Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DES ARMÉES

N°4150/DSAÉ/DIRCAM

RELATIVE

AU PROCESSUS DE SUPERVISION ET DE RÉALISATION DES DÉMONSTRATIONS DE SÉCURITÉ DES PRESTATAIRES DE SERVICES DE NAVIGATION AÉRIENNE DE LA DÉFENSE

La présente instruction entre en vigueur à compter du 1er octobre 2022.

Elle annule et remplace l'instruction n°4150/DSAÉ/DIRCAM du 21 avril 2020.

A Villacoublay, le **19 septembre 2022**

Le général de brigade aérienne Laurent THIEBAUT
directeur de la circulation aérienne militaire
ORIGINAL SIGNÉ

Page intentionnellement blanche

APPROBATION DU DOCUMENT

	Nom et qualité	Date et signature
Rédacteurs	LCL VISCONTI Chef de la division sécurité des systèmes CDT DHERS Division sécurité des systèmes CDT DUTILLOY Division sécurité des systèmes	**ORIGINAL SIGNÉ**
Vérificateur	CC THÉTIOT Division règlementation	**ORIGINAL SIGNÉ**
Vérificateur	COL CRÉACHCADEC Sous-directeur surveillance et audit	**ORIGINAL SIGNÉ**
Approbateur	GBA THIEBAUT Directeur de la circulation aérienne militaire	**ORIGINAL SIGNÉ**

DIFFUSION DE L'INSTRUCTION

Dans un souci d'économie, de préservation de l'environnement et de réactivité, la présente instruction n'est distribuée que sous forme électronique, elle est disponible sur INTRADEF à l'adresse :

« http://portail-dsae.intradef.gouv.fr/index.php/circulation-aerienne/ref-doc-dircam/instructions-cam »

SUIVI DES VERSIONS

Numéro version	Date	Objet du changement	Pages affectées par la modification
1.0	21 septembre 2006	Création IP 2650/DIRCAM.	Toutes.
2.0	27 janvier 2010	Refonte IP 2650 et création instruction 4150/DIRCAM.	Toutes.
3.0	15 mai 2013	Mise à jour de l'instruction.	Toutes.
4.0	15 juillet 2014	Mise à jour de l'instruction.	Toutes.
5.0	1er mars 2015	Mise à jour de l'instruction.	Voir traits dans la marge.
6.0	1er mai 2020	Refonte complète du document. Mise en conformité avec la réglementation européenne REG (UE) 2017/373.	Refonte totale de l'instruction.
6.1	1er août 2022	Mise à jour de l'instruction.	Voir traits dans la marge.

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.

La présente instruction décrit comment la DIRCAM s'assure de la conformité des prestataires de services de la navigation aérienne de la Défense (PSNA/D) vis-à-vis des exigences du règlement d'exécution (UE) 2017/373 du 1er mars 2017 en matière de gestion des changements.

Par cette instruction, le DirCAM assure également par ailleurs sa propre conformité vis-à-vis de ces règlements.

Les changements ATM/ANS initiés par un PSNA/D sont suivis par la DIRCAM au titre du protocole DSAC/DSAÉ [PRO MIXTE].

Cette instruction s'applique à la supervision des changements ATM/ANS par la DIRCAM vis-à-vis des PSNA/D. Elle est organisée en plusieurs thèmes :

- principes généraux des démonstrations de sécurité pour les services de navigation aérienne ;
- responsabilités ;
- modalités d'approbation des procédures utilisées par les PSNA/D ;
- méthodologies préconisées ;
- processus étude de sécurité Défense ;
- traitement des changements ASM[1] ;
- types d'études possibles ;
- formulaires utilisés par la DIRCAM ;
- formulaires préconisés par la DIRCAM à titre d'harmonisation des documents multi-prestataires.

Conformément au règlement d'exécution (UE) 2017/373 du 1er mars 2017, le processus de réalisation des démonstrations de sécurité décrit dans la présente instruction ne revêt un caractère obligatoire que pour les services rendus au profit de la CAG. Toutefois, si un PSNA/D souhaite évaluer et atténuer les risques pour les services rendus au profit de la CAM, il peut :

- appliquer le processus décrit au titre V de la présente instruction, notamment s'il pressent de potentielles interactions avec les services de la CAG ;
- procéder selon une procédure de sa convenance. Le cas échéant, il peut solliciter un conseil auprès de la DIRCAM/SDSA/DSS.

[1] Voir glossaire.

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 ;

[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 ;

[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
« Acceptation du changement » avant sa mise en œuvre		Accord formel du **prestataire de services de circulation aérienne** pour la mise en œuvre d'un changement. Cet accord ne porte que sur la sécurité du changement et n'a pas d'autre signification.
« Analyse fonctionnelle »		Étude consistant à définir et identifier les fonctions d'un système et leurs interactions, indépendamment de son architecture matérielle.
« Approbation »		Engagement de responsabilité sur le contenu de l'étude du DirCAM pour un changement classé « suivi » ou du (des) prestataire(s) pour un changement classé « non suivi ».
« 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[2] 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 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.

[2] Voir glossaire.

Terme	Source	Définition
« Évènement redouté »		Danger affectant la fourniture des services ATM[3], exprimé au plus près des opérateurs de première ligne. C'est un événement indésirable au regard des services attendus.
« 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[4]/D utilisant le système.
« 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.

[3] Voir glossaire.
[4] Voir glossaire.

Terme	Source	Définition
« Objectif de sécurité »		Un énoncé qualitatif ou quantitatif qui définit la fréquence ou la probabilité maximale d'apparition escomptée d'un danger. 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[5] 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 ce dernier, 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 la période allant de la mise en œuvre d'un changement à sa mise en service.
« Point limite de réception de l'étude »		Le PLRE correspond à la date limite à laquelle l'étude de sécurité doit être parvenue à la DIRCAM/SDSA/DSS afin qu'elle ait le temps d'examiner l'ensemble de la démonstration de sécurité et notamment de vérifier la tenue des exigences de sécurité au travers des preuves transmises.
« 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.

[5] Air Traffic Flow Management.

ABRÉVIATIONS

AC	Autorité Compétente
ADD	Arbre De Défaillance
ALAVIA	Commandement de la Force de l'Aéronautique Navale
AMDEC	Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité
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
BDF	Bloc Diagramme de Fiabilité
BMR	Bureau Maîtrise des Risques
CFA	Commandement des Forces Aériennes
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
DT	Dossier Technique
EASA	*European Aviation Safety Agency*
EMA	Etat-Major des Armées
EMx	Etat-Major d'Armée
ENAC	École Nationale de l'Aviation Civile
EPDP	Équipe PluriDisciplinaire de Programme
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/Défense
PSCA	Prestataire de Services de Circulation Aérienne
PSCA/D	Prestataire de Services de Circulation Aérienne/Défense
PSCNS	Prestataire de Services de Communication, Navigation, Surveillance
PSCNS/D	Prestataire de Services de Communication, Navigation, Surveillance/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

Page intentionnellement blanche

TITRE I

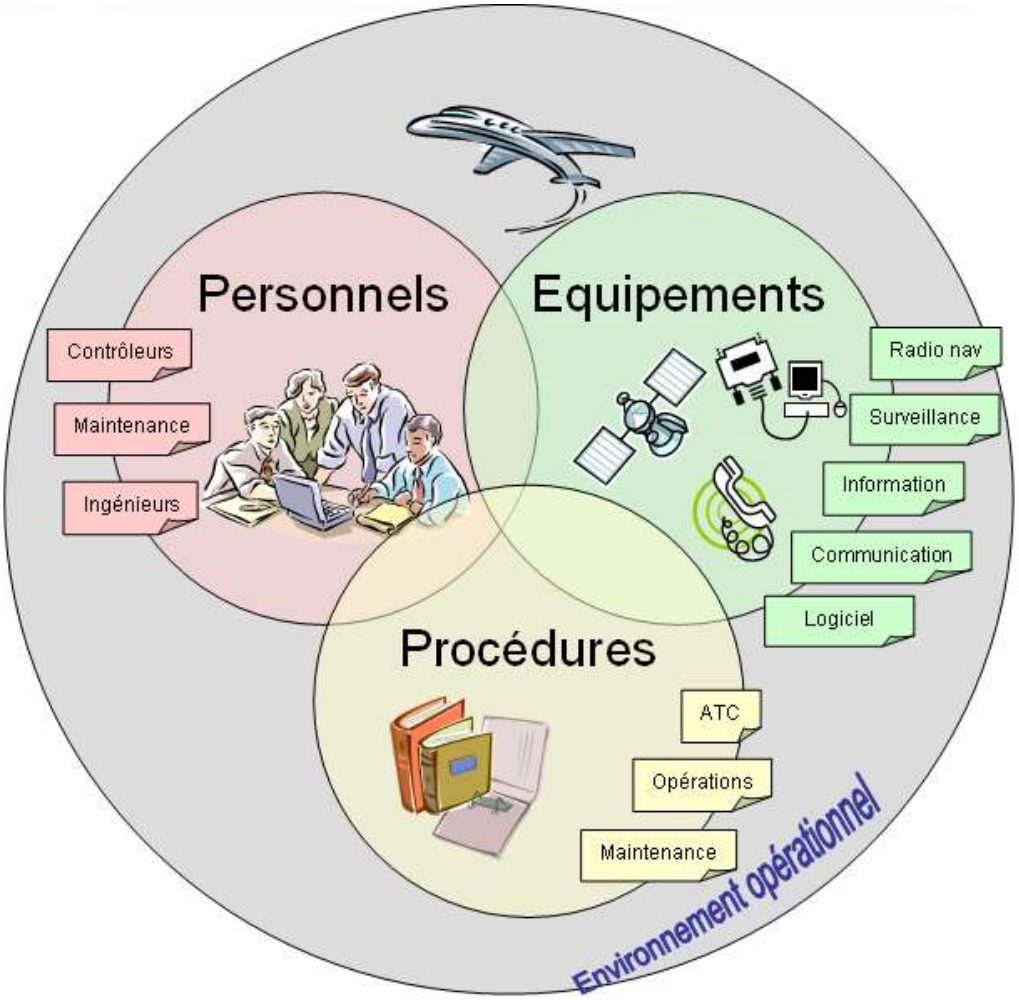
PRINCIPES GÉNÉRAUX D'UNE DÉMONSTRATION DE SÉCURITÉ

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 ;
- 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 NOTION DE CHANGEMENT

La réglementation prescrit qu'« *un prestataire de services utilise des procédures pour gérer, évaluer et, si nécessaire, atténuer l'incidence des changements apportés à ses systèmes fonctionnels* » sans toutefois donner la définition d'un changement. Dans ces conditions, la France, en accord avec les instances européennes, a énoncé sa définition d'un changement.

Un changement est lié à une action volontaire et anticipée d'un prestataire de services. Il peut avoir pour origine l'introduction d'un nouveau (sous-)système, mais également la modification ou le retrait de service d'un (sous-)système existant.

De plus, conformément au règlement [RE373], le changement :

- relève d'une initiative du prestataire de service ;
- découle d'une opération décidée par un autre prestataire ayant une incidence sur les services du prestataire de services.

Le processus de gestion des changements par les armées est l'objet de la présente instruction.

Conformément au règlement [RE373] le prestataire de services notifie tous les changements à l'autorité compétente.

I.3 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 du système 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 nécessaires à l'introduction du changement (phases de transition par exemple). 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, lorsqu'elle est menée par un prestataire de services de circulation aérienne (PSCA). On parle dans ce cas de changement ATS ;
- une étude sur le soutien à la sécurité, lorsqu'elle est menée par un prestataire de services autres que de circulation aérienne. 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* ».

Toute démonstration de sécurité doit être inscrite dans le cadre du SMS.

I.4 CLASSEMENT D'UN CHANGEMENT

Le règlement [RE373] prescrit que l'autorité compétente peut décider de procéder à l'examen et à l'approbation d'une démonstration de sécurité **préalablement** à la mise en œuvre du changement concerné. Dans ce cas, le changement sera classé « suivi ». Dans le cas contraire, le changement sera classé « non suivi ».

Un changement sera classé « suivi » s'il répond à au-moins l'un des critères suivants :

- pour les changement ATS :
  - si la gravité des effets des dangers est élevée (niveau 1 ou 2) ;
  - si le changement impacte plusieurs PSCA/D ;
  - lorsqu'il concerne des travaux d'infrastructure aéronautique avec des interférences avérées sur l'activité ;
  - si le DirCAM le décide.

- pour les changements non-ATS :
  - si le changement impacte plusieurs PSCA/D ;
  - si le changement impacte plusieurs PSCNS/D ;
  - si le changement engendre la modification des spécifications initiales du système ;
  - si le DirCAM le décide.

Il sera classé « non suivi » dans les autres cas.

TITRE II

RESPONSABILITÉS

Le règlement [RE373] fixe des exigences de supervision sur la sécurité des changements apportés aux systèmes fonctionnels des PSNA rendant des services à la circulation aérienne générale.

Du point de vue de la sécurité, le classement d'un changement traduit le niveau requis pour l'approbation de la démonstration de sécurité :

- par le(s) prestataire(s) pour les changements classés « non suivis » ;
- par le DirCAM pour les changements classés « suivis ».

II.1 RESPONSABILITÉS DU DirCAM

Le DirCAM exerce, pour le compte de la DSAC, les fonctions de surveillance pour les services rendus par les PSNA/D au profit de la CAG, conformément à l'[A230216]. A ce titre, il est chargé en particulier :

- d'approuver (ou non) les procédures de réalisation des démonstrations de sécurité, élaborées par les prestataires ;
- d'examiner et d'approuver (ou non) les démonstrations de sécurité relatives aux changements classés « suivis » conformément aux prescriptions du chapitre I.4 ;
- de procéder à des vérifications, *a posteriori,* de démonstrations de sécurité relatives aux changements « non suivis ».

Pour exercer ses responsabilités dans les domaines cités supra, le DirCAM s'appuie sur la division sécurité des systèmes (DSS) de la sous-direction surveillance et audit (SDSA). En particulier, un « correspondant DIRCAM » est désigné en son sein pour examiner les changements notifiés.

Les sous-directions régionales de la circulation aérienne militaire (SDRCAM), dans leurs zones de compétences, assurent un suivi des modifications d'espaces aériens et informent la DIRCAM/SDSA des changements ASM temporaires.

II.2 RESPONSABILITÉS DU PRESTATAIRE

L'ensemble des responsabilités des prestataires est décrit dans le [RE373]. Certaines responsabilités sont communes à l'ensemble des prestataires, d'autres spécifiques en fonction de la nature des services rendus.

Les responsabilités communes des prestataires sont :

- de notifier au DirCAM tous les changements en mettant en exergue les conditions prévalant à un classement « suivi » ou justifiant un classement « non suivi » ;
- d'approuver les démonstrations de sécurité pour les changements classés « non suivis » [6] ;
- de s'assurer, au travers de l'assurance sécurité et durant toute la durée de vie du système, que :
  - pour un changement ATS, le risque reste acceptable ;
  - pour un changement non-ATS, le système se comporte uniquement comme spécifié ;
- de notifier, lorsque c'est applicable[7], la mise en œuvre du changement à la DIRCAM.

Les responsabilités spécifiques d'un prestataire ATS (ou PSCA) sont :

- d'évaluer et, si nécessaire, d'atténuer le risque pour tous les changements (voir chapitre IV.1), conformément à la méthode décidée par le DirCAM, préalablement à leur mise en œuvre ;
- de démontrer que le système, après le changement, sera aussi sûr qu'il l'était avant ou alors que toute réduction du niveau de sécurité présente d'autres conséquences bénéfiques ;
- de s'assurer que le changement ATS ou non-ATS n'engendre pas un risque inacceptable et, *in fine*, d'accepter le changement préalablement à sa mise en œuvre[8] ;

[6] Le PSNA/D doit décrire le processus de validation interne de la démonstration de sécurité et peut décider que la validation en dernier ressort par l'autorité désignée vaut approbation.

[7] Voir V.6.

[8] Seuls les PSCA sont capables d'évaluer l'impact d'un changement sur la sécurité. Afin que le PSCA/D soit en mesure de prononcer l'acceptation pour un changement non-ATS, il conviendra de décrire les modalités de coordination entre le PSCNS/D et le PSCA/D pour les études sur le soutien à la sécurité.

- de notifier la mise en service du changement à la DIRCAM.

Les responsabilités spécifiques d'un prestataire non-ATS (PSCNS/D en ce qui concerne les prestataires de services des armées) sont d'évaluer le comportement et les performances du système, afin de s'assurer qu'il répond aux spécifications relatives aux services de navigation aérienne, conformément à la méthode décidée par le DirCAM, pour tous les changements (voir chapitre IV.2).

N.B. : Le prestataire de service peut confier la réalisation, partielle ou totale, de l'étude de sécurité ou de l'étude sur le soutien à la sécurité à une entité extérieure. Néanmoins, il reste responsable du contenu de l'étude.

En fonction de son implication dans le changement, un PSNA/D peut-être identifié comme « partie prenante ». Dans ce cas, il désigne un coordonnateur qui sera l'interlocuteur privilégié du (des autres) prestataire(s) de services, le cas échéant de la DIRCAM. **Pour un PSNA/D, la qualité de « partie prenante » implique qu'il n'a pas à mettre en œuvre de MRR ou d'exigences de sécurité.**

II.3 RESPONSABILITÉS DES TIERCES PARTIES

La prestation de services de navigation aérienne n'est pas, à l'inverse des prestations commerciales, la raison d'être des PSNA/D. A ce titre, ceux-ci dépendent d'autorités de tutelle et sont soumis à des règles particulières en matière d'acquisition et de gestion des ressources. Toutefois, les règlements CUE ayant été établis dans l'optique de prestations commerciales, l'adaptation aux structures propres à la Défense peut parfois nécessiter l'intervention d'entités non identifiées dans le cadre réglementaire.

II.3.1 Autorités de tutelle

Il s'agit principalement des états-majors d'armée (EMx) et de l'état-major des armées (EMA) qui détiennent la responsabilité en matière de ressources (humaines, financières, etc.) et le pouvoir de décision sur les programmes d'armement. Les prestataires identifiés étant sous leur autorité, ils doivent prendre en compte l'impact sur ces derniers de la réglementation européenne (SES/AESA) tout en préservant la capacité opérationnelle des forces.

Ils constituent ainsi un point clef pour la prise en compte, en amont, des exigences liées à la réalisation des démonstrations de sécurité pour les systèmes fonctionnels des armées.

II.3.2 Direction générale de l'armement (DGA)

La DGA assure l'interface entre les armées et le monde industriel. Elle a donc un rôle majeur à jouer :

- en amont pour assurer, lors de la contractualisation, la prise en compte au juste besoin des impératifs liés à la réalisation de la démonstration de sécurité pour le système concerné ;
- lors du développement du programme, en vérifiant la déclinaison des exigences et la collecte de l'assurance du niveau de sécurité attendu ;
- tout au long de la vie du système, en apportant éventuellement son expertise pour la gestion de la configuration et pour l'exploitation des évènements pour ce qui la concerne.

Dans le cadre des opérations d'armement, la notion « d'experts techniques et opérationnels » doit correspondre à des membres de l'équipe pluridisciplinaire de programme (EPDP) en charge du système concerné.

II.4 TABLEAU DES RESPONSABILITÉS CONCERNANT UN CHANGEMENT

Le tableau ci-dessous répertorie les différentes responsabilités dans le cas de changements menés en interne par les armées.

Pour les changements ayant un impact sur un (des) prestataire(s) civil(s) de services de navigation aérienne, une concertation préalable entre PSNA, à l'initiative du prestataire à l'origine du changement ou de la DIRCAM (éventuellement de la DSAC), permettra de définir les attendus.

Type de changement	Impact du changement	Responsable de la notification	Coordonnateur(s)	Approbateur	Autorité d'acceptation	Notification de MEO	Notification de MES
Changement ATS	Un seul PSCA/D	PSCA/D	PSCA/D	PSCA/D ou DirCAM	PSCA/D	PSCA/D	PSCA/D
	Plusieurs PSCA/D	PSCA/D à l'origine	Un par PSCA/D	DirCAM	Chaque PSCA/D dans son domaine	Chaque PSCA/D	Chaque PSCA/D
Changement non-ATS avec impact sur l'ATS	Un seul PSCA/D	PSCNS/D	PSCNS/D PSCA/D	PSCNS/D et PSCA/D ou DirCAM	PSCA/D	PSCNS/D	PSCA/D
	Plusieurs PSCA/D	PSCNS/D	PSCNS/D PSCA/D	DirCAM	Chaque PSCA/D dans son domaine	PSCNS/D	Chaque PSCA/D
Changement non-ATS sans impact[9] sur l'ATS	Un seul PSCA/D	PSCNS/D	PSCNS/D PSCA/D	PSCNS/D ou DirCAM	PSCA/D	PSCNS/D	PSCA/D
	Plusieurs PSCA/D	PSCNS/D	PSCNS/D PSCA/D	DirCAM	Chaque PSCA/D dans son domaine	PSCNS/D	Chaque PSCA/D

[9] « sans impact » signifie que le changement ne modifie pas les méthodes de travail des contrôleurs aériens. Tout au plus, ils seront concernés par une coupure le temps de la réalisation des travaux.

TITRE III

MODALITÉS D'APPROBATION DES PROCÉDURES UTILISÉES PAR LES PSNA/D

Pour les services rendus par les PSNA/D au profit de la CAG, le DirCAM exerce, pour le compte de la DSAC, les fonctions de surveillance des PSNA/D. À ce titre, il est chargé d'approuver le processus de gestion des changements pour la réalisation des changements, élaboré par les prestataires.

En conséquence, les procédures permettant d'apporter un changement à un système fonctionnel sont approuvées lors de la certification initiale du prestataire.

Lors de la création d'un nouveau processus ou d'une modification d'un processus existant relatif à la gestion des changements, imposée par l'évolution de la réglementation européenne ou par un besoin particulier du prestataire, le PSNA/D doit la transmettre au DirCAM pour approbation.

Cette procédure, approuvée par le prestataire, fera alors l'objet d'une décision d'approbation formelle par le DirCAM conformément au [RE373].

TITRE IV

MÉTHODOLOGIES PRÉCONISÉES

IV.1 PROCESSUS POUR UN CHANGEMENT ATS – MÉTHODE SAM[10]

Contrairement au corpus réglementaire précédent, le règlement [RE373] ne prescrit aucune méthode en tant que moyen acceptable de conformité pour évaluer et atténuer le risque engendré par un changement apporté à un système fonctionnel. Les PSNA/D pratiquent la méthode SAM depuis plus d'une dizaine d'années et en maîtrisent bien les principes. Il est donc préconisé aux PSCA/D de conserver cette méthode pour évaluer et atténuer un risque engendré par un changement ATS. Toutefois, fort de la latitude laissée par le règlement [RE373], la méthode décrite ci-après se veut adaptée aux missions des armées et propose des critères d'acceptabilité du risque en meilleure adéquation avec celles-ci.

Pour le personnel amené à conduire une étude de sécurité, il est vivement conseillé de suivre une formation adaptée au sein d'un organisme compétent.

La méthode SAM se décompose en trois phases principales :

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

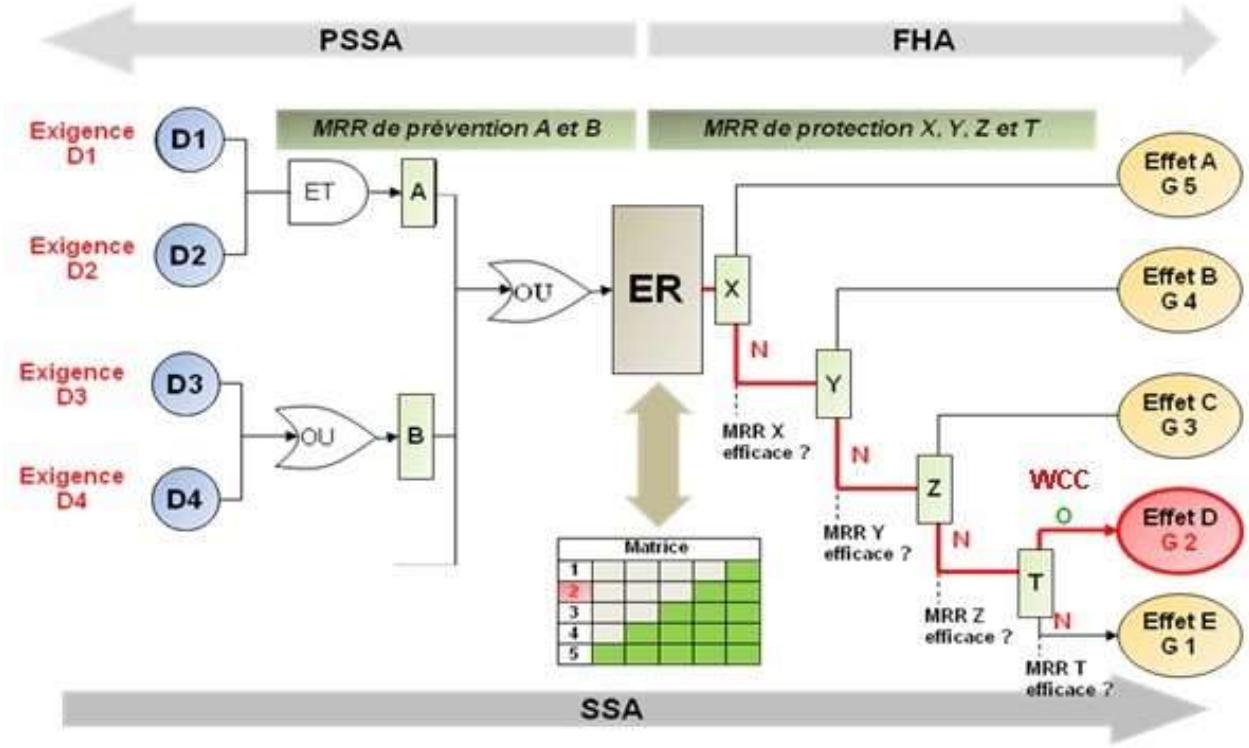


Schéma de principe de la méthode SAM

IV.1.1 MATRICES D'ACCEPTABILITÉ DU RISQUE PRÉCONISÉES

Les matrices préconisées ont été élaborées sur la base des normes OTAN définies dans le [S4720] pour les systèmes de gestion de la sécurité (SMS) utilisés pour la gestion de la circulation aérienne (ATM). Elles permettent l'évaluation et l'atténuation des risques quel que soit le type de circulation (CAG ou CAM). À ce titre, elles prévoient la possibilité d'accepter un risque sous condition, particularité adaptée notamment lorsque les aéronefs volent en CAM.

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

IV.1.1.1 Gravités

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

IV.1.1.2 Probabilité d'occurrence

IV.1.1.2.1 <u>Probabilité d'occurrence quantitative</u>

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.

IV.1.1.2.1 <u>Probabilité d'occurrence qualitative</u>

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.

IV.1.1.3 Matrices d'acceptabilité du risque

IV.1.1.3.1 Tableau des conditions

Catégories		Conditions
A	**Inacceptable**	
B	**Tolérable sous conditions** **Réservé exclusivement aux aéronefs d'État**[11]	Risque très important qui ne peut être réduit en raison de besoins opérationnels ou de contraintes de programmes. 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.
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**	

IV.1.1.3.2 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**

[11] Exemple : une plateforme a de fortes contraintes opérationnelles avec une activité soutenue et accueille de l'aviation commerciale. Sur ordre formel de la plus haute autorité du PSNA/D, 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.

IV.1.1.3.3 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**

IV.1.1.4 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 acceptée par le DirCAM conformément aux procédures décrites au titre III de la présente instruction.

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^{-1}/heure	≤ 10^{-1}/heure	≤ 10^{-2}/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	**C**	**C**	**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.

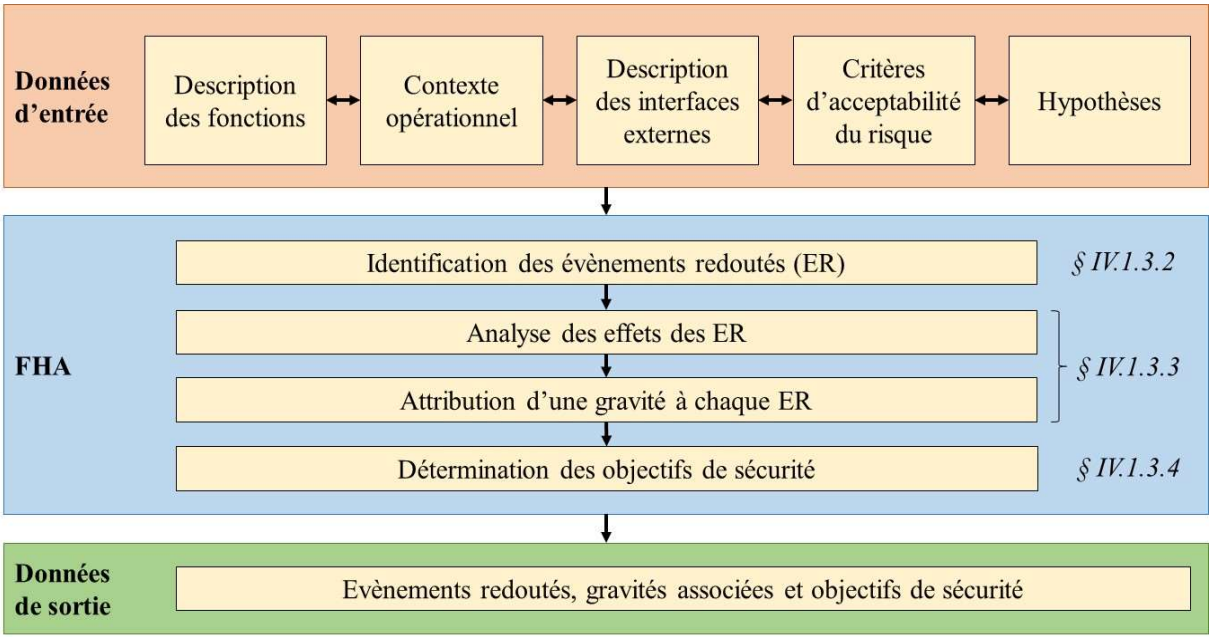
IV.1.2 PHASE PRÉPARATOIRE

En tout premier lieu, il est très important de déterminer le périmètre de l'étude. Il s'agit de mesurer le plus précisément possible l'étendue, les interfaces, les limites du système sur lequel porte l'étude et la (les) composante(s) (équipements, procédures, humain, le cas échéant environnement) affectée(s) par le changement.

Lors de cette phase, il est également possible de faire certaines hypothèses qui faciliteront le déroulement de la démonstration de sécurité mais dont il faudra, *in fine*, vérifier la véracité.

IV.1.3 FHA

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.



La participation des contrôleurs aériens est indispensable en phase de FHA car ils sont les seuls à même de caractériser le danger.

IV.1.3.1 Définition du risque

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

IV.1.3.2 Identification des évènements redoutés (ER)

La première étape de la méthodologie SAM 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 les experts techniques et opérationnels ;
- des méthodes telles que l'AMDEC ou l'APR.

L'évaluation 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 qu'ils sont clairement argumentés.

IV.1.3.3 Analyse des effets opérationnels potentiels 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.

IV.1.3.3.1 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.

IV.1.3.3.2 Détermination de moyens en réduction du risque (MRR) de protection et attribution d'une gravité corrigée

Un MRR de protection est 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 d'un ER. 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.

IV.1.3.4 Objectif de sécurité

Un objectif de sécurité est un énoncé qualitatif ou quantitatif qui définit la fréquence ou la probabilité maximale d'apparition escomptée 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 une lecture de la matrice. Pour une gravité donnée, l'objectif de sécurité est la limite entre la zone B et C de la matrice. Le risque en zone B, tolérable, ne concerne que les aéronefs militaires. Il est donc inacceptable dans le cas général.

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

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

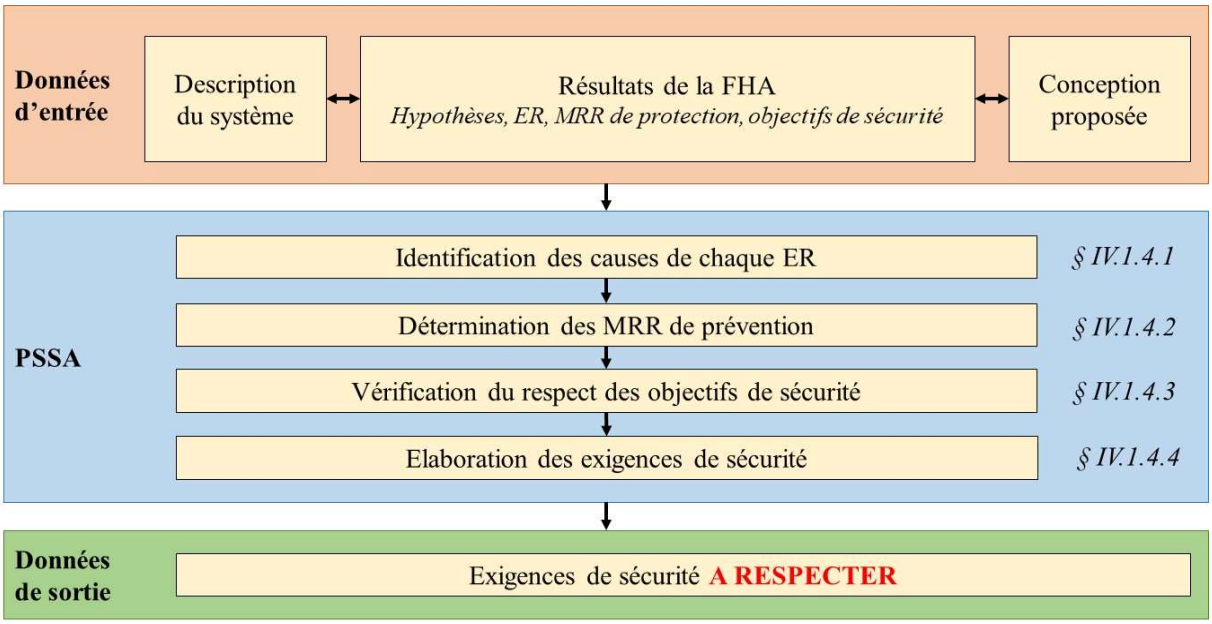
L'objectif de sécurité pour un ER de gravité 3 est une probabilité d'occurrence maximale « occasionnel », c'est-à-dire une à deux fois par an dans l'organisme.

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

IV.1.4 PSSA

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 matériels les plus critiques.

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



IV.1.4.1 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 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.

IV.1.4.2 Détermination des moyens en réduction du risque de prévention

Les MRR de prévention doivent permettre de diminuer l'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 données « constructeur » fournies par l'industriel doivent permettre de déterminer les probabilités d'occurrence liées à une panne.

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 de figure déjà identifiés ou ajouter un/des ER à la liste existante.

IV.1.4.3 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 probabilité d'occurrence, il est alors 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.

IV.1.4.4 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.).

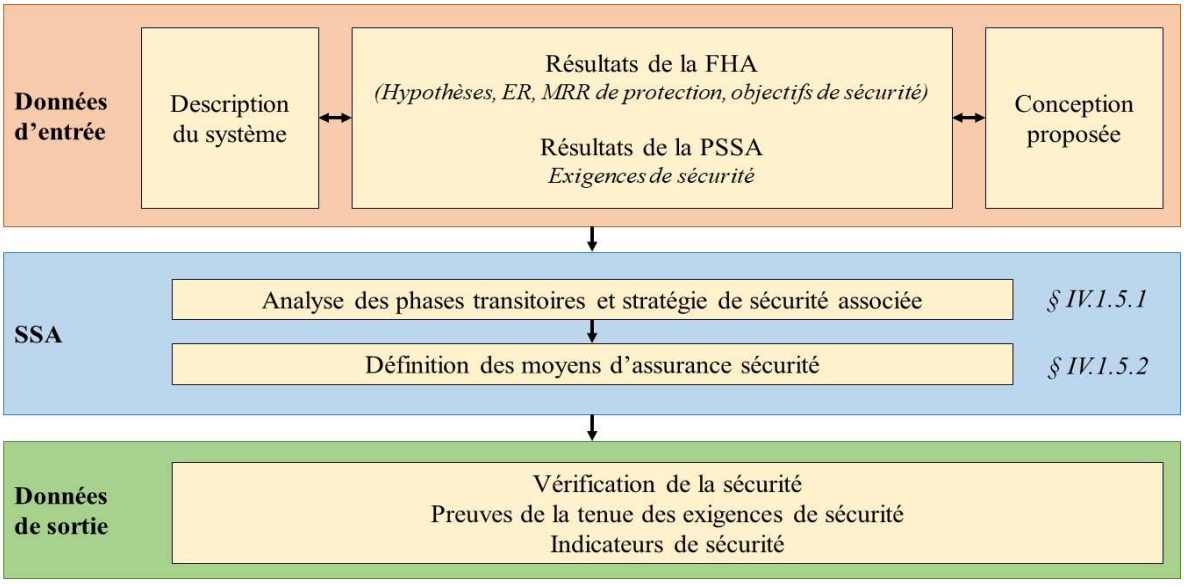
Exemple : En tant que MRR de prévention, il a été identifié la nécessité de la mise en place d'un secours électrique. Compte tenu du contexte, il s'agit d'un groupe électrogène. Cependant, si ce groupe n'est pas branché, entretenu, alimenté en carburant et si le personnel qui l'utilise n'est pas formé, 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 du risque 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 la DIRCAM, il conviendra de transmettre cette nouvelle étude au DirCAM 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.

IV.1.5 SSA

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. Il s'agit de vérifier que les conclusions de l'analyse théorique qu'est la PSSA 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.

IV.1.5.1 Phases transitoires

Les phases de transition d'un système, s'il en existe, font également partie intégrante de la phase SSA. Par phase de transition, on entend toute opération se déroulant entre la mise en œuvre du système sur site (début de la phase de travaux) et la mise en service opérationnel.

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 du système.

IV.1.5.2 Assurance sécurité

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. Ceux-ci doivent faire l'objet d'une attention particulière et, le cas échéant, nécessiter une évolution des exigences de sécurité afin de s'assurer de leur tenue dans le temps (cf. exemple § IV.1.3.4).

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

IV.2 PROCESSUS POUR UN CHANGEMENT NON-ATS

Pour les armées, les changements non-ATS sont menés par les PSCNS/D.

IV.2.1 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 cela, 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'acceptation du DirCAM, les modalités de coordination avec le(s) PSCA/D soutenu(s). Celles-ci figurent également dans les procédures d'évaluation et d'atténuation des risques du (des) PSCA/D.

IV.2.2 MÉTHODOLOGIES POSSIBLES

Les méthodes pour réaliser une étude sur le soutien à la sécurité relèvent de l'ingénierie de la maîtrise du risque et ne peuvent pas être décrites dans la présente instruction.

Les méthodes suivantes sont préconisées car elles ont déjà été utilisées par le passé et ont montré leur pertinence en matière de démonstration de sécurité :

- AMDEC (Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité) ;

- analyse dysfonctionnelle ;
- arbre de défaillance.

Dans le cadre du processus d'acceptation de ses procédures (cf. titre III), le prestataire de services listera l'ensemble des méthodes qu'il souhaite utiliser pour une étude sur le soutien à la sécurité. L'autorité compétente pourra demander à se les faire présenter en tout ou partie afin d'en comprendre les mécanismes particuliers.

IV.2.3 TENUE DES EXIGENCES

Les performances du système définies préalablement ont une incidence sur sa réalisation en terme :
- d'architecture ;
- de disponibilité ;
- de maintenabilité ;
- de résilience ;
- etc.

Il en découle différentes exigences dont le prestataire de services devra apporter la preuve de leur tenue, à l'instar de la tenue des exigences de sécurité d'une étude de sécurité.

Ces preuves sont généralement matérialisées par :
- la schémathèque du système ;
- l'acceptation en usine (FAT[12]) et sur site (SAT[13]) ;
- les résultats des cahiers d'essais et de réception ;
- etc.

IV.2.4 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 donc être étudiée dans le cadre du dossier sur le soutien à la sécurité.

IV.2.4.1 Notion de système d'assurance de la sécurité des logiciels (SASL)

Il n'y a pas de taux de défaillance applicable à un logiciel. Le niveau de confiance accordé à un logiciel ne peut donc pas être quantitatif mais qualitatif.

L'approche retenue pour s'assurer de la sécurité des logiciels du système fonctionnel consiste donc à utiliser des niveaux d'assurance logicielle (« *SoftWare Assurance Level* » – SWAL). Un système d'assurance de la sécurité des logiciels (SASL) permet de décrire les méthodes pour attribuer ces niveaux et pour démontrer que le logiciel les atteint.

Un SASL impose de démontrer, sous la forme d'arguments et de preuves, que les logiciels embarqués dans le système non-ATS n'engendreront pas un risque inacceptable. À ce titre, le SASL :
- attribue un **niveau de confiance** pour tout logiciel impliqué dans un changement du système ATM/ANS (SWAL ou autre qu'il conviendra de définir) ;
- définit des arguments, sous la forme d'objectifs à atteindre pour le logiciel, appelés « **objectifs logiciels**[14] » 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 ;

[12] Factory Acceptance Tests.
[13] Site Acceptance Tests.
[14] 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.

- 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.

Le SASL constitue en définitive un ensemble documenté qui s'inscrit dans la méthodologie de l'étude sur le soutien à la sécurité, garantissant que les risques associés à l'utilisation d'un logiciel dans le système ATM sont réduits à un niveau acceptable. Ainsi, l'étude sur le soutien à la sécurité permet de définir, en fonction des exigences du logiciel, sa criticité et par conséquent le niveau de confiance requis. Ce niveau de confiance 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 niveau ou le degré de rigueur avec lequel le logiciel est réalisé et mis en œuvre.

Nota : ***Il est vivement conseillé qu'un PSCA/D dispose également d'un SASL dans le cadre de la définition des performances du système. Il lui sera ainsi possible de relier la gravité des évènements redoutés au niveau d'assurance sécurité logicielle.***

IV.2.4.1 Démarche d'assurance de la sécurité des logiciels

Dans le cadre du SASL, 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.

Nota : 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 le logiciel concerné. Cette assertion doit toutefois être formalisée dans l'étude sur le soutien à la sécurité.

IV.2.4.1.1 Détermination du niveau de confiance

Le SASL du prestataire de service définit comment le SWAL est alloué à un logiciel. Ce SWAL dépend du risque engendré par le logiciel.

Le SWAL dépend des performances du système qui ont été définies en relation avec le(s) PSCA/D (cf. § IV.2.1), ainsi que de la contribution du logiciel à un dysfonctionnement du système.

Par exemple, de par le risque engendré, il a été identifié un SWAL 2. Comme il existe une redondance indépendante d'un point de vue logiciel et/ou des procédures de contrôle qui permettent de réagir au dysfonctionnement considéré, le SWAL est finalement établi à 3.

IV.2.4.1.2 Satisfaction du niveau de confiance

Le prestataire de service doit ensuite procéder à la démonstration de la satisfaction du niveau de confiance. Cette satisfaction repose sur l'apport d'assurances tout au long du cycle de vie du logiciel. Le respect de normes relatives à l'assurance sécurité logicielle (les normes [ED109] et [ED153] sont celles généralement utilisées) est un moyen acceptable de conformité.

Dans le cadre particulier d'une modification d'une version logicielle déjà en service, 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.2.4.1.3 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 du SASL et des niveaux de confiance attribués.

IV.2.4.2 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. § VII.3.2) au titre de la démonstration de sécurité ;
- si le prestataire de services souhaite apporter de nouvelles fonctionnalités au logiciel, visant ainsi à améliorer son 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 grâce au SASL du prestataire.

IV.3 VÉRIFICATION DE L'ACCEPTABILITÉ DU RISQUE

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 de la circulation aérienne. À ce titre, les PSCNS/D et les PSCA/D décrivent dans leurs procédures soumises à l'acceptation 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.

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 de sécurité antérieure, cette démonstration pourra être faite par comparaison des matrices d'acceptabilité des risques. S'il n'existe pas d'étude de sécurité antérieure, cette exigence sera présumée tenue dès lors que le risque est acceptable.
- Si toutefois il s'avère que le système ne sera pas aussi sûr qu'auparavant, le PSNA/D devra démontrer que le changement apporte des bénéfices qui contrebalancent cette situation. Les éléments devront figurer de manière explicite dans l'étude de sécurité ou dans l'étude sur le soutien à la sécurité.

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

IV.4 VÉRIFICATION DE LA TENUE DANS LE TEMPS DU SYSTEME

Le règlement [RE373] introduit la notion de critères de sécurité. Il s'agit d'indicateurs permettant d'apporter l'assurance que le système ne dérive pas au cours du temps.

Les indicateurs à mettre en place doivent permettre de suivre des éléments concrets :

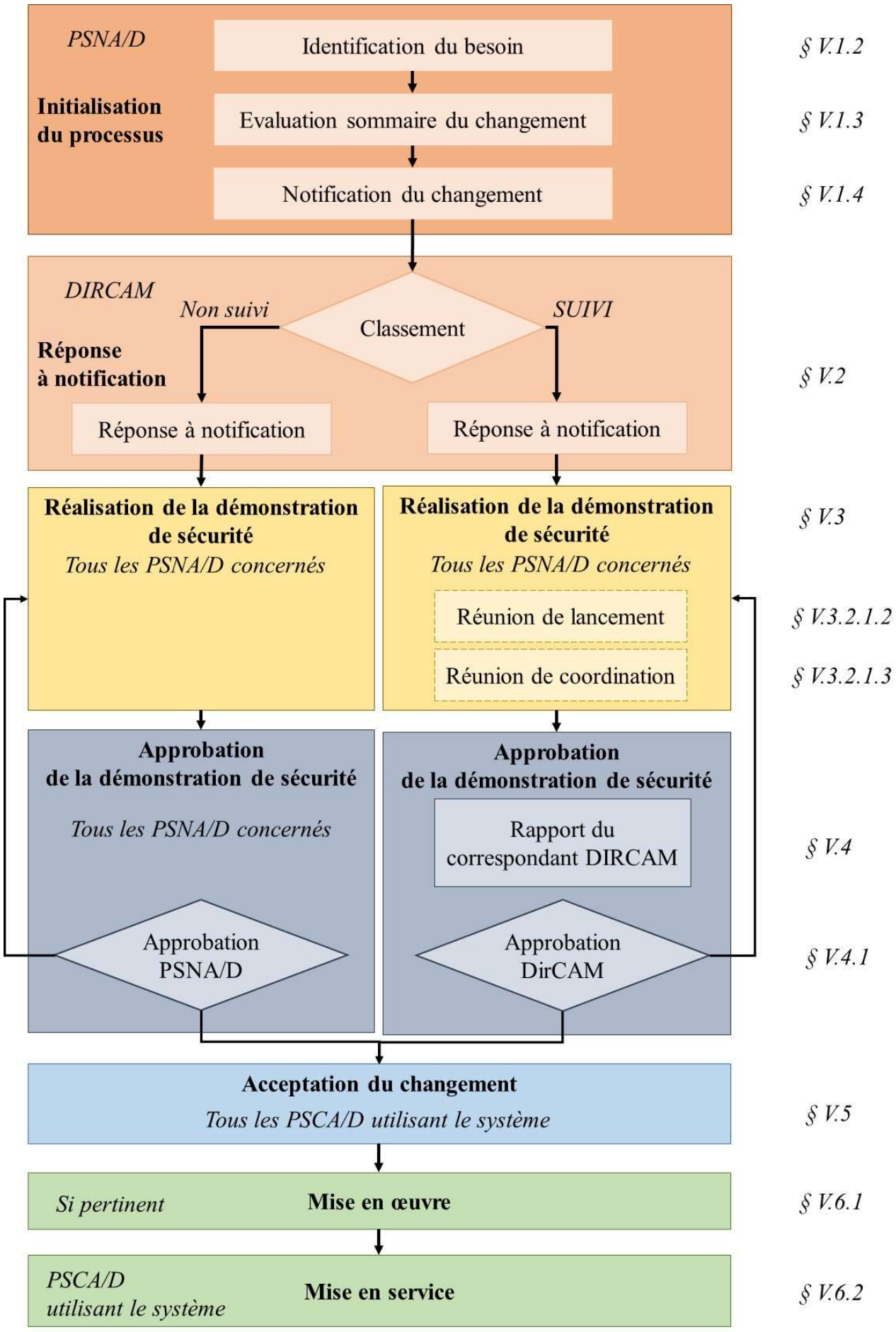
- nombre d'évènements ATM ou techniques afin de montrer que la probabilité d'occurrence de l'ER est en deçà de l'objectif de sécurité ;
- disponibilité, nombre de pannes d'un équipement afin de prouver qu'il continue à rendre un service conforme à ses spécifications ;
- etc.

Les indicateurs sont décrits lors de la définition des exigences sur le système et suivis au titre de l'assurance sécurité.

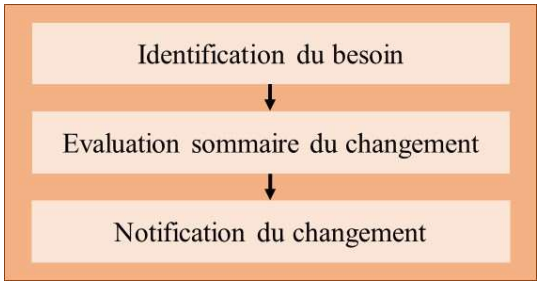
Ces indicateurs sont obligatoires lorsque les ER, une fois le risque atténué, se trouvent dans la partie B ou C de la matrice d'acceptabilité du risque.

TITRE V

PROCESSUS DÉFENSE DE GESTION DES CHANGEMENTS


PSNA/D
Initialisation du processus
Identification du besoin
Evaluation sommaire du changement
Notification du changement
§ V.1.2
§ V.1.3
§ V.1.4
DIRCAM
Réponse à notification
Non suivi
Classement
SUIVI
Réponse à notification
Réponse à notification
§ V.2
Réalisation de la démonstration de sécurité
Tous les PSNA/D concernés
Réalisation de la démonstration de sécurité
Tous les PSNA/D concernés
Réunion de lancement
Réunion de coordination
§ V.3
§ V.3.2.1.2
§ V.3.2.1.3
Approbation de la démonstration de sécurité
Tous les PSNA/D concernés
Approbation de la démonstration de sécurité
Rapport du correspondant DIRCAM
Approbation PSNA/D
Approbation DirCAM
§ V.4
§ V.4.1
Acceptation du changement
Tous les PSCA/D utilisant le système
§ V.5
Si pertinent
Mise en œuvre
§ V.6.1
PSCA/D utilisant le système
Mise en service
§ V.6.2

V.1 NOTIFICATION DU CHANGEMENT



V.1.1 IDENTIFICATION DU BESOIN DE CHANGEMENT

Le point de départ de tout changement est l'identification du besoin de ce changement. Il peut être motivé par des impératifs opérationnels, des demandes d'usagers, une évolution de l'environnement, de la réglementation, des considérations techniques (acquisition de nouveaux équipements, traitements d'obsolescences, par exemple) ou autres.

V.1.2 ÉVALUATION SOMMAIRE DU CHANGEMENT (BRAINSTORMING INITIAL)

Sous forme d'un brainstorming structuré, le prestataire de services évalue sommairement l'impact du changement. Afin que cette évaluation sommaire soit la plus aboutie possible, le prestataire de services convoque, outre ses spécialistes (contrôleur, technicien radar, technicien radio, etc.), ceux des organisations pour lesquelles le changement aura une incidence :

- usagers des services ;
- prestataires extérieurs ;
- autres prestataires de services.

L'oubli d'une partie prenante lors de l'évaluation sommaire du changement peut avoir un impact rédhibitoire sur la mise en œuvre du changement.

L'évaluation sommaire permet au prestataire de préciser ses idées quant au changement et à son impact. Elle permet éventuellement d'identifier les conditions qui prévaudront au classement du changement. À ce titre, il importe de définir aussi finement que possible la nature exacte du changement, en s'affranchissant autant que faire se peut des solutions qui seront adoptées pour le satisfaire. La description du changement doit avant tout être fonctionnelle et doit anticiper les besoins pressentis sur l'intégralité de la vie du système.

L'évaluation sommaire donne lieu à un compte-rendu formel qui sera utilisé dans la suite du processus.

Pour certains changements « simples », si le travail d'analyse de l'évaluation sommaire est suffisamment abouti, il s'avère que la démonstration de sécurité est faite. Il ne reste alors au prestataire de services qu'à mettre en forme son travail et à recueillir les preuves de tenues des exigences de sécurité.

V.1.3 NOTIFICATION DU CHANGEMENT

Conformément au règlement [RE373], le prestataire de service notifie tous les changements à l'autorité compétente.

Le PSNA/D doit garantir que le délai entre la notification et la mise en œuvre du changement sera suffisant pour permettre à la DIRCAM/SDSA/DSS d'analyser la notification afin que le DirCAM prononce un classement adapté. La DIRCAM/SDSA/DSS dispose d'un délai de 10 jours ouvrés maximum pour analyser la notification et proposer le classement du changement. Une procédure d'urgence peut être consentie à titre exceptionnel après concertation entre le PSNA/D et la DIRCAM/SDSA/DSS. Toutefois, même dans cette situation, il est impératif que la notification du changement précède sa mise en œuvre, y compris s'il s'agit d'une prévision.

La notification de changement et la réponse du DirCAM constituent un enregistrement de sécurité et sont donc réalisées au travers d'un échange de courriers formels.

La notification de changement doit, au minimum, contenir tous les éléments décris en annexe 1 – partie 1.2.

V.1.3.1 Responsabilités en matière de notification de changement

Le règlement [RE373] prescrit qu'un changement peut être à l'initiative du prestataire de services ou être la conséquence d'une opération décidée par un autre prestataire de services (cf. I.2). De plus, chaque prestataire de services doit notifier tous les changements à l'autorité compétente (cf. II.2). Les armées comptent cinq prestataires de services. Régulièrement, le changement porté par l'un a des incidences sur le système fonctionnel d'un ou plusieurs autre(s). Dans un souci de cohérence et de rationalisation, la notification de changement faite par le PSNA/D à l'origine du changement vaudra notification pour tous les autres PSNA/D impactés par ce changement[15]. Le PSNA/D qui notifie le changement devra porter une attention particulière afin de bien définir l'impact de son changement sur les autres PSNA/D.

Les responsabilités en matière de notification du changement sont décrites dans le tableau ci-dessous.

Type de changement	Impact du changement	Responsable de la notification
Changement ATS	Un seul PSCA/D	PSCA/D
	Plusieurs PSCA/D	PSCA/D à l'origine
Changement non-ATS		PSCNS/D

Lorsqu'un PSNA/D est impacté par le changement d'un autre, il peut décider de ne contribuer au changement qu'en tant que « partie prenante ». Dans ce cas, au titre de la démonstration de sécurité, il ne devra pas mettre en œuvre d'exigence de sécurité mais désignera un coordonnateur pour y contribuer. La condition de partie prenante d'un PSNA/D devra être motivée dans la notification du changement.

Exemple : pour le changement ATM CLA 2000, la DIRISI a déployé, sur chaque plateforme, deux liens de type T2 sur deux autocommutateurs distincts. Cette prestation, relevant du catalogue de services de la DIRISI, ne représentait pas un changement pour le PSNA/D, seulement une évolution du périmètre des systèmes pris en compte dans le cadre de son management de la sécurité. En conséquence, la DIRISI s'est, à juste titre, déclarée partie prenante.

Lorsqu'un PSNA/D réalise un changement ayant un impact sur un prestataire de services civil, il devra préalablement consulter la DIRCAM/SDSA/DSS qui définira les modalités pour la notification en coordination avec la DSAC/ANA/SMN.

V.1.3.2 Changements particuliers – Processus simplifié

Parfois, il s'avère que l'évaluation sommaire arrive à la conclusion que le changement n'engendre aucun risque inacceptable. Par exemple, c'est souvent le cas :

- pour un changement non-ATS qui n'a aucune incidence sur les services de la circulation aérienne[16] (*exemple : modification de la technologie du support d'une liaison téléphonique*) ;
- quand les méthodes de travail usuelles des contrôleurs aériens suffisent à rendre le risque acceptable.

Dans ce cas, le prestataire de services :

- notifie le changement (cf. § V.1.4) ;
- recueille toutes les preuves pertinentes au titre de l'assurance sécurité (cf. § IV.1.4 et IV.2.3) et les conserve jusqu'au retrait du service du changement considéré.

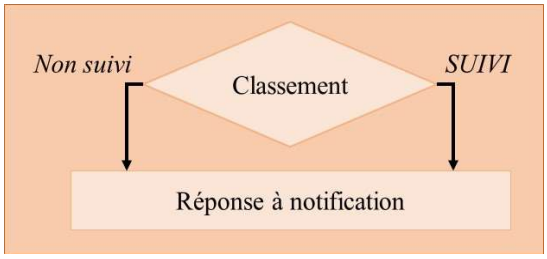
La notification du changement doit contenir les éléments probants qui permettront au DirCAM de décider en ce sens. Pour cela, le PSNA/D utilise les formulaires figurant en annexe 1.

---

[15] Pour des cas particuliers, il peut être nécessaire de ne pas appliquer ce principe. Dans ce cas, le prestataire de services à l'origine du changement expliquera dans la notification pourquoi celle-ci ne vaut pas pour les autres PSNA/D. La réponse à notification validera ou amendera la démarche du prestataire (cf. V.2).

[16] Dans ce cas, l'étude sur le soutien à la sécurité reste indispensable. Seule la vérification de l'acceptabilité du risque engendré (responsabilité du PSCA/D utilisant le système) pourra se faire selon le processus simplifié.

V.2 RÉPONSE A NOTIFICATION



Cette étape formalise l'enregistrement du changement par le DirCAM. Elle se traduit par son classement « suivi » ou « non suivi ».

Après analyse de la notification par la DIRCAM/SDSA/DSS, le DirCAM transmet sa décision de classement, « suivi » ou « non suivi », du changement qui précise :

- la référence du changement ;
- le correspondant DIRCAM ;
- d'éventuelles remarques ou consignes de sécurité.

Cette décision est formalisée par un message d'autorité (NeMO), signé par le DirCAM ou son suppléant, conformément au modèle figurant en annexe 2.

La réponse à notification pour un changement classé « non suivi » peut être déléguée au sous-directeur surveillance et audit de la DIRCAM.

De plus, la DIRCAM/SDSA/DSS dispose d'un tableau de suivi où figurent les informations ayant un intérêt concernant l'ensemble des changements menées par les PSNA/D. Ce tableau est mis à disposition au travers du portail de la DSAÉ sur un espace privatif réservé à la « communauté SMS ».

Toute correspondance ultérieure relative à un changement considéré portera obligatoirement sa référence et son intitulé exact.

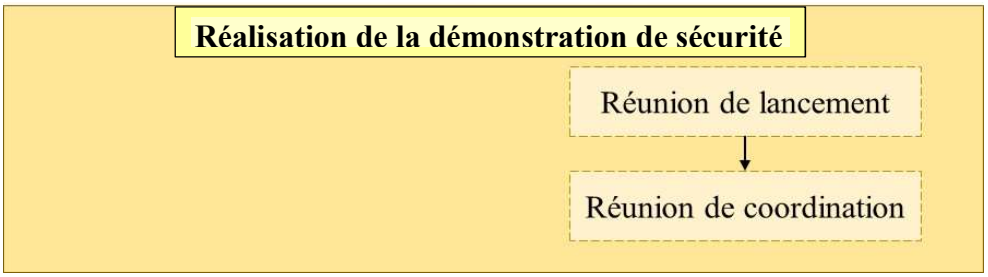
V.2.1 CLASSEMENT DU CHANGEMENT

Le DirCAM classe le changement conformément aux principes décrits au chapitre I.4. Ce classement peut évoluer au regard d'éléments apparaissant lors de la réalisation de la démonstration de sécurité qui n'auraient pas été identifiés lors de l'évaluation sommaire.

V.2.2 CORRESPONDANT DIRCAM

Pour chaque changement, le chef de la DIRCAM/SDSA/DSS désigne parmi son personnel celui qui sera l'interlocuteur privilégié du/des coordonnateur(s) du/des PSNA/D. Il est le « correspondant DIRCAM ». À ce titre, celui-ci dispose des prérogatives pour saisir d'autres services au sein du/des PSNA/D pour toutes questions relatives au changement qu'il est chargé de traiter.

V.3 CONDUITE DE L'ÉTUDE



La démonstration de sécurité est menée sous la responsabilité du prestataire de services et l'enregistrement de sécurité qu'elle constitue est géré conformément aux procédures de gestion documentaire établies par son système de management de la sécurité (SMS).

V.3.1 PRINCIPES GÉNÉRAUX

Conformément au règlement [RE373], les procédures utilisées par les PSNA/D pour évaluer et atténuer le risque lié à un changement doivent être acceptées par le DirCAM. Ces procédures définissent les modalités de réalisation des démonstrations de sécurité pour chaque prestataire.

L'étude doit permettre d'établir une confiance justifiée dans la sécurité du changement étudié en présentant un argumentaire soutenu par des éléments de preuves.

Pour les changements classés « suivis », la démonstration de sécurité doit être remise au correspondant DIRCAM au point limite de réception de l'étude (PLRE), soit au moins **20 jours ouvrés** avant l'échéance d'acceptation du changement par le PSCA/D. Pour des raisons opérationnelles, le prestataire de services menant le changement pourra demander au DirCAM, avec l'accord du PSCA/D qui utilisera le système, une adaptation de ce délai. Cette demande fera l'objet d'une correspondance formelle et argumentée.

Le titre VII du présent document préconise différents formalismes de démonstration de sécurité pour les PSNA/D.

V.3.2 MODALITÉS PARTICULIÈRES POUR LES CHANGEMENTS CLASSÉS « SUIVIS »

V.3.2.1 Niveau de suivi

Le niveau d'intervention exprime le degré d'implication du DirCAM pour le suivi de la démonstration de sécurité. Trois niveaux d'intervention ont été fixés :

- Niveau A : le correspondant DIRCAM vérifie tout au long de l'étude le respect, par le prestataire, de la procédure de réalisation de la démonstration de sécurité. De plus, il vérifie tous les résultats obtenus par le prestataire au cours de l'étude ;
- Niveau B : le correspondant DIRCAM vérifie le respect, par le prestataire, de la procédure de réalisation de la démonstration de sécurité. De plus, il vérifie certains résultats obtenus par le prestataire au cours de l'étude. Les thèmes des résultats qui seront vérifiés sont précisés préalablement lors de la réunion de lancement ou dans le message de réponse à notification ;
- Niveau C : le correspondant DIRCAM vérifie le respect, par le prestataire, de la procédure de réalisation de la démonstration de sécurité et, le cas échéant, des consignes de sécurité stipulées lors de la réunion de lancement ou dans le message de réponse à notification.

Les thèmes possibles pour un suivi de niveau B sont :

- Thème 1 : description du système (*exemple : vérification de la cohérence du périmètre du changement au regard des éléments de la démonstration de sécurité*) ;
- Thème 2 : liste des ER et détermination de leur gravité (*exemple : vérification de la complétude de la liste des ER et de la cohérence de leur gravité*) – détermination des objectifs de sécurité (*exemple : vérification de l'attribution de gravités corrigées aux ER et de la cohérence des MRR de protection*) ;

  ou

  définition des spécifications du système (*exemple : vérification de la cohérence des spécifications vis-à-vis du risque identifié par le PSCA/D*) ;
- Thème 3 : détermination des exigences de sécurité (*exemple : vérification de la crédibilité des exigences de sécurité et de leur efficacité pour atténuer les risques identifiés*) ;
- Thème 4 : évaluation de la sécurité (*exemple : vérification de l'acceptabilité du risque au regard des hypothèses, MRR et de leur justification – vérification des performances réelles du système*) ;
- Thème 5 : assurance de la sécurité (*exemple : vérification du recueil des preuves de la tenue des exigences de sécurité et de la mise en place des éventuels indicateurs – vérification de la cohérence de la méthode de suivi dans le temps du respect des critères de sécurité*).

V.3.2.2 Réunion de lancement

Lorsque le correspondant DIRCAM le juge nécessaire, il organise une réunion de lancement. Celle-ci a principalement pour objet la présentation détaillée du changement par le prestataire à l'ensemble des acteurs concernés. Cette réunion permet également au correspondant DIRCAM de fixer les modalités de suivi.

Sur demande des prestataires, des experts, notamment des sous-directions espace aérien (SDEA) et réglementation (SDR), de la direction générale de l'armement (DGA), des industriels, peuvent y être conviés. À ce stade de l'étude, leur rôle consiste à vérifier la conformité du projet vis-à-vis des règles et directives de leurs domaines de compétences respectifs et, le cas échéant, à apporter un avis d'expert.

L'ordre du jour comprend, *a minima*, les items suivants :

- description du changement par le prestataire porteur du projet (périmètre, contexte, concept d'opération (CONOPS), impacts, etc.) ;
- échéances calendaires (dates prévisionnelles de mise en œuvre et de mise en service, PLRE, transmission du plan de sécurité s'il est demandé par le correspondant DIRCAM, etc.) ;
- modalités pratiques de la procédure de réalisation de la démonstration de sécurité envisagées par le prestataire. Notamment, identification des intervenants dans la procédure et échéances des éventuelles phases intermédiaires ;
- modalités de suivi du changement par le DirCAM, en particulier :
  - niveau d'intervention ;
  - si nécessaire, les dates prévisionnelles des prochaines rencontres ;
- éventuelles consignes de sécurité.

Le prestataire ayant notifié le changement réalise une présentation (PowerPoint) du changement à l'occasion de la réunion de lancement. Cette présentation devra parvenir à la SDSA/DSS au moins une semaine avant la date de la réunion. Elle comporte, *a minima*, les éléments cités *supra*.

A l'issue de la réunion, un compte-rendu (cf. modèle en annexe 3) est rédigé par le correspondant DIRCAM. Il est vérifié par le chef de la division sécurité des systèmes, validé par le sous-directeur surveillance et audit, puis enregistré dans le suivi documentaire de la DIRCAM. Ce compte-rendu est ensuite transmis formellement à l'ensemble des participants et à leur tête de chaîne. Constituant un enregistrement de sécurité, il sera annexé à l'étude de sécurité.

V.3.2.3 Plan de sécurité

Pour certains changements, il peut s'avérer qu'à l'issue de la réunion de lancement, de très nombreuses inconnues subsistent. Dans ce cas, le correspondant DIRCAM pourra demander au prestataire de services que lui soit transmis un plan de sécurité. Suivant la même trame que la réunion de lancement, ce plan apporte au DirCAM les éclaircissements nécessaires à une meilleure compréhension du projet du prestataire et de la méthode de réalisation de la démonstration de sécurité envisagée. L'annexe 4 préconise un formulaire type pour le plan de sécurité.

Le plan de sécurité fait l'objet d'un accord formel du DirCAM.

Une démonstration de sécurité étant un processus itératif, le plan de sécurité, comme tout autre élément de l'étude, peut-être appelé à évoluer. Les justifications des modifications ultérieures du plan de sécurité sont alors tracées et annexées au plan de sécurité initial.

V.3.2.4 Réunion de coordination

Organisée à l'initiative du correspondant DIRCAM ou du prestataire de services, une réunion de coordination permettra :

- de faciliter la compréhension de l'étude afin d'en accélérer l'approbation finale ;
- de permettre au correspondant, au fur et à mesure du déroulement de l'étude, de prendre connaissance du dossier afin d'émettre des remarques et des recommandations sans attendre la

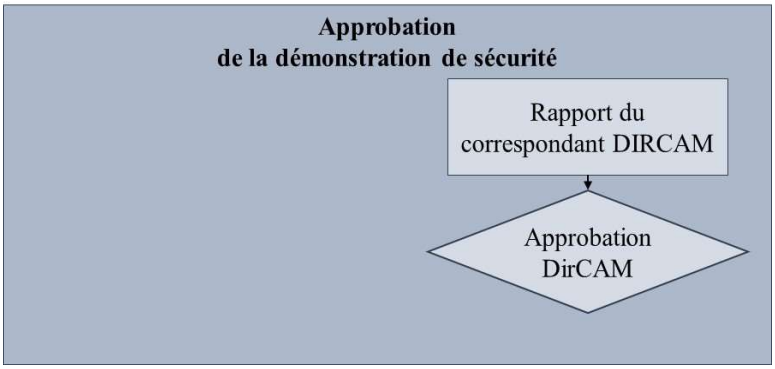
communication de l'étude finalisée. Cette prise en compte anticipée permet d'éviter toute remise en cause lourde de l'étude *a posteriori* ;

- de demander des pièces complémentaires ;
- d'ajuster la procédure de réalisation de la démonstration de sécurité, notamment au travers de la réévaluation des échéances calendaires.

Un compte-rendu est rédigé par le correspondant DIRCAM, vérifié par le chef de la division sécurité des systèmes, validé par le sous-directeur surveillance et audit, puis enregistré dans le suivi documentaire de la DIRCAM. Il est formellement transmis à l'ensemble des participants et organismes concernés. Ce compte-rendu sera annexé à l'étude de sécurité.

Dans le cadre des réunions de conduite d'un projet entre l'État et le maître d'œuvre, le correspondant DIRCAM peut être convié. En fonction de la teneur des débats, le correspondant DIRCAM peut décréter que cette réunion a le caractère d'une réunion de coordination. Il valide cette décision par un message formel. Le cas échéant, le message et le compte-rendu sont annexés à la démonstration de sécurité.

V.4 APPROBATION DE LA DÉMONSTRATION DE SÉCURITÉ



L'approbation de la démonstration de sécurité signifie l'engagement de(s) l'autorité(autorités) désignée(s) sur la véracité et la cohérence du contenu de la démonstration. Les démonstrations de sécurité des changements classés « suivis » sont soumises à l'approbation du DirCAM avant la mise en œuvre des changements considérés.

V.4.1 MODALITÉS PARTICULIÈRES POUR LES CHANGEMENTS CLASSÉS « SUIVIS »

Toute démonstration de sécurité pour un changement « suivi » transmise au DirCAM pour approbation fera préalablement l'objet d'une validation par une autorité désignée au sein du prestataire de services à l'origine du changement.

V.4.1.1 Rapport du correspondant DIRCAM

L'examen de la démonstration de sécurité constitue l'étape au cours de laquelle le correspondant DIRCAM recueille et analyse les informations et les documents pertinents fournis par le ou les PSNA/D. Les conclusions du rapport aboutissent à une proposition de décision du sous-directeur surveillance et audit qui reflète l'avis du correspondant DIRCAM quant à la crédibilité et la cohérence de la démonstration de sécurité.

Les éléments constitutifs du rapport sont collectés tout au long du suivi du changement et de l'élaboration de la démonstration de sécurité. La collecte au plus tôt de ces éléments permet :

- d'éviter les points bloquants en les détectant en amont et en convenant de solutions acceptables ;
- de limiter le délai de traitement de l'étude lorsque le prestataire de services souhaite accélérer la procédure pour des raisons opérationnelles dûment justifiées. Ce dernier point nécessite toutefois la pleine et entière collaboration des diverses parties impliquées.

Un modèle type de rapport du correspondant DIRCAM est donné en annexe 6.

V.4.1.2 Approbation de la démonstration de sécurité par le DirCAM

L'approbation signifie que la démonstration de sécurité démontre que la mise en œuvre du changement est possible et acceptable du point de vue de la sécurité. Règlementairement, le DirCAM se prononce uniquement sur les aspects du changement dans le domaine de la circulation aérienne générale. Les aspects relatifs à circulation aérienne militaire restent de la responsabilité des prestataires de services concernés, la DIRCAM pouvant toutefois donner un avis à titre de conseil.

Le DirCAM prend sa décision aux vues de l'avis motivé du prestataire et des éléments qui lui sont présentés dans le rapport du correspondant DIRCAM. Lorsque, pour des raisons pratiques, il a été décidé de découper le changement en plusieurs phases et autant de démonstrations de sécurité, le DirCAM approuvera chacune de celles-ci. L'approbation est formalisée par un message formel dont le modèle figure en annexe 5. Le DirCAM peut prononcer :

- l'approbation en l'état de la démonstration de sécurité ;
- l'approbation sous réserve de la démonstration de sécurité. Dans ce cas, des consignes de sécurité et les preuves attendues seront précisées dans le message d'approbation ;
- le refus de l'étude de sécurité. Dans ce cas, le correspondant DIRCAM organisera une réunion de coordination afin d'expliquer au(x) PSNA/D en quoi la démonstration de sécurité n'est pas satisfaisante. Celui-ci(ceux-ci) doit(doivent) reprendre leur démonstration et la soumettre à nouveau à l'approbation du DirCAM avant de poursuivre la conduite du projet.

V.4.2 APPROBATION POUR LES CHANGEMENTS CLASSÉS « NON SUIVIS »

Les modalités d'approbation des démonstrations de sécurité relatives aux changements « non suivis » figurent dans le tableau des responsabilités du § II.4.

V.5 ACCEPTATION DU CHANGEMENT

L'acceptation du changement signifie que le risque est acceptable au regard de la démonstration de sécurité approuvée et que l'ensemble des exigences de sécurité ont été mises en place. S'il s'avère qu'il n'est pas possible de démontrer la mise en place de toutes les exigences de sécurité, le risque est présumé inacceptable et le changement ne doit pas être accepté.

L'acceptation du changement est le préalable indispensable à sa mise en œuvre. Elle est prononcée par le(s) PSCA/D concerné(s), y compris dans le cas d'un changement non-ATS sans impact sur les services ATS. La responsabilité de l'acceptation est formalisée lors de la notification du changement, le cas échéant, pour les changements classés « suivis », en réunion de lancement ou dans le plan de sécurité.

Lorsque le changement touche plusieurs organismes de contrôle, l'acceptation du changement peut être globale ou propre à chaque site. Cette disposition est formalisée lors de la notification du changement, le cas échéant, pour les changements classés « suivis », en réunion de lancement ou dans le plan de sécurité.

V.6 MISE EN ŒUVRE / MISE EN SERVICE DU CHANGEMENT

V.6.1 MISE EN OEUVRE

La mise en œuvre correspond au début des travaux lorsque ceux-ci ont une incidence sur la capacité de l'organisme de contrôle à rendre les services de la circulation aérienne. La notification de mise en œuvre permet d'informer le DirCAM quand le projet entre dans sa première phase. Elle est prononcée par un message formel conformément aux prescriptions du tableau des responsabilités du § II.4. Elle doit parvenir à la DIRCAM dans les **20 jours ouvrés** qui suivent la mise en œuvre du changement.

La notification de mise en œuvre doit au minimum indiquer :

- la référence du changement ;
- l'intitulé exact du changement ;
- la date effective de mise en œuvre.

V.6.2 MISE EN SERVICE

La mise en service signifie que le système est pleinement utilisé par l'organisme de contrôle. La notification de mise en service permet d'informer le DirCAM que le système est entré dans sa phase opérationnelle. C'est (ce sont) le(s) PSCA/D, utilisant le système objet du changement, qui notifie(nt) la mise en service au DirCAM, par un message formel, dans un délai de **20 jours ouvrés**.

La notification de mise en service doit au minimum indiquer :

- la référence du changement ;
- l'intitulé exact du changement ;
- la date effective de mise en œuvre.

Souvent, la mise en œuvre et la mise en service d'un changement sont simultanées. C'est le cas pour une majorité de changements à composante circulation aérienne. Dans ce cas, ces deux phases font l'objet d'une notification conjointe.

V.7 SURVEILLANCE

Conformément au règlement [RE373], le DirCAM assure la surveillance des changements. Cette mission incombe à la division sécurité des systèmes de la DIRCAM qui dispose d'outils de suivi appropriés. Afin d'améliorer les échanges avec les PSNA/D, ceux jugés pertinents sont diffusés au travers d'un espace privatif du portail DSAÉ : *http://portail-dsae.intradef.gouv.fr*

Toute demande d'accès doit être formulée auprès de la DIRCAM/SDSA/DSS.

V.7.1 SURVEILLANCE *A PRIORI*

Seuls les changements « suivis » font l'objet d'une surveillance *a priori* au titre de l'approbation de l'étude de sécurité.

V.7.2 SURVEILLANCE *A POSTERIORI*

La surveillance *a posteriori* :

- peut prendre la forme de revues documentaires ou d'audits sur site. Ces derniers peuvent être déclenchés spécifiquement ou s'inscrire dans le cadre des audits programmés dans le cycle de surveillance du prestataire ;
- peut porter sur le processus de réalisation des démonstrations de sécurité de manière globale ou être plus particulièrement orientée sur des changements identifiés.

À ce titre, le DirCAM peut demander aux prestataires toutes les pièces relatives aux démonstrations de sécurité qu'il juge pertinentes.

V.8 PROCESSUS MULTI-PRESTATAIRES

Les armées comptent cinq prestataires de services. Régulièrement, le changement porté par l'un d'entre eux a des incidences sur le système fonctionnel d'un ou plusieurs autre(s). Le présent chapitre pose les principes d'un processus multi-prestataires permettant ainsi de limiter au juste besoin les travaux nécessaires à la réalisation de la démonstration de sécurité.

V.8.1 DISPOSITIONS GÉNÉRALES

Le prestataire de services à l'initiative du changement convie les autres PSNA/D à la réunion d'analyse sommaire de l'impact du changement. Il est responsable de la notification du changement. Celle-ci doit lister les acteurs de la démonstration de sécurité au seins de chacun des PSNA/D, en particulier les autorités l'approuvant et, pour les PSCA/D, celles acceptant le changement (cf. chapitre V.1.3.1). Les modalités de classement (« suivi » ou « non suivi ») du changement sont précisées au chapitre I.4.

Tous les PSNA/D concernés par le changement contribuent à la démonstration de sécurité. Chacun approuve la démonstration de sécurité. Le(s) PSCA/D utilisant le système accepte(nt) le changement.

V.8.2 CAS D'UN CHANGEMENT NON-ATS

Le PSCNS/D à l'initiative du changement convie le(s) PSCA/D qui utilisera(ont) le système à la réunion d'analyse sommaire d'impact. Ainsi, le(s) PSCA/D pourra(ont) définir les performances attendues du système (cf. chapitre IV.2.1) au regard du risque engendré.

Dans la mesure du possible, le(s) PSCA/D participe(nt) à l'étude sur le soutien à la sécurité. Dans ces conditions, sa(leurs) participation(s) à la démonstration de sécurité et surtout son approbation permet de démontrer l'exigence ATS.OR.205 du règlement [RE373]. Sinon, dans le cadre de l'acceptation du changement, il(s) devra(ont) démontrer que l'étude sur le soutien à la sécurité a été vérifiée par ses(leurs) soins.

Le(s) PSCA/D utilisant le système doit(vent) démontrer, au travers d'une étude de sécurité, que le changement non-ATS n'engendre pas un risque inacceptable pour ses(leurs) services. Le cas échéant, lorsque le changement non-ATS est sans impact pour le(s) PSCA/D, un processus simplifié suffit (cf. chapitre V.1.3.2).

Lorsque le changement non-ATS découle d'une prestation demandée par le PSCA/D auprès du PSCNS/D, le premier est le prestataire de services à l'initiative du changement. À ce titre, il est responsable de la notification. Il existe plusieurs cas pour la réalisation de la démonstration de sécurité.

- si la prestation consiste à se raccorder sur un système existant (*par exemple, intégrer dans le calculateur du centre de contrôle les informations d'un radar déjà connecté au réseau*) ayant déjà fait l'objet d'une étude sur le soutien à la sécurité, le PSCNS/D fournit au PSCA/D les éléments pertinents de son étude, ceux-ci permettant au PSCA/D de mener l'étude de sécurité liée à cette nouvelle prestation ;
- si la prestation consiste à se raccorder sur un système existant ancien, n'ayant donc pas fait l'objet d'une démonstration de sécurité, le PSCNS/D évalue l'impact à partir des retour d'expérience acquis sur le système et fournit ces données au PSCA/D pour que celui-ci réalise l'étude de sécurité liée à cette nouvelle prestation ;
- si la prestation consiste à déployer un système nouveau, le PSCNS/D réalise l'étude sur le soutien à la sécurité, si possible en lien avec le PSCA/D (cf. 2ème paragraphe). À partir des résultats de celle-ci, le PSCA/D réalise la démonstration de sécurité associée.

V.9 AIDE À LA COMPRÉHENSION DU PROCESSUS

Afin de faciliter la compréhension de ce processus, la DIRCAM/SDSA/DSS organise, en fonction de sa charge de travail, des séminaires de sensibilisation aux démonstrations de sécurité. Ces séminaires s'adressent plus particulièrement au personnel des unités responsables de l'approbation d'une démonstration de sécurité dont le changement est « non suivi ». Ce personnel est désigné par les PSNA/D.

La DIRCAM/SDSA/DSS peut également réaliser des conférences ponctuelles, à la demande, au profit du personnel des armées souhaitant des informations dans le domaine des processus de supervision de la sécurité. Ces interventions sont effectuées pour une vingtaine de personnes.

Page intentionnellement blanche

TITRE VI

TRAITEMENT DES CHANGEMENTS ASM

VI.1 GÉNÉRALITÉS

Au titre du règlement [RE373], tout changement relatif à l'organisation de l'espace aérien donne lieu à la réalisation d'une démonstration de sécurité préalablement à la mise en service. 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 concernés.

Des procédures relatives à la notification de ces changements auprès du DirCAM, ainsi que les attendus en termes d'évaluation et d'atténuation des risques, font l'objet d'un protocole quadripartite (DTA, DIRCAM, DSAC et DSNA).

Ce protocole a été établi avec la DSAC pour permettre aux PSCA/D de réaliser des démonstrations de sécurité simplifiées locales (DSSL) au lieu d'études de sécurité classiques dans le cadre de changements ASM temporaires. Toutefois, les PSCA/D restent libres de déterminer le type de démonstration de sécurité à utiliser en fonction de l'importance ou de la gravité des ER associés au changement temporaire.

VI.2 LES CHANGEMENTS ASM A TITRE PERMANENT

Lorsqu'un prestataire de services de circulation aérienne est concerné par un changement d'espace aérien 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 notifie le changement au DirCAM et réalise une étude de sécurité selon les procédures définies par son SMS.

Conformément au protocole cité *supra*, l'étude de sécurité doit être établie avec un préavis suffisant avant la mise en service programmée du changement compte-tenu, entre autres, des délais incompressibles du processus de publication de l'information aéronautique.

VI.3 LES CHANGEMENTS ASM A TITRE TEMPORAIRE

VI.3.1 LES CHANGEMENTS CONCERNÉS

Les changements 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).

VI.3.2 PROCESSUS DE DÉMONSTRATION DE SÉCURITÉ

VI.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 applique la procédure de notification classique d'un changement et réalise une étude de sécurité conforme à son SMS.

VI.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 10, sans notification auprès du DirCAM. La transmission par le bureau exécutif permanent des informations relatives au changement ASM temporaire vaut notification du changement considéré.

VI.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*, les unités conserveront leurs DSSL de l'année calendaire en cours, ainsi que celles des deux années précédentes.

Page intentionnellement blanche

TITRE VII

TYPES D'ÉTUDES POSSIBLES

Conformément au règlement [RE373], « *les procédures* [de gestion des changements] *ou tout autre changement important apporté à ces procédures :*

1) sont soumises, pour approbation, par le prestataire de services à l'autorité compétente ;

2) ne sont pas utilisées tant qu'elles ne sont pas approuvées par l'autorité compétente. ».

En conséquence, les procédures relatives à une étude de sécurité ou à une étude sur le soutien à la sécurité, y compris celles préconisées ci-après, devront faire l'objet d'une acceptation formelle par le DirCAM.

VII.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 7.

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

Lors de l'évaluation sommaire, le prestataire de services peut identifier que la démonstration 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'acceptation par le DirCAM.

Un modèle d'EPIS est préconisé en annexe 8.

VII.3 PROCÉDURES PARTICULIÈRES

VII.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 ;
- 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 ;
- 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.

VII.3.2 MÉTHODOLOGIE D'INTERVENTION SUR LES SYSTÈMES OPÉRATIONNELS (MISO)

La méthodologie d'intervention sur les systèmes opérationnels est une procédure d'évaluation et d'atténuation des risques afin 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 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 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 :

- le 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 de contrôle qui 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 opération de 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.). Une MISO répétitive 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 de validité est fixée par le PSNA/D en fonction de sa connaissance du système. Il est préconisé qu'elle soit fixée à 3 ans et, dans tous les cas, celle-ci 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 9.

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 que les maintenances 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.

VII.3.3 DÉMONSTRATION DE SÉCURITÉ SIMPLIFIÉE LOCALE (DSSL)

Dans le cas où un PSCA/D n'est que concerné par le changement, il ne transmet pas de notification au DirCAM et réalise simplement une démonstration de sécurité simplifiée locale (DSSL), dont le format et le guide de rédaction sont proposés en annexe 10. La transmission par les BEP des informations relatives aux changements ASM temporaires à la DIRCAM vaut notification du changement considéré.

Ce document est un outil adapté et proportionné dans les cas de changements temporaires. Toutefois, le prestataire est libre de faire une étude de sécurité plus poussée s'il la juge nécessaire.

ANNEXE 1

FORMULAIRES PRÉCONISÉS DE NOTIFICATION D'UN CHANGEMENT

A1.1 PRÉAMBULE

L'annexe 1 présente les formulaires préconisés aux PSNA/D pour notifier un changement au DirCAM.

Le formulaire « Notification de changement » (§ A1.2) est à renseigner en toutes circonstances. Il contient toutes les informations indispensables au DirCAM pour pouvoir classer le changement en toute connaissance de cause.

Les formulaires « Phase 1 » (§ A1.3) et « Phase 2 » (§ A1.4) sont utilisés lorsque l'évaluation préliminaire conclut que le risque est acceptable avec, au plus, la seule mise en œuvre des méthodes de travail usuelles des contrôleurs aériens.

- « Phase 1 » : ce formulaire permet de lister les ER avec leur gravité et leur probabilité d'occurrence en justifiant tous les éléments. Si, *in fine*, tous les ER sont en zone de risque acceptable, il n'est pas nécessaire de poursuivre l'analyse.
- « Phase 2 » : si à l'issue de la phase 1, il apparait nécessaire de mettre en œuvre des procédures usuelles du métier de contrôleur aérien (publication de NOTAM, rédaction d'un « Quoi de neuf », rappel lors du briefing quotidien, etc.) pour rendre le risque acceptable, elles sont décrites et justifiées dans ce formulaire.

Lorsqu'un PSNA/D notifie un changement en arguant que le risque est acceptable d'emblée, il joint le formulaire phase 1 et, si nécessaire, le formulaire phase 2.

A1.2 FORMULAIRE PRÉCONISÉ DE NOTIFICATION DE CHANGEMENT

LOGO PSNA/D	NOTIFICATION DE CHANGEMENT	***LOGO UNITÉ*** Date : jj/mm/aaaa

Identification du changement				
Intitulé du changement :				
Introduction d'un nouveau système ☐	Modification d'un système existant ☐	Retrait d'un système ☐		
Système concerné :				
Domaines concernés :	Équipements : ☐	Procédures : ☐	Humain : ☐	
	Information aéronautique : ☐	IOP : ☐		
Impact sur :	Les servitudes aéronautiques (PSA) ☐	Les servitudes radioélectriques (PSR) ☐	Non concerné ☐	
Gravité 1 ou 2 ☐	Infrastructures aéronautiques ☐	Plusieurs PSCA/D ☐	Plusieurs PSCNS/D ☐	Modifications spécifications ☐
Références des éventuels changements antérieurs sur le système :				
Références des éventuels changements similaires au sein du PSNA/D :				
Durée du changement :	Permanent : ☐	Temporaire : ☐ Début de validité : jj/mm/aaaa Fin de validité : jj/mm/aaaa		
Prévision de mise en œuvre *Estimation si date précise non connue*	Prévision de mise en service *Estimation si date précise non connue*			
Description :				

PSNA/D et parties prenantes	
Unité(s) concernée(s) :	
Autre(s) PSNA/D concerné(s) :	
Partie(s) prenante(s) :	

Propositions PSNA/D					
Procédure simplifiée[17] : ☐	EPIS :	☐	DS :	☐	
Classement du changement :	NON SUIVI	☐	SUIVI	☐	
Justification de la proposition de classement « non-suivi » (hors procédure simplifiée) :					

Acteurs de l'étude de sécurité				
	Grade NOM	Unité	Adresse Intradef	Téléphone
Rédacteur ops				
Rédacteur tech				
Coordonnateur ops 1				
Coordonnateur ops 2				
Coordonnateur tech 1				
Coordonnateur tech 2				
…				
Partie prenante 1				
Partie prenante 2				
…				
Approbation Changement « non suivi »				
Approbateur ops				
Approbateur tech				
Changement « suivi »				
Validation ops 1				
Validation ops 2				
…				
Validation tech 1				
Validation tech 2				
…				
DirCAM				
Autorité d'acceptation				
PSCA/D 1				
PSCA/D 2				
…				

[17] Si ce formalisme est proposé, ce formulaire devra être accompagné du formulaire phase 1 et éventuellement phase 2. Le classement proposé sera « non suivi » et pour la suite du formulaire, ne remplir que l'autorité d'acceptation.

GUIDE DE RÉDACTION

Identification du changement.

L'intitulé doit être le plus concis possible. Il sera repris dans toutes les correspondances relatives au changement considéré.

Le PSNA/D renseigne les différentes cases en fonction des caractéristiques du changement.

Dans le cas d'un nouveau système, le système éventuellement remplacé sera mentionné.

Dans le cas d'une modification, le système modifié sera précisé et la présence ou non d'études antérieures sur ce système indiquée.

Dans le cas du retrait d'un système, le PSNA/D mentionnera, si elle existe, l'étude réalisée pour sa mise en place.

Dans l'éventualité où, par le passé, des études de sécurité ont déjà été réalisées pour un changement similaire sur un autre site, le PSNA/D indique la référence de ces changements.

Si le PSNA/D ne précise pas la durée du changement temporaire, alors celui-ci sera considéré comme permanent.

La description du changement doit permettre à l'autorité compétente de comprendre sommairement les risques engendrés malgré sa méconnaissance du système. La description peut renvoyer à un document qui sera alors joint à la notification.

PSNA/D et parties prenantes.

Le PSNA/D précise dans cette partie :

- la ou les unité(s) subordonnée(s) où le changement sera mis en service ;
- le ou les éventuel(s) autre(s) PSNA/D impacté(s) par le changement ;
- le ou les entité(s) partie(s) prenante(s) dans le changement.

Propositions PSNA/D.

Le PSNA/D propose :

- le formalisme de la démonstration de sécurité ;
- le classement « suivi » ou « non suivi » ;
- les acteurs de l'étude.

Si le PSNA/D propose une procédure simplifiée ou un classement « non suivi », l'argumentaire devra être obligatoirement renseigné :

- pour une procédure simplifiée, l'argumentaire fera apparaître les éléments importants des formulaires phase 1 et, le cas échéant, phase 2 ;
- pour un classement « non suivi », l'argumentaire doit présenter les éléments garantissant que le PSNA/D maîtrise le processus d'atténuation des risques.

Le PSNA/D propose les acteurs de l'étude en précisant l'identités et les coordonnées :

- du(des) rédacteur(s) ;
- du(des) coordonnateur(s) ;
- de la(des) partie(s) prenante(s) ;
- de l'autorité du(des) PSCA/D d'acceptation du changement.

Pour un changement classé « non suivi », le PSNA/D propose l'identité de la ou des autorité(s)[18] qui approuvera(ont) la démonstration de sécurité et précise leurs coordonnées.

[18] Dans le cas d'une étude de sécurité impliquant plusieurs PSNA/D, une autorité sera désignée au sein de chacun.

Pour un changement classé « suivi », le PSNA/D propose l'identité de la ou des autorité(s)[19] qui validera(ont) le contenu de la démonstration de sécurité avant de la soumettre à l'approbation du DirCAM et précise leurs coordonnées.

[19] Dans le cas d'une étude de sécurité impliquant plusieurs PSNA/D, une autorité sera désignée au sein de chacun.

A1.3 FORMULAIRE PRÉCONISÉ DE PHASE 1

LOGO PSNA/D	Phase 1 RISQUE INITIAL	***LOGO UNITÉ*** Date : jj/mm/aaaa

S'il est rédigé, ce formulaire constitue la suite de la notification de changement dans le cadre d'une procédure simplifiée, les deux formulaires constituant alors un même ensemble.

Intitulé du changement :	

Identification du risque initial

A ce stade, le risque est évalué sans qu'aucune mesure particulière ne soit mise en place, hormis l'application des procédures standards du contrôle aérien.

ER 1 : *Intitulé de l'ER (autant que nécessaire)*

Description :

Justification du positionnement :

ER 2 : *Intitulé de l'ER*

Description :

Justification du positionnement :

ER 3 : *Intitulé de l'ER*

Description :

Justification du positionnement :

Acceptabilité du risque initial

Gravité \ Occurrence	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**

Si l'ensemble des ER définis se trouve en zone acceptable, le PSNA/D notifie le changement et archive l'ensemble des pièces afférentes. En l'absence d'EPIS ou de dossier de sécurité, afin de formaliser l'acceptation du changement, le message de mise en service sera signé par l'autorité désignée dans le premier formulaire de notification.

Seul le message DIRCAM de classement et de référencement du changement valide l'utilisation éventuelle d'une procédure simplifiée.

Liste des participants au brainstorming :	
Grade Nom Prénom :	Fonction :
Grade Nom Prénom	*Fonction*
Grade Nom Prénom	*Fonction*
…	…
Visa de l'autorité rédactrice	

A1.4 FORMULAIRE PRÉCONISÉ DE PHASE 2

LOGO PSNA/D	Phase 2 RISQUE CORRIGÉ	***LOGO UNITÉ*** Date : jj/mm/aaaa

S'il est rédigé, ce formulaire constitue la suite de la notification de changement et de l'analyse du risque initial dans le cadre d'une procédure simplifiée, les trois formulaires constituant alors un même ensemble.

Intitulé du changement :	

Moyens en réduction du risque éprouvés
MRR *PREV ou PRO 1 : Intitulé du MRR*
Justification de l'atténuation du risque :
MRR *PREV ou PRO 2 : Intitulé du MRR*
Justification de l'atténuation du risque :
MRR *PREV ou PRO 3 : Intitulé du MRR*
Justification de l'atténuation du risque :
MRR *PREV ou PRO 4 : Intitulé du MRR*
Justification de l'atténuation du risque :
MRR *PREV ou PRO 5 : Intitulé du MRR*
Justification de l'atténuation du risque :
MRR *PREV ou PRO 6 : Intitulé du MRR*
Justification de l'atténuation du risque :

Acceptabilité du risque corrigé

Gravité \ Occurrence	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**

Si l'ensemble des ER après mise en œuvre des moyens en réduction du risque se trouve en zone acceptable, le PSNA/D notifie le changement et peut proposer une procédure simplifiée d'évaluation et d'atténuation des risques. **Seul le message DIRCAM de classement et de référencement du changement valide l'utilisation éventuelle d'une procédure simplifiée.**

Dans le cas d'une procédure simplifiée, le PSNA/D recueille les preuves de mise en œuvre des moyens en réduction du risque et archive l'ensemble des pièces afférentes à la procédure d'évaluation et d'atténuation des risques. En l'absence d'EPIS ou de dossier de sécurité, afin de formaliser l'acceptation du changement, le message de mise en service sera signé par l'autorité désignée dans le premier formulaire de notification.

Liste des participants au brainstorming :

Grade Nom Prénom :	Fonction :
Grade Nom Prénom	*Fonction*
Grade Nom Prénom	*Fonction*
…	…

Visa de l'autorité rédactrice

ANNEXE 2

DÉCISION DE

RÉPONSE A NOTIFICATION

NON PROTEGE

MINISTERE DES ARMEES **Message Officiel**	**Le** : / / à h : **Emetteur** : **DSAE/DIRCAM**	**N°** **Urgence : ROUTINE**
Dossier suivi par : **DHERS Frédéric CDT** DSAÉ/DIRCAM/SDSA/DSS Mail : frederic.dhers@intradef.gouv.fr PNIA : 8111077654 Tel : 0145073654	**Destinataire(s) (action)** :	
	Objet : **Décision de [SUIVI ou NON SUIVI] relative au changement [REFERENCE]** MCA : SECU/AERIENNE	

PRIMO/ DECISION

Le directeur de la circulation aérienne militaire,

Vu le règlement d'exécution (UE) n°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 ;

Vu le Code de l'Aviation Civile art. D131-10 ;

Vu 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 ;

Vu le décret n°2013-366 du 29 avril 2013 portant création de la direction de la sécurité aéronautique d'État ;

Vu l'instruction n°4150/DSAÉ/DIRCAM du XXXX relative au processus de supervision et de réalisation des études de sécurité des prestataires de services de la navigation aérienne de la défense ;

Vu la décision du xxxxx portant délégation de signature.

Considérant :

La notification du changement formalisée par message XXXXX du jj/mm/aaaa.

Décide :

Le changement [« libellé changement »], au profit de [SITE], notifié par [PSNA/D] en date du jj/mm/aaaa, est référencé [REFERENCE] et classé « SUIVI » conformément au règlement d'exécution n°2017/373 susnommé.

SECUNDO/

Les modalités pratiques XXX.

TERTIO/

Correspondant DIRCAM : XXX

Signé par :

Pour un changement classé « suivi », le message de décision est signé du DirCAM ou du DirCAM adjoint.

ANNEXE 3

MODÈLE DE COMPTE RENDU DE

RÉUNION DE LANCEMENT

DIRCAM/SDSA/DSS	**Réunion de lancement**	DSS-RL V2.0 du 01/09/2017
Titre de l'étude de sécurité concernée par cette réunion	*PSNA/D 20XX-XX : évolution du système X (exemple)*	

RÉFÉRENCE N° /DSAÉ/DIRCAM/SDSA/NP du

LIEU *Lieu de la réunion*

DATE *jj/mm/aaaa*

PARTICIPANTS *Liste des participants*

REDIGE PAR *Correspondant étude de sécurité (DIRCAM/SDSA/DSS)*

Version du document	Date de rédaction	Raison de l'évolution	Auteur
V0.1	*jj/mm/aaaa*	Création du document	*Grade Nom*
V0.2	*jj/mm/aaaa*	Vérification du document	*Grade Nom*
V1.0	*jj/mm/aaaa*	Validation du document	*Grade Nom*

Rédacteur	**Vérificateur**	**Approbateur**
Correspondant DIRCAM	*Chef DSS*	*Sous-directeur SDSA*

DESTINATAIRES : *Participants ;*
Tête de chaine PSNA/D ;
Autres.

ANNEXE(S) : *Rappels sur les attributions du DirCAM et des PSNA/D ;*
Autres.

PIÈCE(S) JOINTE(S) : *Diaporama présenté en séance ;*
Autres.

0. ORDRE DU JOUR

1. PRÉAMBULE

Les raisons qui ont conduit à effectuer cette réunion sont précisées dans cet item.

2. CHANGEMENT *PSNA/D 20XX-XX*

2.1 Présentation du changement

Le prestataire expose les détails du changement.

Périmètre du changement :

Le changement touche les composantes *XXXXX*.

- Au niveau opérationnel :

  Conséquences opérationnelles.

- Au niveau technique :

  Aspects techniques.

- Au niveau du personnel :

  Impacts sur le personnel.

2.2 Confirmation des échéances calendaires

Les échéances suivantes sont systématiquement définies :

- transmission du plan de sécurité au DirCAM :
- point limite de réception de l'étude (PLRE) :
- prévision de mise en œuvre opérationnelle :
- prévision de mise en service opérationnelle :

2.3 Intervenants dans la démonstration de sécurité

Les intervenants suivants sont confirmés :

Rédacteur(s) :

- *XXX ;*
- *YYY.*

Coordonnateur(s) :

- *XXX ;*
- *YYY.*

Validation de l'étude :

- *XXX ;*
- *YYY.*

Approbateur :

- DirCAM.

Autorité(s) d'acceptation :

- *XXX ;*
- *YYY.*

Correspondant de l'étude de sécurité et suppléant :

- *XXX ;*
- *Suppléant : YYY.*

Autres acteurs pour la réalisation de l'étude de sécurité :

En tant que partie prenante : *XXX*.

2.4 Méthodologie retenue par le prestataire en charge de l'étude

La méthodologie retenue est confirmée. Dans le cas d'une étude devant faire l'objet d'un dossier de sécurité et sur proposition du prestataire ayant notifié le changement, les modalités relatives à la constitution du dossier de sécurité sont définies.

2.5 Assurance logicielle

Si applicable, décrire les modalités relatives à l'assurance logicielle.

2.6 IOP

Si applicable, décrire les modalités relatives à l'interopérabilité.

2.7 Modalités de suivi du changement par le DirCAM

Niveau d'intervention retenu pour l'examen de l'étude de sécurité	
☐ **Niveau A**	- Vérification de l'application par le PSNA/D des **procédures** de démonstration de sécurité. - Vérification de **tous les résultats** obtenus par le PSNA/D au cours de la démonstration de sécurité.
☐ **Niveau B**	- Vérification de l'application par le PSNA/D des **procédures** de démonstration de sécurité. - Vérification de **certains résultats** obtenus par le PSNA/D que le correspondant souhaite vérifier.
☐ **Niveau C**	- Vérification de l'application par le PSNA/D des **procédures** de démonstration de sécurité.

Les thèmes suivants ont été choisis :

- *Thème X : XXX ;*
- *Thème Y : YYY.*

2.8 Divers

Ici sont abordées les questions qui n'ont éventuellement pas pu être traitées dans les autres chapitres.

Page intentionnellement blanche

ANNEXE 4

MODÈLE PRÉCONISÉ DE

PLAN DE SÉCURITÉ

LOGO DU PSNA/D *(ayant notifié)*	**Plan de Sécurité**	*Organisme PSNA/D (ayant notifié)*

A – TITRE DU CHANGEMENT	*Identification du changement tel que dans la notification*		
Référence DIRCAM	*Référence telle que définie dans la décision DIRCAM*		
PSNA/D	*Site 1 concerné*	*Site 2 concerné*	*Site 3 concerné*

Suivi du document				
Version	**Date**	**Modifications**	**Chapitre / Page**	**Auteur**

B – PRÉSENTATION DU CHANGEMENT *(reprendre les éléments du plan de sécurité si pas d'évolution)*

B1 – Date et durée du changement

☐ Permanente, à compter du : _ _/_ _/20_ _ (date de mise en service)

☐ Temporaire, du *(mise en service)* : _ _/_ _/20_ _

au *(retrait du service)* : _ _/_ _/20_ _

B2 – Localisation du changement

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

B3 – Objet de l'évolution

Décrire le contexte du changement, l'inscription dans le cadre d'un programme majeur, le positionnement de ce changement par rapport à d'autres, etc.

B4 – Description fonctionnelle du système

Identification des fonctions, liens entre les fonctions. Description des fonctions principales, élémentaires, de base. Cette rubrique peut être associée à des schémas explicatifs.

B5 – Périmètre de l'étude

Définir le périmètre de l'étude de sécurité qui 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.

Enfin, la zone géographique dans laquelle s'opère le changement doit être précisée.

B6 – Hypothèses de travail

Une hypothèse de travail est un postulat de base établi ou éventuel, en amont du changement.

B7 – Interfaces

Déterminer les liaisons pouvant exister avec d'autres systèmes ou composants.

B8 – Environnement opérationnel

Décrire l'environnement opérationnel du changement (météo, densité du trafic, etc.).

B9 – Intégration du système

Présentation du concept d'emploi, intégration dans le système existant.

B10 – Éléments particuliers

Cocher si le changement est concerné par l'un des points suivants :

☐ Modification de norme aéronautique

☐ Interopérabilité (au sens du RE 2018/1139)

☐ Composante logicielle

☐ Impact sur PCU[20] et/ou PFU[21]

☐ Modification de documentation aéronautique

☐ Autre(s) élément(s) particulier(s)

B11 – Modalités de suivi du changement

Rappeler le niveau d'intervention pour le changement tel que défini dans la partie 2.5 du compte-rendu de la réunion de lancement.

C – FORMALISME UTILISÉ

Renseigner le type de formulaire utilisé pour l'étude (EPIS, Dossier de sécurité, MISO pour les phases de transition, etc.).

D – RESPONSABILITÉS

Identification des responsables de l'étude de sécurité pour les PSNA/D.

Acteur	Nom	Fonction	Date Signature
Rédacteur PSNA/D WW			*facultatif*
Rédacteur PSNA/D XX			*facultatif*
Coordonnateur PSNA/D WW			*obligatoire*
Coordonnateur PSNA/D XX			*obligatoire*
Validation PSNA/D WW			*obligatoire*
Validation PSNA/D XX			*obligatoire*

[20] Programme de compétences en unité.
[21] Plan de formation en unité.

E – DOCUMENTS LIÉS AU PLAN

Titre	Référence du document	Annexé
Compte rendu de brainstorming		☐ Oui ☐ Non
Document(s) nécessaire(s) à la compréhension du plan de sécurité		☐ Oui ☐ Non
		☐ Oui ☐ Non
		☐ Oui ☐ Non

F – DIFFUSION POUR ACTION

Organisme	Fonction (PSNA/D, Autres)	Correspondant (facultatif)

G – DIFFUSION POUR INFORMATION

Organisme	Fonction (PSNA/D, Autres)	Correspondant (facultatif)

H – ORGANISMES CONCERNÉS PAR L'ÉTUDE

H1 – PSNA/D concernés

Les PSNA/D intervenant dans le changement sont listés dans cette rubrique.

H2 – Acteurs non PSNA/D de l'étude

Les acteurs industriels ou étatiques (exemple DGA) intervenant dans le changement sont listés dans cette rubrique.

I – CALENDRIER PRÉVISIONNEL (PLAN D'ACTIONS)

N° de l'action	Libellé de l'action	Responsable de l'action *Organisme en charge de la réalisation de l'action*	Échéance *Cette date peut évoluer avec les mises à jour du plan de sécurité*	Statut de l'action *Close, ouverte, à venir*
A01	*Identification des ER*	*EIUOT*	*XX juin 20YY*	*Ouverte*
A02	*Détermination des causes logicielles*	*DGA*	*XX septembre 20YY*	*A venir*

J – STRATÉGIE DU DÉROULEMENT DE L'ÉTUDE

J1 – Phases de transition

J1.1 – Description de chaque phase de transition

N° de phase	Libellé de la phase de transition *Descriptif succinct de la phase de transition*	Période de mise en œuvre *Période pendant laquelle sera conduite la phase de transition*	Formalisme *MISO, EPIS ou autre*	Descriptif de la phase de transition *Descriptif détaillé de la phase de transition*

J1.2 – Résultats relatifs aux phases de transition

N° de phase	Responsable de l'exécution *Personne ou organisme en charge de la phase de transition*	Attendus *Ceux-ci peuvent évoluer avec les mises à jour du plan de sécurité*	Acceptation de mise en œuvre opérationnelle avant le début de la phase de transition
Phase 1	*Tests industriels*	*Rapport(s) de tests*	☐ Oui ☐ Non
Phase 1	*Tests sur site*	*Rapport(s) de tests*	☐ Oui ☐ Non
Phase 2	*Changement de configuration système*	*Conclusions d'acceptabilité, fichier de configuration*	☐ Oui ☐ Non
Phase 3	*Phase miroir*	*Rapport(s) de tests, conclusions d'acceptabilité*	☐ Oui ☐ Non

J2 – Assurance sécurité *(dans la mesure du possible, en fonction des éléments disponibles au moment de la rédaction du plan de sécurité)*

J2.1 – Formations requises pour le personnel opérationnel et technique *(dans l'éventualité où le changement nécessite la mise en place de formations particulières)*

Descriptif des formations, durée, cadencement.

J2.2 – Assurance de la sécurité logicielle *(si concerné)*

Respect de certains standards, livrables envisagés.

J2.3 – Vérification des exigences de sécurité et de mise en place des indicateurs

Indicateurs de sécurité spécifiques ;

Réunions périodiques ;

FNE ;

Eléments de sortie du processus PSNA/D d'analyse des évènements d'une FNE.

☐ un bilan de sécurité sera envisagé par le PSNA/D à l'échéance suivante : **……** Périodicité : **……**
☐ un bilan de sécurité est imposé par le DirCAM ☐Non ☐Oui Date : **……**

ANNEXE 5

MODÈLES DE DÉCISION

DU DirCAM

A5.1 DÉCISION D'APPROBATION DE LA DÉMONSTRATION DE SECURITE D'UN CHANGEMENT « SUIVI »

NON PROTEGE

MINISTERE DES ARMEES **Message Officiel**	**Le** : / / à h :	**N°**
	Emetteur : **DSAE/DIRCAM**	**Urgence : ROUTINE**
Dossier suivi par : **DHERS Frédéric CDT** DSAÉ/DIRCAM/SDSA/DSS	**Destinataire(s) (action)** :	
Mail : frederic.dhers@intradef.gouv.fr PNIA : 8111077654 Tel : 0145073654	**Objet** : **Approbation de la démonstration de sécurité relative au changement [REFERENCE]** MCA : SECU/AERIENNE	

PRIMO/ DECISION

Le directeur de la circulation aérienne militaire,

Vu le règlement d'exécution (UE) n°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 ;

Vu le Code de l'Aviation Civile art. D131-10 ;

Vu 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 ;

Vu le décret n°2013-366 du 29 avril 2013 portant création de la direction de la sécurité aéronautique d'État ;

Vu l'instruction n°4150/DSAÉ/DIRCAM du XXXX relative au processus de supervision et de réalisation des études de sécurité des prestataires de services de la navigation aérienne de la défense ;

Vu la décision du xxxxx portant délégation de signature.

Considérant :

L'étude [de sécurité ou sur le soutien à la sécurité] relative au changement "suivi" [REFERENCE] [et les pièces justificatives jointes] transmise(s) par message de e référence n°XXXX du jj/mm/aaaa.

Décide :

La démonstration de sécurité relative au changement "suivi" [REFERENCE] est approuvée conformément au règlement d'exécution n°2017/373 susnommé.

Signé par :

NON PROTEGE

A5.2 DÉCISION D'APPROBATION D'UN PROCESSUS OU D'UNE PROCÉDURE

NON PROTEGE

MINISTÈRE DES ARMÉES **Message Officiel**	**Le** : / / à h : **Emetteur** : **DSAE/DIRCAM**	**N°** **Urgence : ROUTINE**
Dossier suivi par : **DHERS Frédéric CDT**	**Destinataire(s) (action)** :	
Mail : frederic.dhers@intradef.gouv.fr PNIA : 8611071854 Tel : 0173951854	**Objet** : **approbation [titre du processus / de la procédure] du [PSNA/D]** MCA : SECU/AERIENNE	

Intéresse DSAC/ANA/SMN (servi par mail, pour Mme Marchant, chef de pôle systèmes et matériels de la navigation aérienne).

PRIMO/ DECISION

Le directeur de la circulation aérienne militaire,

Vu le règlement d'exécution (UE) 2017/373 de la commission 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 et (UE) 2016/1377 et modifiant le règlement (UE) n°677/2011 ;

Vu le Code de l'Aviation Civile art. D131-10 ;

Vu 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 ;

Vu le décret n°2013-366 du 29 avril 2013 portant création de la direction de la sécurité aéronautique d'État ;

Vu l'instruction n°4150/DSAÉ/DIRCAM du 21 avril 2020 relative au processus de supervision et de réalisation des études de sécurité des prestataires de services de la navigation aérienne de la défense ;

Vu [décision portant délégation de signature].

Considérant :

[Le processus / la procédure] transmis(e) par [référence].

Décide que :

[Le processus / la procédure] du [PSNA/D], est approuvé par le directeur de la circulation aérienne militaire conformément au règlement d'exécution (UE) 2017/373.

Signé par :

NON PROTEGE

Page intentionnellement blanche

ANNEXE 6

MODÈLE DE RAPPORT

DU CORRESPONDANT DIRCAM

DSAÉ DIRCAM BIRNAV BPEA	DIRCAM/SDSA/DSS	**Rapport du correspondant DIRCAM**
Référence et objet du changement		*Donnés par la DIRCAM*

REFERENCE N° /DSAÉ/DIRCAM/SDSA/NP du

DESTINATAIRE	COPIE POUR INFORMATION
DIRCAM	SDSA

Version du document	Date de rédaction	Raison de l'évolution	Auteur
V 0.1	*jj/mm/aaaa*	Création du document	*XXX*
V 0.2	*jj/mm/aaaa*	Vérification du rapport	*YYY*
V 1.0	*jj/mm/aaaa*	Approbation du rapport	*ZZZ*

Signature du correspondant DIRCAM	Signature du vérificateur du rapport	Signature de l'approbateur du rapport
Grade, Nom, Emargement	*Grade, Nom, Emargement*	*Grade, Nom, Emargement*

0. SOMMAIRE

1. OBJET DU CHANGEMENT

Présentation du changement effectué par le(s) PSNA/D.

Identifier les organismes souhaitant effectuer le changement et ceux en charge de la réalisation de l'étude de sécurité (s'ils sont différents des premiers).

Décrire succinctement la nature du changement et son périmètre : fonction ATM, sous-système, type de procédure, site(s), etc.

Cette présentation peut être complétée par des éléments concernant le planning du changement : date de mise en service souhaitée, grandes échéances du projet pour le(s) PSNA/D, phasage, etc. Ce paragraphe présente également les éléments de justification quant au positionnement du PLRE.

2. CONCLUSION DU PRESTATAIRE

Le correspondant DIRCAM reprend les conclusions du prestataire quant à l'approbation de la démonstration de sécurité et à l'acceptabilité des risques identifiés.

3. DÉMONSTRATION DE SÉCURITÉ

3.1 Processus de réalisation de la démonstration de sécurité

Le correspondant DIRCAM expose la méthode utilisée par le(s) PSNA/D pour réaliser l'évaluation et l'atténuation des risques du changement considéré.

3.2 Analyse de la démonstration de sécurité

L'examen de la démonstration de sécurité s'effectue selon le niveau d'intervention défini. Ce dernier est rappelé dans le compte-rendu de la réunion de lancement.

Le correspondant DIRCAM rédige un avis motivé sur l'acceptabilité des risques liés au changement identifiés par le(s) prestataire(s). En particulier, cet avis, en fonction du niveau d'intervention retenu, devra préciser :

- les points principaux qui pourront permettre de conduire à une proposition de décision quant à l'acceptation du changement. Ces points peuvent être une liste des risques résiduels les plus élevés (avec leur gravité et leur fréquence d'occurrence, ainsi que les moyens d'atténuation correspondants), l'analyse générale de la validité des arguments exposés pour les étapes principales de l'étude, etc. ;
- si les événements redoutés ont des effets dont les risques restent acceptables après la mise en place des moyens en réduction de risque ;
- la pertinence et l'efficacité des moyens en réduction de risque et des exigences de sécurité ;
- les éventuelles opérations de vérification sur site (OV[22]/DBF[23]) et les faits techniques identifiés ;
- si applicable, l'assurance sécurité logicielle ;
- si applicable, la prise en compte de l'interopérabilité ;
- éventuellement, les actions prises lors des réunions de coordination avec le(s) PSNA/D.

3.3 Suivi du correspondant DIRCAM

Le correspondant DIRCAM présente les éléments de contexte du suivi, notamment le niveau de suivi.

3.3.1 Présentation du changement

Dans cette partie, le correspondant DIRCAM juge la pertinence de la présentation du changement par le(s) prestataire(s) de services, en particulier ce qui concerne le périmètre du changement.

3.3.2 Evaluation des risques

Dans cette partie, le correspondant DIRCAM statue sur la logique de la démonstration de sécurité du(des) prestataire(s) de services.

3.3.3 Atténuation des risques

Dans cette partie, le correspondant DIRCAM statue sur la pertinence et l'efficacité supposée des mesures d'atténuation des risques.

4. CONCLUSION DU RAPPORT

4.1 Réserves ou limitations éventuelles

Lister, le cas échéant, les réserves et/ou limitations que le correspondant DIRCAM propose d'associer à la décision : limitations en terme de périmètre du changement, de coordination préalable avec d'autres entités de surveillance (étrangères, de certification des aéronefs) avant décision définitive, etc.

Peuvent également figurer dans ce paragraphe d'éventuels prérequis à la mise en service du changement : livraison de certains documents à la DIRCAM, réalisation/validation de tests sur un système avant sa mise en service effective, etc.

4.2 Conclusion du correspondant DIRCAM

Après la prise en compte des différents points traités dans le rapport, le correspondant DIRCAM effectue une synthèse et expose sa proposition de décision finale quant à l'approbation de la démonstration de sécurité.

[22] Opérations de vérification.
[23] Démonstration de bon fonctionnement.

4.3 Proposition de décision du sous-directeur surveillance et audit

Aux vues des conclusions du(des) prestataire(s) ayant validé l'étude et de la conclusion du correspondant DIRCAM, le sous-directeur surveillance et audit élabore une proposition motivée relative à la décision d'approbation de la démonstration de sécurité.

ANNEXE 1 : Références des documents relatifs au processus de la démonstration de sécurité

ANNEXE 2 : Bilan des exigences de sécurité

ANNEXE 3 : Acceptabilité du risque

ANNEXE 4 : Traitement des faits techniques identifiés

Page intentionnellement blanche

ANNEXE 7

PRÉCONISATIONS

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 ATS, vérification de l'acceptabilité du risque ;

  ou

  pour un changement non ATS, vérification des spécifications du système ;
- assurance relative à l'ensemble de ces éléments.

2. MODÈLE DE DOSSIER DE SÉCURITÉ

Rédaction réservée

ANNEXE 8

MODÈLE PRÉCONISÉ 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 – Présence de phase(s) de transition ☐ Oui ☐ Non

Description des phases	Formalisme	Résultat(s) attendu(s)
Tests industriels	*C/R d'opérations de vérification (OV)*	*Rapport(s) de tests*
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.4 – Conditions de retour en arrière

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

Justifications :

C.5 – 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
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 9

FORMULAIRES PRÉCONISÉS

DE 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 prestataires de la Défense, constituée d'un formulaire et de son guide d'utilisation, a reçu l'acceptation formelle du 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 acceptation 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, 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.

Un guide associé à ce formulaire est présenté en partie A9.2 de cette instruction.

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 LOCALE 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 LOCALE 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 LOCALE 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 LOCALE 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 10

FORMULAIRE PRÉCONISÉ DE DSSL

A10.1 FORMULAIRE PRÉCONISÉ DE 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]				

A10.2 GUIDE DE RÉDACTION

« En tête du formulaire »

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

Un 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.