurait pu imaginer des moyens de bascule automatique vers le système secours. Mais il faudrait alors une interconnexion entre les deux systèmes, nominal et secours, ce qui serait préjudiciable à leur indépendance et serait source de risque de mode commun entraînant la perte des deux systèmes.

D'où un principe majeur que l'on peut énoncer : *Le recours à l'action humaine pour mettre en œuvre le système secours est un facteur clé pour assurer l'indépendance technologique entre le système nominal et le système secours.*

Un rapport de FHA est émis par l'industriel à l'issue des travaux du GT. Il comprend :

- La description fonctionnelle du système,
- Le tableau d'analyse dysfonctionnelle sous la forme d'une AMDE par services unitaires,
- La liste des ER caractérisés par leur intitulé, leur niveau de gravité, les scénarios dysfonctionnels qui les génèrent, les objectifs de sécurité qui leur sont attribués,
- La liste des MRR jugés efficaces.

A ce stade, on peut faire un premier bilan de l'action humaine.

Action humaine	Apport de l'action humaine	Risque facteur humain
Réalisée au stade du projet : groupe de travail	Mise en présence des utilisateurs et de l'industriel permettant de confronter la couche technique et la couche métier Analyse par scénarios concrets	Prise en compte de MRR qui s'avéreront inefficaces Description de scénarios irréalistes (raideur méthodologique) ER mal définis, rendant leur analyse difficile en PSSA
Prévue en phase d'exploitation : procédures	Indépendance du système nominal et du système secours Maintien d'un niveau de connaissance du système par les opérateurs	Procédures insuffisamment décrites Formation insuffisante Erreur humaine résiduelle toujours possible en utilisation

Tableau 2 : Bilan facteur humain de la phase FHA

V. PHASE PSSA

La PSSA est réalisée chez l'industriel, par des spécialistes de l'analyse de risque, avec l'aide des référents SATM et de l'équipe d'architectes du projet. Elle étudie l'architecture du système tel que défini (on est en phase de conception détaillée) et son aptitude à tenir les objectifs de sécurité associés aux ER. Ces objectifs sont en relation avec les niveaux de gravité des ER tels que présentés au Tableau 1Tableau 1 : Matrice des gravités. Ils sont exprimés sous forme quantitative par la probabilité ou la

fréquence d'occurrence admissible pour chaque niveau de gravité. Plus l'ER est grave, plus il doit être improbable ou rare. Ces objectifs sont fixés par les prestataires de service de la navigation aérienne.

La PSSA comprend :

- Une analyse des chaînes fonctionnelles qui réalisent les services unitaires, avec les éléments matériels et logiciels qui contribuent à cette réalisation,
- Une analyse par arbres de défaillance des ER qui identifie, à partir des scénarios dysfonctionnels issus de la FHA et de l'analyse des chaînes fonctionnelles, la contribution de tous les éléments matériels et logiciels à chaque ER, et également la contribution du facteur humain.

La décomposition de l'ER en événements de base prend donc une forme hybride, comme représenté de façon typique en Figure 5, avec des événements dus aux matériels, aux logiciels et au facteur humain (ici au sens mise en œuvre). Il faut tenir compte du fait que les événements dus aux logiciels peuvent résulter d'erreur humaine en spécification, conception, réalisation, intégration, validation.

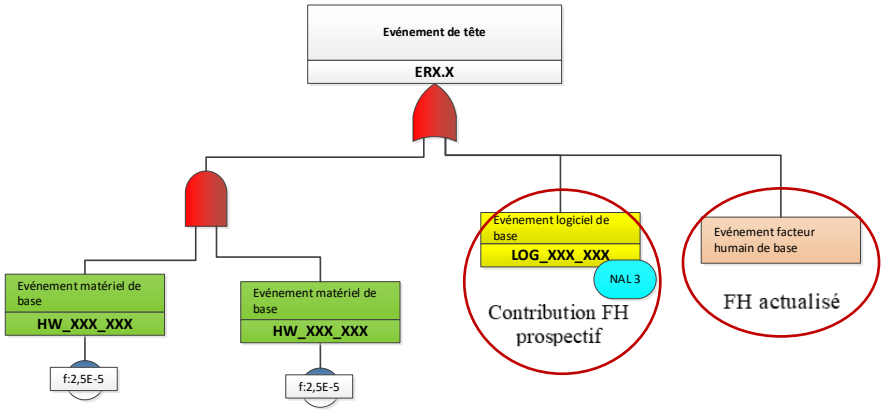

Figure 5 : Type d'arbre de défaillance combiné

L'analyse qualitative de l'arbre permet d'identifier les rangs des coupes minimales. L'attention est portée sur les matériels en redondance porteurs d'une même solution logicielle : la redondance ne porte dans ce cas que sur l'entité matérielle, le logiciel pouvant être source de mode commun. Un logiciel ne peut être redondant avec un autre logiciel que s'il assure les mêmes fonctions tout en apportant une solution différente et indépendante.

Un arbre de défaillance pourra incorporer des MRR de prévention, positionnés sous une porte « ET » avec différents événements de base, et permettant de réduire leur contribution à l'ER.

L'analyse quantitative de l'arbre ne porte que sur les contributeurs matériels, affectés de MTBF.

Les logiciels sont, eux, caractérisés par un niveau d'assurance logicielle (NAL, ou SWAL en anglais) qui leur est spécifié en fonction de la gravité de l'ER (Tableau 1) et du rang de coupe minimale par rapport à l'ER. Les NAL spécifiés par la norme EUROCAE ED-153, pour une contribution directe à l'ER, sont les suivants :

- Gravité 1 → NAL 1 : c'est le niveau maximum d'exigence pour une solution logicielle. Sa défaillance peut conduire directement à la catastrophe. On doit être à même de tester l'exécutable pas à pas.
- Gravité 2 → NAL 2 : le code source du logiciel doit pouvoir être testé ligne à ligne.
- Gravité 3 → NAL 3 : le produit logiciel doit pouvoir être testé au niveau de ses composants de base, considérés comme boîtes noires.
- Gravité 4 → NAL 4 : le produit logiciel peut être testé comme boîte noire, sans descendre au niveau des composants.

L'analyse par arbres de défaillance amène aux conclusions :

- Tenue des objectifs quantitatifs, avec un récapitulatif des contributeurs matériels, de leur MTBF et de leurs rangs de coupe minimale,
- Exigences sur le NAL des produits logiciels,
- Exigences qualitatives relatives au facteur humain, en fonction de sa contribution.

Cette analyse est complétée par des exigences déclinées des MRR de protection et des MRR de prévention, tracées par rapport aux différents scénarios accidentels. Ces exigences portent sur :

- La solution technique qui permet de spécifier et réaliser les MRR d'ordre technique,
- L'installation de ces MRR techniques, dans le contexte d'utilisation

- Les procédures de mise en œuvre des MRR techniques et d'autres actions humaines de maintien de la sécurité,
- Les actions de formation, propres aux MRR techniques et aux procédures.

La validation du rapport de PSSA fait l'objet d'une revue de pairs qui permet d'établir la bonne cohérence entre la modélisation effectuée et le système développé. Au jalon projet correspondant (RCD), l'architecture est encore susceptible d'évoluer, ce qui peut entraîner un décalage avec les études de sécurité.

Le bilan de l'action humaine en phase PSSA est le suivant.

Action humaine	Apport de l'action humaine	Risque facteur humain
Réalisée au stade du projet : - Travaux des spécialistes d'analyse de risque - Aide des référents et architectes - Revue de pairs	Niveaux d'expertise Lectures par un regard extérieur	Ecarts entre l'étude et l'architecture, du fait du caractère encore évolutif de celle-ci Effet surcharge à une phase critique du projet, qui nuit à la qualité de la validation des études Erreurs de conception/réalisation par rapport à la prise en compte des exigences de sécurité
Prévue en phase d'exploitation : procédures	Rôles identifiés	Procédures insuffisamment décrites Formation insuffisante Erreur humaine résiduelle toujours possible en utilisation

Tableau 3 : Bilan facteur humain de la phase PSSA

VI. PHASE SSA

En phase SSA, la tenue des exigences est faits sur les 3 volets :

- Tenue des exigences quantitatives,
- Tenue des exigences qualitatives,
- Tenue des exigences logicielles.

A. Tenue des exigences quantitatives

La tenue des exigences quantitatives est donnée par les résultats des arbres de défaillance, traités en PSSA. Une vérification est faite en cas d'évolution de références de matériels depuis la revue de conception détaillée. Ce volet n'a pas un impact important en termes de facteur humain, si ce n'est l'attention à suivre les évolutions de ces matériels, de leur fiabilité et de leur aptitude à s'intégrer dans une architecture redondée.

B. Tenue des exigences qualitatives

La tenue des exigences qualitatives se décline des MRR :

- Conception : documents SSS (System / Subsystem Specification) et SSDD (System / Subsystem Detailed Design),
- Installation : spécifications propres à la SATM reportées dans les dossiers d'installation,
- Procédures et organisation : portées dans la Documentation Technique Utilisateur (DTU),
- Formation : conception et réalisation des sessions de formation.

1) Conception

En conception, il s'agit de s'assurer que les mises à jour des documents ont bien pris en compte les exigences issues des MRR. Ces exigences sont ensuite déclinées et tracées en phases de réalisation, intégration et validation au même titre que l'ensemble des fonctionnalités traitées par la conception (déclinées en solutions matérielles et logicielle), mais font également l'objet de justifications spécifiques en réponse aux exigences de la norme ED-153, ce qui a un impact sur les livrables, les tâches et l'organisation du projet.

La déclinaison en solutions matérielles et logicielles renvoie aux 2 autres volets de tenue aux exigences, avec les impacts facteur humain correspondants.

2) Installation

Les exigences d'installation portent notamment sur la radio secours : sa présence effective et l'ergonomie de son accès quand elle doit être utilisée. C'est un fort enjeu FH en exploitation qui doit être validé par une démonstration de mise en œuvre.

Le type de disposition adopté est le fonctionnement permanent de la radio secours, et sa réception sur des haut-parleurs de veille installés dans les salles de contrôle. Un appel sur la radio secours est donc immédiatement entendu par les opérateurs, permettant :

- De considérer un probable défaut de la radio nominale,
- De se reporter sur les ressources radio secours des postes de contrôle,
- D'engager les procédures de sécurité conséquentes à une panne de la radio nominale.

Remarque : L'ergonomie des casques audio utilisés par les contrôleurs leur permet d'entendre les appels autres que ceux relatifs à la communication radio nominale transmise par le casque : demandes d'autres opérateurs, en direct ou via la téléphonie/interphonie, perception des messages sur haut-parleurs de veille.

3) Procédures

Les procédures sont portées dans les manuels DTU, pour l'utilisation et l'administration du système. La traçabilité doit être établie entre le contenu de la DTU et les exigences de procédures constituant des MRR. L'exécution des procédures doit être validée par une démonstration, où les risques d'erreur humaine résiduels sont identifiés et font l'objet d'actions correctives sur la DTU.

En phase d'exploitation, des mises à jour de la DTU prendront en compte le retour d'expérience apporté par des événements touchant la SATM et nécessitant une reprise des procédures.

4) Formation

La première session de formation est assurée en amont de la phase de qualification et s'adresse aux référents client qui vont conduire la campagne de qualification. Ces profils sont au plus près des aspect techniques de la solution développée et donc à même de mener les tests des éléments techniques qui ont directement un impact sur la SATM. Ils sont donc destinataires de tous les éléments de solution répondant aux exigences formulées par la PSSA, pour les aspects matériel et logiciel.

Les sessions suivantes sont dispensées en phase de déploiement et s'adressent aux opérationnels (contrôleurs aériens, superviseurs, administrateurs, maintenanciers). Elles peuvent être directement assurées par l'industriel auprès des opérationnels, ou par des formateurs appartenant à l'instance cliente, et préalablement formés par l'industriel. La formation précise les points de compétence ayant un impact direct sur les MRR. Ces points d'acquisition doivent être mentionnés dans les supports de formation, puis contrôlés et tracés lors du bilan de formation.

En phase d'exploitation, des sessions de formation visant au maintien des compétences prendront en compte le retour d'expérience apporté par des événements touchant la SATM.

C. Tenue des exigences logicielles

La tenue des exigences logicielles reprend la liste des logiciels avec NAL requis et établit un bilan sur le NAL atteignable pour chaque produit identifié.

La doctrine usuellement retenue dans la conception de l'architecture du système vise à ne pas dépasser une exigence plus sévère que NAL 3. Cette disposition est obtenue en faisant en sorte qu'aucun produit logiciel retenu ne soit point de défaillance unique conduisant à un ER de gravité 2, soit parce que la gravité de l'ER a été ramenée à un niveau pas plus sévère que 3 grâce à un MRR efficace, soit parce que le produit logiciel intervient en redondance avec une autre entité fonctionnelle (matérielle, logicielle ou FH). La tenue du NAL 2 requiert en effet des moyens et procédures très spécifiques et coûteux.

Pour rappel, les vérifications pour les niveaux préconisés sont :

- NAL 3 : le produit logiciel doit pouvoir être testé au niveau de ses composants de base, considérés comme boîtes noires.
- NAL 4 : le produit logiciel peut être testé comme boîte noire, sans descendre au niveau des composants.

Les procédures de test mise en œuvre pour ces 2 niveaux sont classiques dans l'ingénierie des logiciels développés en répondant à des exigences de fiabilité (voir notamment le guide publié par le GTR63 de l'IMdR).

L'attention particulière est portée sur le niveau de granularité du logiciel : quel est le niveau « produit » (susceptible d'être décliné en composants pour répondre aux exigences du NAL 3), quel est le niveau « composant ». Ce point est particulièrement important dans la mesure où la compréhension du fonctionnement interne du produit est nécessaire lorsque des dysfonctionnements apparaissent en exploitation, alors que les tests de bon fonctionnement ont donné des résultats conformes en phase de qualification, voire pendant une exploitation prolongée.

Ce cas se présente typiquement lorsque des briques logicielles assurant des fonctions d'interface sont réutilisées dans des architectures, en tant qu'éléments éprouvés. L'exemple proposé est celui d'un composant qui s'insère dans un produit logiciel pour assurer l'interface avec un système extérieur (généralement un réseau d'infrastructure) de spécification réputée connue et maîtrisée.

La situation rencontrée est la suivante : le système a été déployé dans des pays donnés, avec un réseau d'infrastructure répondant à la spécification. Il est ensuite déployé en réutilisant les interfaces dans d'autres pays où le réseau d'infrastructure répond théoriquement à la spécification, mais est confronté à des problèmes de vétusté, qui se traduisent par des signaux non nominaux (parasites) interprétés de façon aléatoire par le système, ce qui entraîne des dysfonctionnements.

Bien entendu, l'exigence de déployer et mettre en service le système en toute sécurité subsiste. Il faut, à ce stade, se pencher sur deux exigences relatives au facteur humain, avec les risques associés :

- Prendre en compte une granularité suffisamment fine pour définir le niveau « produit » et le niveau « composant ». Dans le cas présent, la brique considérée dans un premier temps comme composant « boîte noire » se trouve dans une problématique « produit » dont on doit pouvoir analyser le fonctionnement interne.
- Les compétences nécessaires doivent être présentes pour traiter les dysfonctionnement, en caractérisant les signaux parasites à l'aide d'analyseurs, et en analysant les effets internes au produit, de façon à trouver une solution de robustesse. Il faut donc un maintien suffisant de compétences sur la connaissance du produit réutilisé, dans un contexte où les durées de vie des systèmes développés sont longues (15 à 20 ans).

Une autre attention est portée sur l'utilisation de logiciels du commerce (Component Off The Shelf – COTS). Ces produits ont généralement des cycles de vie beaucoup plus courts que les systèmes considérés et sont sujets à obsolescence. La stratégie de mises à jour doit être définie dès le présent stade du projet, dans le cadre de la veille technologique.

Il faut ajouter que les éditeurs de COTS n'ont généralement pas la connaissance de la couche métier qui nous intéresse, sauf dans les cas de produits très spécialisés, ce qui demande des structures de collaboration adaptées.

D. Récapitulatif des enjeux du facteur humain en phase SSA

Les analyses ci-dessus permettent de faire un bilan des impacts du facteur humain en SSA.

Action humaine	Apport de l'action humaine	Risque facteur humain
Réalisée au stade du projet :		
- Conception	Tenue des exigences ED-153	Ecart architecture étudiée/développée Couverture validation insuffisante
- Installation	Ergonomie des moyens de secours	Alerte difficilement détectable en situation de travail
- Procédures	Prise en compte des procédures de sécurité dans la DTU	Validation insuffisante des procédures
- Formation	Formation des référents aux solutions techniques impactant la SATM Prise en compte des exigences SATM de formation des utilisateurs	Formation insuffisante Formation insuffisante, turn-over
- Détermination de la granularité des solutions logicielles Connaissance des solutions au niveau de granularité défini	Arbitrages sur la granularité des produits logiciels Maintien des compétences	Niveau trop macroscopique Maintien insuffisant
- Utilisation de COTS	Anticipation de la veille technologique Implication des éditeurs de COTS	Obsolescence non prévue Méconnaissance des risque apportés par les COTS
Prévue en phase d'exploitation : procédures	Rôles identifiés	Procédures insuffisamment décrites Formation insuffisante Erreur humaine résiduelle toujours possible en utilisation

Tableau 4 : Bilan facteur humain de la phase SSA

VII. RESULTATS

Le déroulement pas à pas des différentes phases de l'étude de SATM conduite en cohérence du programme d'implémentation d'un système radio dédié à la circulation aérienne a permis de relever différentes actions humaines avec les risques inhérents. Il convient maintenant d'en faire un récapitulatif global en apportant des éléments de quantification du risque, en termes de gravité et de probabilité.

Risque FH pointé	Gravité	Probabilité	Action identifiée en réduction de risque
Prise en compte de MRR qui s'avéreront inefficaces	Elevée	Faible	Risque suffisamment anticipé par la FHA et l'étude des scénarios
Description de scénarios irréalistes (raideur méthodologique)	Moyenne	Moyenne	Vérification d'impact à l'issue de la PSSA : toutes les causes d'ER ont-elles bien été prise en comptes ? Impact important sur les coûts et délais du projet
ER mal définis, rendant leur analyse difficile en PSSA	Moyenne	Moyenne	Vérification d'impact à l'issue de la PSSA : toutes les causes d'ER ont-elles bien été prise en comptes ? Impact important sur les coûts et délais du projet
Ecarts entre l'étude et l'architecture, du fait du caractère encore évolutif de celle-ci	Elevée	Elevée (PSSA) puis réduction	Mise en cohérence en cours de projet. Impact surtout sur les coûts et délais du projet
Effet surcharge à une phase critique du projet, qui nuit à la qualité de la validation des études	Moyenne	Elevée	Relecture et éventuelles mises à jour des études SATM à des jalons intermédiaires, veille sur les retours sur conception
Erreurs de conception/réalisation par rapport à la prise en compte des exigences de sécurité	Elevée	Moyenne	Couverture des tests de validation unitaires des produits constitutifs du système, et de l'ensemble du système en phase d'intégration
Alerte difficilement détectable en situation de travail (pour utilisation des MRR)	Elevée	Faible	Test des scénarios et convergence vers une ergonomie adaptée
Description et validation insuffisantes des procédures	Elevée	Moyenne	Tenue d'un retour d'expérience et mises à jour périodiques
Formation référents et utilisateurs insuffisante	Elevée	Moyenne	Sessions complémentaires, entraînement sur simulateur, retour d'expérience sur incidents survenus
Niveau composant trop macroscopique	Moyenne	Moyenne	Complément d'études sur le contexte d'emploi et le fonctionnement interne des composants
Maintien des compétences industrielles insuffisant	Moyenne	Moyenne	Identification des produits à longue durée de vie, actions de formation et transfert de compétence
Obsolescence non prévue Méconnaissance des risques apportés par les COTS	Moyenne à élevée	Moyenne	Veille technologique Collaboration rapprochée avec les éditeurs
Erreur humaine résiduelle toujours possible	Elevée	Faible	Analyse du retour d'expérience, actions sur les aspects techniques, procéduraux, de formation

Tableau 5 : Bilan de l'impact du facteur humain

Ce récapitulatif met en évidence les impacts les plus sévères (couple « Gravité élevée » / « Probabilité moyenne » ou « Gravité moyenne » / « Probabilité élevée »). Ces impacts se retrouvent :

- En phase d'exploitation : défaut de procédure ou de formation. C'est le schéma classique qui fait redouter l'erreur humaine, mais pour lequel l'action en réduction de risque est clairement identifiée.
- Mais aussi en phase de conception et réalisation :
  - Effet surcharge dans le projet qui nuit à la qualité de validation des études, et à terme, à la capacité de la solution technique à tenir les exigences de sécurité,
  - Risques liés aux solutions COTS insuffisamment maîtrisées,
  - Erreurs de conception/réalisation par rapport à la prise en compte des exigences de sécurité.

Les actions en réduction de risque montrent la nécessité d'intervention mettant en jeu le facteur humain et de considérer son action positive.

VIII. DISCUSSION ET PERSPECTIVES

L'étude de cas proposée a permis de mettre en évidence les effets de l'action humaine dans le contexte d'un programme qui implique la sécurité, et dans un domaine où une doctrine de recherche d'équilibre entre la solution technique et le facteur humain est déjà sous-jacente. Différents points saillants montrent que le risque lié au facteur humain intervient à des étapes antérieures

à la phase d'exploitation et a des conséquences sur la sécurisation de la solution technique, alors qu'a contrario, l'action humaine en exploitation permet toujours d'apporter des solutions en situation non prévue et de garder un regard critique sur le système utilisé et son niveau de sécurité.

Les axes d'étude qui en découlent pourraient être les suivants :

- Comment envisager, dès le début d'un projet, le périmètre de l'action humaine pour assurer le niveau de sécurité requis, dans le contexte à risques où doit évoluer le système concerné. Ce principe permet de ne pas se trouver tributaire d'une solution technique verrouillée, empêchant l'intervention humaine, ou d'un « coup de génie » de l'opérateur dont l'efficacité n'est pas prévisible.
- Poursuivre l'analyse sur le facteur humain « prospectif », comme abordé dans la présente étude à travers les différents tableaux récapitulatifs, en l'enrichissant avec les retours d'expérience d'autres domaines d'activité et en élaborant des indicateurs pertinents. Ce volet du facteur humain reste très ouvert, et à confronter avec le facteur humain « actualisé ».
- Comment intéresser tous les acteurs intervenant sur le système, depuis le concepteur jusqu'à l'utilisateur final (le contrôleur aérien), pour définir une posture de réactivité à des situations non prévues. Il y a là une notion de connaissance étendue et d'intérêt pour les activités techniques et métier sous-jacentes au système étudié. Une réponse est déjà apportée par les prestataires de la circulation aérienne qui assurent à leurs contrôleurs des entraînement sur simulateurs, prenant notamment en compte le rejeu d'incidents ou d'accidents déjà survenus.
- Les autres grands axes classiques de l'amélioration de la conduite d'un projet, tels que la cohérence entre la solution retenue et les études de sécurité qui y sont menées, la couverture de tests, ou le maintien des compétences dans la durée sur les produits développés.

IX. Conclusion

Une étude concrète a pu démontrer comment l'acteur humain, formé et motivé, est susceptible d'apporter une assurance de fiabilité dans la conduite d'un système engageant la sécurité. Elle montre aussi comment cadrer la solution technique pour la rendre accessible à l'acteur humain, au vu des problèmes non prévisibles liés à l'état de l'art technologique et son appréhension par les personnes qui développent et réalisent le système. C'est là que le facteur humain dit « prospectif » entre en ligne de compte et doit être fiabilisé pour la bonne marche du facteur humain dit « actualisé ».

Cette règle de prudence s'impose face à la séduction des solutions technologiques promues par des effets de mode. Là où y a bien des apports de nouveaux services et des évolutions dans la manière de travailler, il convient d'en comprendre concrètement les apports et comment s'établit le dialogue avec l'acteur humain, qui ne peut pas se défausser à bon compte sur la machine. Celle-ci ne fait qu'intégrer les résultats de travaux humains qui sont eux-mêmes discutables.

Dans ce contexte, il ne faut pas oublier l'accroissement du domaine d'incertitude lié à des actions malveillantes, notamment les attaques qui affectent la sécurité informatique. Une solution technique verrouillée devient alors un obstacle aux possibilités de réaction et de traitement, face à une situation qu'on n'a pas été en mesure de prévoir.

Remerciements

Nous tenons à remercier celles et ceux qui ont contribué, au sein de CS GROUP, à la réalisation des présents travaux, en particulier l'encadrement de la filière expert, les représentants RH, la direction technique, qui promeuvent ce type de démarche, et les référents métier qui ont participé à la relecture.

References

Règlement (CE) n°549/2004 du Parlement Européen et du Conseil du 10 mars 2004 fixant le cadre pour la réalisation du ciel unique européen

EUROCAE ED-153 Guidelines for ANS software safety assurance

IMdR – GTR63 Guide – Démarche et méthodes de sûreté de fonctionnement des logiciels

CS GROUP Référentiel de mise en œuvre de l'ED-153 au sein des projets (documents non publics)

CS GROUP Les différentes études de sécurité ATM (FHA, PSSA, SSA) sur les systèmes radio du contrôle aérien, dans les domaines civil et militaire (documents non publics)