



N° 5731... DAC/DNA/SCA

Rabat, le 23 SEPT 2016.....

**Circulaire relative
au contenu et à la forme d'une
étude de sécurité dans le domaine
de la navigation aérienne**

Objet : La présente circulaire a pour objet de spécifier le contenu et la forme d'une étude de sécurité exigée lors des études d'évaluation et d'atténuation des risques, menées avant toute mise en place d'un changement impactant la sécurité du système ATM/CNS.

1-La structure générale de l'étude de sécurité se présente en six parties. Ces parties s'intitulent :

- Partie1.** Présentation de l'étude de sécurité.
- Partie2.** Exigences de sécurité.
- Partie3.** Evaluation de la sécurité.
- Partie4.** Analyse des phases de transition.
- Partie5.** Principes d'assurance sécurité.
- Partie6.** Synthèse.

2- Le contenu de chacune de ces parties est précisé sous forme de canevas en annexe à la présente circulaire.

3- Le canevas présenté en annexe à la présente circulaire est destiné à aider le fournisseur des services de la navigation aérienne à constituer et présenter un dossier complet.

4- L'étude sécurité, établie dans le cadre du système de gestion de la sécurité du fournisseur des services de la navigation aérienne, doit être communiquée à la Direction de l'Aéronautique Civile.

5- la présente circulaire prend effet à partir de la date de sa signature.

Zakaria BELHAZI
Directeur de l'Aéronautique Civile



Annexe : Plan type de l'étude de sécurité

Sommaire

I-	Présentation du dossier de sécurité.....	3
I.1	Objet de l'évolution	3
I.2	Documents de référence.....	3
I.3	Périmètre de l'étude (FHA/OED).....	4
I.3.1	Les contours du système étudié.	4
I.3.2	Les interfaces.....	4
I.3.3	L'utilisation opérationnelle	4
I.4	Organisation.....	5
I.4.1	Rôle et responsabilités	5
I.4.2	Le planning.....	5
II-	Exigences de sécurité (FHA - PSSA).....	5
II.1	Exigences et standards locaux, nationaux ou internationaux	5
II.2	Objectifs de sécurité (FHA)	6
II.3	Exigences de sécurité (PSSA).....	8
III-	Evaluation de la sécurité (SSA).....	9
IV-	Analyse des phases de transition (SSA)	10
V-	Principes d'assurance sécurité	11
VI-	Synthèse.....	11

I- Présentation de l'étude de sécurité

I.1 Objet du changement

Texte du plan type

Ce paragraphe décrit l'évolution envisagée, avec un niveau de détail permettant d'évaluer la pertinence des analyses conduites afin :

- d'attribuer les exigences aux différentes composantes du système (**Cf. partie II**) ;
- d'évaluer le niveau de sécurité (**Cf. partie III**).

Objectif du §

Permettre au lecteur de se faire une idée **générale** des fonctions (au sens des services rendus), objets de l'étude, et des conditions dans lesquelles elles seront utilisées (type de trafic, conditions météo ...). Par exemple, pour un système tel que le SMGCS (Surface Movement Guidance and Control System), on pourra expliquer que le système est une aide au contrôleur pour la visualisation de la circulation des avions au sol, qu'il n'est utilisé qu'en conditions LVP (par exemple), qu'il est destiné à être mis en service à Casablanca/Mohammed V, que tous les mobiles de la plateforme sont capables de transmettre leur identification (ou seulement les avions), qu'il a une fonction d'alerte (ou pas) à proximité des pistes, ...

Commentaires

Ainsi, on trouvera notamment dans ce chapitre de l'étude de sécurité :

- Une description générale du changement ;
- Les fonctions opérationnelles réalisées (ou services rendus), **en termes généraux** ;
- Les composantes impliquées (procédures, équipement etc...).

On peut y synthétiser éventuellement :

- Les performances sécurités visées ;
- Les dispositions prises pour rendre la mise en œuvre sûre si certaines ont déjà été envisagées.

I.2 Documents de référence

Texte du plan type

Ce paragraphe comprend :

- la liste des documents applicables ;
- la liste des documents jugés utiles à la compréhension du dossier de sécurité.

Objectif du §

Présenter une bibliographie du dossier de sécurité.

Commentaires

On présente ici les documents applicables (ayant un caractère réglementaire ou non), c'est-à-dire ceux auxquels doit se conformer le dossier de sécurité (référentiel réglementaire, manuels qualité/sécurité etc), ainsi que tous les documents qui peuvent permettre une bonne compréhension du dossier de sécurité, qu'ils soient relatifs à l'évolution ou relatifs aux activités d'analyse, évaluation et atténuation des risques de l'évolution (expression de besoin, cahier des charges, les différentes contributions au dossier de sécurité dont les résultats sont présentés dans le dossier de sécurité etc).

I.3 Périmètre de l'étude (FHA₁/OED₂)

Texte du plan type

Ce paragraphe décrit :

- les contours du système sur lequel porte l'étude ;
- les interfaces du système (données en entrée/sortie...) ;
- l'utilisation opérationnelle prévue.

Objectif du §

Le but de cette section est de limiter le champ du dossier de sécurité aux seules parties du système ATM concernées par l'évolution, dont on juge pertinente l'analyse d'un point de vue sécurité. **Ainsi, il peut ne pas y avoir une totale correspondance entre le contour de la modification et le périmètre de l'étude de sécurité.** Par exemple, dans le cas de l'A-SMGCS, composé de radars primaires, de Syletrack, de multilatération Mode S alimentant le cœur du système, il avait été décidé de ne pas inclure dans l'étude de sécurité les radars primaires, leurs modes de défaillance étant supposés connus.

Inversement, il peut être décidé d'étendre la couverture de l'étude de sécurité au-delà du périmètre strict de l'évolution, en particulier lorsque des sous-systèmes en interface n'ont jamais faits l'objet d'analyses de sécurité. Comme on l'a vu plus haut, le sous-ensemble du système ATM concerné par l'évolution constitue lui-même un **système** dont on va déterminer le contour, les interfaces avec l'extérieur, et l'utilisation opérationnelle prévue.

Commentaires :

1.3.1 Les contours du système étudié.

Il faut identifier ce qui est dans le système objet du dossier de sécurité, ce qui est en dehors. Les éléments externes seront pris comme tels, c'est-à-dire qu'on ne fixera pas d'exigences particulières issues de l'étude. Toutefois, on analysera les modes de défaillance sur les échanges avec les éléments externes, afin d'en déduire l'impact sur le système étudié, les événements redoutés et les éventuels moyens en réduction de risques à mettre en place. Les éléments externes ne seront donc pas évalués du point de vue de la sécurité dans le cadre du dossier mais les interfaces le seront.

1.3.2 Les interfaces

Les interfaces avec les systèmes externes doivent être identifiées et décrites car elles rentreront dans l'analyse de la sécurité du système. Ce sont par exemple : des échanges de données entre un équipement du système objet du dossier de sécurité et des systèmes hors champ du dossier ; des modes de coordination entre organismes de contrôle type lettre d'accord etc... Les échanges et le support de ces échanges peuvent faire l'objet de modes de défaillance, à évaluer.

1.3.3 L'utilisation opérationnelle

Il faudra définir ou décrire l'utilisation opérationnelle prévue, car celle-ci peut influencer l'évaluation du risque : par exemple des défaillances relatives à l'utilisation d'une image radar à des fins d'information n'auront vraisemblablement pas la même criticité que si cette image était utilisée à des fins de guidage radar (d'un point de vue facteur humain, il conviendra toutefois de s'assurer de l'efficacité des moyens mis en œuvre pour éviter les dérives du mode d'utilisation

¹ Functional Hazard Analysis

² Operational Environment Description

opérationnelle initialement prévu, c'est-à-dire dans le cas présent l'utilisation pour du guidage radar d'un système « qualifié » pour ne permettre que de l'information).

I.4 Organisation

Texte du plan-type

Ce paragraphe décrit :

- *le rôle et les responsabilités de chaque acteur dans la réalisation du dossier de sécurité ;*
- *le planning relatif à l'établissement du dossier de sécurité.*

Objectif du §

En terme d'organisation du travail, cette section doit permettre de savoir « qui fait quoi » dans l'élaboration du dossier de sécurité, mais aussi de connaître le processus : « comment », « quand » ; afin de pouvoir estimer si l'organisation choisie offre les garanties souhaitables vis-à-vis du résultat attendu (le dossier de sécurité).

Commentaires:

Cette section reprend éventuellement tout ou partie de ce qui a déjà été présenté dans le plan de sécurité.

Le niveau de description va dépendre :

- de la complexité de l'organisation mise en place pour élaborer l'évolution,
- de la segmentation de l'étude de sécurité en fonction des différentes contributions nécessaires, impliquant différents acteurs ou entités.

L'organisation mise en place devra permettre d'assurer la gestion et le suivi global des analyses de sécurité effectuées au niveau de chaque acteur.

1.4.1 Rôle et responsabilités

On identifiera notamment :

- les entités (Services, divisions, subdivisions, équipes, SSII, individus, ...) concernées et leur contribution au dossier de sécurité. On trouvera ici le(s) responsable(s) sécurité, dont le coordonnateur du dossier de sécurité et le(s) chef(s) de projet, mais également toutes les personnes (ou équipes) dont la contribution est prévue ;
- les processus de validation des différentes contributions (gestion des sous-traitants, processus de validation interne des analyses..). On pourra se référer ici aux processus qualité des organismes considérés ;
- les modes éventuels de communication, circulation d'information, traçabilité et capitalisation des résultats (réunions, gestion du référentiel documentaire lié à l'étude de sécurité, gestion des recommandations issues des analyses de sécurité etc.).

1.4.2 Le planning

Le phasage des activités sécurité doit être présenté en lien avec les activités afférentes au changement.

II- Exigences de sécurité (FHA - PSSA₃)

II.1 Exigences et standards locaux, nationaux ou internationaux

Texte du plan type

³ Preliminary System Safety Assessment

Ce paragraphe rappelle les exigences ou standards locaux, nationaux ou internationaux applicables au système objet du dossier.

Commentaires

On recensera ici les exigences de sécurité pertinentes (quand elles existent) pour le système objet de l'étude, sous forme de standards nationaux ou internationaux (Annexe 11 de l'OACI,...).

II.2 Objectifs de sécurité (FHA)

Texte du plan-type

Ce paragraphe explique comment sont déterminés les objectifs de sécurité (définis par le prestataire de services de navigation aérienne ou par l'autorité compétente) associés à l'évolution considérée.

Plus particulièrement, la détermination des objectifs de sécurité associés au sous-ensemble considéré se fait en trois phases :

- 1. l'identification des dangers et des modes de défaillance plausibles associés à l'ATM, ainsi que celle de leurs incidences combinées;*
- 2. l'évaluation des incidences potentielles des facteurs précités sur la sécurité des aéronefs, ainsi qu'une évaluation de la gravité de ces incidences, en utilisant le mécanisme de classification de la gravité fourni à l'**appendice 1** ;*
- 3. la détermination des objectifs de sécurité proprement dit, exprimés comme la probabilité maximale d'occurrence d'un danger, et déterminés à partir de la gravité et de la probabilité maximale d'occurrence de ses incidences.*

Objectif du §

A partir de l'analyse du système objet de l'étude, identifier les dangers (événements redoutés) qu'il peut engendrer et, pour chacun d'eux, spécifier la fréquence d'occurrence acceptable relativement à la gravité estimée.

On pourra également recenser ici des objectifs de haut niveau sur le **temps de séjour** acceptable dans un état dégradé (qui pourra par exemple se traduire par une exigence sur le temps de relance d'une application logicielle), ou le **séquençement de restauration** de certaines fonctionnalités du système (priorité de la restauration de l'image radar sur les informations plan de vol par exemple).

Ces objectifs, exprimés sur le système objet du dossier, seront ensuite déclinés au §2.3 en exigences sur les différents éléments de ce système.

Commentaires

« 1. L'identification des dangers et des modes de défaillance et de leurs incidences combinées »

On doit retrouver ici les résultats des différentes étapes conduisant à l'identification des événements redoutés pour l'évolution:

- **L'analyse technique et fonctionnelle du système** : le niveau de description du système et de ses interactions avec l'environnement est déterminant pour l'identification des défaillances potentielles.
- **L'identification des événements redoutés** : A partir de l'analyse technique et fonctionnelle précédemment effectuée, on analysera les différents modes de défaillances pour recenser leurs effets jusqu'à l'utilisateur, où ils se traduisent par des événements redoutés. Ceci doit être fait pour chaque phase ou état de fonctionnement du système.

« 2. L'évaluation des incidences potentielles des facteurs précités sur la sécurité des aéronefs, ainsi qu'une évaluation de la gravité de ces incidences, en utilisant le mécanisme de classification de la gravité fourni à l'appendice 1; »

Evaluation des « incidences potentielles »

Les événements redoutés doivent être caractérisés précisément afin de pouvoir en évaluer les conséquences potentielles du point de vue de la sécurité :

- Conséquences opérationnelles
- Moyens de détection
- Moyens en réduction des risques
- ...

Plus les événements redoutés seront caractérisés précisément, plus il sera facile au groupe d'utilisateurs chargé d'évaluer la gravité de s'accorder sur le niveau de gravité. Par exemple, au lieu de « perte de l'image radar normale », on préférera « perte de l'image radar normale dans toute la salle de contrôle, pendant plus de x minutes ».

Evaluation de « la gravité de ces incidences »

Le niveau de gravité, choisi en utilisant le mécanisme de classification préconisé dans l'appendice 1, doit être déterminé par « **l'incidence plausible la plus néfaste raisonnablement envisageable dans l'environnement opérationnel.** »

Le niveau de gravité tient compte des moyens d'atténuation de risques (redondances, méthodes de travail, moyens de détection...) éprouvés lorsqu'ils existent, et/ou résulte de la spécification de nouveaux moyens compensatoires (techniques, procéduraires, humains, dont il faudra justifier l'efficacité, qui donneront lieu éventuellement à des exigences en §2.3). Par exemple, vis-à-vis d'un événement redouté tel que « perte de l'image radar normale (ie issue du STR) sur une position de contrôle pendant plus de x minutes », le secours ultime radar et les strips peuvent être considérés comme des moyens en réduction de risque.

Il est important de préciser que des barrières « ultimes » comme le filet de sauvegarde et le TCAS ne sont pas utilisables dans les dossiers de sécurité pour réduire la gravité ou la fréquence d'occurrence estimée. La réduction de risque doit se faire en amont de tels dispositifs, censés éviter la collision.

Par ailleurs, il y a un certain nombre de critères à considérer pour évaluer la gravité, liste non limitative mais qu'il est intéressant de rappeler :

« Pour déduire l'incidence d'un danger sur les opérations et en déterminer la gravité, l'approche/la procédure systématique doit inclure (sans s'y limiter) les incidences des dangers sur les différents éléments constitutifs du système ATM, telles que :

- Incidence du danger sur l'équipage (charge de travail, aptitude à exercer ses fonctions etc.) ;
- Incidence du danger sur les contrôleurs de la circulation aérienne (charge de travail, aptitude à exercer ses fonctions etc.) ;
- Incidence du danger sur les capacités fonctionnelles des aéronefs ;
- Incidence du danger sur les capacités fonctionnelles de la composante sol du système ATM ;
- Incidence du danger sur l'aptitude à fournir des services de gestion de la circulation aérienne dans de bonnes conditions de sécurité (ampleur de la perte/dégradation des services/fonctions ATM). »

On pourra également rajouter dans ces critères le nombre d'avions potentiellement impactés par l'événement redouté considéré, toujours en raisonnant sur une situation de trafic chargée (ou autre condition d'environnement « raisonnablement pessimiste » pertinente pour l'étude).

« 3. la détermination des objectifs de sécurité proprement dits, exprimés comme la probabilité maximale d'occurrence d'un danger, et déterminés à partir de la gravité et de la probabilité maximale d'occurrence de ses incidences. »

Expression de la « probabilité maximale d'occurrence d'un danger »

Il s'agit de fixer, pour chaque événement redouté identifié au travers des analyses précédentes, le seuil d'acceptabilité opérationnel en terme de fréquence maximale d'occurrence de l'événement redouté.

Le terme « fréquence d'occurrence » s'entend au sens mathématique du terme (i.e un nombre), ou au sens qualitatif (i.e fréquence du type « improbable », « rare », « probable », etc) lorsqu'il n'est pas possible de fixer un objectif chiffré précis (néanmoins, il est souhaitable dans ce cas de viser des « ordres de grandeur » plutôt que de se fixer des objectifs purement qualitatifs difficiles à appréhender dans l'analyse).

Détermination « de la probabilité maximale d'un danger à partir de la gravité »

Pour déterminer l'objectif de sécurité acceptable, il est recommandé d'utiliser une grille de correspondance entre les classes de gravité et les seuils d'acceptabilité. Cela permet d'avoir une démarche d'acceptabilité du risque cohérente pour l'ensemble des événements redoutés du système considéré.

L'approche quantitative pour spécifier la probabilité d'occurrence acceptable relativement à la gravité estimée peut être utilisée une fois les notions de données chiffrées seront bien établies. Dans le cas présent la grille qualitative sera utilisée pour déterminer les objectifs de sécurité relative aux événements redoutés.

En conclusion, le risque s'exprime comme une combinaison de la probabilité d'occurrence et de la gravité. Le cadrage des objectifs de sécurité est donc un mécanisme itératif visant à diminuer soit la gravité, soit la probabilité d'occurrence des événements redoutés pour atteindre les zones de risque « acceptable ».

II.3 Exigences de sécurité (PSSA)

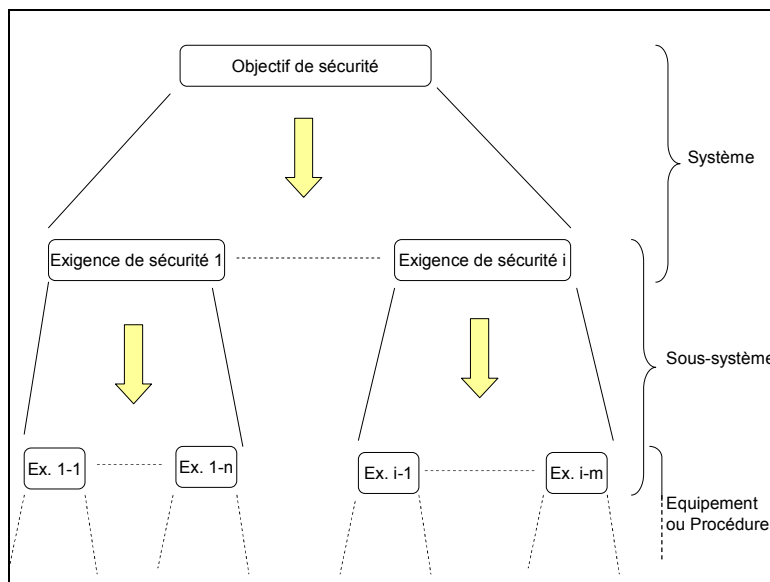
Texte du plan-type

Ce paragraphe explique comment, à partir des résultats obtenus aux II.1 et II.2, les objectifs de sécurité sont déclinés et traduits en exigences portant sur les différentes composantes de l'évolution envisagée.

Objectif du §

Définir la stratégie d'atténuation des risques, en particulier en dérivant sur les différents éléments du système les objectifs associés aux événements redoutés (par exemple au moyen d'arbres de défaillance).

On pourra également trouver tout type d'exigences dérivées : exigences en terme de formation des opérateurs, moyens de détection etc.



Arbre de défaillances

Commentaires

Cette section traduit l'impact sur les différents éléments du système de la mise en place des moyens techniques, procéduraux et/ou humains, qui permettent de « cadrer » et garantir la tenue des objectifs de sécurité au §2.2 (cadrage en particulier de la gravité et /ou de la fréquence d'occurrence des événements redoutés). Des **mesures ou exigences** pourront être par exemple au niveau opérationnel :

- Des recommandations dont il faut assurer la traçabilité dans la documentation utilisateurs ;
- L'élaboration de consignes ;
- L'application de procédures particulières ;
- De la formation sur tel ou tel point critique

Cette démarche peut être itérative, une exigence à un certain niveau pouvant ensuite être déclinée à un niveau plus détaillé lorsque la définition du système s'affine.

III- Evaluation de la sécurité (SSA)

Texte du plan-type:

Ce chapitre comprend l'ensemble des analyses de sécurité réalisées dans l'objectif de vérifier que l'évolution respecte les objectifs de sécurité qui lui ont été assignés pour la phase d'exploitation opérationnelle.

Dans le cadre de cette évaluation, les analyses peuvent conduire à identifier des points critiques (techniques, organisationnels, etc.) des recommandations ou encore des modifications de conception.

Objectif du §

Démontrer, par tous les moyens dont on dispose, que le système tel qu'on prévoit de le concevoir est capable de tenir les objectifs de sécurité qui lui ont été assignés.

Commentaires

Des objectifs ont été assignés au niveau du système objet du dossier, des événements redoutés déterminés (§II.2), des exigences dérivées peuvent avoir été spécifiées au niveau des éléments du système (§II.3). Il faut ensuite fournir, et c'est l'objet de ce §III :

« La démonstration que les objectifs de sécurité sont atteints, comprenant en particulier l'assurance de la mise en œuvre effective des mesures d'atténuation de risques présentées. Il est reconnu qu'un argumentaire reposant sur une combinaison d'éléments quantitatifs (modèle mathématique, analyses probabilistes) et qualitatifs (bon processus de travail, jugement professionnel, amélioration de la sécurité par rapport au système précédemment en service) peut être utilisé pour démontrer, avec un niveau suffisant de confiance, que certains des objectifs et exigences de sécurité sont atteints »

IV- Analyse des phases de transition (SSA)

Texte du plan-type

Ce chapitre contient l'analyse des phases de transition, à savoir :

- *l'installation dans un organisme de contrôle de la circulation aérienne d'un système avant toute mise en service opérationnelle ;*
- *toutes les opérations de retrait provisoire et de remise en service correspondantes ;*
- *le retrait d'exploitation dès lors qu'il est envisagé.*

Cette analyse doit démontrer que toutes les dispositions nécessaires sont prises afin de ne pas dégrader les niveaux de performance sécurité lors de chacune des phases de transition. Le cas échéant des procédures de repli sont mises en évidence.

Objectif du §

Fournir l'assurance que les phases de transitions ne dégradent pas les niveaux de sécurité de l'ATM.

Ce chapitre s'applique principalement aux équipements. Pour les procédures de Circulation Aérienne, la seule phase de transition à considérer serait celle de la mise en œuvre opérationnelle, et cette phase spécifique fait l'objet du §1.5 du dossier de sécurité.

Commentaires

Par « **phases de transition** », il faut entendre :

- Les phases qui vont du début de l'installation sur site et qui précèdent la mise en service opérationnel (celle-ci étant analysée spécifiquement au §1.5)
- Après mise en service, les phases qui vont du retrait de service provisoire (pour maintenance, réglage, modification ...) à la remise en service.
- Les phases de retrait du service opérationnel.

On démontrera essentiellement que le système et les interventions éventuelles dont il fait l'objet ne peuvent entraîner d'effets indésirables sur le fonctionnement opérationnel du système ATM pendant ces phases. Par exemple, lors du retrait de service d'un équipement opérationnel, on effectue généralement des travaux en salle technique (dépose de câbles, déplacement de baies techniques, ...) ou en salle de contrôle, pouvant générer des dangers spécifiques (dépose du mauvais câble, chute de baie sur des équipements en service, nuisance sonore en salle de contrôle, etc.). L'analyse visera ici à maîtriser ces risques par des procédures adaptées.

Ce chapitre sera complété au fil de la vie du système.

V- Principes d'assurance sécurité

Texte du plan-type

Ce chapitre présente les moyens mis en œuvre afin de maintenir dans le temps les niveaux de performance de sécurité atteints en termes de sécurité. Il présente la stratégie d'atténuation des risques appliquée en phase d'exploitation par le prestataire des services de navigation aérienne.

Objectif du §

Exposer l'ensemble des hypothèses, indicateurs, ou autres moyens identifiés au cours de l'étude comme devant être surveillés pendant la vie opérationnelle du système, afin de garantir son niveau de sécurité. Au cours d'une étude, il n'est pas rare de s'apercevoir que certaines hypothèses, ou certaines « données » utilisées pour évaluer les événements redoutés sont dimensionnantes pour la tenue des objectifs. Il faut donc imaginer des moyens permettant de garantir dans le temps la tenue des objectifs de sécurité.

Commentaires

L'assurance sécurité recouvre des mesures de surveillance et de maintien dans le temps des objectifs de sécurité. Parmi celles-ci, on peut mentionner à titre d'exemples :

- le contrôle de la mise en place et de l'efficacité des mesures identifiées de réduction de risques,
- le suivi de la mise en œuvre opérationnelle de l'évolution (mise en place d'un processus de retour d'expérience),
- le suivi des hypothèses faites pour l'élaboration du dossier de sécurité sur l'environnement opérationnel et les conditions d'exploitation du système (dérives dans l'application d'une procédure ou dans l'utilisation d'un équipement), notamment celles qui peuvent être considérées comme des exigences de sécurité,
- le contrôle de la mise en place et de l'efficacité d'indicateurs pouvant prévenir et détecter les éventuelles dégradations des performances sécurité ainsi que le non respect des exigences sécurité ;
- les audits internes au sein des entités locales et/ou des prestataires extérieurs,
- la maîtrise des processus de modifications du système ATM (existence de procédures spécifiques d'intervention, briefings lors d'évolutions de procédures, ...).

VI- Synthèse

Texte du plan type

Ce chapitre présente une synthèse de l'ensemble des résultats prouvant que les niveaux de sécurité évalués correspondent aux objectifs.

L'exposé de ces résultats doit permettre:

- *la formulation d'un argumentaire complet pour démontrer que le sous-ensemble considéré, de même que l'ensemble du système ATM offrent et continueront d'offrir un niveau de sécurité conforme aux exigences, cet argumentaire pouvant être étayé, le cas échéant, par la spécification des techniques de prévision, de suivi, et d'enquêtes utilisées*
- *la traçabilité des indicateurs de sécurité associés à la mise en œuvre d'un changement par rapport à l'exploitation et aux fonctions*

Objectif du §

Présenter de manière synthétique un résumé justifiant la tenue des objectifs de sécurité, accompagné des hypothèses, indicateurs ou recommandations à suivre pour garantir dans le temps la pérennité des résultats.

Appendice 1: Grille de Gravité

Degré de gravité ⁴	A	B	C	D	E
Incidence sur les opérations	Accidents	Incidents graves	Incidents majeurs	Incidents significatifs	Aucune incidence immédiate sur la sécurité
<p>Exemples d'incidences sur les opérations (évaluation a priori)</p>	<p>Un ou plusieurs accidents catastrophiques ;</p> <p>Une ou plusieurs collisions en vol ;</p> <p>Une ou plusieurs collisions au sol entre aéronefs ;</p> <p>Un ou plusieurs impacts sans perte de contrôle ;</p> <p>Perte totale de contrôle du vol ;</p> <p>Aucune source indépendante de mécanisme de rétablissement, telle la surveillance ou les procédures ATC et/ou de vol, n'est raisonnablement censée prévenir le ou les accidents.</p>	<p>- Diminution importante de la séparation (par ex. séparation < 50% des minima prescrits), sans que les équipages, ni l'ATC ne maîtrisent pleinement la situation ou soient à même de la redresser.</p> <p>- Un ou plusieurs aéronefs s'écartant de l'autorisation prévue de sorte qu'une manœuvre soudaine d'évitement d'un autre aéronef ou du relief est requise pour éviter un accident (ou lorsqu'une mesure d'évitement serait indiquée).</p>	<p>Diminution importante de la séparation (par ex < 50% minima prescrits), les équipages ou l'ATC maîtrisant la situation et étant à même de la redresser.</p> <p>Diminution réduite de la séparation, sans que les équipages, ni l'ATC ne maîtrisent pleinement la situation, compromettant ainsi toute perspective de rétablissement (sans recourir à des manœuvres d'évitement des autres aéronefs ou du relief)</p>	<p>Accroissement de la charge de travail des contrôleurs ou des équipages de conduite ou légère dégradation de la capacité fonctionnelle du système ATC.</p> <p>Diminution réduite de la séparation, les équipages ou l'ATC maîtrisant la situation et étant à même de la redresser.</p>	<p>Situation génératrice de danger : aucune incidence directe ou indirecte sur la sécurité.</p>

⁴ Le degré de gravité est déterminé par l'incidence plausible la plus néfaste dans l'environnement opérationnel.

Appendice 2 : Grille de probabilité

Le principe est qu'une grille gravité-fréquence permet d'établir un lien systématique entre la gravité associée à un événement redouté et sa fréquence d'occurrence acceptable.

Afin de vérifier que les objectifs de sécurité sont tenus, il convient d'évaluer, pour chaque événement redouté identifié, un ordre de grandeur de sa fréquence d'occurrence, c'est-à-dire le nombre de fois où il pourrait être observé par les opérationnels. Compte tenu de la nature des événements redoutés étudiés ici, on évalue des fréquences d'occurrence par des ordres de grandeur jugés significatifs d'un point de vue opérationnel.

L'information obtenue à partir de la gravité n'est pas une probabilité précise, mais un ordre de grandeur du type :

1. *Extrêmement rare* : peut se produire une fois tous les 1000 ans
2. *Rare* : peut se produire 1 fois tous les 5 à 10 ans
3. *Occasionnel* : 1 à 2 fois par an
4. *Fréquent* : plusieurs fois par an
5. *Très fréquent* : plusieurs fois par mois

Fréquence de l'occurrence	Très fréquent	Fréquent	Occasionnel	Rare	Extrêmement rare
	Plusieurs fois par mois	Plusieurs fois par an	1 à 2 fois par an	1 fois tous les 5 à 10 ans	1 fois tous les 1000 ans

Appendice 3 grille d'acceptabilité

Probabilité	5 Très fréquent Plusieurs fois par mois dans l'organisme de contrôle	4 Fréquent Plusieurs fois par an dans l'organisme	3 Occasionnel Une à deux fois par an dans l'organisme	2 Rare Une fois tous les 5 à 10 ans dans l'organisme	1 Extrêmement rare Une fois tous les 1000 ans dans l'organisme, soit en termes plus concrets, jamais à la connaissance de l'organisme
A Accident	A5	A4	A3	A2	A1
B Incidents graves	B5	B4	B3	B2	B1
C Incidents majeurs	C5	C4	C3	C2	C1
D Incidents significatifs	D5	D4	D3	D2	D1
E Aucune incidence immédiate sur la sécurité	E5	E4	E3	E2	E1

Appendice 4 : canevas d'identification et évaluation d'un événement redouté

Evènement Redouté (ER1)				
ER1:	Définition de l'ER :			
Estimation de la sévérité sans atténuation				
<input type="checkbox"/> Aucune incidence	<input type="checkbox"/> Incid Significatif	<input type="checkbox"/> Incid Majeur	<input type="checkbox"/> Incid Grave	<input type="checkbox"/> Accidents
Estimation de la fréquence d'occurrence sans atténuation				
<input type="checkbox"/> Ext Rare	<input type="checkbox"/> Rare	<input type="checkbox"/> Occasionnel	<input type="checkbox"/> Fréquent	<input type="checkbox"/> Très Fréquent
Sévérité sur la base d'atténuation				
<input type="checkbox"/> Aucune incidence	<input type="checkbox"/> Incid Significatif	<input type="checkbox"/> Incid Majeur	<input type="checkbox"/> Incid Grave	<input type="checkbox"/> Accidents
Fréquence d'occurrence sur la base d'atténuation				
<input type="checkbox"/> Ext. Rare	<input type="checkbox"/> Rare	<input type="checkbox"/> Occasionnel	<input type="checkbox"/> Fréquent	<input type="checkbox"/> Très Fréquent
Description détaillées de l'ER				
.....				
Causes du danger		Conséquences du danger		
.....		
Actions internes pour atténuer le risque		Actions externes pour atténuer le risque		
.....		
Justifications/explications (efficacité des barrières de sécurité et de l'acceptabilité du risque)				
.....				