Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DES ARMÉES

DSAÉ
DIRCAM DIRNAV BFEA

GUIDE MÉTHODOLOGIQUE

DÉMONSTRATIONS DE SÉCURITÉ POUR LES SERVICES DE LA NAVIGATION AÉRIENNE

A Villacoublay, le 19 SEP. 2024

Le général de brigade aérienne Lionel BAVEREY
directeur de la circulation aérienne militaire

Page intentionnellement blanche

APPROBATION DU DOCUMENT

	Nom et qualité	Date et signature
Rédacteurs	LCL VISCONTI Chef de la division sécurité des systèmes LCL DUTILLOY Division sécurité des systèmes CDT DHERS Division sécurité des systèmes	
Vérificateur	CV GUENIN Bureau règlementation-affaires juridiques	
Vérificateur	COL DORANGE Sous-directeur surveillance et audit	
Approbateur	GBA BAVEREY Directeur de la circulation aérienne militaire	

DIFFUSION

Dans un souci d'économie, de préservation de l'environnement et de réactivité, le présent guide n'est distribué que sous forme électronique. Il est disponible sur INTRADEF à l'adresse :

« https://portail-dircam.intradef.gouv.fr/index.php/fr/lien-utile/instructions-dircam#4150 »

SUIVI DES VERSIONS

Numéro version	Date	Objet du changement	Pages affectées par la modification
1.0		Création du guide.	

SOMMAIRE

PRÉAMBULE

Le règlement (CE) n°549/2004 est le texte fondateur pour le ciel unique européen. Il précise en particulier que les états membres désignent ou établissent un ou plusieurs organismes faisant fonction d'autorité nationale de surveillance (ANS) chargée d'assurer les tâches qui lui sont assignées.

A ce titre et par le décret 2005-471 du 16 mai 2005, l'autorité compétente française est le directeur de la sécurité de l'aviation civile (DSAC). Conformément aux dispositions de l'article D 131-10 du code de l'aviation civile et de l'arrêté du 23 février 2016 relatif aux fonctions de surveillance exercées par le directeur de la sécurité aéronautique d'État pour le compte de la direction de la sécurité de l'aviation civile, le directeur de la circulation aérienne militaire (DirCAM) exerce les fonctions de surveillance pour le compte de la DSAC pour les services rendus par les prestataires de services de navigation aérienne de la Défense (PSNA/D) au profit de la CAG.

A ce titre, et conformément au protocole DSAC/DSAÉ [PRO MIXTE], le DirCAM assure également la supervision des changements apportés aux systèmes fonctionnels par les prestataires de services de navigation aérienne de la défense (PSNA/D). Cette supervision est régie par l'instruction n°4150/DSAÉ/DIRCAM.

Venant en complément de cette instruction, le présent guide présente les outils permettant de réaliser les démonstrations de sécurité afférentes aux changements.

Elle est organisée autour des thèmes suivants :

- les principes généraux des démonstrations de sécurité ;
- les outils pour réaliser les démonstrations de sécurité, thème divisé en cinq parties afin de mettre en évidence les étapes du processus ;
- le cas particulier des changements apportés à l'organisation de l'espace aérien ;
- les types d'études possibles ;
- les modèles de formulaires.

Les outils décrits dans le « guide méthodologique – démonstration de sécurité pour les services de navigation aérienne » permettent de réaliser indifféremment les démonstrations de sécurité pour des services rendus au profit de la circulation aérienne générale (CAG) et ceux rendus au profit de la circulation aérienne militaire (CAM).

Une démonstration de sécurité pour des services rendus à la CAM n'est pas couverte par un référentiel réglementaire. Si un PSNA/D décide d'en réaliser une, il peut porter des adaptations mesurées aux prescriptions du présent guide. Le cas échéant, il devra solliciter l'approbation du DirCAM qui demeure l'autorité de surveillance de la CAM pour le compte du ministre des Armées.

TEXTES DE RÉFÉRENCE

[RE1139] Règlement (UE) 2018/1139 du 4 juillet 2018 concernant des règles communes dans le domaine de l'aviation civile et instituant une agence de l'Union européenne pour la sécurité aérienne, et abrogeant les règlements (CE) n°552/2004 et (CE) n°216/2008 ;

[RE549] Règlement européen (CE) n°549/2004 modifié du 10 mars 2004, fixant le cadre pour la réalisation du ciel unique européen (« règlement cadre ») ;

[RE550] Règlement européen (CE) n°550/2004 modifié du 10 mars 2004, relatif à la fourniture de services de navigation aérienne dans le ciel unique européen (« règlement sur la fourniture de services ») ;

[RE373] Règlement d'exécution (UE) 2017/373 du 1er mars 2017 établissant des exigences communes relatives aux prestataires de services de gestion du trafic aérien et de services de navigation aérienne ainsi que des autres fonctions de réseau de la gestion du trafic aérien, et à leur supervision, abrogeant le règlement (CE) n°482/2008, les règlements d'exécution (UE) n°1034/2011, (UE) n°1035/2011 ;

[RE1768] Règlement délégué (UE) 2023/1768 de la commission du 14 juillet 2023 établissant des règles détaillées relatives à la certification et à la déclaration des systèmes de gestion du trafic aérien et de services de navigation aérienne ainsi que des composants de gestion du trafic aérien et de services de navigation aérienne ;

[RE1769] Règlement d'exécution (UE) 2023/1769 de la commission du 12 septembre 2023 fixant les exigences techniques et les procédures administratives applicables à l'agrément des organismes participant à la conception ou à la production des systèmes et composants de gestion du trafic aérien et de services de navigation aérienne et modifiant le règlement d'exécution (UE) 2023/203 ;

[RE1770] Règlement d'exécution (UE) 2023/1770 de la commission du 12 septembre 2023 établissant des dispositions relatives aux équipements d'aéronef nécessaires pour l'utilisation de l'espace aérien du ciel unique européen, ainsi que des règles d'exploitation relatives à l'utilisation de l'espace aérien du ciel unique européen et abrogeant le règlement (CE) no 29/2009 et les règlements d'exécution (UE) no 1206/2011, (UE) no 1207/2011 et (UE) no 1079/2012 ;

[RE1771] Règlement d'exécution (UE) 2023/1771 de la commission du 12 septembre 2023 modifiant le règlement d'exécution (UE) 2017/373 en ce qui concerne les systèmes et composants relatifs à la gestion du trafic aérien et aux services de navigation aérienne, et abrogeant les règlements (CE) no 1032/2006, (CE) no 633/2007 et (CE) no 262/2009 ;

[RE1772] Règlement d'exécution (UE) 2023/1772 de la commission du 12 septembre 2023 modifiant le règlement d'exécution (UE) no 923/2012 en ce qui concerne les règles d'exploitation relatives à l'utilisation des systèmes et composants de gestion du trafic aérien et de services de navigation aérienne dans l'espace aérien du ciel unique européen et abrogeant le règlement (CE) no 1033/2006 ;

[S4720] STANAG 4720 ;

[I4050] Instruction n°4050/DSAÉ/DIRCAM relative à la surveillance par l'autorité nationale de surveillance Défense des prestataires de services de navigation aérienne de la Défense ;

[I4150] Instruction n°4150/DSAÉ/DIRCAM relative au processus de supervision des changements apporté par les prestataires de services de navigation aérienne de la Défense.

[ED109] *Software integrity assurance considerations for communication, navigation, surveillance and air traffic management systems ;*

[ED153] *Guidelines for ANS software safety assurance ;*

[PRO MIXTE] Protocole mixte DSAC/ANA et DSAÉ/DIRCAM/SDSA relatif à la surveillance des prestataires de services de navigation aérienne de la Défense ;

[A230216] Arrêté du 23 février 2016 relatif aux fonctions de surveillance exercées par le directeur de la sécurité aéronautique d'État pour le compte de la direction de la sécurité de l'aviation civile.

DÉFINITIONS

Terme	Source	Définition
« Analyse fonctionnelle »		Étude consistant à définir et identifier les fonctions d'un système et leurs interactions, indépendamment de sa conception.
« Assurance sécurité »		Toutes actions planifiées et systématiques nécessaires pour donner l'assurance requise qu'un produit, un service, une organisation ou un système fonctionnel atteint un seuil de sécurité acceptable ou tolérable.
« Changement »		Introduction d'un nouveau (sous-)système, modification ou retrait de service d'un (sous-)système existant. Le changement peut être à l'initiative du prestataire ou d'un autre prestataire.
« Consigne de sécurité »	[RE373]	Un document délivré ou adopté par une autorité compétente qui impose des actions à effectuer sur un système fonctionnel ou qui fixe des restrictions à son utilisation opérationnelle pour rétablir la sécurité, lorsqu'il est constaté qu'autrement, la sécurité aérienne peut être compromise.
« Danger »	[RE373]	Toute situation, événement ou circonstance qui pourrait mener à un effet dommageable.
« Démonstration de sécurité »		Méthodologie formelle et documentée, assortie de preuves, démontrant que le système, après changement, n'engendrera pas un risque inacceptable s'il s'agit d'un changement ATS[1] ou se comportera uniquement comme spécifié s'il s'agit d'un changement non-ATS.
« Environnement opérationnel »		L'environnement opérationnel rassemble les caractéristiques physiques et institutionnelles de l'espace aérien dans lequel se déroulent les vols. Il englobe les services ATM[1] fournis, les technologies utilisées à cette fin, l'organisation de l'espace aérien, les conditions ambiantes et les acteurs humains.
« Étude de sécurité »		Terme équivalent à « démonstration de sécurité » dans le cas des changement ATS.
« Étude sur le soutien à la sécurité »		Terme équivalent à « démonstration de sécurité » dans le cas des changements non-ATS.
« Évènement redouté »		Danger affectant la fourniture des services ATM, exprimé au plus près des opérateurs de première ligne. C'est une situation indésirable au regard des services attendus.

[1] Voir glossaire.

Terme	Source	Définition
« Exigence de sécurité »		Une mesure concrète découlant de la stratégie d'atténuation des risques qui permet d'atteindre un objectif de sécurité (changement ATS) ou une spécification du système (changement non-ATS), y compris les exigences organisationnelles, opérationnelles, procédurales, fonctionnelles, de performance, les exigences d'interopérabilité ou les caractéristiques environnementales.
« Gravité »		Caractérise l'incidence des effets d'un danger sur la sécurité des vols, y compris la capacité à redresser la situation. La gravité est traduite par un niveau chiffré de 1 (accident) à 5 (pas de conséquence immédiate sur la sécurité).
« Gravité initiale »		Gravité ne tenant pas compte de moyens en réduction du risque de protection.
« Gravité corrigée »		Gravité tenant compte de moyens en réduction du risque de protection.
« Hypothèse »		Proposition d'une démonstration de sécurité, établie généralement en début d'étude, imposant des conditions spécifiques sur un système ou un environnement et devant être vérifiée au cours de l'étude.
« Logiciels »		Les programmes informatiques et les données de configuration correspondantes, y compris les logiciels prédéveloppés, à l'exclusion des éléments électroniques tels que les circuits intégrés spécifiques d'une application, les réseaux de portes programmables ou les dispositifs de contrôle de logique sur support physique.
« Mise en œuvre d'un changement »		La notion de mise en œuvre ne concerne que les changements pour lesquels les conditions de travail des contrôleurs aériens seront perturbées par les opérations de déploiement du système nouveau. La mise en œuvre du changement correspond au début de la réalisation (exemple : début des travaux). Cette échéance est notifiée au DirCAM par le PSNA/D responsable de ces opérations.
« Mise en service d'un changement »		Première mise en exploitation. Cette échéance doit faire l'objet d'une notification au DirCAM par le PSCA[2]/D utilisant le système.

[2] Voir glossaire.

Terme	Source	Définition
« Moyen en réduction du risque »		Un moyen en réduction du risque peut jouer sur l'occurrence (prévention) ou sur les effets (protection) d'un événement redouté. Un moyen en réduction du risque, pour être pertinent, est caractérisé par : - la capacité à détecter la défaillance (pour les moyens en réduction du risque de protection) ; - sa disponibilité en toutes circonstances ; - une mise en œuvre dans un délai compatible avec la problématique de sécurité ; - son efficacité ; - son indépendance vis-à-vis de la fonction défaillante.
« Objectif de sécurité »		Un énoncé qualitatif ou quantitatif qui définit la fréquence ou la probabilité maximale d'apparition escomptée d'un évènement redouté. L'objectif de sécurité correspond au « critère de sécurité applicable au changement ».
« Organisme »		Soit un prestataire de services de navigation aérienne, soit une entité assurant l'ATFM[3] ou l'ASM ou d'autres fonctions de réseau.
« Partie prenante »		Entité impliquée dans la gestion d'un changement. Il peut s'agir d'un usager des services, d'un prestataire extérieur ou d'un autre prestataire de services. Pour qu'un prestataire de services soit qualifié de « partie prenante », son implication doit être minime et ne doit pas se traduire par la mise en œuvre de moyens en réduction du risque ou d'exigences de sécurité.
« Phases de transition »		Elles correspondent généralement à des périodes se déroulant entre de la mise en œuvre d'un changement et sa mise en service.
« Prestataire de services de navigation aérienne »	[RE550]	Tout prestataire de services de navigation aérienne fournissant les services de la gestion du trafic aérien aux aéronefs évoluant selon les règles de la circulation aérienne générale (CAG).
« Risque »	[RE373]	La combinaison de la probabilité la plus élevée ou de la fréquence d'un événement aux conséquences dommageables provoqué par un danger et de la gravité de ces conséquences.
« Système fonctionnel »	[RE373]	Une combinaison de procédures, de ressources humaines et d'équipements, y compris le matériel informatique et les logiciels, organisée afin de remplir une fonction dans le cadre de l'ATM/ANS et d'autres fonctions de réseau ATM.

[3] Air Traffic Flow Management.

GLOSSAIRE

AC	Autorité Compétente
ADD	Arbre De Défaillance
ALAVIA	Commandement de la Force de l'Aéronautique Navale
AMDE	Analyse des Modes de Défaillance et de leurs Effets
ANS	*Air Navigation Services*
APR	Analyse Préliminaire de Risques
ASM	*AirSpace Management*
ASU	Analyse de Sécurité Usagers
ATC	*Air Traffic Control*
ATFM	*Air Traffic Flow Management*
ATM	*Air Traffic Management*
ATM/ANS	*Air Traffic Management/Air Navigation Services*
ATS	*Air Traffic Services*
BEP	Bureau Exécutif Permanent
BMR	Bureau Maîtrise des Risques
CLA	Contrôle Local d'Aérodrome
CNS	Communication, Navigation, Surveillance
CUE	Ciel Unique Européen
COMALAT	Commandement de l'Aviation Légère de l'Armée de Terre
CONOPS	Concept Opérationnel
COTS	*Commercial Off The Shelf*
CRG	Comité Régional de Gestion
DAE	Déclaration d'Aptitude à l'Emploi
DC	Déclaration de Conformité
DGAC	Direction Générale de l'Aviation Civile
DGA	Direction Générale de l'Armement
DGA TA	Direction Générale de l'Armement – Techniques Aéronautiques
DGA EV	Direction Générale de l'Armement – Essais en Vol
DIRCAM	Direction de la Circulation Aérienne Militaire
DirCAM	Directeur de la Circulation Aérienne Militaire
DIRISI	Direction Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information de la Défense
DSAC	Direction de la Sécurité de l'Aviation Civile
DSNA	Direction des Services de la Navigation Aérienne
DSSL	Démonstration de Sécurité Simplifiée Locale
DSS	Division Sécurité des Systèmes de la SDSA
EASA	*European Aviation Safety Agency*
EMA	Etat-Major des Armées

EMAAE	Etat-Major de l'Armée de l'Air et de l'Espace
EMx	Etat-Major d'armée
ENAC	École Nationale de l'Aviation Civile
EPIS	Étude Prestataire d'Impact sur la Sécurité (Défense)
ER	Évènement Redouté
ESARR	*Eurocontrol Safety Regulatory Requirement*
FHA	*Functional Hazard Assessment*
GPCSC	Groupe Permanent de Coordination pour les Systèmes de Communication
GTA	Gestion du Trafic Aérien
IANS	*Institute of Air Navigation Services*
IOP	Interopérabilité
MEO	Mise En Œuvre
MES	Mise En Service
MISO	Méthodologie d'Intervention sur les Systèmes Opérationnels
MRR	Moyen en Réduction du Risque
NeMO	Nouvelle Messagerie Officielle
PLRE	Point Limite de Réception de l'Étude
PSSA	*Preliminary System Safety Assessment*
PSNA	Prestataire de Services de Navigation Aérienne
PSNA/D	Prestataire de Services de Navigation Aérienne de la Défense
PSCA	Prestataire de Services de Circulation Aérienne
PSCA/D	Prestataire de Services de Circulation Aérienne de la Défense
PSCNS	Prestataire de Services de Communication, Navigation, Surveillance
PSCNS/D	Prestataire de Services de Communication, Navigation, Surveillance de la Défense
SAM	*Safety Assessment Methodology*
SASL	Système d'Assurance de la Sécurité des Logiciels
SES	*Single European Sky*
SSA	*System Safety Assessment*
SDF	Sureté De Fonctionnement
SDRCAM	Sous-Direction Régionale de la Circulation Aérienne Militaire
SDSA	Sous-Direction Surveillance et Audit de la DIRCAM
SMS	*Safety Management System* / Système de Gestion de la Sécurité
SWAL	*SoftWare Assurance Level* / Niveau d'assurance logicielle
WCC	*Worst Credible Case* / Cas le plus raisonnablement pessimiste

TITRE I

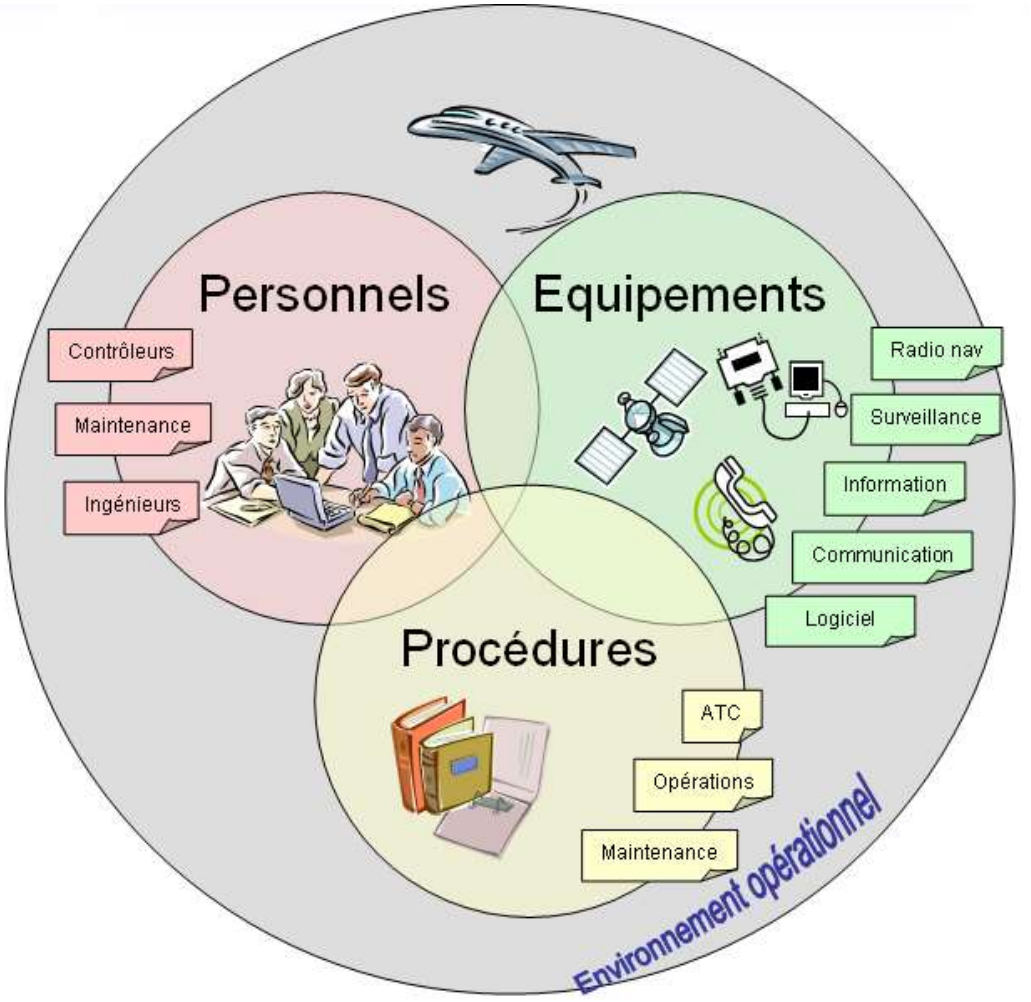
PRINCIPES GÉNÉRAUX D'UNE DÉMONSTRATION DE SÉCURITÉ

I.1. NOTION DE SYSTÈME FONCTIONNEL

Le système fonctionnel (ou système ATM/ANS) est constitué de trois composantes :

- les équipements (matériels et logiciels) ;
- le personnel (effectif, formation, organisation) ;
- les procédures.

Ce système doit être considéré dans le contexte de son environnement opérationnel, y compris les interfaces avec les systèmes adjacents et les prestations de support.



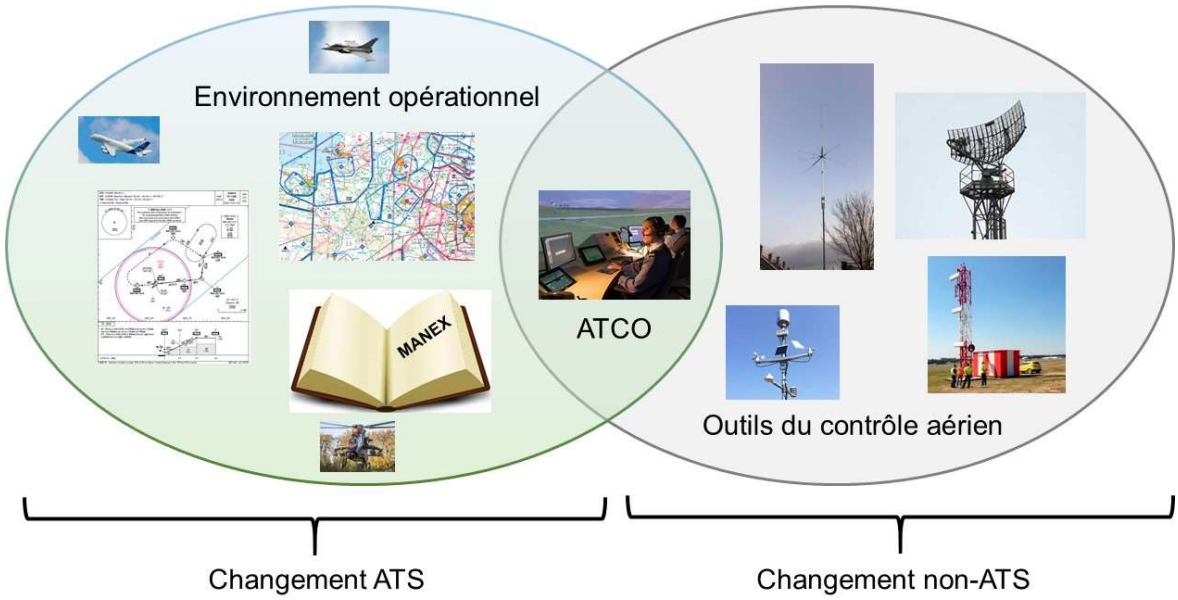
I.2. OBJECTIF D'UNE DÉMONSTRATION DE SÉCURITÉ

La démonstration de sécurité a pour objectif de fournir l'assurance, avant tout au prestataire mais également à l'autorité compétente, qu'un changement envisagé ne remet pas en cause la sécurité des services de la circulation aérienne et ce, de manière continue. A ce titre, elle doit prendre en compte le système modifié, ses modes de fonctionnement dégradés, ainsi que toutes les étapes intermédiaires, notamment les phases de transition, nécessaires à l'introduction du changement. Au-delà, elle doit couvrir la vie opérationnelle du système et, dans la mesure du possible, son retrait du service.

La démonstration de sécurité doit prendre en compte l'impact du changement sur l'ensemble du système fonctionnel (personnel, procédures, équipements), dans le contexte de son environnement opérationnel.

Selon le règlement [RE373], la démonstration de sécurité peut être :

- une étude de sécurité, lorsque le changement consiste à faire évoluer la manière de rendre les services du contrôle aérien. On parle dans ce cas de changement ATS ;
- une étude sur le soutien à la sécurité, lorsque le changement intervient sur un équipement utilisé par le contrôleur aérien pour rendre les services. On parle dans ce cas de changement non-ATS.



Au travers de la démonstration de sécurité, le prestataire de services *« offre l'assurance, avec une confiance suffisante, au moyen d'un* ***argumentaire complet, documenté et valide*** *»* que :

- pour les changements ATS :
  - *« les critères de sécurité identifiés sont valides et qu'ils seront et resteront respectés »* ;
  - *« le système fonctionnel, après le changement, sera aussi sûr qu'il l'était avant le changement, ou alors […] que toute réduction temporaire de la sécurité sera contrebalancée par une future amélioration de la sécurité ou que toute réduction permanente de la sécurité présente d'autres conséquences bénéfiques »* ;
- pour les changements non-ATS, *« le système se comportera et continuera de se comporter uniquement comme précisé dans le contexte spécifié »*.

I.3. CHOIX DE LA MÉTHODE

Lors de son entrée en vigueur, la réglementation du ciel unique européen imposait la méthode SAM[4] comme outil pour réaliser les démonstrations de sécurité. Contrairement au corpus réglementaire antérieur, le règlement [RE373] ne contient aucune prescription en matière d'outil pour la réalisation des démonstrations de sécurité.

Les PSNA/D pratiquent la méthode SAM depuis près de vingt ans et en maîtrisent bien les principes. Lors des travaux entre les PSNA/D et la DIRCAM relatif à l'application du règlement [RE373], il a été convenu de maintenir la méthode SAM pour réaliser les démonstrations de sécurité associées aux changements ATS. Cette méthode, telle qu'appliquée dans les Armées, est décrite au titre III du présent guide.

En ce qui concerne les changements non-ATS, les prescriptions du règlement [RE373] vise à la réalisation d'études sur la sûreté de fonctionnement sur les systèmes. En conséquence, les

[4] *Safety Assessment Methodology* : Méthodologie d'évaluation de la sécurité d'un système de navigation aérienne.

outils pour réaliser les démonstrations de sécurité associées aux changements non-ATS sont choisis parmi ceux utilisés dans l'ingénierie de la maîtrise des risques. Ils font l'objet du titre IV du présent guide.

I.4. CORRÉLATION ÉTUDE DE SÉCURITÉ / ÉTUDE SUR LE SOUTIEN À LA SÉCURITÉ

Conformément à l'exigence ATS.OR.205 du règlement [RE373] « *un prestataire de services de la circulation aérienne veille à ce que l'évaluation du soutien à la sécurité comprenne […] l'évaluation des risques et, si nécessaire, l'atténuation des risques pour la modification afin qu'elle puisse respecter les critères de sécurité applicables* ».

Ainsi, toute étude sur le soutien à la sécurité sera accompagnée d'un volet ATS permettant de garantir que le changement non-ATS n'engendre pas un risque inacceptable. Ce point est abordé aux titres IV et V du présent guide.

TITRE II

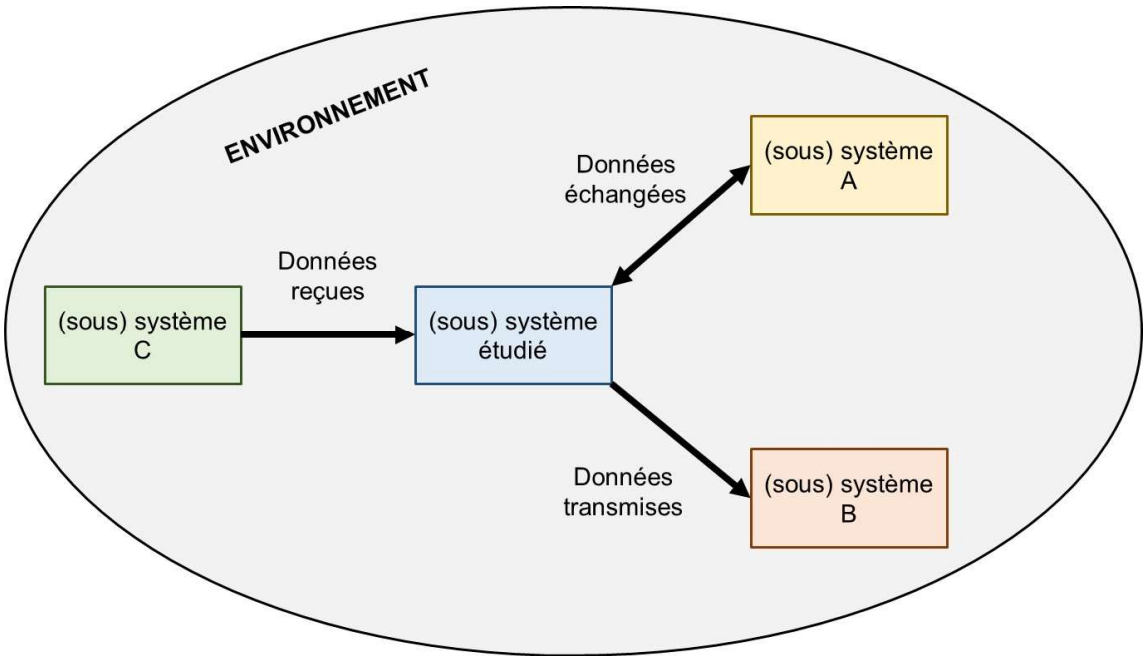
DÉFINITION DU CHANGEMENT

Que ce soit dans le cas d'un changement ATS ou celui d'un changement non-ATS la première et indispensable étape d'une démonstration de sécurité est la définition du changement.

Une définition du changement insuffisante ou imprécise mènera quasi-systématiquement à une démonstration de sécurité incomplète et/ou faussée voire non-conforme.

II.1. DESCRIPTION DU SYSTÈME

Tout système peut être schématisé par les échanges de données avec son environnement.



Pour mener une démonstration de sécurité cohérente, il est indispensable de bien connaitre le système sur lequel le changement intervient. La description du système doit comprendre :

- la description du système en lui-même ;
- le système dans son environnement : interfaces et interactions ;
- les limites de l'étude.

II.2. ANALYSE FONCTIONNELLE

L'analyse fonctionnelle permet de décrire les fonctions du système affectées par le changement. Si cela s'avère nécessaire pour la cohérence de l'étude, l'analyse fonctionnelle doit être étendue aux fonctions en relation avec les interfaces et/ou interactions qui, toutefois, ne sont pas affectées directement pas le changement[5].

Une fonction se formule par un verbe à l'infinitif suivi d'un ou plusieurs complément(s).

L'analyse fonctionnelle doit impérativement être indépendante de la (des) solution(s) technique(s) et/ou procédurale(s) et/ou humaine(s)envisagée(s) pour le système futur.

C'est à partir des (sous-)fonctions qu'il est possible de déterminer les évènements redoutés (cf. chapitre III.3) ou les défaillances (cf. chapitre IV.2).

[5] Par exemple, le changement étant une modification technologique (traitement d'obsolescence) sur la liaison entre deux équipements d'ancienne génération, lors de la démonstration de sécurité, il pourrait apparaitre nécessaire de confirmer le bon fonctionnement de l'ensemble voire de modifier le protocole de communication en entrée/sortie des équipements d'extrémité afin de le faire cohabiter avec la nouvelle technologie.

L'analyse fonctionnelle est obligatoire pour une étude sur le soutien à la sécurité (changement non-ATS).

Exemples de fonctions pour un changement ATS

- Transférer un aéronef à un secteur / centre.
- Coordonner entre l'approche et la vigie / avec un centre adjacent.
- Assurer la traversée de la zone.

Exemples de fonctions pour un changement non-ATS

- Communiquer avec le pilote.
- Recueillir les données de détection.
- Traiter les informations de surveillance.
- Afficher les données de météorologie.

II.3. PÉRIMÈTRE DU CHANGEMENT

La définition du périmètre du changement consiste à identifier quelle(s) partie(s) du système (équipement, procédure, humain, environnement opérationnel) sera(ont) affectée(s) par le changement.

Si « équipement » figure dans le périmètre, alors le changement est de type non-ATS et donnera lieu à une étude sur le soutien à la sécurité.

Il est indispensable de bien définir le périmètre du changement pour garantir l'exhaustivité de l'étude tout en la limitant au strict nécessaire.

II.4. HYPOTHÈSES EN PHASE DE DÉFINITION DU CHANGEMENT

Lors de la phase de définition du changement, il peut s'avérer nécessaire de formuler des hypothèses afin de faciliter l'étude. Ces hypothèses sont à mentionner dans la démonstration de sécurité et, le cas échéant, doivent être traduites en exigences de sécurité (cf. titre VI).

Page intentionnellement blanche

TITRE III

DÉMONSTRATION DE SÉCURITÉ D'UN CHANGEMENT ATS

Safety Assessment Methodology

La méthode SAM décrite au présent titre est une adaptation des prescriptions des règlements antérieurs au [RE373], elles-mêmes adaptées des travaux d'EUROCONTROL et du STANAG[6] 4720 ([S4720]), celui-ci permettant la prise en compte des spécificités des missions des armées.

Seule la méthode décrite au présent titre permet de justifier de la conformité méthodologique de l'étude de sécurité.

III.1. MÉTHODE SAM - GÉNÉRALITÉS

La méthode SAM se décompose en trois phases principales :

- *Functional Hazard Assessment* (FHA) ;
- *Preliminary System Safety Assessment* (PSSA) ;
- *System Safety Assessment* (SSA).

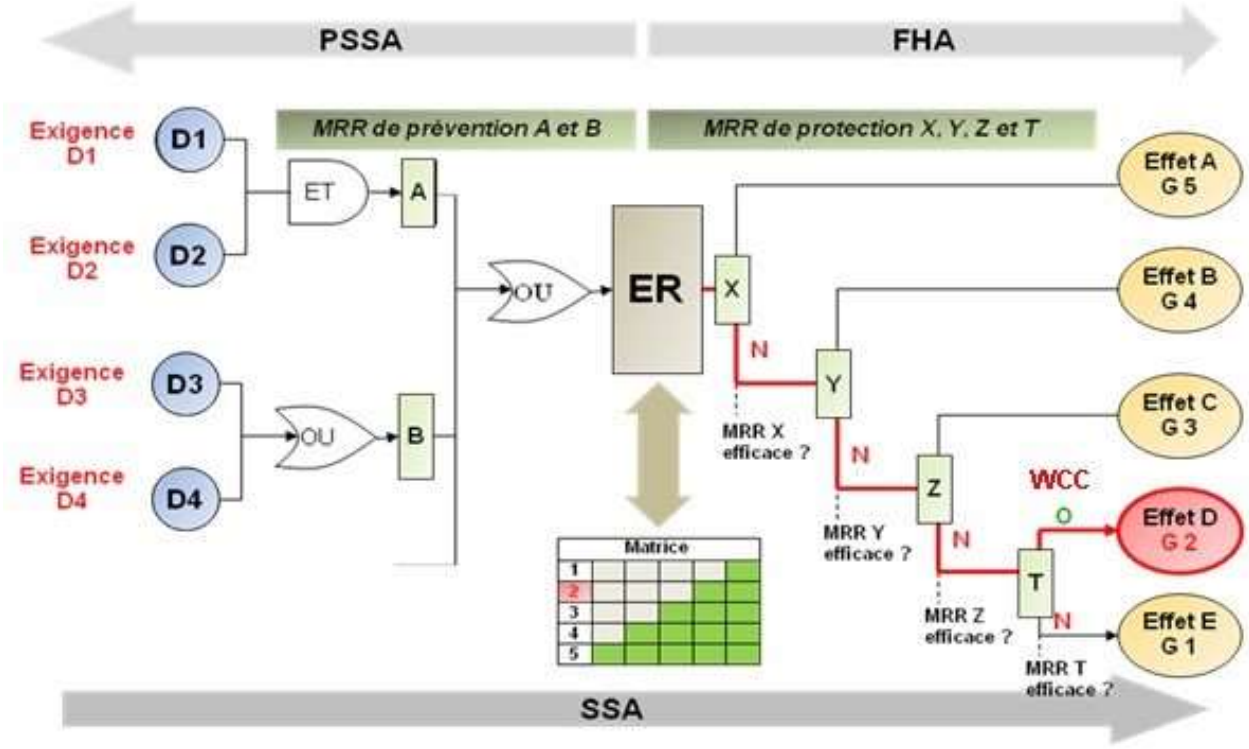


Schéma de principe de la méthode SAM

III.2. MATRICES D'ACCEPTABILITÉ DU RISQUE

Les matrices d'acceptabilité du risque utilisées par les PSCA/D ont été élaborées sur la base des normes OTAN définies dans le [S4720]. Elles permettent d'évaluer et d'atténuer le risque quel que soit le type de circulation aérienne (CAG ou CAM). Dans le cadre des missions régaliennes de l'état, en particulier pour les missions en CAM, elles offrent la possibilité de tolérer le risque « sous condition », situation dans laquelle il sera admis un risque supérieur à la norme mais uniquement pour l'aviation d'État. Un risque toléré « sous condition » suppose l'engagement de responsabilité de l'autorité adéquate.

6 STANdard AGriment.

III.2.1. Gravité

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 entraîner 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.

Gravité 2 *signifie que ni le contrôleur, ni le pilote ne maîtrisent la situation.*
Gravité 3 *signifie que le contrôleur et/ou le pilote maîtrise(nt) encore la situation.*
Gravité 4 *se traduit par une augmentation de la charge de travail du contrôleur et/ou du pilote.*
Gravité 5 *signifie que, même si le contrôleur et le pilote ont connaissance de la situation, ils jugent qu'elle n'engendre aucun risque à court terme.*

III.2.2. Probabilité d'occurrence

III.2.2.1. Occurrence quantitative

La probabilité d'occurrence quantitative est utilisée pour les systèmes pour lesquels il est possible de calculer un taux de disponibilité/défaillance. Il s'agit essentiellement de systèmes techniques. Les normes utilisées sont celles de l'industrie qui considère qu'une année compte 10 mois et 10 000 heures (8760 en réalité). Dans ces conditions :

- 10^{-3} signifie une fois par mois ;
- 10^{-4} signifie une fois par an ;
- 10^{-5} signifie une fois tous les 10 ans ;
- 10^{-6} signifie une fois par siècle ;
- etc.

III.2.2.2. Occurrence qualitative

Lorsqu'il n'est pas possible de calculer le taux de défaillance d'un système, le recours à une analyse qualitative permet de statuer sur l'acceptabilité du risque. Ainsi, les probabilités d'occurrence qualitatives suivantes sont définies :

- très fréquente : peut se produire plusieurs fois par mois dans l'organisme ;
- fréquente : peut se produire plusieurs fois par an dans l'organisme ;
- occasionnelle : peut se produire une à deux fois par an dans l'organisme ;
- rare : peut se produire une fois tous les 5 à 10 ans dans l'organisme ;
- extrêmement rare : ne s'est jamais produit à la connaissance de l'organisme.

III.2.3. Matrice d'acceptabilité du risque

III.2.3.1. Tableau des conditions

Catégories		Conditions
A	**Inacceptable**	
B	**Tolérable sous conditions** **Réservé exclusivement aux aéronefs d'État**[7]	Risque très important qui ne peut être réduit en raison de besoins opérationnels ou de contraintes de programmes. Un risque de ce niveau ne peut être tolérer que pour répondre à une **situation exceptionnelle**. Dans ce cadre, une revue de programme et/ou une autorisation formelle de l'autorité technique et/ou de l'autorité d'emploi sont indispensables. Si le niveau de gravité associé à ce risque n'excède pas 3 (majeur), cette décision peut être prononcée par la plus haute autorité du PSNA/D. Pour un niveau de gravité 1 ou 2, cette décision est obligatoirement prononcée par le chef d'état-major d'armée ou équivalent, voire le chef d'état-major des Armées ou le ministre.
C	**Acceptable sous conditions**	Risque acceptable moyennant des consignes opérationnelles (concept d'emploi, recommandations de l'autorité d'emploi, précautions d'emploi) et/ou des recommandations techniques (précautions et recommandations de l'autorité technique). Ces mesures constituent les exigences de sécurité. Afin de vérifier que le système ne dérive pas, des indicateurs relatifs au comportement du système seront mis en place et suivis.
D	**Acceptable**	

[7] Exemple :
Une plateforme a de fortes contraintes opérationnelles avec une activité soutenue et accueille de l'aviation commerciale. Sur ordre formel de l'autorité idoine, il est décidé que les minimas de séparation radar sont plus faibles pour l'aviation d'État (par exemple 3 Nm) alors qu'une marge de sécurité est prise pour les aéronefs civils (par exemple 5 Nm). Il en découle que l'étude de sécurité démontre que la probabilité d'une perte de séparation radar est en zone B (tolérable sous conditions) pour les aéronefs d'État mais en zone C (acceptable sous conditions) pour les aéronefs civils.

III.2.3.2. Matrice quantitative

Occurrence / Gravité	> 10^{-4}/heure	< 10^{-4}/heure	< 10^{-5}/heure	< 10^{-6}/heure	< 10^{-8}/heure
1 Accident	**A**	**A**	**A**	**B**	**C**
2 Grave	**A**	**A**	**B**	**C**	**C**
3 Majeure	**A**	**B**	**C**	**C**	**D**
4 Mineure	**B**	**C**	**C**	**D**	**D**
5 Négligeable	**C**	**C**	**D**	**D**	**D**

III.2.3.3. Matrice qualitative

Occurrence / Gravité	Très fréquente	Fréquente	Occasionnelle	Rare	Extrêmement rare
1 Accident	**A**	**A**	**A**	**B**	**C**
2 Grave	**A**	**A**	**B**	**C**	**C**
3 Majeure	**A**	**B**	**C**	**C**	**D**
4 Mineure	**B**	**C**	**C**	**D**	**D**
5 Négligeable	**C**	**C**	**D**	**D**	**D**

Nota : La colonne « 10^{-8} » de la matrice quantitative ou « extrêmement rare » de la matrice qualitative signifie, qu'en réalité, l'ER ne se produira jamais. Une attention toute particulière est à porter à l'argumentaire lorsqu'un ER est positionné dans cette colonne.

III.2.3.4. Matrice de risque adaptée

Pour certains changements particuliers, il peut être pertinent de recourir à une matrice adaptée en fonction des conditions d'emploi du système et/ou de ses spécificités. Cette adaptation est proposée par le PSNA/D et approuvée par le DirCAM conformément aux procédures décrites dans l'instruction [I4150].

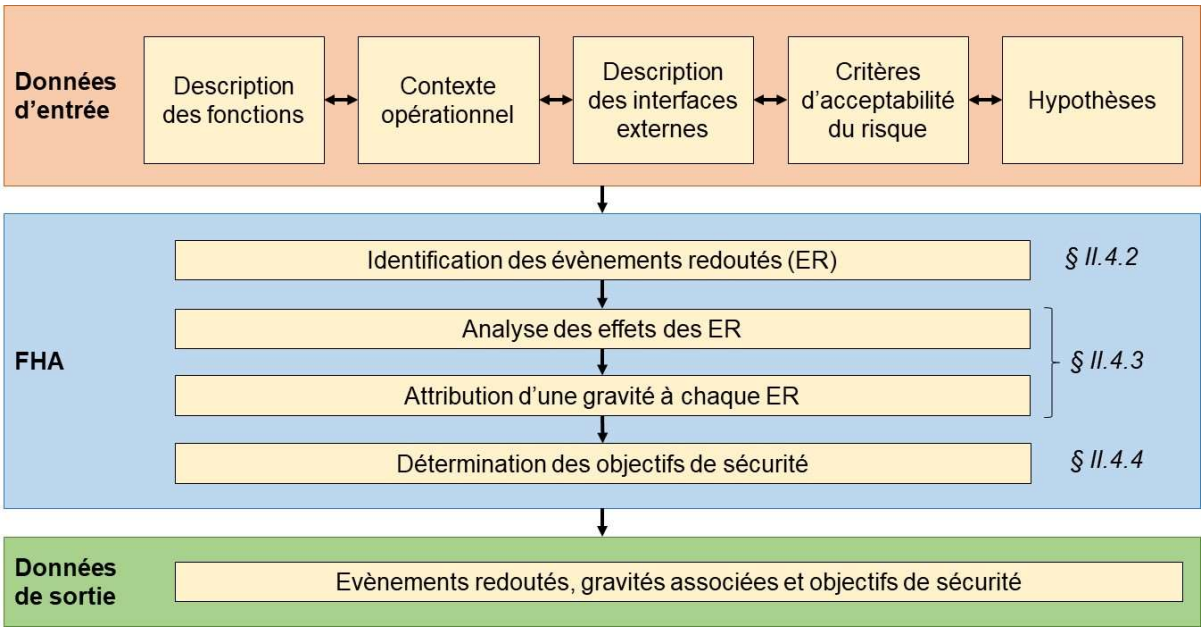
Exemple : Pour un système qui ne fonctionnerait pas H24, le PSNA/D pourrait, en accord avec l'autorité d'emploi et l'autorité technique, adapter ses objectifs de sécurité en fonction du besoin et des conditions d'emploi opérationnels. Une matrice possible pourrait alors être :

Occurrence / Gravité	> 10^{-2}/heure	≤ 10^{-2}/heure	≤ 10^{-3}/heure	≤ 10^{-4}/heure	≤ 10^{-6}/heure
1 Accident	A	A	A	B	C
2 Grave	A	A	B	C	C
3 Majeure	A	B	C	C	D
4 Mineure	B	C	C	D	D
5 Négligeable	D	D	D	D	D

Par heure de fonctionnement ramenée sur 24h/jour.

Pour ce type de système, il est nécessaire de prendre en compte des éléments complémentaires tels que la probabilité de panne à la sollicitation du système, le nombre de sollicitations du système en une période donnée, etc.

III.3. FHA – *FONCTIONAL HAZARD ASSESSMENT*

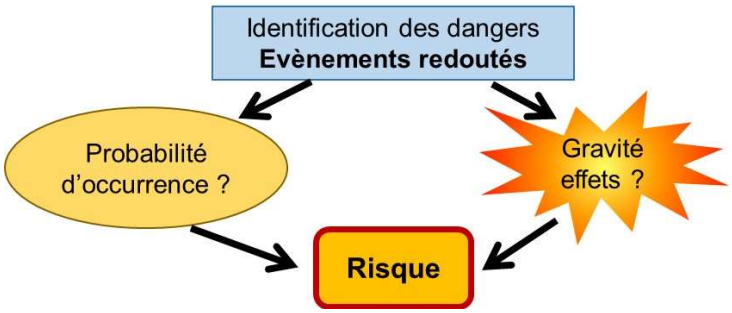


La phase FHA consiste à identifier les dangers (évènement redouté – ER), à déterminer leur gravité en prenant en compte les éventuels moyens en réduction du risque de protection, et à fixer les objectifs de sécurité.

Seul un contrôleur aérien est capable de caractériser le danger ATM. A ce titre, la FHA est conduite par un (idéalement plusieurs) contrôleur(s) aérien(s) ayant une bonne connaissance de l'environnement dans lequel le changement intervient.

III.3.1. Définition du risque

Le risque est la combinaison de la fréquence d'occurrence d'un évènement redouté et de la gravité de ses effets.



III.3.2. Identification des évènements redoutés (ER)

Cette phase consiste à identifier les dangers, ou évènements redoutés (ER), qui pourraient survenir dans le cadre du changement étudié.

Un ER est un danger susceptible d'affecter la fourniture des services ATM/ANS, exprimé au plus près des opérateurs de première ligne. C'est une situation indésirable au regard des services attendus.

L'identification des ER peut :

- être obtenue par un ou plusieurs *brainstormings* structurés entre experts du domaine ;
- découler d'une analyse basée sur l'utilisation d'un outil de l'ingénierie de la maîtrise des risque (principalement AMDE).

La définition des événements redoutés est difficile. Il ne faut pas les confondre avec des causes ou des effets. Cependant, il n'y a pas de « mauvais » événements redoutés dès lors que les choix sont clairement et irréfutablement argumentés.

III.3.3. Analyse des effets des ER

Pour chacun des ER identifiés à l'étape précédente, il faut définir au mieux les effets ou les incidences possibles sur les opérations. Ceci étant fait, il convient d'attribuer une gravité à ces effets. La gravité doit être attribuée en prenant en compte l'effet le plus raisonnablement pessimiste (*Worst Credible Case* – WCC). Ainsi, pour un évènement redouté donné, on ne partira pas du principe que l'effet le plus probable est un accident, mais on s'attachera à identifier l'effet le plus raisonnablement pessimiste. Cela revient à identifier le scénario du pire cas crédible concernant cet ER.

III.3.3.1. Gravité initiale

Dans un premier temps, l'analyse de la gravité des effets doit être menée sans tenir compte de la capacité de réaction face à la survenue d'un évènement redouté. Il s'agit donc de déterminer la gravité initiale qui est la gravité dans un scénario du pire cas crédible (WCC), sans tenir compte des moyens en réduction du risque de protection.

III.3.3.2. Détermination de moyens en réduction du risque (MRR) de protection et attribution d'une gravité corrigée

Un MRR de protection représente la capacité du contrôleur, du pilote ou même du système (par exemple, au travers d'un dispositif automatique d'alerte) à réagir face à la survenue d'un évènement redouté. Les MRR de protection permettent, lorsqu'ils sont suffisamment robustes, de diminuer la gravité des effets. On parle alors de gravité corrigée. Un PSNA/D peut juger que son MRR de protection est efficace mais n'est pas assez robuste pour agir sur la gravité.

Il est parfois difficile d'identifier une gravité initiale dans un pire cas crédible sans tenir compte des MRR de protection. Il est donc opportun, dans ce cas-là, de ne pas avoir de gravité initiale pour les ER mais directement des gravités incluant la prise en compte de l'ensemble des MRR de protection.

Pour la suite de la démonstration de sécurité, seule la gravité corrigée sera prise en compte, bien qu'il sera fait mention de la gravité initiale et du MRR de protection ayant permis de la diminuer.

III.3.4. Objectif de sécurité

Un objectif de sécurité est un énoncé qualitatif ou quantitatif qui définit la fréquence ou la probabilité maximale d'apparition d'un danger en fonction de sa gravité. Il correspond au critère de sécurité énoncé par le [RE373]. Les objectifs de sécurité sont de deux types :

- quantitatif pour les ER dont l'apparition des causes peut être mesurée par un calcul probabiliste ;
- qualitatif pour les ER dont l'apparition des causes ne peut être quantifiée.

La détermination de l'objectif de sécurité se fait par lecture de la matrice. Pour une gravité donnée, l'objectif de sécurité est la limite entre la zone B et C. Le risque en zone B, tolérable, ne concerne que les aéronefs d'état. Il est donc inacceptable dans le cas général.

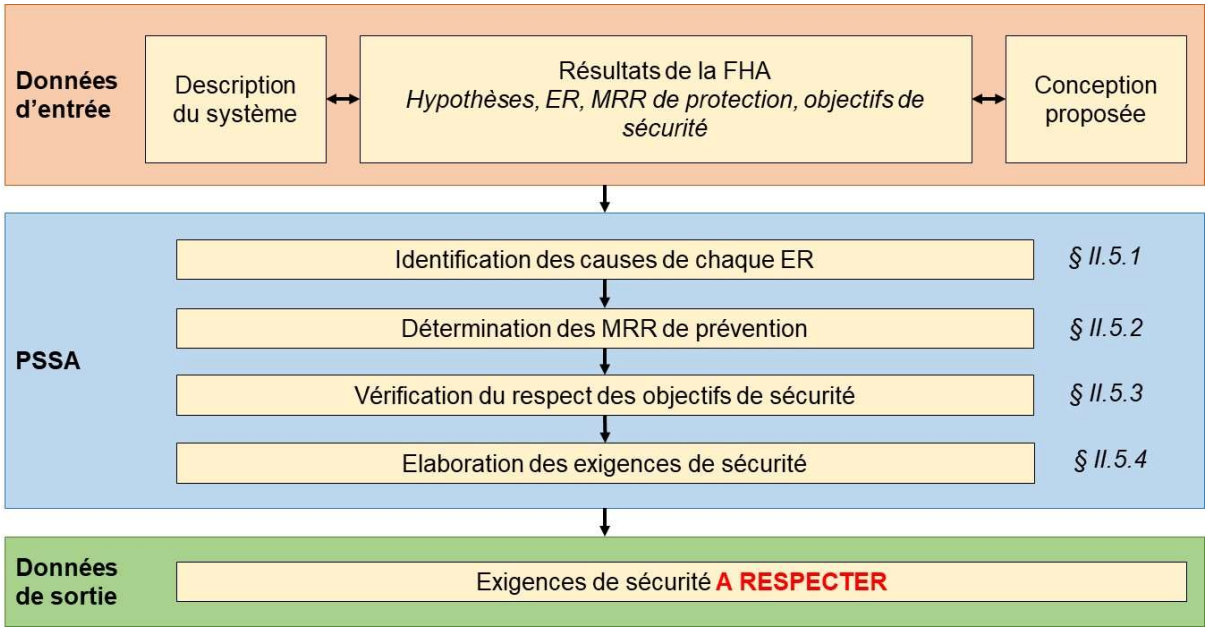
Exemple : La gravité d'un ER a été évaluée à 3.

Occurrence / Gravité	Très fréquente	Fréquente	Occasionnelle	Rare	Extrêmement rare
1 Accident	**Risque inacceptable**				
2 Grave					
3 Majeure					
4 Mineure					
5 Négligeable				**Risque**	**acceptable**

Dans le cas d'un risque justifiant d'une étude qualitative, l'objectif de sécurité pour une gravité 3 est une probabilité d'occurrence maximale « occasionnel », c'est-à-dire une à deux fois par an dans l'organisme.

La détermination d'un objectif de sécurité s'applique à chaque évènement redouté pris individuellement.

III.4. PSSA – *PRELIMINARY SYSTEM SAFETY ASSESSMENT*



La phase PSSA consiste à déterminer les causes des ER pour définir les MRR de prévention qui, en abaissant leur probabilité d'occurrence, permettront de rendre le risque acceptable. Elle permet, en outre, de déceler d'éventuels problèmes de conception du système et de mettre en évidence les points critiques.

La vérification de la tenue des objectifs de sécurité fixés en FHA est réalisée durant la PSSA.

La PSSA permet de définir les exigences de sécurité, à partir des hypothèses prises et des MRR identifiés, à mettre en place afin de garantir que la stratégie d'atténuation du risque est respectée.

III.4.1. Identification des causes des ER

Afin de définir la stratégie d'atténuation des risques, il est nécessaire de connaître les causes pouvant conduire à un ER. Dans certains cas, un *brainstorming* structuré peut être suffisant pour établir la liste exhaustive des causes. Une méthode plus systématique consiste à établir un arbre de défaillances (ou arbre des causes). Les causes d'un ER peuvent être d'origine technique, procédurale ou humaine.

Exemple : l'ER est la « pénétration d'un aéronef dans une zone dangereuse active ».

Les causes peuvent être :

- *la méconnaissance du statut de zone par le contrôleur car :*
  - *il n'a pas pris connaissance des informations nouvelles ;*
  - *une panne (matériel ou logiciel) sur le système de visualisation n'a pas permis d'afficher la zone ;*
  - *une erreur de paramétrage de la visualisation n'a pas permis d'afficher la zone ;*
  - *un oubli du chef de quart devant afficher les zones lorsqu'elles sont activées ;*
- *la méconnaissance du statut de zone par le pilote car :*
  - *il n'a pas pris connaissance des informations nouvelles ;*
  - *il n'y a pas eu de communication sur l'activation de la zone (défaut matériel, logiciel ou de procédure) ;*
- *une erreur de procédure de la part du contrôleur et/ou du pilote ;*
- *etc.*

Cette liste non exhaustive montre à quel point il est important de bien définir le périmètre du changement et ses limites lors de la phase préparatoire (cf. § IV.1.2). Avec un changement bien décrit et délimité, nombre de causes sont, de fait, supprimées.

III.4.2. Détermination des moyens en réduction du risque de prévention

Les MRR de prévention doivent permettre de diminuer la probabilité d'occurrence des ER.

Les MRR de prévention agissent sur les causes des ER. L'utilisation d'un arbre de défaillance, permettant d'avoir une vision exhaustive du problème, est pertinente dans le cas de combinaisons complexes. Elle permet notamment d'identifier les points faibles et/ou les fausses redondances.

Concernant les équipements, les résultats de l'étude sur le soutien à la sécurité permettent de déterminer les probabilités d'occurrence liées à une panne, donc la contribution à l'ER.

La formation et l'expérience du personnel réalisant l'étude de sécurité sont indispensables pour garantir le bon déroulement de cette phase. En effet, il est indispensable d'apporter à la démonstration de sécurité des éléments concrets quant à la pertinence des MRR de prévention et à leur efficacité.

Nota : il est possible qu'à ce stade de l'étude, de nouveaux phénomènes, non anticipés en FHA, soient découverts. Il est alors nécessaire d'effectuer une itération pour les rattacher aux cas déjà identifiés où ajouter un/des ER à la liste existante.

III.4.3. Vérification de la tenue des objectifs de sécurité

Les hypothèses fixées en phase préparatoire et les MRR de prévention permettent de définir la probabilité d'occurrence théorique de chaque ER. Si celle-ci est inférieure ou égale à l'objectif de sécurité, le risque associé à un évènement redouté sera considéré acceptable et l'objectif de sécurité est atteint.

Ceci se vérifie aisément au travers d'une lecture de la matrice d'acceptabilité du risque. En effet, avec la gravité des effets et la probabilité d'occurrence, il est possible de situer chaque ER dans la matrice. Les objectifs de sécurité sont atteints si tous les ER se situent dans la zone de risque acceptable.

III.4.4. Élaboration des exigences de sécurité

Les exigences de sécurité découlent :

- des hypothèses ;
- des MRR de protection, rarement puisque ceux-ci relèvent généralement d'une action réflexe ;
- des MRR de prévention.

Une exigence de sécurité est une **action concrète dont la réalisation peut être prouvée**. À ce titre, elle doit être précisément décrite dans les attendus (responsabilités pour la mise en œuvre, preuves à produire, etc.).

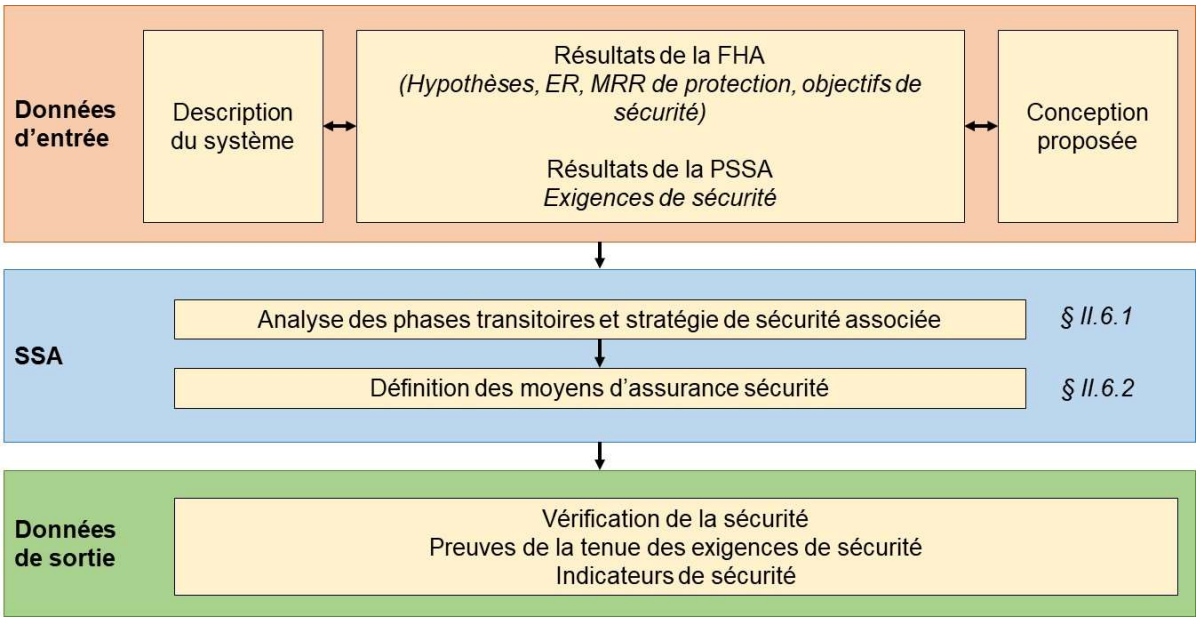
Exemple : En tant que MRR de prévention, il a été identifié la nécessité de la mise en place d'un secours électrique. Compte tenu du contexte, il s'agit d'un groupe électrogène. Cependant, si ce groupe n'est pas branché, entretenu, alimenté en carburant et si le personnel qui l'utilise n'est pas formé, ce MRR n'aura pas l'efficacité attendu. L'exigence de sécurité qui découle de ce MRR sera la mise en place d'un groupe électrogène et décrira également toutes les procédures de mise en œuvre et de soutien. Les preuves à fournir seront une copie du suivi de la formation du personnel, des maintenances du groupe, des éventuelles procédures écrites...

Le respect de l'ensemble des exigences de sécurité garantit que la stratégie d'atténuation des risques a été menée dans son intégralité et donc que le risque est acceptable. Elles devront être tenues durant toute la vie du système mais pourront évoluer avec le retour d'expérience. Dans ce cas, l'étude de sécurité devra être amendée pour préciser cette évolution. Si l'étude de sécurité initiale a été classée « SUIVI » par le DirCAM (cf. [I4150]), il conviendra de transmettre cette nouvelle étude pour approbation.

Exemple : Une exigence de sécurité concerne la formation du personnel sur le nouveau système et la preuve associée est l'attestation de formation produite par l'industriel. Par la suite, pour le personnel nouvellement affecté, cette formation sera inscrite dans le plan de formation en unité et réalisée localement. Il sera donc nécessaire de prévoir cette disposition dans l'étude de sécurité initiale ou de faire évoluer le document le temps venu.

III.5. SSA – *SYSTEM SAFETY ASSESSMENT*

La phase SSA a pour objectif d'apporter les assurances que les actions définies en phases FHA et PSSA ont bien été mises en place et, ce, de façon pérenne. Elle est avant tout un recueil de preuves mais permet également l'analyse du risque intrinsèque aux phases de transition lors de la mise en œuvre du système.



Lors du recueil des preuves de la tenue des exigences de sécurité, il est indispensable de porter une attention particulière à la validité et à la pérennité des hypothèses et/ou MRR qu'elles couvrent. La PSSA étant une analyse théorique, il s'agit de vérifier que les conclusions restent vraies dans la pratique, c'est-à-dire que tous les évènements redoutés se situent effectivement en zone de risque acceptable.

La méthodologie SAM est une méthode itérative. Ainsi, au cours de la phase SSA des éléments nouveaux peuvent apparaitre et, le cas échéant, donner lieu à de nouveaux ER. Il sera alors nécessaire de les étudier en phases FHA et PSSA avant de poursuivre le processus.

III.5.1. Phases transitoires

Par phase de transition, on entend toute opération se déroulant entre la mise en œuvre du système (début de la phase de travaux) et sa mise en service pour utilisation opérationnel. Une phase transitoire se caractérise par un impact avéré sur l'environnement de travail du contrôleur aérien (perte d'une partie des capacités, gêne visuelle, bruit…). Ainsi, des travaux qui, à terme,

intéresseront le centre de contrôle et se déroulant sans le moindre impact sur le système au sens large ne sont pas qualifiés de phase transitoire.

L'analyse des risques propres aux phases de transition d'un système, s'il en existe, fait partie intégrante de la SSA.

L'étude de sécurité doit prendre en compte cette phase extrêmement importante pour la mise en service d'un système. L'analyse des phases de transition est indispensable pour démontrer que toutes les dispositions ont été prises durant ces phases afin de ne pas dégrader le niveau de sécurité.

En général, l'analyse des phase transitoire fait l'objet d'un document à part de l'étude de sécurité et couvre un court délai dans la vie du système. Ce document est néanmoins conservé avec l'étude de sécurité tout au long de la vie du système.

III.5.2. Assurance sécurité

L'assurance sécurité consiste à suivre les critères de sécurité tout au long de la vie opérationnelle du système. Elle débute avec le recueil des preuves de la tenue des exigences de sécurité et se poursuit tout au long de la vie de système.

L'assurance sécurité, étant un principe général aux démonstrations de sécurité quel que soit le type de changement, ATS ou non-ATS, elle fait l'objet du titre VI.

TITRE IV

DÉMONSTRATION DE SÉCURITÉ D'UN CHANGEMENT non-ATS

Ingénierie de la maîtrise des risques

Pour les armées, les changements non-ATS sont généralement menés par les PSCNS/D, le cas échéant par des prestataires extérieurs fournissant un service de soutien.

Les démonstrations de sécurité pour les changements non-ATS utilisent les outils de l'ingénierie de la maîtrise du risque, principalement, analyse des modes de dysfonctionnement et de leurs effets (AMDE), arbre de défaillance et réseau de Pétri. D'autres méthodes existent mais, n'étant pas communément utilisées dans les démonstrations de sécurité réalisées par les PSNA/D, leur utilisation est soumise à l'approbation préalable du DirCAM (cf. [I4150]).

Le présent titre décrit sommairement ces méthodes et ne constitue pas le référentiel méthodologique pour un changement non-ATS dans les armées. En outre, la mise en œuvre d'un réseau de Pétri demandant une expertise importante, seul le principe de cet outil est abordé.

L'application des méthodes décrites au présent titre ne doit se faire qu'au travers de l'utilisation des publications officielles relatives à celles-ci, garantes du respect des règles de l'art.

Dans le cas d'un changement non-ATS avec impact ATS justifiant d'une étude de sécurité, l'étude sur le soutien à la sécurité s'inscrit dans la phase PSSA (cf. paragraphe III.4) puisque les dysfonctionnements du système non-ATS contribuent plus ou moins directement à l'apparition des évènements redoutés.

IV.1. DÉFINITION DES PERFORMANCES DU SYSTÈME

Les performances minimales d'un système utilisé pour rendre les services de la navigation aérienne sont intrinsèquement liées au niveau de risque engendré par celui-ci. Ainsi, préalablement à la définition des performances, il est indispensable de caractériser le risque engendré par le système. Cette opération doit impérativement se faire avec une participation active des PSCA/D.

Pour établir les performances attendues du système, il existe deux possibilités :

- dans le cas général, il est préconisé d'utiliser la FHA de la méthode SAM, les performances minimales du système découlant des objectifs de sécurité ainsi définis ;
- si le changement consiste à remplacer un système existant, il est admis que les performances attendues soient au moins équivalentes aux performances actuelles si celles-ci satisfont au niveau de sécurité voulu par le(s) PSCA/D.

Dans un souci de cohérence, cette première étape de l'étude sur le soutien à la sécurité doit impérativement se faire en collaboration avec le(s) PSCA/D qui utilisera(ont) le système. À ce titre, le PSCNS/D décrit, dans les procédures qu'il soumet à l'approbation du DirCAM, les modalités de coordination avec le(s) PSCA/D soutenu(s). Ces procédures figurent également dans le processus de gestion des changements du (des) PSCA/D.

IV.2. AMDE

L'AMDE est un outil systématique et qualitatif permettant d'identifier les défaillances d'un système lors de la définition de la modification à apporter (changement) ainsi que dans le cadre de la conception du système. L'AMDE permet également d'évaluer l'impact relatif d'une défaillance afin d'identifier les points faibles du système.

L'AMDE consiste à appliquer des défaillances types sur chaque (sous-)fonction du système afin d'en définir les effets. Afin d'affiner l'étude, on applique des attributs à chacune de ces défaillances types.

Dans le cadre de la conception du système, l'AMDE peut être complétée en décrivant les moyens de détection / palliatifs sur chaque défaillance type de (sous-)fonction.

Lorsque l'AMDE est menée avec la participation de contrôleurs aérien, il est possible de relier certaines défaillances à des évènements redoutés[8].

L'inconvénient de l'AMDE réside dans le fait qu'elle ne permet pas de traiter une combinaison de défaillance.

IV.2.1. Défaillances types utilisées pour une étude sur le soutien à la sécurité

Perte de fonction : la fonction est opérante et cesse de fonctionner de manière inattendue.

Pas de fonction : la fonction ne se déclenche pas alors que l'opérateur l'appelle / la séquence de fonctionnement suppose son démarrage.

Fonction dégradée : la fonction est opérante mais avec une efficacité moindre / une perte dans le résultat présenté.

Fonction intempestive : la fonction se déclenche alors qu'elle n'est pas attendue.

IV.2.2. Attributs utilisés pour une étude sur le soutien à la sécurité

Détection : la défaillance type est immédiatement[9] détectée. Des mesures palliatives / alternatives permettant d'atténuer l'effet de cette défaillance sont possibles.

Non-détection : la défaillance type n'est pas détectée ou trop tardivement. Il n'est pas admis d'imaginer des mesures palliatives / alternatives permettant d'atténuer l'effet de cette défaillance.

Une position : une seule position de contrôle est affectée par la défaillance type, les autres restent pleinement opérantes.

Ensemble des positions / du centre : La défaillance type affecte l'ensemble du centre.

IV.3. ARBRE DE DÉFAILLANCES

Un arbre de défaillances (aussi appelé arbre de pannes ou arbre de fautes) est un outil graphique très utilisé dans les études de fiabilité des systèmes. Il s'agit d'une une méthode déductive basée sur la représentation des combinaisons possibles d'événements qui mènent à la survenue d'un événement indésirable[10] prédéfini. Une telle représentation graphique met en évidence les relations de cause à effet et permet de calculer la probabilité d'occurrence d'un évènement indésirable.

Un arbre de défaillances est généralement présenté de haut en bas. La ligne la plus haute ne comporte que l'évènement dont on cherche à décrire comment il peut se produire. Chaque ligne détaille la ligne supérieure en présentant la combinaison ou les combinaisons susceptibles de produire l'évènement de la ligne supérieure auquel elles sont rattachées. Ces relations sont représentées par des liens logiques, dont la plupart sont des portes « OU » ou « ET ».

Le processus se poursuivit niveau par niveau jusqu'à ce qu'il soit jugé qu'il n'est plus nécessaire (ou plus possible) de continuer l'analyse. Les événements non décomposés de l'arbre sont appelés événements élémentaires (ou événements de base).

L'analyse par arbre de défaillance n'est pertinente qu'à condition que les évènements de base soient indépendants.

---

[8] Une défaillance du système ne se traduit pas nécessairement par une situation à risque pour le contrôleur aérien. Ainsi, une défaillance n'est pas systématiquement reliée à un évènement redouté.

[9] Il y a quelques années, l'aviation civile d'une part, la DIRCAM et les PSNA/D d'autre part ont travaillé sur le temps d'exposition à un évènement redouté / une défaillance. Ces travaux n'aillant pas permis de développer un modèle satisfaisant pour justifier d'un risque maîtrisé avec une détection différée, il a été décidé de prendre l'attribut « détection » comme immédiat ou quasi-immédiat (inférieur à cinq secondes).

[10] Pour l'ATM, l'évènement indésirable est soit un dysfonctionnement du système, soit directement l'évènement redouté (ER). Cependant, dans le cadre d'une étude sur le soutien à la sécurité le terme ER est à proscrire.

IV.3.1. Analyse qualitative de l'arbre de défaillance

L'analyse qualitative de l'arbre de défaillance permet :

- l'identification des scénarios critiques (combinaisons les plus courtes appelées coupes minimales) susceptibles de conduire à l'événement indésirable ;
- la mise en œuvre d'une procédure d'allocation de barrières qui permet d'allouer un certain nombre de barrières de sécurité (techniques ou d'utilisation) en fonction de la gravité de l'événement indésirable et des contraintes normatives éventuelles.

IV.3.2. Analyse quantitative de l'arbre de défaillance

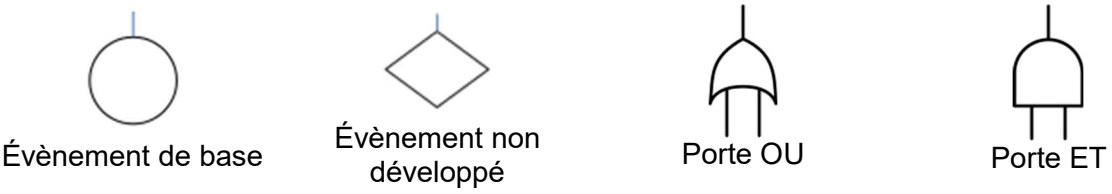
L'analyse quantitative de l'arbre de défaillance permet :

- l'évaluation rigoureuse de la probabilité d'occurrence de l'événement indésirable ;
- le tri des scénarios critiques (en partant coupes minimales de plus fortes probabilités).

Ces calculs ne peuvent se concevoir que si chaque événement de base peut être probabilisé.

IV.3.3. Symboles utilisés dans les arbres de défaillances

Les symboles ci-dessous sont ceux les plus communément utilisés dans les arbres de défaillance d'étude sur le soutien à la sécurité.



Porte OU : il suffit qu'un des évènements en entrée se produise pour que l'évènement en sortie se produise.

Porte ET : il faut que l'ensemble des évènements en entrée se produise pour que l'évènement en sortie se produise.

IV.4. RÉSEAU DE PÉTRI

Un réseau de Pétri est un modèle mathématique servant à représenter divers systèmes (informatiques, industriels…) travaillant sur des variables discrètes. C'est un outil graphique et mathématique permettant de modéliser et de vérifier le comportement dynamique des systèmes.

Un réseau de Pétri vient en complément de l'arbre de défaillance afin d'identifier les points faibles du système liés au comportement des composants.

Compte tenu de la complexité de cet outil, il n'est pas détaillé dans le présent guide méthodologique. Le cas échéant, se reporter aux publications idoines.

IV.5. OUTIL PARTICULIER AUX PHASES DE SOUTIEN / PARAMÉTRAGE

Afin de garantir le maintien de leurs performances, les équipements nécessitent un processus de maintenances systématiques ou conditionnelles. Dans ce cadre, il peut être nécessaire de reprendre le paramétrage de sous-systèmes.

Pour l'étude sur le soutien à la sécurité, il peut être opportun d'étudier la contribution d'une erreur de maintenance ou de paramétrage à un comportement inapproprié du système.

Il s'agit de l'étude « des cas d'emploi ». Elle utilise des outils spécifiques qui permette de mettre en exergue la criticité d'une erreur de maintenance / paramétrage sur le comportement / les performances du système au regard de la probabilité que l'opérateur commette cette erreur.

L'étude des cas d'emploi permet de définir des exigences spécifiques aux phases de maintenance / paramétrage pour justifier d'un fonctionnement du système conforme aux performances attendues (cf. paragraphe IV.1). Ces exigences spécifiques se traduisent généralement par des prescriptions sur les méthodes d'intervention et la formation des opérateurs et constituent des exigences de sécurité.

IV.6. EXIGENCES DE SÉCURITÉ D'UNE ÉTUDE SUR LE SOUTIEN A LA SÉCURITÉ

A l'instar d'une étude de sécurité, une étude sur le soutien à la sécurité vise à définir des moyens concrets permettant de garantir que le système justifiera des performances attendues (définies lors de l'initiation de l'étude). Ces moyens concrets sont les exigences de sécurité de l'étude sur le soutien à la sécurité.

Ces performances ont une incidence sur la réalisation du système en terme :

- d'architecture ;
- de disponibilité ;
- de maintenabilité ;
- de résilience ;
- etc.

Les preuves de tenue de ces exigences de sécurité sont généralement matérialisées par :

- l'acceptation en usine (FAT[11]) et sur site (SAT[12]) ;
- les résultats des cahiers d'essais et de réception ;
- la documentation technique, en particulier la bibliothèque de schémas ;
- etc.

IV.7. PROBLÉMATIQUE DE LA COMPOSANTE LOGICIELLE

Le logiciel est une composante de plus en plus importante dans les équipements. Sa contribution aux dysfonctionnements du système doit être prise en compte dans le cadre de l'étude sur le soutien à la sécurité.

IV.7.1. Notion d'assurance de la sécurité des logiciels

Un logiciel ne peut être caractérisé par un taux de défaillance. La défaillance du logiciel ne peut donc qu'être abordée d'un point de vue qualitatif.

L'approche retenue pour s'assurer de la sécurité des logiciels consiste à attribuer un niveau d'assurance logicielle (« *SoftWare Assurance Level* » – SWAL) à chaque logiciel en fonctions de leur contribution à l'apparition d'une défaillance système. L'assurance de la sécurité des logiciels décrit les méthodes pour attribuer ces SWAL et démontrer leur atteinte. Cela impose de produire l'argumentaire et les preuves justifiant que les logiciels n'engendreront pas un comportement inapproprié du système. À ce titre, l'assurance de la sécurité des logiciels :

- attribue un **niveau de confiance** pour tout logiciel apparaissant dans le périmètre du changement non-ATS ;

[11] Factory Acceptance Tests.
[12] Site Acceptance Tests.

- définit des arguments, sous la forme d'objectifs à atteindre pour chaque logiciel, appelés « **objectifs logiciels**[13] » pour satisfaire le niveau de confiance. L'atteinte des objectifs logiciels apportent les assurances nécessaires sur :
  - la validité des exigences logicielles ;
  - la gestion de configuration du logiciel ;
  - la vérification du logiciel ;
  - la traçabilité des exigences logicielles ;
  - l'absence de fonction logicielle nuisible à la sécurité ;
- précise avec quel degré de rigueur les assurances sont établies, en termes d'activités et de production de preuves, attestant de la tenue des « objectifs logiciels ». Le niveau de confiance est une mesure de cette rigueur, laquelle augmente en fonction de la criticité du logiciel.

L'assurance de la sécurité des logiciels constitue en définitive un ensemble documenté figurant dans l'étude sur le soutien à la sécurité. Elle permet de garantir que la contribution de chaque logiciel à une défaillance du système est en adéquation avec les performances requises (cf. paragraphe IV.1).

Le SWAL ne se substitue en aucun cas aux autres exigences de sécurité identifiées dans l'étude sur le soutien à la sécurité mais il fixe le degré de rigueur avec lequel chaque logiciel est réalisé.

Afin de démontrer l'assurance de la sécurité logicielle, les prestataires de services se basent sur des normes.

Pour démontrer l'assurance de la sécurité logicielle, les PSNA/D utilisent la norme [ED153]. La norme [ED109] peut également l'être.

IV.7.2. Démarche d'assurance de la sécurité des logiciels

L'ensemble des activités à réaliser pour prendre en compte la composante logicielle dans l'étude sur le soutien à la sécurité afin de fournir les preuves requises peut se résumer à trois phases :

- la détermination du niveau de confiance ;
- la satisfaction du niveau de confiance (les assurances à apporter) ;
- l'assurance sécurité logicielle.

Si l'analyse démontre que l'introduction ou la modification d'un logiciel n'a pas d'impact sur la sécurité, aucune assurance sécurité logicielle n'est requise pour ce logiciel. Cette assertion doit toutefois être formalisée dans l'étude sur le soutien à la sécurité.

IV.7.2.1. Détermination du niveau de confiance

Afin de définir le niveau de SWAL, il existe deux méthodes. Celles-ci nécessitent impérativement la contribution du (des) PSCA/D à l'analyse puisqu'elles s'appuient sur le niveau de risque au sens de l'ATS (cf. paragraphes III.2 et III.3).

La première méthode consiste à évaluer comment la défaillance logicielle contribue au danger (conséquence de l'ER selon le scénario du pire cas crédible). La seconde consiste à positionner la défaillance logicielle dans l'arbre des causes associé à l'ER. La définition du niveau de SWAL s'obtient par lecture de la matrice pertinente ci-dessous.

[13] Les « objectifs logiciels » sont les propriétés exigées pour la réalisation et/ou la mise en œuvre d'un logiciel en fonction du niveau de confiance requis.

Contribution de la défaillance logicielle à l'effet de l'ER

	Gravité de l'effet				
Contribution au danger	1	2	3	4	5
Très possible	SWAL 1	SWAL 2	SWAL 3	SWAL 4	SWAL 4
Possible	SWAL 2	SWAL 3	SWAL 3	SWAL 4	SWAL 4
Improbable	SWAL 3	SWAL 3	SWAL 4	SWAL 4	SWAL 4
Extrêmement improbable	SWAL 4	SWAL 4	SWAL 4	SWAL 4	SWAL 4

Contribution de la défaillance logicielle à l'ER

	Gravité associée à l'évènement redouté				
Contribution à l'ER	1	2	3	4	5
Directe	SWAL 1	SWAL 2	SWAL 3	SWAL 4	SWAL 4
Combinaison simple	SWAL 2	SWAL 3	SWAL 3	SWAL 4	SWAL 4
Combinaison multiple	SWAL 3	SWAL 3	SWAL 4	SWAL 4	SWAL 4

Exemple : Dans le cadre de l'analyse du risque, un niveau de gravité 2 est défini. En l'état, cela représenterait un SWAL 2. Néanmoins :
Argumentaire méthode 1 : le dysfonctionnement est facilement identifiable et il existe des procédures de contrôle permettant de rétablir facilement la situation. Ainsi, la contribution de la défaillance logicielle à l'effet est jugée improbable donc un SWAL 3 est suffisant.
Argumentaire méthode 2 : il existe une redondance indépendante d'un point de vue logiciel. Dans ces conditions, une combinaison (dans ce cas simple) d'éléments est nécessaire à l'apparition de l'ER donc un SWAL 3 est suffisant.
ATTENTION : dans cet exemple, les arguments permettant d'abaisser le niveau de SWAL constituent également des moyens en réduction du risque de protection, c'est-à-dire qui permettent d'abaisser la gravité. Dans un cas similaire, un MRR ne pouvant être utilisé qu'une fois pour réduire un risque, l'argumentaire sera utilisé soit pour baisser la gravité, soit pour baisser le niveau de SWAL mais en aucun cas pour baisser les deux.

IV.7.2.2. Démonstration du niveau de confiance

La démonstration de la satisfaction du niveau de confiance du logiciel repose sur l'apport d'assurances tout au long du cycle de vie du logiciel. L'application des normes [ED153] et [ED109] à privilégier car elle sont un moyen acceptable de conformité et ont été choisies par les PSNA/D.

Dans le cadre particulier d'une modification d'une version logicielle déjà en service et ayant fait l'objet d'une démonstration de sécurité, la satisfaction du niveau de confiance requis peut se démontrer en travaillant par mesure des différences entre la version logicielle avant modification et la nouvelle version logicielle après modification. L'intérêt de cette démarche est de démontrer la satisfaction du niveau de confiance requis en apportant des assurances limitées au seul périmètre de la modification. Toutefois, pour procéder ainsi, le prestataire de services doit disposer des éléments sur les assurances apportées sur la version avant modification.

IV.7.2.3. Assurance sécurité logicielle

Dans le cadre de l'étude sur le soutien à la sécurité, une surveillance spécifique de la composante logicielle doit être mise en place par le prestataire de service. Celle-ci est principalement basée sur le retour d'expérience et permet de vérifier :

- l'efficacité des moyens en réduction du risque externes au logiciel ;
- le caractère adéquat de l'assurance de la sécurité du logiciel et des niveaux de confiance attribués.

IV.7.3. Correction de logiciels

Il est très fréquent que les versions logicielles soient amenées à évoluer. Certaines évolutions peuvent être considérées comme majeures (*exemple : ajout de nombreuses fonctionnalités*), alors que d'autres restent mineures (*exemple : changement de la taille de police sur une interface homme-machine*). Les actions à réaliser, découlant de la criticité de la modification logicielle, seront ainsi différentes. À titre de recommandation, on peut considérer les deux cas suivants :

- dans le cadre de l'application d'un « patch » ou de toute mise à jour d'un logiciel ayant pour objectif la correction de bugs ou d'anomalies mineures, le PSNA/D pourra ne rédiger qu'une simple MISO (cf. § VIII.3.2) au titre de la démonstration de sécurité ;
- si le prestataire de services souhaite modifier son logiciel en profondeur, voire apporter de nouvelles fonctionnalités visant ainsi à améliorer l'utilisation et n'ayant aucun aspect curatif, une étude sur le soutien à la sécurité sera nécessaire. Le SWAL du logiciel en question sera alors mis à jour à l'aune des éléments nouveaux.

IV.8. INTEROPÉRABILITÉ DES SYSTEMES

IV.8.1. Exigences réglementaires

L'interopérabilité (IOP) des systèmes est portée par les règlement [RE1768], [RE1769], [RE1770], [RE1771] [RE1772]. Elle se décline à trois niveaux :

- les « *équipements ATM/ANS les plus critiques »* sont **certifiés** :
  - *« services ATC permettant la séparation des aéronefs ou la prévention des collisions » ;*
  - *« communication sol-air directe […] entre le contrôleur aérien et le pilote » ;*
- les « *équipement C*NS, *de criticité moindre*, *utilisés directement par l'ATS pour garantir la sécurité »* font l'objet d'une déclaration de conformité de la conception :
  - *« communication sol-sol » ;*
  - *« appui à la navigation ou à la surveillance » ;*
- les équipements pour les services supports « *les moins critiques* » font l'objet d'une attestation de conformité :
  - *« météorologie » ;*
  - *« information aéronautique » ;*
  - *« gestion de l'espace aérien » ;*
  - *« etc. ».*

La certification et la déclaration de conformité de la conception sont prononcées par l'EASA. L'attestation de conformité est produite par le PSNA/D.

IV.8.2. Processus interopérabilité

Rédaction réservée

TITRE V

VÉRIFICATION DE L'ACCEPTABILITÉ DU RISQUE

V.1. GÉNÉRALITÉS

Conformément au règlement [RE373], la responsabilité de statuer sur l'acceptabilité du risque, que ce soit pour une étude de sécurité ou pour une étude sur le soutien à la sécurité, revient au prestataire de services ATS (PSCA/D). À ce titre, les PSCNS/D et les PSCA/D décrivent dans leurs procédures soumises à l'approbation du DirCAM les modalités de coordination concernant les études sur le soutien à la sécurité. De plus, les PSCA/D disposent dans le cadre de leur SMS d'un processus décrivant comment l'acceptabilité est mesurée et prononcée.

V.2. CAS D'UN CHANGEMENT ATS

Concernant les changement ATS, l'acceptabilité du risque est acquise si :

- la l'étude de sécurité permet de justifier que, *in fine*, l'ensemble des ER figure dans les parties « risque acceptable » ou « risque acceptable sous condition » ;
- le prestataire de services dispose des preuves de la tenue de l'ensemble des exigences de sécurité[14].

V.3. CAS D'UN CHANGEMENT non-ATS SANS IMPACT SUR L'ATS

Dans le cas d'un changement non-ATS sans impact sur l'ATS, le risque est réputé acceptable dès lors que l'étude sur le soutien à la sécurité prouve que le système présente des performances en adéquation avec celles définies à l'initialisation de l'étude et que le prestataire de services dispose des preuves de la tenue de l'ensemble des exigences de sécurité[14].

L'acceptabilité du risque sera validée par la signature de la démonstration de sécurité par le PSCA/D. Cette validation vaut acceptation du changement par ce dernier (cf. [I4150]).

V.4. CAS D'UN CHANGEMENT non-ATS AVEC IMPACT SUR L'ATS

Dans le cas d'un changement non-ATS avec impact sur l'ATS, il conviendra de mener une étude de sécurité en complément de l'étude sur le soutien à la sécurité. L'étude de sécurité prendra une forme en adéquation avec le niveau de risque identifié à l'initialisation de l'étude sur le soutien à la sécurité :

- processus simplifié dans le cas de gravités peu élevées (maximum 3) et de mise en place de MRR, au niveau du prestataire ATS, constituant des tâches quotidiennes du métier de contrôle aérien (cf. [I4150]) ;
- étude prestataire d'impact sur la sécurité (EPIS - cf. [I4150]) dans le cas de gravités élevées (1 ou 2) et/ou de la mise en place de MRR, au niveau du prestataire ATS, complexes, dépassant le cadre habituel du métier du contrôle aérien ;
- dossier de sécurité dans le cas d'un changement très complexe avec de nombreux impact sur l'environnement du contrôleur aérien (*par exemple, modification intégrale des interfaces homme-machine – nouvelle ergonomie et nouvelles fonctionnalités – en salle de contrôle*).

Pour un changement non-ATS avec impact sur l'ATS, le risque est réputé acceptable si :

- l'étude sur le soutien à la sécurité prouve que le système présente des performances en adéquation avec celles définies à l'initialisation de l'étude ;
- le prestataire de services non-ATS dispose des preuves de la tenue de l'ensemble des exigences de sécurité[14] définies dans l'étude sur le soutien à la sécurité ;
- l'étude de sécurité associée conclut à un risque acceptable ;

[14] Par définition, s'il n'est pas possible d'apporter la preuve de la tenue d'une seule exigence de sécurité, le risque est réputé inacceptable.

- le prestataire de services ATS utilisant le système objet du changement dispose des preuves de la tenue de l'ensemble des exigences de sécurité[14] définies dans l'étude de sécurité.

L'acceptabilité du risque sera validée par l'acceptation de l'étude de sécurité associée à l'étude sur le soutien à la sécurité et l'acceptation du changement prononcée par le PSCA/D utilisant le système (cf. [I4150]).

V.5. AMÉLIORATION DE LA SÉCURITÉ

Le règlement [RE373] impose de démontrer que le système, une fois le changement appliqué, est au moins aussi sûr qu'auparavant.

- Lorsqu'il existe une étude antérieure à la démonstration de sécurité objet du changement, cette exigence sera tenue au travers d'une comparaison des matrices d'acceptabilité des risques. S'il n'existe pas d'étude antérieure, cette exigence sera présumée tenue dès lors que le risque est acceptable.
- S'il s'avère que le système n'est pas aussi sûr qu'auparavant, le PSNA/D doit démontrer que le changement apporte des bénéfices qui contrebalancent cette situation. Les éléments devront figurer de manière explicite dans la démonstration de sécurité.

Les modalités pratiques pour répondre à cette exigence sont décrites dans les procédures des PSNA/D soumises à l'acceptation du DirCAM.

Page intentionnellement blanche

TITRE VI

ASSURANCE SÉCURITÉ

VI.1. EXIGENCES DE SÉCURITÉ

Les exigences de sécurité découlent des choix fait au cours de la réalisation de la démonstration de sécurité. Elles portent sur :

- les hypothèses ;
- dans le cas d'une étude de sécurité, les moyens en réduction du risque (MRR) ;
- dans le cas d'une étude sur le soutien à la sécurité, les choix de conception pour réaliser le système mais également les normes applicables au type d'équipement objet du changement (notamment interopérabilité), lorsqu'elles existent.

Une exigence de sécurité doit s'appuyer sur du concret, être vérifiable et sera impérativement vérifiée dans le cadre de l'acceptation du changement. A ce titre, une exigence de sécurité est assortie d'une (de) preuve(s). Dans le cadre de sa démonstration de sécurité, le PSNA/D doit recueillir l'ensemble des preuves de la tenue des exigences de sécurité.

S'il s'avère impossible de recueillir une preuve de la tenue d'une exigence de sécurité, le risque associé au changement est réputé inacceptable et le changement ne peut être mis en œuvre/service.

Toutefois, pour certains changements (en particulier non-ATS), des preuves de la tenue d'exigences de sécurité résulte de tests *in situ*. Dans ce cas, la démonstration de sécurité fera l'objet d'une approbation « sous-réserve » et, le cas échéant, le changement sera accepté « sous-réserve » afin de ménager le délai nécessaire à établir les preuves afférentes. Lorsque l'ensemble des preuves auront été recueillies, les réserves seront levées.

L'ensemble des preuves recueillies doit figurer avec la démonstration de sécurité. Elles pourront être examinée *a posteriori*, notamment lors des audits internes du PSNA/D ou externes de la DIRCAM.

VI.2. ASSURANCE SÉCURITÉ

L'assurance sécurité consiste à garantir, tout au long de la vie du système :

- que le risque est durablement acceptable s'il s'agit d'un changement ATS ;
- qu'il se comporte uniquement comme spécifié s'il s'agit d'un changement non-ATS.

Dans ce cadre, le PSNA/D doit définir une stratégie de vérification périodique de points particuliers :

- suivi d'indicateurs sur le fonctionnement du système (changement non-ATS) ou évènement ATM (changement ATS) ;
- maintien de preuves de la tenues d'exigences de sécurité (par exemple, formation du personnel) ;
- etc.

Les moyens mis en œuvre au titre de l'assurance sécurité sont décrits dans la démonstration de sécurité.

Lorsque la démonstration de sécurité prouve que la probabilité d'occurrence d'un ER (éventuellement liée à une probabilité de défaillance) est proche de l'objectif de sécurité, voire concerne un ER en zone « tolérable sous condition » (cf. paragraphe III.2), la mise en place et le suivi d'indicateurs sont obligatoires.

Le suivi d'indicateurs constitue un excellent moyen en matière d'assurance sécurité et a pour finalité le suivi de points critiques du système. Particulièrement pertinent pour les systèmes techniques, ils ont vocation à être utilisés comme une alarme afin d'éviter une éventuelle dérive.

Au cours de la vie opérationnelle du système, il n'est pas rare de s'apercevoir que certains points ont plus d'incidences sur la sécurité que d'autres. Cela peut se traduire par :

- un système offrant des garanties de sécurité supérieure à l'attendu ;
- des problématiques non identifiées à la réalisation de la démonstration de sécurité.

Dans ce cas, la démonstration de sécurité sera amendée en conséquence :

- arrêt du suivi d'une partie de l'assurance sécurité ;
- mise en place d'un suivi lié au problématiques nouvelles, le cas échéant compte tenu de la définition d'une nouvelle exigence de sécurité.

Page intentionnellement blanche

TITRE VII

TRAITEMENT DES CHANGEMENTS ASM

VII.1. GÉNÉRALITÉS

Conformément au règlement [RE373] et à la définition d'un changement (cf. titre I), une modification à l'organisation de l'espace aérien (ASM) constitue un changement et doit faire l'objet d'un processus idoine.

Néanmoins un changement ASM constitue un cas d'espèce. Il peut s'agir :

- d'un changement à caractère permanent à l'initiative du PSCA/D gestionnaire de l'espace en question ;
- d'un changement à caractère permanent à l'initiative d'un autre PSCA et ayant une incidence sur l'espace géré par le PSCA/D ;
- d'un changement à caractère temporaire à l'initiative du PSCA/D gestionnaire de l'espace en question ;
- d'un changement à caractère temporaire à l'initiative d'un autre PSCA et ayant une incidence sur l'espace géré par le PSCA/D.

Les dispositifs particuliers de sûreté aérienne (DPSA) et certaines mesures d'interdiction de survol prises par les autorités préfectorales sont exclus du périmètre des changements ASM.

Dans le cadre des relations entre les armées et l'aviation civile, un protocole formel a été établi. Il traite des changements ASM et prévoit des procédures adaptées. En outre, il prévoit des démonstrations de sécurité simplifiées locales (DSSL) au lieu d'études de sécurité classiques dans le cadre de changements ASM temporaires.

VII.2. CHANGEMENTS ASM A TITRE PERMANENT

Lorsqu'un PSCA/D est concerné par un changement ASM à titre permanent (que ce soit par la modification d'un espace dans lequel il rend les services de la CAG ou par l'impact sur son système fonctionnel d'une évolution d'un espace adjacent), il gère ce changement comme un changement ATS.

Compte tenu des délais incompressibles du processus de publication de l'information aéronautique, le PSCA/D doit impérativement anticiper sa notification de changement, l'étude de sécurité devant figurer dans le dossier soumis à l'approbation du DirCAM pour publication.

VII.3. CHANGEMENTS ASM A TITRE TEMPORAIRE

VII.3.1. Changements concernés

Les changements ASM concernés sont les changements temporaires apportés à l'organisation et à la gestion de l'espace aérien, qui font obligatoirement l'objet d'une consultation par le bureau exécutif permanent (BEP) des membres du comité régional de gestion de l'espace aérien (CRG).

VII.3.2. Processus pour la démonstration de sécurité

VII.3.2.1. Étude de sécurité

Lorsque le PSCA/D est, soit à l'origine du changement, soit identifié comme en étant le principal bénéficiaire, il gère le changement ASM temporaire comme un changement ATS et réalise une étude de sécurité conforme aux prescription en la matière.

VII.3.2.2. Démonstration de sécurité simplifiée locale

Si le PSCA/D n'est que concerné par le changement, il réalise une démonstration de sécurité simplifiée locale (DSSL), dont le format et le guide de rédaction sont proposés en annexe 4, sans notification auprès du DirCAM. La transmission par le bureau exécutif permanent des

informations relatives au changement ASM temporaire vaut notification du changement considéré.

VII.4. MODALITÉS ET DURÉE D'ARCHIVAGE

Lorsque le PSCA/D réalise une étude de sécurité, celle-ci est archivée conformément aux procédures de son SMS, de sorte que l'intégralité du cycle de vie du changement ASM permanent soit couverte.

Dans le cas des changements ASM temporaires, les démonstrations de sécurité réalisées (études de sécurité ou DSSL) ne sont valables que pour la durée de mise en œuvre prévue pour le changement. Il appartient à chaque PSCA/D de définir les modalités de conservation et la durée d'archivage après la fin du changement ASM concerné. La durée minimale de conservation des DSSL préconisée par la DSAC est de **18 mois** après la fin du changement considéré. Afin de permettre la surveillance *a posteriori*, il est préconisé que les unités conservent leurs DSSL de l'année calendaire en cours, ainsi que celles des deux années précédentes.

Page intentionnellement blanche

TITRE VIII

TYPES D'ÉTUDES POSSIBLES

VIII.1. DOSSIER DE SÉCURITÉ

Le dossier de sécurité est un outil polyvalent apte à couvrir la démonstration de sécurité pour tout type de changement. Il peut être une étude unique ou un ensemble de sous-études.

Le contenu d'un dossier de sécurité est fixé lors de la réunion de lancement. Les préconisations relatives au dossier de sécurité sont définies en annexe 1.

VIII.2. ÉTUDE PRESTATAIRE D'IMPACT SUR LA SÉCURITE (EPIS)

Faute, actuellement, d'avoir pu établir un modèle d'EPIS pour les changements non-ATS, ce paragraphe ne concerne que les changements ATS.

Lors de l'évaluation sommaire, le PSCA/D peut identifier que l'étude de sécurité associée au changement ne comporte pas de difficulté particulière. Dans ce cas, il peut utiliser l'EPIS, y compris si le changement justifie d'un classement « suivi ».

Le canevas de ce formulaire garantit une approche globale, simplifiée et pragmatique du processus démonstration de sécurité. Le retour d'expérience montre que cet outil permet de réaliser la plupart des démonstrations de sécurité.

Le formulaire utilisable par les unités est celui qui est fourni par le prestataire dans son SMS ayant fait l'objet d'une décision d'approbation du DirCAM.

Un modèle d'EPIS est préconisé en annexe 2.

VIII.3. PROCÉDURES PARTICULIÈRES

VIII.3.1. Étude générique

Lorsque qu'un changement se répète avec des éléments caractéristiques suffisamment stables sur plusieurs sites, le PSNA/D peut décider de recourir à une étude générique, « modèle » à décliner et à adapter sur chaque site.

Lorsqu'un PSNA/D utilise une étude générique, chaque site devra la compléter en prenant en compte ses spécificités locales et vérifier les éléments relatifs à :

- l'inscription du changement dans le cadre défini par l'étude générique ;
- le contexte opérationnel et les interfaces ;
- pour une étude de sécurité :
    - l'applicabilité des ER identifiés dans l'étude générique ;
    - la nécessité d'adapter la liste des ER ;
    - la pertinence et l'exhaustivité des causes des ER identifiés ;
    - l'applicabilité, la pertinence et l'exhaustivité des MRR ;
- pour une étude sur le soutien à la sécurité :
    - la cohérence des architectures locale vis-à-vis de celle définie dans l'étude générique ;
    - l'existence d'équipements locaux pouvant justifier de performances attendues différentes (généralement moindre) que celles définies dans l'étude générique ;
- l'applicabilité et l'analyse des exigences de sécurité ;
- l'analyse des phases de transition et les moyens d'assurance sécurité.

La partie « évaluation de la sécurité » (les preuves) et la mise en œuvre de l'assurance sécurité sont à réaliser obligatoirement lors de la déclinaison locale.

En tout état de cause, le PSNA/D qui souhaite recourir à une étude générique doit, préalablement à la notification de changement, coordonner avec la DIRCAM/SDSA/DSS.

VIII.3.2. Méthodologie d'intervention sur les systèmes opérationnels (MISO)

La méthodologie d'intervention sur les systèmes opérationnels est une procédure de maîtrise des risques permettant de coordonner, entre les différents intervenants, des interventions programmées qu'on ne peut qualifier de changement. À ce titre, les interventions en question ne sont pas notifiées au DirCAM.

La MISO n'est pas une démonstration de sécurité et ne peut pas couvrir un changement à elle seule.

La MISO doit aider le responsable de l'intervention à évaluer rapidement et le plus objectivement possible les risques sur les services de la gestion du trafic aérien et les contraintes associées à cette intervention. En identifiant les MRR à mettre en œuvre, tant du point de vue technique qu'en termes d'exploitation, la MISO permet de préparer l'opération.

Les interventions programmées peuvent avoir pour origine :

- un PSNA/D : intervention sur les équipements effectuée par un organisme PSCNS/D ayant un impact (ou susceptible d'avoir un impact) sur les services de la circulation aérienne. Dans ce cas, l'unité concernée du PSCNS/D initie le formulaire MISO et évalue l'impact de cette intervention avec le(s) organisme(s) du PSCA/D concerné(s) ;
- un prestataire extérieur (fournisseur d'énergie, personnel d'entretien de la plate-forme, etc.) : intervention sur un service support ayant un impact (ou susceptible d'avoir un impact) sur les services de la circulation aérienne. Dans ce cas, l'organisme du PSNA/D concerné initie le formulaire MISO et évalue, en lien avec le prestataire extérieur et le(s) organisme(s) du PSCA/D concerné(s), l'impact de cette intervention. Si l'intervention relève d'une opération plus vaste ayant une incidence dépassant le cadre local (*par exemple, la mise à jour au niveau régional des équipements de l'opérateur de téléphonie*), il s'avère généralement impossible d'adapter le créneau d'intervention à l'activité aéronautique. Dans ce cas, la MISO permet d'informer l'organisme PSCA/D qu'il doit prendre les mesures pertinentes pour garantir un risque maîtrisé.

La MISO peut également constituer un des éléments d'un dossier de sécurité. Cette procédure est particulièrement indiquée pour couvrir des phases transitoires afférentes aux travaux de déploiement ou à toute intervention ne constituant pas un changement en soi. Dans ce cadre, les installations de « patchs » logiciels correctifs peuvent être encadrées par une MISO, sous réserve qu'ils n'introduisent pas de nouvelles fonctionnalités au système considéré.

Une modification du paramétrage d'un système peut être encadrée par une MISO si cette opération s'inscrit dans une enveloppe définie au préalable par une démonstration de sécurité.

Afin de faciliter la compréhension de l'impact de l'opération, une MISO sera réalisée conjointement entre toutes les parties impliquées avec un préavis jugé suffisant par les différents PSNA/D. Les modalités particulières dans ce cadre doivent être définies au titre des relations formelles.

Suivant le type d'intervention, les formulaires ci-après sont utilisés par le(s) PSNA/D :

- la MISO spécifique, pour des opérations uniques ;
- la MISO répétitive, pour les opérations à caractère périodique (maintenance préventive, entretien des zones herbeuses, etc.). Celle-ci dispose d'une date de validité au-delà de laquelle le PSNA/D devra reconsidérer tous les éléments du document et, le cas échéant, les mettre à jour. Cette limite est fixée par le PSNA/D en fonction de sa connaissance du système et ne pourra pas excéder 5 ans.

Dans le cas de MISO répétitives, il pourra être fait référence à une MISO spécifique précédemment réalisée. Cependant, le PSNA/D devra pouvoir prouver que les caractéristiques de l'intervention programmée sont stables par rapport à la MISO de référence.

Des formulaires de MISO spécifique et répétitive sont présentés en annexe 3.

Cas particulier des maintenances programmées :

Dans le cas d'un système ancien, en l'absence de démonstration de sécurité globale, il est préconisé de réaliser des MISO pour toutes les maintenances programmées.

Dans le cas d'un nouveau système, il est indispensable de prendre en compte le concept de maintenance dans la démonstration de sécurité, afin qu'elles ne soient pas considérées comme un changement et puissent être traitées au travers de MISO.

Dans le cas où un organisme doute sur le fait qu'une intervention soit un changement ATM ou pas, le PSNA/D s'adresse par courriel à la DIRCAM en précisant les points clés (le formulaire de notification peut être utilisé en support). La DIRCAM statuera alors aux vues des éléments présentés par le prestataire.

VIII.3.3. Démonstration de sécurité simplifiée locale (DSSL)

Voir titre VII.

ANNEXE 1

SUR LE DOSSIER DE SÉCURITÉ

1. CONTENU DU DOSSIER DE SÉCURITÉ

Un dossier de sécurité contient toujours les items suivants :

- description du système et de ses fonctions ;
- description du changement, de son périmètre, de ses limites et des éventuels interfaces ;
- pour un changement ATS, détermination des évènements redoutés , de leurs effets, de la gravité associée et déclinaison des objectifs de sécurité associés à chaque évènement redouté ;

  ou

  pour un changement non ATS, définition des spécifications du système ;
- déclinaison des objectifs de sécurité ou des spécifications du système en exigences de sécurité ;
- vérification de la tenue des exigences et, pour un changement ATS, des objectifs de sécurité ;
- pour un changement non-ATS, vérification des spécifications du système ;
- pour un changement ATS, vérification de l'acceptabilité du risque ;
- assurance relative à l'ensemble de ces éléments.

2. MODÈLE DE DOSSIER DE SÉCURITÉ

Rédaction réservée

ANNEXE 2

MODÈLE D'EPIS

Le présent modèle n'est utilisable
que pour une démonstration de sécurité associée à un changement ATS
(Étude de sécurité)

Le modèle préconisé ne présente que les grands principes. Le PSCA/D souhaitant l'utiliser doit préalablement se l'approprier en l'adaptant à son besoin (entête à son effigie, etc.).

Les annotations en bleu sont des indications afin d'aider le rédacteur et doivent disparaitre dans la version finale de l'EPIS.

A – TITRE DE L'EPIS	*Telle que dans la notification et la décision DIRCAM*
Référence DIRCAM	
Centre(s) bénéficiaire(s) du changement	
Autre(s) PSNA/D concerné(s)	
PSCNS/D concerné(s)	
Entité(s) non prestataires(s) concernée(s)	

A.1 – Suivi du document

Version	Date	Modifications	Chapitre / page	Auteur
V1		Version initiale	Tout le document	
V2		*MRR PRO 1*	*ER1 et partie L2*	

B – DESCRIPTION *(du changement objet de l'EPIS)*

B.1 – Particularités

EPIS associée à une étude sur le soutien à la sécurité ☐ Oui ☐ Non

Changement « suivi » ☐ Oui ☐ Non

B.2 – Date et durée du changement

☐ Permanente, à compter du :

☐ Temporaire, du (mise en service) : au (retrait du service) :

B.3 – Localisation du changement

Sites, organisme de rattachement opérationnel, organisme de rattachement organique/soutien.

B.4 – Description du changement

Le niveau de détail est modulé en fonction de l'ampleur du changement et de ses spécificités. Cette description doit permettre aux lecteurs d'appréhender le changement, ses tenants et ses aboutissants.

C – PERIMETRE DE L'ETUDE DE SECURITE

Compte-rendu de brainstorming annexé ☐ Oui ☐ Non

Le périmètre de l'étude de sécurité est en premier lieu défini par l'impact du changement dans l'environnement ou dans l'exploitation. Les systèmes, sous-systèmes ou fonctionnalités qui sont concernés par le changement doivent être précisés ici. Il est important de bien stipuler si le changement implique l'introduction, la modification ou le retrait d'un système.

Il convient également d'indiquer dans cette partie si une démonstration de sécurité a déjà été réalisée en amont du changement limitant ainsi le périmètre de la présente étude.

C.1 – Hypothèse(s) de travail

Une hypothèse de travail est un postulat de base établi ou éventuel en amont du changement. Elle est à la base de la démonstration de sécurité. Remarque : une hypothèse peut devenir une exigence de sécurité et être traitée comme telle. Elle peut également devenir une recommandation ou une remarque faite au prestataire.

Exemple dans le cadre du changement « Utiliser la poursuite multi-radars sans le radar local » : l'intégration des radars qui composent la poursuite multi-radars doit avoir fait l'objet d'une étude sur le soutien à la sécurité. Ceci est un préalable avant la mise en service du changement.

C.2 – Evènement(s) redouté(s) non pris en compte dans l'étude

Certains ER identifiés au premier abord (ou issus d'une étude de sécurité générique) peuvent par la suite être écartés de l'étude de sécurité s'ils ne sont pas applicables selon le périmètre défini. Cet encart permet de justifier la non prise en compte de ces ER.

C.3 – EPIS associée à une étude sur le soutien à la sécurité ☐ Oui ☐ Non

Préciser les points clés de l'étude sur le soutien à la sécurité, en particulier les conclusions sur les performances du système.

C.4 – Présence de phase(s) de transition ☐ Oui ☐ Non

Description des phases	Formalisme	Résultat(s) attendu(s)
Tests sur site	*Revue d'aptitude opérationnelle (RAO)*	*Rapport(s) de tests*
Phase d'expérimentation	*Note d'expérimentation*	*C/R d'expérimentation*
Phase de transition	*EPIS*	*Conclusions d'acceptabilité*
Phase miroir	*EPIS*	*Conclusions d'acceptabilité*
Transition sur système OPS	*MISO*	*…*
Retrait de service de l'ancien système	*…*	*…*

C.5 – Conditions de retour en arrière

☐ Sans objet ☐ Retour simple ☐ Retour avec précautions
☐ Retour compliqué ☐ Retour impossible

Justifications :

C.6 – Éléments particuliers

☐ Impact sur PCU et/ou PFU

☐ Modification de documentation aéronautique (si coché DIRCAM/DIA destinataire de l'EPIS)

☐ Autre(s) élément(s) particulier(s) : ……

D – DOCUMENTS LIÉS A L'ETUDE

Titre	Référence du document	Annexé
CR de brainstorming	*L'absence de CR de brainstorming devra être justifiée*	☐ Oui ☐ Non
Étude sur le soutien à la sécurité		☐ Oui ☐ Non
Autre EPIS, MISO, document chapeau de l'étude, …		☐ Oui ☐ Non
Assurance logicielle, tests, complément à l'EPIS, dossier de sécurité		☐ Oui ☐ Non
Etude sur le soutien à la sécurité		☐ Oui ☐ Non

E – SYNTHÈSE DE L'ETUDE	
Zone de risque la plus élevée liée au changement :	☐ **Acceptable** ☐ **Acceptable sous conditions** ☐ **Tolérable sous conditions et réservés aux aéronefs d'État**

Acceptabilité du risque :

Dans ce cadre, qui doit résumer la démonstration de sécurité pour les signataires de l'étude, doivent être listés tous les éléments permettant de justifier de l'acceptabilité du risque identifié pour le changement considéré.

Le périmètre restreint du changement peut être un critère permettant de montrer que les interactions éventuelles avec d'autres systèmes n'engendrent pas de risque supplémentaire. Le nombre de fonctionnalités (ajout, modification, retrait) concernées par le changement constitue également un bon indicateur pour justifier de l'acceptabilité du risque. Les moyens en réduction de risque (MRR) doivent être pertinents vis-à-vis des évènements redoutés identifiés. Dans cette optique, leur efficacité dans le temps doit être évaluée et une trop faible durabilité pour certains MRR pourrait remettre en cause l'acceptabilité du risque.

Dans le cas où le risque est jugé inacceptable, le changement ne peut être mis en service et le processus d'évaluation et d'atténuation du risque doit être réitéré.

Dans le cas où le risque est acceptable sous conditions, celles-ci doivent être décrites ici. Si le périmètre du changement devient acceptable s'il est réservé aux aéronefs d'état, la mesure permettant cette distinction sera mise en exergue.

F – CIRCUIT DE SIGNATURE			
	Nom	**Fonction**	**Date – Signature**
Rédacteur			
Coordonnateur TECH			*Dans le cadre d'une étude rattachée à un dossier de soutien à la sécurité*
Coordonnateur OPS			*Dans le cadre d'une étude impactant d'autres prestataires ou parties prenantes*
Partie prenante			*Le cas échéant*
Vérificateur			
Approbateur			*Uniquement si changement « non suivi »*
Pour un changement « suivi », approbation DirCAM			*Date et signature ou référence du document d'acceptation du DirCAM*

Autorité d'acceptation
Pour le PSCA/D : Grade, Nom : Fonction : Date : Signature : *Signature ou référence du document d'acceptation*

G – DIFFUSION POUR ACTION		
Organisme	**Fonction (PSNA/D, Autres)**	**Correspondant (facultatif)**

H – DIFFUSION POUR INFORMATION		
Organisme	**Fonction (PSNA/D, Autres)**	**Correspondant (facultatif)**

I – CRITÈRES D'ACCEPTABILITÉ DE L'INSTRUCTION 4150/DSAÉ/DIRCAM					
I.1 – Grille de gravité					
Niveau de gravité	**1 Accident**	**2 Grave**	**3 Majeure**	**4 Mineure**	**5 Négligeable**
Conséquences possibles d'un événement sur les personnes	Nombreux morts	Un mort et/ou de nombreux blessés	Quelques blessés graves	Un blessé grave et/ou des blessés légers	Éventuellement un blessé léger
Conséquences possibles d'un événement sur les équipements	Destruction équipement(s)	Équipement(s) gravement endommagé(s)	Dommages majeurs sur plusieurs sous-ensembles	Dommages mineurs sur un ou plusieurs sous-ensemble(s)	Éventuelles vérifications de bon fonctionnement
Conséquences possibles d'un événement sur la mission	Échec de la mission	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	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	La mission peut se dérouler grâce à des adaptations de circonstance. L'effet recherché est globalement atteint	La mission ne s'est pas vraiment déroulée dans les conditions prévues mais est un succès

I.2 – Grille d'occurrence					
	Très fréquente	**Fréquente**	**Occasionnelle**	**Rare**	**Extrêmement rare**
Définition quantitative	> 10^{-4}/heure	< 10^{-4}/heure	< 10^{-5}/heure	< 10^{-6}/heure	< 10^{-8}/heure
Définition qualitative	Peut se produire plusieurs fois par mois dans l'organisme	Peut se produire plusieurs fois par an dans l'organisme	Peut se produire une à deux fois par an dans l'organisme	Peut se produire une fois tous les 5 à 10 ans dans l'organisme	Ne s'est jamais produit à la connaissance de l'organisme

I.3 – Matrice d'acceptabilité du risque

		Occurrence				
		Très fréquente	Fréquente	Occasionnelle	Rare	Extrêmement rare
Gravité	1. Accident	A	A	A	B	C
	2. Grave	A	A	B	C	C
	3. Majeure	A	B	C	C	D
	4. Mineure	B	C	C	D	D
	5. Négligeable	C	C	D	D	D

A	Risque inacceptable en l'état.
B	Risque tolérable sous conditions – Réservé exclusivement aux aéronefs d'État et après décision formelle de l'autorité désignée ou ordonnant la mission (exemple : CNOA)
C	Risque acceptable sous conditions ou la situation nécessite la mise en place d'une atténuation des risques et, si possible, d'indicateurs pertinents afin d'identifier une potentielle dérive.
D	Risque acceptable.

J – ANALYSE DÉTAILLÉE

Liste des évènements redoutés (ER) :

N° des ER	Libellé des ER
ER 01	*Identification de l'ER*
ER 02	*Identification de l'ER*

Faire autant de fiches que d'événements redoutés

ER 01				
Libellé de l'ER :				
Description détaillée des causes potentielles de l'ER				
Description détaillée des effets potentiels de l'ER				
Niveau de gravité INITIAL HORS moyens en réduction de risque (MRR) de protection				
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Description détaillée de l'évènement redouté et justification de la gravité initiale				
Utiliser la notion de pire cas crédible (WCC)				
MRR de PROTECTION immédiats				
Si l'analyse montre que des moyens de protection immédiats sont possibles, les indiquer ici ; sinon, passer directement aux objectifs de sécurité. **MRR PRO 01** : **MRR PRO 02** :				
Justifications / Explications sur l'efficacité durable des MRR				
Niveau de gravité CORRIGÉ en tenant compte des MRR de protection immédiats				
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Objectif de sécurité :	***Occurrence occasionnelle / <10^{-5}/heure*** *(l'objectif de sécurité correspond, pour une sévérité donnée, à la probabilité maximum permettant de placer l'événement dans la zone « C » de risque modéré sous conditions)*			

Probabilité *a priori*

Placer l'ER dans la matrice en fonction du niveau de sécurité corrigé et de la probabilité estimée de la survenue de l'ER

		Occurrence				
		Très fréquente	Fréquente	Occasionnelle	Rare	Extrêmement rare
Gravité	1. Accident					
	2. Grave					
	3. Majeure					
	4. Mineure					
	5. Négligeable					

Justification sur la probabilité estimée de survenue de l'ER

Moyens en réduction des risques (MRR) de <u>PRÉVENTION</u>
(obligatoires si l'ER se situe en dehors de la zone verte)

Si aucun MRR de prévention n'est identifié, l'objectif de sécurité devient donc la probabilité maximum permettant, pour une sévérité donnée, d'être en zone « D » acceptable sans conditions.

MRR PREV 01 :

MRR PREV 02 :

Justifications / Explications sur l'efficacité durable des MRR

Justification sur l'efficacité des MRR à diminuer la probabilité de survenue de l'ER et de la tenue dans le temps de cette mesure.

Probabilité corrigée :	*Rare*

Exigences de sécurité liées aux MRR de prévention (et de protection le cas échéant)

ES 01 : *La formulation des exigences de sécurité doit permettre de garantir quelle sera valable dans le temps car ce sont les ES qui sont à suivre dans le temps.*

ES 02 :

K – ACCEPTABILITÉ DU RISQUE (APRÈS mise en œuvre des MRR)

(Reprendre tous les ER dans la matrice)

		Occurrence				
		Très fréquente	Fréquente	Occasionnelle	Rare	Extrêmement rare
Gravité	1.Accident					
	2.Grave					
	3.Majeure					
	4.Mineure					
	5.Négligeable					

Zone de risque la plus élevée liée au changement :	**D**	☐ **Acceptable**
	C	☐ **Acceptable sous conditions**
	B	☐ **Tolérable sous conditions et réservés aux aéronefs d'État**

L – ÉVALUATION DE LA SECURITE					
L.1 – Vérification des exigences associées aux hypothèses identifiées dans la partie C.1					
Id. de l'hypothèse	**Libellé de l'exigence**	**Exigence de sécurité**	**Vérification**	**Responsable de la mise en œuvre**	**Responsable au sein du PSNA/D**
H1	*L'opérateur dispose d'une console de repli offrant l'accès à toutes les fonctions nécessaires au contrôle et permettant la récupération au plus vite de tous les éléments perdus nécessaires pour rendre les services de la CA en cas de panne de sa console*	*Une console de repli offrant l'accès à toutes les fonctions nécessaires au contrôle et permettant la récupération au plus vite de tous les éléments perdus nécessaires pour rendre les services de la CA doit être disponible*	☐ Oui ☐ Non		*Chef de centre*
…					

L.2 – Garanties de sécurité associées aux MRR ***(Traçabilité des preuves relatives aux exigences de sécurité mise en place pour garantir l'efficacité des MRR)***						
Id. du MRR	**Libellé du MRR**	**ER**	**Exigence de sécurité**	**Preuve(s) associée(s)**	**Responsable de la mise en œuvre**	**Responsable au sein du PSNA/D**
PREV 01	*Mise en place d'un groupe électrogène*	*ER 01*	*Le système dispose d'un système électrique secours*	*Compte-rendu d'intervention de l'USID*	*USID*	*Chef de quart*

O – Assurance sécurité ***(maintien dans le temps de la tenue des objectifs de sécurité associés au changement)***	
Moyens mis en œuvre	**Périodicité (si besoin)**
Indicateurs de sécurité spécifiques	
Réunions périodiques	
FNE *Les éléments de sortie du processus prestataire d'analyse des évènements d'une FNE*	
A minima : *Le centre de contrôle assurera un suivi de l'occurrence de la survenue des ER pendant x mois afin de vérifier la pertinence et l'efficacité des MRR*	*Mensuelle*
☐ Un bilan de sécurité sera envisagé par le prestataire à l'échéance suivante : **.....** Périodicité : **.....**	
☐ Un bilan de sécurité est imposé par le DirCAM ☐ Non ☐ Oui Date : **.....**	

ANNEXE 3

MISO MULTI-PRESTATAIRES

Cette procédure a été créée par un groupe de travail dont le mandat était d'élaborer une méthodologie d'intervention sur les systèmes opérationnels (MISO) simplifiée, unique et commune à la Défense.

Cette procédure MISO commune à l'ensemble des PSNA/D, constituée d'un formulaire autoporteur, est approuvé par le DirCAM conformément au règlement [RE373].

L'introduction ou la modification, par un PSNA/D, d'une procédure de type MISO dans son système de management de la sécurité, devra être soumise au DirCAM pour approbation en préalable à sa mise en œuvre.

Ce formulaire MISO, commun à tous les PSNA/D, permet une uniformisation du recueil des informations concernant chaque intervention. Il doit aider le responsable d'une intervention programmée sur un système opérationnel à évaluer rapidement et le plus objectivement possible :

- les risques opérationnels sur les services de la gestion du trafic aérien ;
- les contraintes associées.

L'identification des moyens en réduction de risque (techniques, humains, procédures, exploitation) à mettre en œuvre permet la préparation de l'opération.

LOGO PSNA/D	**MISO – PSNA/D** (Méthodologie d'intervention sur les systèmes opérationnels)				
RÉFÉRENCE **(Propre à l'unité du PSNA/D)**	*PSNA/D-ANNÉE-CENTRE-N°ORDRE* *Exemple : DIRISI-2017-MDM-15*				**SPÉCIFIQUE**
TITRE INTERVENTION	*Remplacement d'un équipement actif de réseau.*				
LIEU	*BA XXX – BAN XXXXXXXX – X RHC*				
DATE DE L'INTERVENTION	*JJ/MM/AAAA*	**HEURE Z DE DÉBUT DE L'INTERVENTION**	*XXHXX Z*	**DURÉE PRÉVUE**	*(j, h, min)*
DESCRIPTIF	*Remplacement du chiffreur*				
RÉFÉRENCE EPIS EXISTANTE	*EPIS PSNA/D AAAA-XX*				
RÉFÉRENCES DOCUMENTAIRES APPLICABLES	*Fiche réflexe, message NeMO, OP SIC, n° PFE, n° FAI*				

CONTRAINTES	**REPORT POSSIBLE**	***OUI*** ☐ ***NON*** ☐	*Si NON justification*	*Exemple 1 : Intervention d'un prestataire extérieur à la Défense sans clause SMS.* *Exemple 2 : Décalage du chantier relatif à l'implantation de la nouvelle tour de contrôle.* *Exemple 3 : Moyen inutilisable (hors calibration).*
	INFORMATIONS COMPLÉMENTAIRES	*Exemple 1 : Possibilité de report de l'heure d'intervention.*		
	RETOUR EN ARRIERE	***OUI*** ☐ ***NON*** ☐	*Si NON justification*	*Exemple : La fibre optique étant coupée l'opération doit continuer.*

SYSTEMES CONCERNÉS	*Radio (centre), Radars (X, Y), Téléphonie (MTBA, RDTM, RIAM), Interphonie, Messagerie aéro, …*

ORGANISMES CONCERNÉS	**NOMS DES ORGANISMES**	**IDENTITÉ DU POINT DE CONTACT**	**N° TÉLÉPHONE**
	ESCA XXXXX	*XXXXXX*	*XX XXX*
	CIRISI YYYYY	*YYYYYY*	*YY YYY*
	PRESTATAIRE EXTERIEUR Z	*ZZZZZZ*	*ZZ ZZ ZZ ZZ ZZ*

ACTIONS CHRONOLOGIQUES DE L'INTERVENTION	**CONSÉQUENCES TECHNIQUES**
Coupure de l'énergie primaire.	*Perte des liaisons radar XXX, téléphonie YYY, interphonie ZZZ.*
Remplacement du chiffreur.	*Perte des liaisons radar XXX, téléphonie YYY, interphonie ZZZ.*
Redémarrage des équipements + tests.	*Retour à la normale.*

ALÉAS TECHNIQUES POTENTIELS POUR L'EXPLOITATION (pendant l'intervention) *Cette rubrique permet au contrôleur de connaitre les systèmes qui pourraient être concernés si l'intervention se passe mal, comme une coupure totale de l'énergie dans la pièce ou se déroule l'intervention.*
Perte du radar local.
Perte du réseau téléphonie secours.

ÉVALUATION ET ATTÉNUATION DES RISQUES DU PSCA/D

CONSÉQUENCES TECHNIQUES	EFFETS OPÉRATIONNELS (EO)
Perte des liaisons radar.	*EO1 : Capacité de contrôle limitée (secteur interdit), augmentation A/HMSR, …*
Perte de la téléphonie normale avec le centre YYY. *Perte de la téléphonie normale avec tous les centres.*	*EO2 : Liaison avec le centre YYY uniquement en secours.* *EO3 : Liaison avec tous les centres uniquement en secours.*
Interphonie ZZZ.	*Sans impact immédiat ou* *EO3 : Perte moyen de coordination si couplé avec la perte de la téléphonie.*

EFFETS OPÉRATIONNELS (EO)	MESURES PALLIATIVES (MP)
EO1	*MP01 : Vérification du planning de maintenance du radar local, édition d'un NOTAM, information des contrôleurs (OJ).*
EO2	*MP02 : Vérification des numéros, tests, information du centre YYY, information des contrôleurs (OJ) ou créneau sans activité à coordonner ou fermeture du centre (NOTAM).*
EO3	*MP03 : Créneau sans activité à coordonner ou fermeture du centre (NOTAM).*

Rédaction optionnelle si les mesures palliatives sont suffisantes pour que l'intervention se déroule sans risques particuliers	
ALÉAS TECHNIQUES POTENTIELS POUR L'EXPLOITATION (pendant l'intervention) *Permet au contrôleur de reprendre les aléas techniques communiqués par le technicien et/ou de les compléter.*	**ÉVÉNEMENTS REDOUTÉS INDUITS (ER)**
Perte du radar local.	*ER01 : Perte de la situation aérienne.*
Perte du réseau téléphonie secours.	*ER02 : Impossibilité de contacter l'organisme YYY.*
…	*ER03 : Non connaissance par un usager de la fermeture du centre.*

MOYENS EN RÉDUCTION DE RISQUE DE PRÉVENTION – MRR s'appliquant avant la survenue de l'ER		
N° ER	N° MRR	LIBELLÉ DU MRR (technique ou opérationnel)
ER01	*PREV01*	*Guidage / contrôle au plus près des trajectoires publiées.*
ER01	*PREV02*	*Augmentation de la marge de séparation.*
ER02	*PREV03*	*Avertir le centre YYY de la perte de la téléphonie normale.*
ER03	*PREV04*	*Edition d'un NOTAM.*
MOYENS EN RÉDUCTION DE RISQUE DE PROTECTION – MRR s'appliquant après la survenue de l'ER		
N° ER	N° MRR	LIBELLÉ DU MRR
ER01	*PROT01*	*Passage à vue (en fonction de la météo).*
ER01	*PROT02*	*Passage en contrôle sans radar.*
ER01	*PROT03*	*Avertir les centres adjacents de la régulation du trafic sans radar.*
ER02	*PROT04*	*Contacter un autre centre pour informer le centre YYY de la perte totale de la téléphonie.*
ER03	*PROT05*	*Message spécifique sur le RAIZ.*

EXIGENCES DE SÉCURITÉ – Actions à réaliser pour garantir la mise en œuvre des MP ou MRR			
N° MP ou MRR	N° ES	LIBELLÉ DE L'EXIGENCE DE SÉCURITÉ	RESPONSABLE
MP01	*ES MP11*	*Limitation de la capacité de contrôle (OJ, NOTAM).*	*ESCA*
	ES MP12	*Calcul A/HMSR, diffusion des OJ.*	*ESCA*
MP02	*ES MP21*	*Vérification de la ligne secours avant le créneau de maintenance.*	*ESCA*
MP03	*ES MP31*	*Diffusion de la fermeture par NOTAM (CNOA, escadrons, …).*	*ESCA*
PREV01-PREV02	*ES PREV11*	*Information des contrôleurs sur les procédures à utiliser (OJ).*	*ESCA*
PREV03	*ES PREV31*	*Informer le centre YYY lors du test de la ligne secours.*	*ESCA*
…	*…*	*…*	*…*
MPxx	*ES MPx1*	*Le CIRISI informera le chef de quart XX minutes avant le début de l'intervention.*	*CIRISI*
	ES MPx2	*Le CIRISI informera le chef de quart du retour à la normale.*	*CIRISI*

RÉDACTEUR PSCNS/D	**RÉDACTEUR PSCA/D**
GRADE *XXX* NOM *XXXXXXXXXX* FONCTION *XXXXXXXXXX* Date *JJ/MM/AAAA* Signature	GRADE *XXX* NOM *XXXXXXXXXX* FONCTION *XXXXXXXXXX* Date *JJ/MM/AAAA* Signature
APPROBATEUR PSCNS/D	**APPROBATEUR PSCA/D**
GRADE *XXX* NOM *XXXXXXXXXX* FONCTION *XXXXXXXXXX* Date *JJ/MM/AAAA* Signature	GRADE *XXX* NOM *XXXXXXXXXX* FONCTION *XXXXXXXXXX* Date *JJ/MM/AAAA* Signature

PRISE EN COMPTE DE L'INTERVENTION PAR LE PSCA/D

Observations

1. *Le chef de quart s'assurera de la mise en place de l'ensemble des moyens en réduction de risque à l'ouverture du terrain.*
2. *Rappeler à tout aéronef entrant en zone les limitations et les indisponibilités.*

GRADE *XXX* NOM *XXXXXXXXXX* Date *JJ/MM/AAAA*
FONCTION *XXXXXXXXXX* Signature

Page intentionnellement blanche

LOGO PSNA/D	**MISO – PSNA/D** **(Méthodologie d'intervention sur les systèmes opérationnels)**				
RÉFÉRENCE **(Propre à l'unité du PSNA/D)**	*PSNA/D-ANNÉE-CENTRE-N°ORDRE* *Exemple : DIRISI-2017-MDM-15*			**RÉPÉTITIVE**	
TITRE INTERVENTION	*Maintenance préventive et contrôle incendie abri SOCRATE*				
LIEU	*BA XXX – BAN XXXXXXXX – X RHC*				
DATE DE LA PREMIÈRE INTERVENTION	*JJ/MM/AAAA*	**HEURE Z DE DÉBUT DE LA PREMIÈRE INTERVENTION**	*XXHXX Z*	**DURÉE PRÉVUE**	*(j, h, min)*
DESCRIPTIF	*Maintenance semestrielle des équipements d'énergie et de climatisation avec décharge des batteries et contrôle des équipements de détection et d'extinction incendie avec test du coup de poing.*				
RÉFÉRENCE EPIS EXISTANTE	*EPIS DIRISI AAAA-XX*				
RÉFÉRENCES DOCUMENTAIRES APPLICABLES	*Fiche réflexe, message NeMO, OP SIC, n° PFE, n° FAI*				

DATE VALIDITÉ POUR MISO RÉPÉTITIVE (maxi *X* ans) *Ne peut pas dépasser 5 ans.*	*JJ/MM/AAAA*

SUIVI DU DOCUMENT

Version	Date	Modifications	Chapitre / Page	Auteur
1.0		*Version initiale*	*Toutes*	
2.0		*ER et MRR suite à l'analyse du FNE XX*	*Pages 2 et 3*	

CONTRAINTES	**REPORT POSSIBLE**	***OUI*** ☐ ***NON*** ☐	*Si NON* *justification*	*Exemple 1 : Intervention d'un prestataire extérieur à la Défense sans clause SMS.* *Exemple 2 : Décalage du chantier relatif à l'implantation de la nouvelle tour de contrôle.* *Exemple 3 : Moyen inutilisable (hors calibration).*
	INFORMATIONS COMPLÉMENTAIRES	*Exemple 1 : Possibilité de report de l'heure d'intervention.*		
	RETOUR EN ARRIÈRE	***OUI*** ☐ ***NON*** ☐	*Si NON* *justification*	*Exemple : La fibre optique étant coupée l'opération doit continuer.*

SYSTÈMES CONCERNÉS	*Radio (centre), Radars (X, Y), Téléphonie (MTBA, RDTM, RIAM), Interphonie, Messagerie aéro, ...*

ORGANISMES CONCERNÉS	**NOMS DES ORGANISMES**	**IDENTITÉ DU POINT DE CONTACT**	**N° TÉLÉPHONE**
	ESCA XXXXX	*XXXXXX*	*XX XXX*
	CIRISI YYYYY	*YYYYYY*	*YY YYY*
	PRESTATAIRE EXTÉRIEUR Z	*ZZZZZZ*	*ZZ ZZ ZZ ZZ ZZ*

ACTIONS CHRONOLOGIQUES DE L'INTERVENTION	**CONSÉQUENCES TECHNIQUES**
Coupure de l'énergie primaire, décharge des batteries.	*Perte des liaisons radar XXX, téléphonie YYY, interphonie ZZZ.*
Essai coup de poing et simulation incendie.	*Perte des liaisons radar XXX, téléphonie YYY, interphonie ZZZ.*
Redémarrage des équipements + tests.	*Retour à la normale.*

ALÉAS TECHNIQUES POTENTIELS POUR L'EXPLOITATION (pendant l'intervention)

Cette rubrique permet au contrôleur de connaitre les systèmes qui pourraient être concernés si l'intervention se passe mal, comme une coupure totale de l'énergie dans la pièce ou se déroule l'intervention.

Perte du radar local.
Perte du réseau téléphonie secours.

ÉVALUATION ET ATTÉNUATION DES RISQUES DU PSCA/D

CONSÉQUENCES TECHNIQUES	EFFETS OPÉRATIONNELS (EO)
Perte des liaisons radar.	*EO1 : Capacité de contrôle limitée (secteur interdit), augmentation A/HMSR, …*
Perte de la téléphonie normale avec le centre YYY. *Perte de la téléphonie normale avec tous les centres.*	*EO2 : Liaison avec le centre YYY uniquement en secours.* *EO3 : Liaison avec tous les centres uniquement en secours.*
Interphonie ZZZ.	*Sans impact immédiat ou* *EO3 : Perte moyen de coordination si couplé avec la perte de la téléphonie.*

EFFETS OPÉRATIONNELS (EO)	MESURES PALLIATIVES (MP)
EO1	*MP01 : Vérification du planning de maintenance du radar local, édition d'un NOTAM, information des contrôleurs (OJ).*
EO2	*MP02 : Vérification des numéros, tests, information du centre YYY, information des contrôleurs (OJ) ou créneau sans activité à coordonner ou fermeture du centre (NOTAM).*
EO3	*MP03 : Créneau sans activité à coordonner ou fermeture du centre (NOTAM).*

Rédaction optionnelle si les mesures palliatives sont suffisantes pour que l'intervention se déroule sans risques particuliers	
ALÉAS TECHNIQUES POTENTIELS POUR L'EXPLOITATION (pendant l'intervention) *Permet au contrôleur de reprendre les aléas techniques communiqués par le technicien et/ou de les compléter.*	**ÉVÉNEMENTS REDOUTÉS INDUITS (ER)**
Perte du radar local.	*ER01 : Perte de la situation aérienne.*
Perte du réseau téléphonie secours.	*ER02 : Impossibilité de contacter l'organisme YYY.*
…	*ER03 : Non connaissance par un usager de la fermeture du centre.*

MOYENS EN RÉDUCTION DE RISQUE DE PRÉVENTION – MRR s'appliquant avant la survenue de l'ER		
N° ER	N° MRR	LIBELLÉ DU MRR (technique ou opérationnel)
ER01	*PREV01*	*Guidage / contrôle au plus près des trajectoires publiées.*
ER01	*PREV02*	*Augmentation de la marge de séparation.*
ER02	*PREV03*	*Avertir le centre YYY de la perte de la téléphonie normale.*
ER03	*PREV04*	*Edition d'un NOTAM.*
MOYENS EN RÉDUCTION DE RISQUE DE PROTECTION – MRR s'appliquant après la survenue de l'ER		
N° ER	N° MRR	LIBELLÉ DU MRR
ER01	*PROT01*	*Passage à vue (en fonction de la météo).*
ER01	*PROT02*	*Passage en contrôle sans radar.*
ER01	*PROT03*	*Avertir les centres adjacents de la régulation du trafic sans radar.*
ER02	*PROT04*	*Contacter un autre centre pour informer le centre YYY de la perte totale de la téléphonie.*
ER03	*PROT05*	*Message spécifique sur le RAIZ.*

EXIGENCES DE SÉCURITÉ – Actions à réaliser pour garantir la mise en œuvre des MP ou MRR			
N° MP ou MRR	N° ES	LIBELLÉ DE L'EXIGENCE DE SÉCURITÉ	RESPONSABLE
MP01	*ES MP11*	*Limitation de la capacité de contrôle (OJ, NOTAM).*	*ESCA*
	ES MP12	*Calcul A/HMSR, diffusion des OJ.*	*ESCA*
MP02	*ES MP21*	*Vérification de la ligne secours avant le créneau de maintenance.*	*ESCA*
MP03	*ES MP31*	*Diffusion de la fermeture par NOTAM (CNOA, escadrons, …).*	*ESCA*
PREV01-PREV02	*ES PREV11*	*Information des contrôleurs sur les procédures à utiliser (OJ).*	*ESCA*
PREV03	*ES PREV31*	*Informer le centre YYY lors du test de la ligne secours.*	*ESCA*
…	*…*	*…*	*…*
MPxx	*ES MPx1*	*Le CIRISI informera le chef de quart XX minutes avant le début de l'intervention.*	*CIRISI*
	ES MPx2	*Le CIRISI informera le chef de quart du retour à la normale.*	*CIRISI*

RÉDACTEUR PSCNS/D	**RÉDACTEUR PSCA/D**
GRADE *XXX* NOM *XXXXXXXXXX* FONCTION *XXXXXXXXXX* Date *JJ/MM/AAAA* Signature	GRADE *XXX* NOM *XXXXXXXXXX* FONCTION *XXXXXXXXXX* Date *JJ/MM/AAAA* Signature
APPROBATEUR PSCNS/D	**APPROBATEUR PSCA/D**
GRADE *XXX* NOM *XXXXXXXXXX* FONCTION *XXXXXXXXXX* Date *JJ/MM/AAAA* Signature	GRADE *XXX* NOM *XXXXXXXXXX* FONCTION *XXXXXXXXXX* Date *JJ/MM/AAAA* Signature

PRISE EN COMPTE DE L'INTERVENTION PAR LE PSCA/D

Observations

1. *Le chef de quart s'assurera de la mise en place de l'ensemble des moyens en réduction du risque à l'ouverture du terrain.*
2. *Rappeler à tout aéronef entrant en zone les limitations et les indisponibilités.*

GRADE *XXX* NOM *XXXXXXXXXX* Date *JJ/MM/AAAA*
FONCTION *XXXXXXXXXX* Signature

PRISE EN COMPTE D'INTERVENTION POUR MISO RÉPÉTITIVE (AI)
A REMPLIR AVANT L'INTERVENTION

RÉFÉRENCE AI (Propre à l'unité du PSNA/D)	*PSNA/D-ANNÉE-CENTRE-N°ORDRE-N°D'INTERVENTION* *Exemple : DIRISI-2017-MDM-15-3*	**MISO VALABLE JUSQU'AU**	*JJ/MM/AAAA*
RAPPEL DESCRIPTIF DE L'INTERVENTION	*Maintenance semestrielle des équipements d'énergie et de climatisation avec décharge des batteries et contrôle des équipements de détection et d'extinction incendie avec test du coup de poing.*		
DATE DE LA NOUVELLE INTERVENTION	*JJ/MM/AAAA*		
HEURE Z DE DÉBUT DE LA NOUVELLE INTERVENTION	*XXHXX loc*		
DURÉE PRÉVUE	*(j, h, min)*		
Grade Nom Prénom du technicien devant réaliser l'intervention		**COORDONNÉES TÉLÉPHONIQUES**	
Grade Nom Prénom du responsable de l'organisme CA (chef de quart, chef OPS, etc.)		**DATE et SIGNATURE**	

PRISE EN COMPTE D'INTERVENTION POUR MISO RÉPÉTITIVE (AI)
A REMPLIR AVANT L'INTERVENTION

RÉFÉRENCE AI (Propre à l'unité du PSNA/D)	*PSNA/D-ANNÉE-CENTRE-N°ORDRE-N°D'INTERVENTION* *Exemple : DIRISI-2017-MDM-15-3*	**MISO VALABLE JUSQU'AU**	*JJ/MM/AAAA*
RAPPEL DESCRIPTIF DE L'INTERVENTION	*Maintenance semestrielle des équipements d'énergie et de climatisation avec décharge des batteries et contrôle des équipements de détection et d'extinction incendie avec test du coup de poing.*		
DATE DE LA NOUVELLE INTERVENTION	*JJ/MM/AAAA*		
HEURE Z DU DÉBUT DE LA NOUVELLE INTERVENTION	*XXHXX loc*		
DURÉE PRÉVUE	*(j, h, min)*		
Grade Nom Prénom du technicien devant réaliser l'intervention		**COORDONNÉES TÉLÉPHONIQUES**	
Grade Nom Prénom du responsable de l'organisme CA (chef de quart, chef OPS, etc.)		**DATE et SIGNATURE**	

ANNEXE 4

FORMULAIRE DSSL

1. FORMULAIRE DSSL

Cette annexe définit la procédure relative à la démonstration de sécurité simplifiée locale (DSSL). Elle est destinée à l'évaluation et à l'atténuation des risques pour les changements ASM temporaires. L'application de ce formulaire doit être conforme au SMS du prestataire.

Cette procédure a été créée par un groupe de travail civil et militaire dont le mandat était d'élaborer une méthodologie d'évaluation et d'atténuation des risques simplifiée. Le DirCAM préconise le formulaire donné ci-après.

La procédure DSSL, élaborée par le prestataire, doit recevoir l'acceptation formelle du DirCAM conformément au règlement [RE373]. Elle est donc intégrée uniquement à titre de recommandation dans cette instruction.

A. Changement concerné	[Titre du changement]
B. Référence de la DSSL	[DSSL_PSNA/D_N° du dossier de consultation du BEP]
C. Entité consultée	[CRNA, SNA, prestataire militaire, organisme militaire, …]

D. Impact sur la sécurité – Point de vue « navigation aérienne »				
D-i. Classes d'espace impactées et services de la CA rendus par le PSNA/D :	**A,C,D,E,G**	☐ **ALRT**	☐ **IV**	☐ **CTRL**
D-ii. Impact sur la sécurité dans le volume d'espace aérien où le prestataire rend les services de la CA ?			☐ **OUI**	☐ **NON**
D-iii. *Réponse négative – Justification* :				
D-iv. *Réponse positive – Description de l'impact* :				
D-v. *Moyens en réduction de risque (MRR) à mettre en œuvre pour rendre l'impact acceptable* : - [Publications aéronautiques] ? - [Modification du projet de changement ASM] ? - [Modification des créneaux proposés] ? - [Briefing / Formation contrôleur] ? - [Consignes opérationnelles temporaires] ? - [Ségrégation des activités] ? - [Information des usagers] ? - [Etablissement de protocoles ou de lettres d'accord] ? - […]				
D-vi. Impact jugé acceptable par le PSNA/D ? (sous réserve de la mise en œuvre des MRR)			☐ **OUI**	☐ **NON**
D-vii. *Signature de la DSSL* : [Nom / Fonction / Date / Signature]				

2. GUIDE DE RÉDACTION

En tête du formulaire

Le champ « mise à jour » permet de tracer la date de la dernière mise à jour de la DSSL effectuée par le PSNA/D.

Le champ « version » permet de tracer les évolutions de la DSSL. Ce champ ne correspond pas à la version du formulaire mais à la version de la DSSL en cours de réalisation ou réalisée par le PSNA/D.

« Changement concerné »

Renseigner ici le titre du changement « espace » qui fait l'objet de la DSSL. Ce titre doit, dans la mesure du possible, être le même que celui figurant dans le dossier de consultation envoyé par le BEP.

« Référence de la DSSL »

Créer ici une référence afin de pouvoir identifier la DSSL de manière unique. La référence peut être réalisée selon le modèle suivant : *DSSL_XXXX_####* où :

- « *XXXX* » est à remplacer par le nom du PSNA/D consulté ;

- « #### » est à remplacer par la référence du dossier de consultation du BEP (ou, à défaut, le numéro du bordereau d'envoi).

« Entité consultée »

Indiquer ici le nom de l'entité consultée qui réalise la DSSL.

« Impact sur la sécurité – Point de vue « navigation aérienne »

« Classes d'espace concernées et services de la CA rendus par le PSNA/D : »

Renseigner dans la première case les classes d'espace aérien impactées par le changement.

Cocher parmi les trois cases suivantes celles qui correspondent aux services de la circulation aérienne rendus par le PSNA/D qui remplit la DSSL.

ALRT = Service d'alerte.

IV = Service d'information de vol.

CTRL = Service de contrôle.

« Impact sur la sécurité dans le volume d'espace aérien où le prestataire rend les services de la circulation aérienne ? »

Analyser les éléments transmis dans la consultation du BEP et déterminer s'il existe ou non un impact sur la sécurité dans le volume d'espace aérien où le prestataire rend les services de la circulation aérienne. L'impact doit être évalué au regard des services rendus.

Cocher la case correspondante.

« Réponse négative – Justification : »

Renseigner cette case si une réponse négative a été donnée au champ D-ii.

Justifier ici brièvement l'absence d'impact sur la sécurité du changement « espace » dans le volume d'espace aérien où le prestataire rend les services de la circulation aérienne.

« Réponse positive – Description de l'impact : »

Renseigner cette case si une réponse positive a été donnée au champ D-ii.

Décrire ici l'impact identifié sur la sécurité dans le volume d'espace aérien où le prestataire rend les services de la circulation aérienne. L'impact doit être identifié et décrit au regard des services rendus (ou qui seront rendus) par le PSNA/D.

« Moyens en réduction de risque (MRR) à mettre en œuvre pour rendre l'impact acceptable : »

Renseigner cette case si une réponse positive a été donnée au champ D-ii.

S'il a été identifié un impact sur la sécurité dans le volume d'espace aérien où le prestataire rend les services de la circulation aérienne, mentionner ici les moyens en réduction de risque pris ou proposés par le PSNA/D dont la mise en œuvre est nécessaire afin de rendre cet impact acceptable par ce dernier.

Ces moyens en réduction de risque sont identifiés par le PSNA/D, néanmoins leur mise en œuvre peut ne pas se révéler du ressort de ce dernier. Le PSNA/D mentionne alors cette précision dans ce champ D-v.

« Impact jugé acceptable par le PSNA/D ? (sous réserve de la mise en œuvre des MRR) »

Renseigner cette case si une réponse positive a été donnée au champ D-ii.

Indiquer ici si l'impact identifié précédemment est considéré comme acceptable par le PSNA/D sous réserve que les moyens en réduction de risque mentionnés au champ D-v soient effectivement mis en œuvre.

Un avis favorable ou sans objection à la consultation du BEP ne peut être donné que si une réponse positive est renseignée dans le champ D-vi.

« Signature de la DSSL »

Indiquer ici la fonction et le nom de la personne signant la DSSL.

Dater et signer la DSSL.